Cisco IOS XR Interface and Hardware Component Command Reference for the Cisco XR 12000 Series Router, Release 5.1.x

First Published: June 06, 2013

Last Modified: September 10, 2013

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

Text Part Number: OL-30348-01

CONTENTS

Preface

This command reference describes the Cisco IOS XR Interfaces commands. The preface for the *Cisco IOS XR Interface and Hardware Component Command Reference for the Cisco XR 12000 Series Router* contains the following sections:

Changes to This Document

This section lists technical changes made to this document since it was first published.

Revision	Date	Change Summary
OL-30348-02	January 2014	Republished with documentation updates for Cisco IOS XR Release 5.1.1 features.
OL-30348-01	September 2013	Initial Release of this document.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

ATM Commands on the Cisco IOS XR Software

This module provides command line interface (CLI) commands for configuring ATM on your router.

atm address-registration

To enable the router to engage in address registration and callback functions with the Interim Local Management Interface (ILMI), use the **atm address-registration** command in interface configuration mode. To disable ILMI address registration functions, use the **no** form of this command.

atm address-registration

no atm address-registration

Syntax Description

This command has no keywords or arguments.

Command Default

If ILMI is configured on a PVC and its host ATM interface, then address registration and callback function enabled on the router by default.

If ILMI is not configured on a PVC and its host ATM interface, then address registration and callback functionality is disabled on the router and must be enabled with the **atm address-registration** command.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

Note The **atm address-registration** command is effective only when an ILMI PVC is created under the physical ATM interface.

Task ID

Task ID	Operations
atm	read, write

Examples

The following example shows how to enable the ATM interface 0 in slot 6 to register its address:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/0/CPU0:router(config-if)# atm address-registration
```

atm ilmi-config disable

To disable Interim Local Management Interface (ILMI) on an ATM interface, use the **atm ilmi-config disable** command in interface configuration mode. To re-enable ILMI on an ATM interface, use the **no** form of this command.

atm ilmi-config disable

no atm ilmi-config disable

Syntax Description

This command has no keywords or arguments.

Command Default

If an ILMI PVC is configured on the ATM interface, then ILMI is automatically enabled on the ATM interface that hosts that PVC.

If an ILMI PVC is not configured on the ATM interface, then ILMI is disabled by default on the ATM interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

Note The **atm ilmi-config disable** command is effective only when an ILMI PVC is created under the physical ATM interface.

Task ID

Task ID	Operations
atm	read, write

Examples

The following example shows how to disable ILMI on an ATM interface:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/0/CPU0:router(config-if)# atm ilmi-config disable
```

The following example shows how to re-enable ILMI on an ATM interface:

```
RP/0/0/CPU0:router# configure
```

```
RP/0/0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/0/CPU0:router(config-if)# no atm ilmi-config disable
```

Related Commands

Command	Description
show atm ilmi-status, on page 57	Displays status information that is related to ILMI.

atm ilmi-keepalive

To enable Interim Local Management Interface (ILMI) keepalives on an ATM interface and configure keepalive polling frequency, use the **atm ilmi-keepalive** command in interface configuration mode. To disable ILMI keepalives, use the **no** form of this command.

atm ilmi-keepalive [**act-poll-freq** *frequency*] [**retries** *count*] [**inact-poll-freq** *frequency*]

no atm ilmi-keepalive [**act-poll-freq** *frequency*] [**retries** *count*] [**inact-poll-freq** *frequency*]

Syntax Description

act-poll-freq *frequency*	(Optional) Number of polling seconds between active keepalives. Range is from 1 through 65535 seconds. Default is 5 seconds.
retries *count*	(Optional) ILMI keepalive retry count. Range is from 2 through 5. Default is 4 retries.
inact-poll-freq *frequency*	(Optional) Number of polling seconds between inactive keepalives. Range is from 1 through 65535 seconds. Default is 1 second.

Command Default

act-poll-freq *frequency*: 5

retries *count*: 4

inact-poll-freq *frequency*: 1

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

Note The **atm ilmi-keepalive** command is effective only when an ILMI PVC is created under the physical ATM interface.

Task ID

Task ID	Operations
atm	read, write

Examples

The following example shows how to enable ILMI keepalives for the ATM interface 0 in slot 6:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/0/CPU0:router(config-if)# atm ilmi-keepalive
```

The following example shows how to configure the ATM interface 1 in slot 6 to poll the number of inactive keepalives every 10 seconds:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/6/0/1
RP/0/0/CPU0:router(config-if)# atm ilmi-keepalive inact-poll-freq 10
```

The following example shows how to disable ILMI keepalives for the ATM interface 0 in slot 6:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/0/CPU0:router(config-if)# no atm ilmi-keepalive
```

Related Commands

Command	Description
show atm ilmi-status, on page 57	Displays status information that is related to ILMI.

atm ilmi-trap disable

To disable Interim Local Management Interface (ILMI) trap generation on an ATM interface, use the **atm ilmi-trap disable** command in interface configuration mode. To reenable ILMI trap generation, use the **no** form of this command.

atm ilmi-trap disable

no atm ilmi-trap disable

Syntax Description

This command has no keywords or arguments.

Command Default

Support for ATM ILMI trap generation is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
atm	read, write

Examples

The following example shows how to disable ILMI trap generation on the ATM interface 0 in slot 6:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/0/CPU0:router(config-if)# atm ilmi-trap disable
```

The following example shows how to reenable ILMI trap generation on the ATM interface 0 in slot 6:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/6/0/1
RP/0/0/CPU0:router(config-if)# no atm ilmi-trap disable
```

Related Commands

Command	Description
show atm interface atm, on page 60	Displays ATM-specific information about an ATM interface.

atm maxvpi-bits 12

To enable support for the 12-bits virtual path identifier (VPI) Network-Node Interface (NNI) cell format, use the **atm maxvpi-bits 12** command in interface configuration mode. To disable support for the 12-bits VPI NNI cell format, use the **no** form of this command.

atm maxvpi-bits 12

no atm maxvpi-bits 12

Syntax Description

This command has no keywords or arguments.

Command Default

Support for the 12-bits VPI NNI cell format is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelin

Note Out of the twelve bits, four bits in the ATM UNI cell header are reserved for local standardized generic flow control (GFC).

Task ID

Task ID	Operations
atm	read, write

Examples

The following example shows how to enable support for the 12-bits VPI NNI cell format on the ATM interface 0 in slot 6:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/0/CPU0:router(config-if)# atm maxvpi-bits 12
```

The following example shows how to disable support for the 12-bits VPI NNI cell format on the ATM interface 1 in slot 6:

```
RP/0/0/CPU0:router# configure
```

```
RP/0/0/CPU0:router(config)# interface atm 0/6/0/1
RP/0/0/CPU0:router(config-if)# no atm maxvpi-bits 12
```

Related Commands

Command	Description
show atm interface atm, on page 60	Displays ATM-specific information about an ATM interface.

atm mcpt-timers

To define the three Maximum Cell Packing Timeout (MCPT) timers under a main ATM interface, use the **atm mcpt-timers** command in interface configuration mode. To return the three timers to the default configuration, use the **no** form of this command.

atm mcpt-timers *timer-1 timer-2 timer-3*

no atm mcpt-timers

Syntax Description

timer-1	Maximum number of microseconds to wait to complete cell packing on a single packet before that packet is transmitted. Range is from 50 through 4095. **Note** To associate this timer with an interface, use the **cell-packing** command and replace the *timer* argument **1**.
timer-2	Maximum number of microseconds to wait to complete cell packing on a single packet before that packet is transmitted. Range is from 50 through 4095. **Note** To associate this timer with an interface, use the **cell-packing** command and replace the *timer* argument **2**.
timer-3	Maximum number of microseconds to wait to complete cell packing on a single packet before that packet is transmitted. Range is from 50 through 4095. **Note** To associate this timer with an interface, use the **cell-packing** command and replace the *timer* argument **3**.

Command Default

timer-1 : 50

timer-2 : 50

timer-3 : 50

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

Use the **cell-packing** command to attach one of the three MCPT timers to an individual L2VPN port, PVC, or PVP. If the associated MCPT timer expires before the maximum number of cells that can be packed is reached, then the packet is transmitted with the number of cells that have been packed thus far.

Note We recommend configuring a low, medium, and high value for the three MCPT timers to accommodate the different ATM traffic classes. Low- latency CBR traffic typically uses a low MCPT timer value, while high-latency UBR traffic typically requires a high MCPT timer value. VBR-rt and VBR-nrt traffic typically use a median MCPT timer value.

Task ID

Task ID	Operations
atm	read, write

Examples

The following example shows how to configure the three MCPT timers and then apply one of them to an interface with the **cell-packing** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/0/CPU0:router(config-if)# atm mcpt-timers 50 100 200
RP/0/0/CPU0:router(config-if)# l2transport
RP/0/0/CPU0:router(config-if-l2)# cell-packing 6 1
```

Related Commands

Command	Description
cell-packing, on page 15	Configures the maximum number of cells allowed per packet, and specifies a MCPT timer for cell packing.
show atm interface atm, on page 60	Displays ATM-specific information about an ATM interface.

atm oam flush

To drop all current and future Operation, Administration, and Maintenance (OAM) cells received on an ATM interface, use the **atm oam flush** command in interface configuration mode. To receive OAM cells on an ATM interface, use the **no** form of this command.

atm oam flush

no atm oam flush

Syntax Description

This command has no keywords or arguments.

Command Default

The dropping of OAM cells is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
atm	read, write

Examples

The following example shows how to enable the dropping of all current and future OAM cells received on the ATM interface 0 in slot 6:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/0/CPU0:router(config-if)# atm oam flush
```

The following example shows how to disable the dropping of all current and future OAM cells received on the ATM interface 1 in slot 6:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/0/CPU0:router(config-if)# no atm oam flush
```

Related Commands

Command	Description
show atm interface atm, on page 60	Displays ATM-specific information about an ATM interface.
show atm class-link, on page 53	Displays configuration information for the parameters on a VC class that is associated with a particular PVC.
show atm vc-class, on page 81	Displays information about all ATM VC classes on the router or for a specific ATM VC-class.
show atm vp-tunnel, on page 85	Displays VP tunnel information for the entire router or for a specific interface.

cell-packing

To configure the maximum number of cells allowed per packet, and specify a Maximum Cell Packing Timeout (MCPT) timer for cell packing, use the **cell-packing** command in the appropriate mode. To return the interface to the default cell packing configuration, use the **no** form of this command.

cell-packing *cells timer*

no cell-packing

Syntax Description

cells	Maximum number of cells to use per packet. Range is from 2 through 86.
timer	Indicates the appropriate MCPT timer to use for cell packing. Can be **1**, **2**, or **3**. **Note** You can configure up to three different MCPT values for a single main interface with the **atm mcpt-timers** command.

Command Default

If you do not configure the maximum number of cells allowed per packet, only one cell is carried per packet.

Command Modes

ATM layer 2 transport interface configuration (config-if-l2)

ATM layer 2 transport PVC configuration (config-atm-l2transport-pvc)

ATM layer 2 transport PVP configuration (config-atm-l2transport-pvp)

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

Use the atm mcpt-timers, on page 11 command to configure the three MCPT timers under the main ATM interface.

Task ID

Task ID	Operations
atm	read, write

Examples

The following example shows how to configure cell packing parameters on an ATM interface:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/0/CPU0:router(config-if)# l2transport
RP/0/0/CPU0:router(config-if-l2)# cell-packing 6 3
```

Related Commands

Command	Description
atm mcpt-timers, on page 11	Defines the three MCPT timers under a main ATM interface.
show atm cell-packing, on page 51	Displays cell packing information for the Layer 2 attachment circuits (ACs) configured on your system.
show atm interface atm, on page 60	Displays ATM-specific information about an ATM interface.
show atm pvc, on page 67	Displays ATM PVC and traffic information for the entire router.
show atm pvp, on page 75	Displays ATM PVP and traffic information for the entire router, or a specific VPI or ATM interface.

class-int

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

class-int *vc-class-name*

no class-int *vc-class-name*

Syntax Description

vc-class-name	Name of the VC-class you are assigning to your ATM main interface or subinterface.

Command Default

No VC-class is assigned to an ATM main interface or subinterface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

When you create a VC-class for an ATM main interface or subinterface, you can use the **shape** and **encapsulation** commands to define your parameters.

Parameters that are applied to an individual VC supersede interface- and subinterface-level parameters. Parameters that are configured for a VC through discrete commands entered in interface-ATM-VC configuration mode supersede VC-class parameters assigned to an ATM main interface or subinterface by the **class-int** command.

Note This command is not available for Layer 2 interfaces.

Task ID

Task ID	Operations
atm	read, write

Examples

The following example shows how to create a class called “classA” and then apply that class to ATM main interface 1 in slot 6:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)#vc-class atm classA
RP/0/0/CPU0:router(config-vc-class-atm)# shape cbr 40000
RP/0/0/CPU0:router(config-vc-class-atm)# encapsulation aal5snap
RP/0/0/CPU0:router(config-vc-class-atm)# oam-pvc manage 300
RP/0/0/CPU0:router(config-vc-class-atm)# commit
RP/0/0/CPU0:router(config-vc-class-atm)# exit
RP/0/0/CPU0:router(config)# interface atm 0/6/0/1
RP/0/0/CPU0:router(config-if)# class-int classA
RP/0/0/CPU0:router(config-if)#
```

Related Commands

Command	Description
show atm class-link, on page 53	Displays configuration information for the parameters on a VC class that is associated with a particular PVC.
show atm vc-class, on page 81	Displays information about all ATM VC classes on the router or for a specific ATM VC-class.

class-vc

To attach a virtual circuit (VC) class to an ATM permanent virtual circuit (PVC), use the **class-vc** command in ATM PVC configuration mode for a PVC that is configured on an ATM subinterface. To remove a VC-class from a PVC, use the **no** form of this command.

class-vc *vc-class-name*

no class-vc *vc-class-name*

Syntax Description

vc-class-name	Name of the VC-class you are assigning to your ATM PVC.

Command Default

No VC-class is assigned to an ATM PVC.

Command Modes

ATM PVC configuration (config-atm-vc)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

When you create a VC-class for an ATM subinterface PVC, you can use the **shape** and **encapsulation** commands to define your parameters.

Parameters that are applied to an individual VC supersede PVC-level parameters. Parameters that are configured for a VC through discrete commands entered in interface-ATM-VC configuration mode supersede VC-class parameters assigned to a PVC by the **class-vc** command.

Note The **class-vc** command is available in ATM PVC configuration mode for a PVC that is configured on an ATM subinterface only. This command is not available in ATM PVC configuration mode for an ATM main interface.

Task ID

Task ID	Operations
atm	read, write

Examples

The following example shows how to create a class called “classA” and then apply that class to the subinterface 1 on the ATM main interface 1 in slot 6:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# vc atm classA
RP/0/0/CPU0:router(config-vc-class-atm)# shape cbr 40000
RP/0/0/CPU0:router(config-vc-class-atm)# commit
RP/0/0/CPU0:router(config-vc-class-atm)# exit
RP/0/0/CPU0:router(config)# interface atm 0/6/0/1.1 point-to-point
RP/0/0/CPU0:router(config-if)# pvc 10/100
RP/0/0/CPU0:router(config-atm-vc)# class-vc classA
RP/0/0/CPU0:router(config-atm-vc)#
```

Related Commands

Command	Description
show atm class-link, on page 53	Displays configuration information for the parameters on a VC class that is associated with a particular PVC.
show atm vc-class, on page 81	Displays information about all ATM VC classes on the router or for a specific ATM VC-class.

encapsulation (ATM)

To configure the ATM adaptation layer (AAL) and encapsulation type for a virtual circuit (VC) class, ATM permanent virtual circuit (PVC), or ATM permanent virtual path (PVP), use the **encapsulation** command in the appropriate configuration mode. To remove an encapsulation type, use the **no** form of this command.

For point-to-point ATM PVCs and vc-classes:

encapsulation {**aal5mux ipv4**| **aal5nlpid**| **aal5snap**}

no encapsulation {**aal5mux ipv4**| **aal5nlpid**| **aal5snap**}

For ATM Layer 2 PVCs:

encapsulation {**aal0**| **aal5**}

no encapsulation {**aal0**| **aal5**}

Syntax Description

aal5mux ipv4	Specifies IPv4 encapsulation for multiplex (MUX)-type VCs. **Note** The **aal5mux ipv4** keywords are available in ATM PVC configuration and ATM VC-class configuration modes only.
aal5nlpid	Specifies the AAL and encapsulation type that allows ATM interfaces to interoperate with High-Speed Serial Interfaces (HSSIs), which are using an ATM data service unit (ADSU) and running ATM-Data Exchange Interface (DXI). Supported on ATM PVCs only. **Note** The **aal5nlpid** keyword is available in ATM PVC configuration and ATM VC-class configuration modes only.
aal5snap	Specifies the AAL encapsulation type that supports Inverse ARP. Logical Link Control/Subnetwork Access Protocol (LLC/SNAP) precedes the protocol datagram. **Note** The **aal5snap** keyword is available in ATM PVC configuration and ATM VC-class configuration modes only.
aal0	Specifies the AAL encapsulation type that contains 48 bytes of data within an ATM cell. AAL0 cells are also referred to as “raw cells.” The payload consists of 48 bytes. **Note** The **aal0** keyword is available in the ATM Layer 2 transport PVC configuration mode only.
aal5	Specifies the AAL encapsulation type that carries higher-layer datagrams while enhancing the link layer with services available through ATM. AAL5 is defined in the ITU standard I.363.5, and is typically used to carry IP datagrams over ATM. **Note** The **aal5** keyword is available in the ATM Layer 2 transport PVC configuration mode only.

Command Default

For point-to-point PVCs, the default encapsulation type is **aal5snap**.

For Layer 2 PVCs, the default encapsulation type is **aal5**.

Command Modes

ATM PVC configuration (config-atm-vc)

ATM VC-class configuration (config-vc-class-atm)

ATM layer 2 transport PVC configuration (config-atm-l2transport-pvc)

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.4.1	To support Layer 2 VPN ACs, the **encapsulation** command was updated to include the **aal0** and **aal5** keywords in ATM Layer 2 transport PVC configuration mode.

Usage Guidelines

Use the **aal5mux ipv4** encapsulation option to dedicate the specified PVC to a single protocol; use the **aal5snap** encapsulation option to multiplex two or more protocols over the same PVC. Whether you select **aal5mux ipv4** or **aal5snap** encapsulation depends on the type of network you are configuring, and the pricing offered by that network. If the pricing of the network depends on the number of PVCs set up, we recommend **aal5snap** encapsulation. If pricing depends on the number of bytes transmitted, we recommend **aal5mux ipv4** encapsulation because it has less overhead than **aal5snap** and **aal5mux ipv4** encapsulation.

If you configure VC-class parameters for a PVC after that PVC is configured, you must enter the **shutdown** command followed by the **no shutdown** command on the ATM subinterface that hosts the PVC. This action restarts the interface, causing the newly configured VC-class parameters to take effect on that interface.

Unless specifically configured otherwise, a PVC automatically inherits the encapsulation type of the VC-class that is assigned to the main interface or subinterface that hosts the PVC. If no VC-class is assigned, then the PVC inherits the encapsulation type of the main interface or subinterface that hosts the PVC. If no encapsulation is configured of the main interface or subinterface, then the PVC inherits the default **aal5snap** encapsulation.

Use the **encapsulation** command in ATM PVC configuration mode to modify the inherited or default encapsulation assigned to a PVC. You can modify the encapsulation for each individual PVC to be different from the encapsulation configured for the VC-class that is assigned to the ATM main interface or subinterface that hosts the PVC.

If you do not use the **encapsulation** command to configure the encapsulation type for a new ATM PVC, then the PVC inherits the one of the following default configurations (listed in order of precedence from lowest to highest):

- The encapsulation assigned to the VC-class that is assigned to the PVC itself.
- The encapsulation assigned to the VC-class that is assigned to the ATM subinterface that hosts the PVC.
- The encapsulation assigned to the VC-class that is assigned to the ATM main interface that hosts the PVC
- The default **aal5snap** encapsulation

When configuring a PVC range or an individual PVC within a PVC range, the following encapsulation types are supported:

- **encapsulation aal5mux ipv4**

- **encapsulation aal5snap**

Note For Layer 2 PVCs, the default encapsulation type is **aal5**, and the encapsulation type is not inherited from the VC-class.

Task ID

Task ID	Operations
atm	read, write

Examples

The following example shows how to configure a VC-class with **aal5snap** encapsulation:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# vc atm classA
RP/0/0/CPU0:router(config-vc-class-atm)# encapsulation aal5snap
```

The following example shows how to configure an individual PVC with **aal5mux** encapsulation:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/2/0/0.1 point-to-point
RP/0/0/CPU0:router(config-subif)# pvc 10/100
RP/0/0/CPU0:router(config-atm-vc)# encapsulation aal5mux
```

The following example shows how to remove **aal5mux ipv4** encapsulation from a VC-class:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# vc atm classA
RP/0/0/CPU0:router(config-vc-class-atm)# no encapsulation aal5mux ipv4
```

The following example shows how to configure an individual Layer 2 PVC with **aal0** encapsulation:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/6/0/1.10 l2transport
RP/0/0/CPU0:router(config-if)# pvc 30/300
RP/0/0/CPU0:router(config-atm-l2transport-pvc)# encapsulation aal0
```

Related Commands

Command	Description
show atm pvc, on page 67	Displays ATM PVC and traffic information for the entire router.
show atm vc-class, on page 81	Displays information about all ATM VC classes on the router or for a specific ATM VC-class.

f4oam disable

To disable the F4 Operations Administration and Maintenance (OAM) packets for a VP-tunnel, enter the **f4oam disable** command in ATM VP-tunnel configuration mode. To re-enable F4 OAM packets for a VP-tunnel, enter the **no** form of this command.

f4oam disable

no f4oam disable

Syntax Description

This command has no keywords or arguments.

Command Default

F4 OAM is enabled by default.

Command Modes

ATM Vp-tunnel configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
atm	read, write

Examples

The following example shows how to restrict a VP from passing OAM packets:

```
RP/0/0/CPU0:router# config
RP/0/0/CPU0:router (config)# interface atm 0/6/0/0
RRP/0/0/CPU0:router(config-if)# vp-tunnel 10
RP/0/0/CPU0:router(config-atm-vp-tunnel)# f4oam disable
```

The following example shows how to re-enable the passing of OAM packets on a VP:

```
RP/0/0/CPU0:router# config
RP/0/0/CPU0:router (config)# interface atm 0/6/0/0
RRP/0/0/CPU0:router(config-if)# vp-tunnel 10
RP/0/0/CPU0:router(config-atm-vp-tunnel)# no f4oam disable
```

Related Commands

Command	Description
show atm interface atm, on page 60	Displays ATM-specific information about an ATM interface.

Command	Description
show atm class-link, on page 53	Displays configuration information for the parameters on a VC class that is associated with a particular PVC.
show atm vc-class, on page 81	Displays information about all ATM VC classes on the router or for a specific ATM VC-class.
show atm vp-tunnel, on page 85	Displays VP tunnel information for the entire router or for a specific interface.

interface atm

To configure an ATM interface and enter ATM interface configuration mode, use the **interface atm** command in global configuration mode. To delete the interface configuration, use the **no** form of this command.

interface atm *interface-path-id*[**.** *subinterface*][**point-to-point**| **l2transport**]

no interface atm *interface-path-id*[**.** *subinterface*]

Syntax Description

*interface-path-id***.** [*subinterface*]	Physical interface or virtual interface followed by the optional subinterface path ID. Naming notation is *interface-path-id***.***subinterface*. The period in front of the subinterface value is required as part of the notation. For more information about the syntax for the router, use the question mark (?) online help function.
point-to-point	Interface functions as one endpoint of a point-to-point link.
l2transport	Interface functions as one endpoint on an Layer 2 link.

Command Default

No interfaces are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.4.1	To support Layer 2 VPN ATM ACs, this command was updated to include the **l2transport** keyword.

Usage Guidelines

The **interface** command enters interface configuration mode to allow you to configure interfaces. If a virtual interface is configured, then the interface is created if it did not already exist.

When you issue the **interface atm** command in global configuration mode, the CLI prompt changes to "config-if," indicating that you have entered interface configuration submode for an ATM interface.

Note Although the CLI prompt looks the same in the interface configuration mode for an ATM main interface and for an ATM subinterface, the commands that are available under each interface type vary.

In the following sample output, the question mark (**?**) online help function displays all the commands available under the interface configuration submode for a ATM main interface:

```
RP/0/0/CPU0:router(config)# interface atm 0/2/0/0
RP/0/0/CPU0:router(config-if)#?

affinity       Affinity to include/exclude
  atm            Global ATM interface configuration subcommands
  bandwidth      Set the bandwidth of an interface
  cdp            Enable CDP on an interface
  class-int      Apply a VC class
  commit         Commit the configuration changes to running
  crypto         Set crypto parameters
  dampening      configure state dampening on the given interface
  describe       Describe a command without taking real actions
  description    Set description for this interface
  do             Run an exec command
  exit           Exit from this submode
  flow           Netflow configuration
  frame-relay    Frame Relay interface configuration commands
  ipv4           IPv4 interface subcommands
  ipv6           IPv6 interface subcommands
  l2transport    Enable Layer 2 transport and enter its configuration submode
  load-interval  Specify interval for load calculation for an interface
  mpls           MPLS interface subcommands
  mtu            Set the MTU on an interface
  no             Negate a command or set its defaults
  pvc            Configure a pvc on this interface
  root           Exit to the global configuration mode
  show           Show contents of configuration
 --More--
```

In the following sample output, the question mark (**?**) online help function displays all the commands available under the interface configuration submode for a point-to-point ATM subinterface:

```
RP/0/0/CPU0:router(config)# interface atm 0/2/0/0.1 point-to-point
RP/0/0/CPU0:router(config-if)# ?

  affinity       Affinity to include/exclude
  bandwidth      Set the bandwidth of an interface
  cdp            Enable CDP on an interface
  class-int      Apply a VC class
  commit         Commit the configuration changes to running
  crypto         Set crypto parameters
  dampening      configure state dampening on the given interface
  describe       Describe a command without taking real actions
  description    Set description for this interface
  do             Run an exec command
  exit           Exit from this submode
  flow           Netflow configuration
  frame-relay    Frame Relay interface configuration commands
  ipv4           IPv4 interface subcommands
  ipv6           IPv6 interface subcommands
  load-interval  Specify interval for load calculation for an interface
  logging        Per-interface logging configuration
  mpls           MPLS interface subcommands
  mtu            Set the MTU on an interface
  no             Negate a command or set its defaults
  pvc            Configure a pvc on this interface
  root           Exit to the global configuration mode
  show           Show contents of configuration
  shutdown       shutdown the given interface
 --More--
```

In the following sample output, the question mark (**?**) online help function displays all the commands available under the interface configuration submode for an ATM Layer 2 subinterface:

```
RP/0/0/CPU0:router(config)#interface atm 0/2/0/0.1 l2transport
```

```
RP/0/0/CPU0:router(config-if)#?

bandwidth      Set the bandwidth of an interface
  cdp            Enable CDP on an interface
  commit         Commit the configuration changes to running
  crypto         Set crypto parameters
  dampening      configure state dampening on the given interface
  describe       Describe a command without taking real actions
  description    Set description for this interface
  do             Run an exec command
  exit           Exit from this submode
  firewall       Configure a Virtual Firewall on this Interface
  flow           Netflow configuration
  frame-relay    Frame Relay interface configuration commands
  ipv4           IPv4 interface subcommands
  ipv6           IPv6 interface subcommands
  load-interval  Specify interval for load calculation for an interface
  logging        Per-interface logging configuration
  mpls           MPLS interface subcommands
  mtu            Set the MTU on an interface
  no             Negate a command or set its defaults
  pvc            Configure a pvc on this interface
  pvp            Configure a pvp on this interface
  pwd            Commands used to reach current submode
  root           Exit to the global configuration mode
  show           Show contents of configuration
```

Cisco IOS XR software supports bulk removal of subinterfaces. To remove several subinterfaces with a single command enter, replace the *subinterface* argument with an asterisk (*), as shown in the following example:

```
RP/0/0/CPU0:router(config)# no interface atm 0/6/0/1.*
```

Note Before you can perform a bulk removal of several subinterfaces, OAM F5 loopback cell generation must be enabled on the PVCs that are configured under the subinterfaces you want to remove. To enable OAM F5 loopback cell generation on a PVC, use the oam-pvc manage, on page 34 command.

Note The **l2transport** keyword is mutually exclusive with any Layer 3 interface configuration.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter interface configuration mode for the ATM main interface 1 in slot 6:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/6/0/1
RP/0/0/CPU0:router(config-if)#
```

The following example shows how to enter ATM interface configuration mode for a point-to-point subinterface. In this example, the user adds a subinterface to the ATM main interface 0 in slot 2:

```
RP/0/0/CPU0:router# configure
```

```
RP/0/0/CPU0:router(config)# interface atm 0/2/0/0.1 point-to-point
RP/0/0/CPU0:router(config-if)#
```

The following example shows how to enter ATM interface configuration mode for a Layer 2 subinterface. In this example, the user adds a subinterface to the ATM main interface 0 in slot 2:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/2/0/0.1 l2transport
RP/0/0/CPU0:router(config-if)#
```

Related Commands

Command	Description
show atm interface atm, on page 60	Displays ATM-specific information about an ATM interface.

l2transport (ATM)

To enable Layer 2 transport port mode on an ATM interface and enter Layer 2 transport configuration mode, use the **l2transport** command in interface configuration mode. To disable Layer 2 transport port mode on an ATM interface, use the **no** form of this command.

l2transport

no l2transport

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

When you issue the **l2transport** command in interface configuration mode, the CLI prompt changes to "config-if-l2," indicating that you have entered the Layer 2 transport configuration submode. In the following sample output, the question mark (**?**) online help function displays all the commands available under Layer 2 transport configuration submode for an ATM interface:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/2/0/0
RP/0/0/CPU0:router(config-if)# l2transport
RP/0/0/CPU0:router(config-if-l2)# ?

cell-packing    Configure L2VPN cell packing parameters
  commit          Commit the configuration changes to running
  describe        Describe a command without taking real actions
  do              Run an exec command
  exit            Exit from this submode
  no              Negate a command or set its defaults
  pwd             Commands used to reach current submode
  root            Exit to the global configuration mode
  service-policy  Configure QoS Service policy
  show            Show contents of configuration

RP/0/0/CPU0:router(config-if-l2)#
```

Note The **l2transport** command is mutually exclusive with any Layer 3 interface configuration.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to enable Layer 2 transport port mode on an ATM interface and enter Layer 2 transport configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface ATM 0/2/0/0
RP/0/0/CPU0:router(config-if)# l2transport
RP/0/0/CPU0:router(config-if-l2)#
```

Related Commands

Command	Description
show l2vpn xconnect	Displays brief information on configured xconnects.

oam ais-rdi

To configure the behavior of an ATM permanent virtual circuit (PVC) when it receives Operation, Administration, and Maintenance (OAM) alarm indication signal and remote defect indication (AIS/RDI) cells, use the **oam ais-rdi** command in ATM PVC configuration or ATM VC-class configuration mode. To return the PVC to the default behavior, use the **no** form of this command.

oam ais-rdi [*down-count* [*up-count*]]

no oam ais-rdi [*down-count* [*up-count*]]

Syntax Description

down-count	(Optional) Number of consecutive OAM AIS/RDI cells received on a PVC before that PVC is brought down. Range is from 1 through 60. The default is 1.
up-count	(Optional) Number of seconds after which a down PVC is brought up if no OAM AIS/RDI cells are received. Range is from 3 through 60. The default is 3. The specified *up-count* applies under the following conditions only: • OAM F5 loopback cell generation must be enabled on the PVC. • The PVC is in a down state because it received AIS/RDI cells. **Note** To enable OAM F5 loopback cell generation on a PVC, use the oam-pvc manage, on page 34 command.

Command Default

down-count: 1

up-count: 3

Command Modes

ATM VC-class configuration (config-vc-class-atm)

ATM PVC configuration (config-atm-vc)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

Use the **oam ais-rdi** command to configure the following:

- the maximum number of Operation, Administration, and Maintenance (OAM) alarm indication signals and remote defect indication (AIS/RDI) cells that can be received on a PVC before it is brought down.
- the interval after which a downed PVC comes back up if no OAM AIS/RDI cells have been received.

Use the **oam ais-rdi** command in ATM PVC configuration mode to configure the OAM AIS/RDI down count and up count for a specific PVC.

Use the **oam ais-rdi** command in ATM VC-class configuration mode to configure the OAM AIS/RDI down count and up count for all PVCs that are associated with the specified class map.

Keep the following in mind when configuring the OAM AIS/RDI down count and up count:

- Unless specifically configured otherwise, a PVC automatically inherits the OAM AIS/RDI down count and up count of the VC-class that is assigned to the main interface or subinterface that hosts the PVC.
- If the OAM AIS/RDI down count and up count is not configured for the VC-class, or if no VC-class is assigned to the main interface or subinterface that hosts the PVC, or to the PVC itself, then the PVC inherits the default OAM AIS/RDI down count and up count.

The default values for the OAM AIS/RDI down count and up count are used in the following situations:

- If the **oam ais-rdi** command has not been entered
- If the **oam ais-rdi** command is entered without the *up-count* or *down-count* argument
- If the **no oam ais-rdi** command is entered

If the **oam ais-rdi** command is entered without the *up-count* or *down-count* argument, the command does not appear in the **show running-config** command output.

Task ID

Task ID	Operations
atm	read, write

Examples

The following example shows how to bring down a PVC after 25 consecutive OAM AIS/RDI cells have been received on the PVC. The PVC is brought up when no OAM AIS/RDI cells have been received for 5 seconds.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/2/0/0.1 point-to-point
RP/0/0/CPU0:router(config-subif)# pvc 50/100
RP/0/0/CPU0:router(config-atm-vc)# oam ais-rdi 25 5
```

The following example shows how to configure the OAM AIS/RDI down count and up count for a VC-class. In this example, all PVCs that are associated with the VC-class called “classA” inherit an OAM AIS/RDI down count of 30 and up count of 10:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# vc atm classA
RP/0/0/CPU0:router(config-vc-class-atm)# oam ais-rdi 30 10
```

Related Commands

Command	Description
show atm class-link, on page 53	Displays configuration information for the parameters on a VC class that is associated with a particular PVC.
show atm pvc, on page 67	Displays ATM PVC and traffic information for the entire router.

oam-pvc manage

To enable ATM Operation, Administration, and Maintenance (OAM) F5 loopback cell generation and configure continuity check (CC) management for an ATM permanent virtual circuit (PVC), use the **oam-pvc manage** command in ATM PVC configuration or ATM VC-class configuration mode. To disable OAM F5 continuity checking on a PVC, use the **no** form of this command.

In ATM PVC configuration mode:

oam-pvc manage [*f* **requency**] **[disable]** [**keep-vc-up [seg-aisrdi-failure]**]

no oam-pvc manage [frequency] [disable] [**keep-vc-up [seg-aisrdi-failure]**]

In ATM VC class configuration mode:

oam-pvc manage [frequency]

no oam-pvc manage [frequency]

Syntax Description

frequency	(Optional) Frequency (in seconds) at which end-to-end F5 OAM loopback cells are transmitted. Range is from 0 through 600.
disable	(Optional) Disables OAM management on the specified PVC. **Note** The **disable** keyword is available in ATM PVC configuration mode only.
keep-vc-up	(Optional) Specifies that PVC remains in the UP state when CC cells detect connectivity failure. **Note** The **keep-vc-up** keyword is available in ATM PVC configuration mode only.
seg-aisrdi-failure	(Optional) Specifies that if segment AIS/RDI cells are received, the VC will not be brought down because of end CC failure or loopback failure. **Note** The **seg-aisrdi-failure** keyword is available in ATM PVC configuration mode only.

Command Default

frequency: 10 seconds

Command Modes

ATM PVC configuration (config-atm-vc)

ATM VC class configuration (config-vc-class-atm)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

Keep the following in mind when configuring the OAM F5 loopback cell generation and CC management for an ATM PVC:

- Unless specifically configured otherwise, a PVC automatically inherits the OAM F5 loopback cell management configuration from the VC-class that is assigned to the main interface or subinterface that hosts the PVC.
- If OAM F5 loopback cell generation is not enabled for the assigned VC-class, or if no VC-class is assigned to the PVC itself, or to main interface or subinterface that hosts the PVC, then OAM F5 loopback cell generation is disabled on that PVC. To enable OAM F5 loopback cell generation on that PVC, you need to use the **oam-pvc manage** command in ATM PVC configuration mode.
- VC-classes support the configuration of the *seconds* argument only; the **keep-vc-up**, **disable**, and **seg-aisrdi-failure** keywords are available in ATM PVC configuration mode only and are configured directly on each individual PVC.

Task ID

Task ID	Operations
atm	read, write

Examples

The following example shows how to enable OAMF5 loopback cell generation on a PVC, and configure the PVC to remain up when CC cells detect connectivity failure:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/2/0/0.1 point-to-point
RP/0/0/CPU0:router(config-subif)# pvc 10/100
RP/0/0/CPU0:router(config-atm-vc)# oam-pvc manage 200 keep-vc-up
```

The following example shows how to disable OAMF5 loopback cell generation on a PVC:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/2/0/0.1 point-to-point
RP/0/0/CPU0:router(config-subif)# pvc 10/100
RP/0/0/CPU0:router(config-atm-vc)# oam-pvc manage disable
```

The following example shows how to configure the OAM F5 loopback frequency for a VC-class. In this example, all PVCs associated with the VC-class called “classA” transmit end-to-end F5 OAM loopback cells every 300 seconds:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# vc atm classA
RP/0/0/CPU0:router(config-vc-class-atm)# oam-pvc manage 300
```

The following example shows how to remove the configured ATM OAM F5 loopback frequency from a VC-class:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# vc atm classA
RP/0/0/CPU0:router(config-vc-class-atm)# no oam-pvc manage
```

Related Commands

Command	Description
show atm class-link, on page 53	Displays configuration information for the parameters on a VC class that is associated with a particular PVC.
show atm pvc, on page 67	Displays ATM PVC and traffic information for the entire router.

oam retry

To configure the number of F5 Operation, Administration, and Maintenance (OAM) loopback cells that need to be successfully transmitted by a down ATM permanent virtual circuit (PVC) before it is brought up, use the **oam retry** command in ATM PVC configuration or ATM VC-class configuration mode. To return the PVC to the default behavior, use the **no** form of this command

oam retry [*up-count* [*down-count* [*retry-frequency*]]]

no oam retry [*up-count* [*down-count* [*retry-frequency*]]]

Syntax Description

retry-count	(Optional) Number of consecutive end-to-end F5 OAM loopback cell responses that must be received to change a connection state to up.
down-count	(Optional) Number of consecutive unreceived end-to-end F5 OAM loopback cells allowed on a PVC before its state changes to down.
retry-frequency	(Optional) Frequency (in seconds) at which end-to-end F5 OAM loopback cells are transmitted when a change in the up or down state is being verified. For example, if a PVC is up and a loopback cell response is not received after the frequency (in seconds) is specified using the **oam-pvc manage** command, loopback cells are sent at the retry frequency to verify whether the PVC is down.

Command Default

up-count: 3

down-count: 5

retry-frequency: 1 second

Command Modes

ATM PVC configuration (config-atm-vc)

ATM VC-class configuration (config-vc-class-atm)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

Keep the following in mind when configuring the OAM AIS/RDI down count and up count:

- Unless specifically configured otherwise, a PVC automatically inherits the OAM AIS/RDI down count and up count of the VC-class that is assigned to the main interface or subinterface that hosts the PVC.

- If no encapsulation is configured for the VC-class, or if no VC-class is assigned to the main interface or subinterface that hosts the PVC, or to the PVC itself, then the PVC inherits the default OAM AIS/RDI down count and up count.

Keep the following in mind when configuring the F5 OAM loopback cell up count, down count, and retry frequency:

- Unless specifically configured otherwise, a PVC automatically inherits the F5 OAM loopback cell up count, down count, and retry frequency of the VC-class that is assigned to the main interface or subinterface that hosts the PVC.
- If the F5 OAM loopback cell up count, down count, and retry frequency are not configured for the VC-class, or if no VC-class is assigned to the PVC itself, or to the main interface or subinterface that hosts the PVC, then the PVC inherits the default F5 OAM loopback cell up count, down count, and retry frequency.

In other words, if the **oam retry** command is not explicitly configured on an individual PVC, then that PVC inherits the following default configuration (listed in order of precedence):

- F5 OAM loopback cell up count, down count, and retry frequency configured for the VC-class that is assigned to the PVC itself
- F5 OAM loopback cell up count, down count, and retry frequency configured for VC-class assigned to the ATM subinterface that hosts the PVC
- F5 OAM loopback cell up count, down count, and retry frequency configured for the VC-class assigned to the ATM main interface that hosts the PVC

Note For the defaults, it is assumed that OAM loopback cell generation is enabled on the PCV. To enable OAM F5 loopback cell generation, use the **oam-pvc manage** command.

Task ID

Task ID	Operations
atm	read, write

Examples

The following example shows how to OAM management parameters for an ATM PVC. In this example, the PVC is brought down after five consecutive OAM AIS/RDI cells are received and then brought back up when no OAM AIS/RDI cells are received for 10 seconds. End-to-end F5 OAM loopback cells are transmitted every five seconds if a change in the up or down state is verified.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/2/0/0.1 point-to-point
RP/0/0/CPU0:router(config-subif)# pvc 10/100
RP/0/0/CPU0:router(config-atm-vc)# oam retry 5 10 5
```

The following example shows how to configure OAM management parameters for a VC-class. In this example, all PVCs that are associated with the VC-class called “classA” inherit an OAM up-count of 3, down-count of 5, and retry-frequency of 10:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# vc atm classA
RP/0/0/CPU0:router(config-vc-class-atm)# oam retry 10 20 10
```

Related Commands

Command	Description
show atm class-link, on page 53	Displays configuration information for the parameters on a VC class that is associated with a particular PVC.
show atm pvc, on page 67	Displays ATM PVC and traffic information for the entire router.

ping atm interface atm

To verify connectivity between two ATM connection endpoints through a permanent virtual circuit (PVC) or VP-tunnel, use the **ping atm interface atm** command in EXEC mode.

ping atm interface atm *interface-path-id* [. *subinterface*] [*vpi*/*vci*] [**end-loopback** *packets*| **seg-loopback** *packets*] [**timeout** *seconds*]

Syntax Description

interface-path-id [.*subinterface*]	Physical interface or virtual interface followed by the optional subinterface path ID. Naming notation is *interface-path-id.subinterface*. The period in front of the subinterface value is required as part of the notation. For more information about the syntax for the router, use the question mark (?) online help function.
vpi/*vci*	(Optional) ATM virtual path identifier (VPI) and virtual channel identifier (VCI) numbers. The absence of the slash (/) and a *vpi* value defaults the *vpi* value to 0. **Note** A VPI of 0 is not applicable to VP-tunnels or Layer 2 PVPs.
end-loopback *packets*	(Optional) Sends a specified number of end-to-end OAM loopback packets over the connection. Replace *packets* with the number of end-to-end OAM loopback packets you want to send over the ATM interface.
seg-loopback *packets*	(Optional) Sends a specified number of segmented OAM loopback packets over the connection. Replace *packets* with the number of OAM loopback packets you want to send over the ATM interface.
timeout *seconds*	Predetermined time during which the destination can send an OAM loopback response cell back to the source. Replace *seconds* with number of seconds to wait for an OAM loopback response before the ping times out. The default value of the timeout is 2 seconds on Cisco routers.

Command Default

seconds: 2

Command Modes

EXEC (#)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

The following guidelines apply to PVCs and VC-classes.

The **ping atm interface atm** command sends an OAM packet to verify ATM PVC connectivity. The status of the PVC is displayed when a response to the OAM packet is received. This is a common method for testing the accessibility of the devices.

The **ping atm interface atm** command is used to determine the following:

- Whether a remote host is active or inactive.
- The round-trip delay in communicating with the host.
- Packet loss.

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.
- If specifying a virtual interface, the number range varies, depending on interface type.

Include the **end-loopback** *packets* keyword argument with the **ping atm interface atm** command to verify end-to-end PVC integrity.

Include the **seg-loopback** *packets* keyword argument with the **ping atm interface atm** command to verify PVC integrity to the immediate neighboring ATM device.

Note The **ping** command is not available for Layer 2 ACs.

Task ID

Task ID	Operations
basic-services	execute
atm	read

Examples

The following example shows how verify connectivity between two ATM connection endpoints through a PVC with a VPI of 10 and a VCI of 100.

```
RP/0/0/CPU0:router# ping atm interface atm 0/2/0/0.10 10/100
```

Related Commands

Command	Description
show atm interface atm, on page 60	Displays ATM-specific information about an ATM interface.

pvc (ATM)

To create an ATM permanent virtual circuit (PVC) with Interim Local Management Interface (ILMI) encapsulation and enter ATM virtual circuit configuration mode, use the **pvc** command in interface configuration mode or subinterface configuration mode. To remove an ATM PVC from an interface, use the **no** form of this command.

In interface configuration mode for a point-to-point ATM main interface:

pvc *vpi*/*vci* **ilmi**

no pvc *vpi*/*vci* **ilmi**

In interface configuration mode for an ATM subinterface:

pvc *vpi*/*vci*

no pvc *vpi*/*vci*

Syntax Description

vpi/	ATM network virtual path identifier (VPI) for this PVC. If support for the 12-bits VPI Network-Node Interface (NNI) cell format is enabled on the ATM main interface that hosts this PVC, then the range is from 0 through 4095. If support for the 12-bits VPI NNI cell format is not enabled on the host ATM main interface, then the range is from 0 through 255. **Note** To enable support for the 12-bits VPI NNI cell format on the main ATM interface hosting the specified PVC, use the **atm maxvpi-bits 12** command.
vci	ATM network virtual channel identifier (VCI) for this PVC. Range is from 1 through 65535. The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only. **Note** Typically, lower values from 1 through 18 are reserved for specific traffic (for example, F4 OAM, ILMI, and so on), and should not be used. **Note** *The vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0.
ilmi	Sets up communication with the Interim Local Management Interface (ILMI). The associated VPI is 0, and VCI the associated VCI is any VCI. **Note** VCI 16 is typically used for ILMI. **Note** The **ilmi** keyword is available for point-to-point ATM interfaces only.

Command Default

No PVC is defined.

Command Modes

Interface configuration (config-if)

Subinterface configuration (config-subif)

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.4.1	This command was supported in subinterface configuration mode for ATM subinterface attachment circuits (ACs).

Usage Guidelines

The **pvc** command creates a PVC and attaches it to the specified VPI and VCI. Both the *vpi* and *vci* arguments cannot be simultaneously specified as 0; if one is 0, the other cannot be 0.

Cisco IOS XR software dynamically creates rate queues as necessary to satisfy the requests of the PVC commands.

When you issue the **pvc** command in interface or subinterface configuration mode for a point-to-point ATM main interface, the CLI prompt changes to "config-atm-vc," indicating that you have entered the ATM virtual circuit configuration submode.

Note Although the CLI prompt looks the same for the ATM virtual circuit configuration submode under the ATM main interface and the ATM subinterface in point-to-point configurations, the commands that are available under each interface type vary.

When you issue the **pvc** command in subinterface configuration mode for an ATM AC, the CLI prompt changes to "config-atm-l2transport-pvc," indicating that you have entered the ATM layer 2 transport PVC configuration submode.

Note For the 4-Port OC-3 and 4-Port OC-12 line cards, the VCI range is 19 through 65535.

In the following sample output, the question mark (**?**) online help function displays all the commands available under the ATM virtual circuit configuration submode for the main ATM interface:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/2/0/0.1 point-to-point
RP/0/0/CPU0:router(config-if)# pvc 10/100
RP/0/0/CPU0:router(config-atm-vc ?

  commit    Commit the configuration changes to running
  describe  Describe a command without taking real actions
  do        Run an exec command
  exit      Exit from this submode
  no        Negate a command or set its defaults
  root      Exit to the global configuration mode

RP/0/0/CPU0:router(config-atm-vc)#
```

In the following sample output, the question mark (**?**) online help function displays all the commands available under the ATM virtual circuit configuration submode for the ATM subinterface:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config-if)# interface atm 0/2/0/0.1 point-to-point
```

```
RP/0/0/CPU0:router(config-subif)# pvc 20/200
RP/0/0/CPU0:router(config-atm-vc)# ?

  class-vc        Configure vc-class
  commit          Commit the configuration changes to running
  describe        Describe a command without taking real actions
  do              Run an exec command
  encapsulation   Configure encapsulation on this PVC
  exit            Exit from this submode
  no              Negate a command or set its defaults
  oam             Configure ATM OAM VC commands
  oam-pvc         Enter OAM to generate OAM cells
  root            Exit to the global configuration mode
  service-policy  Configure QoS Service policy
  shape           ATM Traffic Shaping
  show            Show contents of configuration

RP/0/0/CPU0:router(config-atm-vc)#
```

In the following sample output, the question mark (**?**) online help function displays all the commands available under the ATM layer 2 transport PVC configuration submode for the ATM interface:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config-if)# interface atm 0/2/0/0.1 l2transport
RP/0/0/CPU0:router(config-subif)# pvc 20/200
RP/0/0/CPU0:router(config-atm-l2transport-pvc)# ?

  cell-packing    Configure L2VPN cell packing parameters
  class-vc        Configure vc-class
  commit          Commit the configuration changes to running
  describe        Describe a command without taking real actions
  do              Run an exec command
  encapsulation   Configure encapsulation on this PVC
  exit            Exit from this submode
  no              Negate a command or set its defaults
  oam             Configure ATM OAM VC commands
  oam-ac          Configure L2VPN OAM parameters
  oam-pvc         Enter OAM to generate OAM cells
  pwd             Commands used to reach current submode
  root            Exit to the global configuration mode
  service-policy  Configure QoS Service policy
  shape           ATM Traffic Shaping
  show            Show contents of configuration
```

Task ID

Task ID	Operations
atm	read, write

Examples

The following example shows how to create an ATM PVC with ILMI encapsulation on an ATM main interface, and enter ATM virtual circuit configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/6/0/1
RP/0/0/CPU0:router(config-if)# pvc 5/100 ilmi
RP/0/0/CPU0:router(config-atm-vc)#
```

The following example shows how to create an ATM PVC on a point-to-point ATM subinterface and enter ATM virtual circuit configuration mode:

```
RP/0/0/CPU0:router# configure
```

```
RP/0/0/CPU0:router(config-if)# interface atm 0/2/0/0.1 point-to-point
RP/0/0/CPU0:router(config-subif)# pvc 20/200
RP/0/0/CPU0:router(config-atm-vc)#
```

The following example shows how to create an ATM PVC on an ATM layer 2 subinterface and enter ATM layer 2 transport PVC configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config-if)# interface atm 0/2/0/0.1 l2transport
RP/0/0/CPU0:router(config-subif)# pvc 20/200
RP/0/0/CPU0:router(config-atm-l2transport-pvc)#
```

Related Commands

Command	Description
show atm class-link, on page 53	Displays configuration information for the parameters on a VC class that is associated with a particular PVC.
show atm pvc, on page 67	Displays ATM PVC and traffic information for the entire router.

pvp (ATM)

To create an ATM permanent virtual path (PVP) and enter ATM layer 2 transport PVP configuration mode, use the **pvp** command in subinterface configuration mode. To remove an ATM PVP from an interface, use the **no** form of this command.

pvp *vpi*

no pvp *vpi*

Syntax Description

vpi	ATM network virtual path identifier (VPI) for this PVC. If support for the 12-bit VPI Network-Node Interface (NNI) cell format is enabled on the ATM main interface that hosts this PVP, then the range is from 1 through 4095. If support for the 12-bit VPI NNI cell format is not enabled on the host ATM main interface, then the range is from 1 through 255. **Note** To enable support for the 12-bits VPI NNI cell format on the main ATM interface hosting the specified PVP, use the **atm maxvpi-bits 12** command.

Command Default

No PVC is defined.

Command Modes

Subinterface configuration (config-subif)

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

The **pvp** command creates a PVP and attaches it to the specified VPI.

Cisco IOS XR software dynamically creates rate queues as necessary to satisfy the requests of the PVP commands.

When you issue the **pvp** command in subinterface configuration mode, the CLI prompt changes to "config-atm-l2transport-pvp," indicating that you have entered the ATM layer 2 transport PVP configuration submode.

Note The **pvp** command is available for layer 2 subinterfaces only.

Note PVPs do not support a VPI of 0.

In the following sample output, the question mark (**?**) online help function displays all the commands available under the ATM layer 2 transport PVP configuration submode for the ATM subinterface:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config-if)# interface atm 0/2/0/0.1 l2transport
RP/0/0/CPU0:router(config-subif)# pvp 20
RP/0/0/CPU0:router(config-atm-l2transport-pvp)# ?

  cell-packing    Configure L2VPN cell packing parameters
  commit          Commit the configuration changes to running
  describe        Describe a command without taking real actions
  do              Run an exec command
  exit            Exit from this submode
  no              Negate a command or set its defaults
  pwd             Commands used to reach current submode
  root            Exit to the global configuration mode
  shape           ATM Traffic Shaping
  show            Show contents of configuration
```

Task ID

Task ID	Operations
atm	read, write

Examples

The following example shows how to create an ATM PVP on an ATM subinterface, and enter ATM layer 2 transport PVP configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config-if)# interface atm 0/2/0/0.1 l2transport
RP/0/0/CPU0:router(config-subif)# pvp 20
RP/0/0/CPU0:router(config-atm-l2transport-pvp)#
```

Related Commands

Command	Description
show atm pvp, on page 75	Displays ATM PVP and traffic information for the entire router, or a specific VPI or ATM interface.

shape

To configure ATM traffic shaping for a PVC, use the **shape** command in the appropriate command mode. To remove the configured ATM traffic shaping and return the PVC to using the default constant bit rate (CBR) traffic shaping, use the **no** form of this command.

shape {**cbr** *peak_output_rate*| **ubr** *peak_output_rate*| **vbr-nrt** *peak_output_rate sustained_output_rate burst_size*| **vbr-rt** *peak_output_rate sustained_output_rate burst_size*}

no shape

Syntax Description

cbr	Configures the service class for the VC or VP-tunnel to be CBR. Range is from 38 through 622000 kbps. This is the default service class.
ubr	Configures the service class for the VC or VP-tunnel to be unspecified bit rate (UBR). UBR is intended for non-real-time applications that do not require any maximum bound on the transfer delay or on the cell loss ratio. Ranges follow: • OC12—from 38 through 622000 • OC3—from 38 through 155000
vbr-nrt	Configures the service class for the VC or VP-tunnel to be variable Bit Rate-Non Real Time (VBR-nrt).
vbr-rt	Configures the service class for the VC or VP-tunnel to be variable bit rate-real time (VBR-rt).
peak_output_rate	Peak output rate for the bit rate. Replace the *peak_output_rate* argument with the peak output rate in kbps. For VP-tunnels, the ranges follow: • OC12—84 through 622000 • OC3—84 through 155000 For VCs, the ranges follow: • OC12—38 through 622000 • OC3—38 through 155000 **Note** The *peak_output_rate* must be to be greater than *sustained_output_rate*.

sustained_output_rate	Sustained output rate for the bit rate. Replace the *sustained_output_rate* argument with the sustained output rate in kbps. For VP-tunnels, the ranges follow: • OC12—84 through 622000 • OC3—84 through 155000 For VCs, the ranges follow: • OC12—38 through 622000 • OC3—38 through 155000 **Note** The *sustained_output_rate* must be to be less than *peak_output_rate*.
burst_size	Burst cell size for the bit rate. Replace the *sustained_output_rate* argument with the burst size. Range is from 1 through 8192.

Command Default

The default service class for the VC is **cbr**.

Command Modes

ATM PVC configuration (config-atm-vc)

ATM VC-class configuration (config-vc-class-atm)

ATM Layer 2 transport PVC configuration (config-atm-l2transport-pvc)

ATM Layer 2 transport PVP configuration (config-atm-l2transport-pvp)

ATM VP tunnel configuration mode (config-atm-vp-tunnel)

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.4.1	This command was supported in ATM layer 2 transport PVC configuration mode and ATM layer 2 transport PVP configuration mode.

Usage Guidelines

Task ID

Task ID	Operations
atm	read, write

Examples

The following example shows how to configure the service class for a PVC to be UBR, with a peak output of 150,000 kbps:

```
RP/0/0/CPU0:router#config
RP/0/0/CPU0:router(config)# interface atm 0/6/0/0.2 point-to-point
RP/0/0/CPU0:router(config-subif)# pvc 20/200
RP/0/0/CPU0:router(config-atm-vc)# shape ubr 150000
```

The following example shows how to configure the service class for a VP-tunnel to be CBR, with a peak output of 150,000 kbps:

```
RP/0/0/CPU0:router#config
RP/0/0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/0/CPU0:router(config-if)# vp-tunnel 10
RP/0/0/CPU0:router(config-atm-vp-tunnel)# shape cbr 150000
```

The following example shows how to configure the service class for a VC to be VBR-nrt:

```
RP/0/0/CPU0:router# config
RP/0/0/CPU0:router(config)# vc-class atm class1
RP/0/0/CPU0:router(config-vc-class-atm)# shape vbr-nrt 100000 100000 8000
RP/0/0/CPU0:router(config-vc-class-atm)# exit
RP/0/0/CPU0:router(config)# exit
Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:y
RP/0/0/CPU0:router#
```

Related Commands

Command	Description
show atm pvc, on page 67	Displays ATM PVC and traffic information for the entire router.
show atm pvp, on page 75	Displays ATM PVP and traffic information for the entire router, or a specific VPI or ATM interface.
show atm vp-tunnel, on page 85	Displays VP tunnel information for the entire router or for a specific interface.

show atm cell-packing

To display cell packing information for the Layer 2 attachment circuits (ACs) configured on your system, use the **show atm cell-packing** command in EXEC mode.

show atm cell-packing

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

EXEC (#)

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
atm	read

Examples

The following sample output is from the **show atm cell-packing** command:

```
RP/0/0/CPU0:router# show atm cell-packing

                                      avg #                   avg #
     Circuit                   local  cells/pkt  negotiated  cells/pkt    MCPT
     Type                      MNCP    rcvd       MNCP        sent        (us)
ATM0/2/0/1.200    vc 1/200      1       0          1           0           50
ATM0/2/0/1.300    vc 1/300      1       0          1           0           50
```

Table 1: show atm cell-packing Field Descriptions

Field	Description
Circuit Type	AC instance and virtual channel identifier. • The AC instance is expressed in the *rack/slot/module/port.subinterface* format. • The virtual channel identifier is expressed in the *subinterface/vci* format.

Field	Description
Local MNCP	Maximum number of cells that can be packed on the local AC.
AVG cells/pkt rcvd	Average number of cells in a packed cell received from the peer, or the average number of cells packed by the peer.
negotiated MNCP	Negotiated maximum number of cells that can be packed on a psuedowire between PE routers.
AVG cells/pkt sent	Maximum number of cells that can be packed on the peer AC.
MCPT	Maximum number of cells allowed per packet configured on the local MCPT.

show atm class-link

To display configuration information for the parameters on a virtual circuit (VC) class that is associated with a particular PVC, use the **show atm class-link** command in privileged EXEC mode.

show atm class-link *vpi*/*vci*

Syntax Description

vpi/*vci*	ATM VPI and VCI numbers. The absence of the slash (/) and a *vpi* value defaults the *vpi* value to 0. **Note** A VPI of 0 is not applicable to VP-tunnels.

Command Default

The absence of the slash (/) and a *vpi* value defaults the *vpi* value to 0.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.4.1	The **show atm class-link** command output was modified to include Layer 2 VPN parameters when appropriate.

Usage Guidelines

Note If a PVC or its host interface is associated with a VC-class, then that PVC inherits all the values configured for that VC-class. If no VC-class is configured for a PVC or its host interface, then the command output displays a message that says "VC class not supported on this VC."

Task ID

Task ID	Operations
atm	read

Examples

The following sample output is from the **show atm class-link** command:

```
RP/0/0/CPU0:router# show atm class-link 10/100

ATM0/2/0/0.1: VPI: 10 VCI: 100
```

```
shape : cbr 100000 (VC-class configured on VC)
encapsulation : aal5snap (VC-class configured on VC)
oam-pvc : manage 300   (VC-class configured on VC)
oam retry : 3 5 1 (Default value)
oam ais-rdi : 1 3 (Default value)
```

Table 2: show atm class-link Field Descriptions, on page 54 describes the significant fields shown in the display.

Table 2: show atm class-link Field Descriptions

Field	Description
ATM *rack*/*slot*/*module*/*port*	Interface instance, expressed in the *rack*/*slot*/*module*/*port* format.
VPI	Virtual path identifier.
VCI	Virtual channel identifier.
shape	Service class for the VC or VP-tunnel and the peak output rate for the bit rate. Possible service classes follow: • cbr • ubr • vbr-nrt • vbr-rt
encapsulation	Encapsulation type for this VC.
oam-pvc	Frequency (in seconds) at which end-to-end F5 OAM loopback cells are transmitted on this PVC. Range is from 0 through 600. **Note** Use the **oam-pvc manage** command to modify the current configuration for this field.

Field	Description
oam retry	Displays the following F5 OAM loopback cell retry count, down count, and retry frequency that has been configured on the VC-class that is associated with the specified PVC: • Number of consecutive end-to-end F5 OAM loopback cell responses that must be received to change a connection state to up. (Retry count) • Number of consecutive unreceived end-to-end F5 OAM loopback cells allowed on a PVC before its state changes to down. (down count) • Frequency (in seconds) at which end-to-end F5 OAM loopback cells are transmitted when a change in the up or down state is being verified. (retry frequency) **Note** Use the **oam retry** command to modify the current configuration for this field. **Note** If the F5 OAM loopback cell retry count, down count, or retry frequency was not configured on the VC-class map that is associated with the specified PVC, then the command output does not display information for the oam retry field.
oam ais-rdi	Displays the following OAM AIS/RDI-related information for the PVC: • the maximum number of OAM AIS/RDI cells that can be received on a PVC before it is brought down. • the interval after which a downed PVC comes back up if no OAM AIS/RDI cells have been received. **Note** Use the **oam ais-rdi** command in to modify the current configuration for this field.

The following sample output is from the **show atm class-link** command when there is no VC-class associated with the specified PVC:

```
RP/0/0/CPU0:router# show atm class-link 0/50

Detailed display of VC(s) with VPI/VCI = 0/50

Class link for VC 0/50
ATM0/2/0/2: VPI: 0 VCI: 50
ILMI VC (VC class not supported on this VC)
```

Related Commands

Command	Description
class-int, on page 17	Assigns a VC class to an ATM main interface.
vc-class atm, on page 94	Creates a VC class for an ATM PVC or an ATM interface and enters VC-class configuration mode.

show atm ilmi-status

To display status information that is related to Interim Local Management Interface (ILMI), use the **show atm ilmi-status** command in EXEC mode.

show atm ilmi-status[**atm** *interface-path-id*[*.subinterface*]]

Syntax Description

atm	(Optional) ATM interface for which you want to display information.Use the *interface-path-id* argument to specify the ATM interface.
interface-path-id[*.subinterface*]	Physical interface or virtual interface followed by the optional subinterface path ID. Naming notation is *interface-path-id.subinterface*. The period in front of the subinterface value is required as part of the notation. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

Entering the **show atm ilmi-status** command without specifying an interface displays ILMI-related status information for all ATM interfaces.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
atm	read

Examples

The following sample output is from the **show atm ilmi-status** command:

```
RP/0/0/CPU0:router# show atm ilmi-status

Interface : ATM0/2/0/1 Interface Type : Private UNI (User-side)
ILMI VCC : (20, 30)
ILMI Keepalive : Disabled
ILMI State:       WaitDevType
Peer IP Addr : 0.0.0.0         Peer IF Name : ATM1/2
Active Prefix(s) :
```

The following sample output is from the **show atm ilmi-status** command with the **atm** *instance* keyword and argument:

```
RP/0/0/CPU0:router# show atm ilmi-status atm 0/2/0/2

Interface : ATM0/2/0/2 Interface Type : Private UNI (User-side)
ILMI VCC : (0, 16) ILMI Keepalive : Disabled
ILMI State:       UpAndNormal
Peer IP Addr:     0.0.0.0         Peer IF Name:     ATM1/2
Active Prefix(s) :
```

Table 3: show atm ilmi-status Field Descriptions

Field	Description
Interface	Interface type and instance. The instance is displayed in the *rack*/*slot*/*module*/*port* format.
Interface Type	ATM interface type (Private or Public), and the communication protocol used by this interface. **Note** Currently, Cisco IOS XR software supports UNI only.
ILMI VCC	The virtual channel connection associated with this interface.
ILMI Keepalive	ILMI keepalives polling frequency configured on this interface. To modify the ILMI keepalives polling frequency, use the **atm ilmi-keepalive** command.
ILMI State	Status of ILMI for this interface. Possible ILMI states are: • Link failing • Establishing connection • Configuring peer information • Retrieving network prefix from peer • Registering network prefix to peer • Retrieving ATM network addresses from peer • Registering ATM network addresses to peer • Verifying configuration and ATM network addresses • WaitDevType — ILMI process is initialized and in the process of sending ILMI packets to a neighbor. In this case, the ILMI PVC is not yet established. • UpAndNormal — ILMI traps are received by the neighbors, and the PVC is established.

Field	Description
Peer IP Addr	IP address for the remote (neighbor) end point of the connection.
Peer IF Name	Identifies the interface at the remote (neighbor) end point of the connection.
Active Prefix(s)	Network prefix that is registered from the switch side and is active and valid.

Related Commands

Command	Description
atm ilmi-config disable, on page 4	Disables ILMI on an ATM interface.
atm ilmi-keepalive, on page 6	Enables ILMI keepalives on an ATM interface and configure keepalive polling frequency.

show atm interface atm

To display ATM-specific information about an ATM interface, use the **show atm interface atm** command in EXEC mode.

show atm interface atm *interface-path-id*

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values

Command Modes

EXEC (#)

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.4.1	The **show atm interface atm**command output was modified to include Layer 2 VPN parameters when appropriate.

Usage Guidelines

Task ID

Task ID	Operations
atm	read

Examples

The following sample output is from the **show atm interface atm** command:

```
RP/0/0/CPU0:router# show atm interface atm 0/2/0/3

Interface                           : ATM0/2/0/3
AAL Enabled                         : AAL5
Max-VP                              : 254
Max-VC                              : 2046
Configured L2 PVPs                  : 0
Configured L2 PVCs                  : 0
Configured L3 VP-Tunnels            : 0
```

```
Configured L3 PVCs                    : 1
L2 PVPs in Down State                 : 0
L2 PVCs in Down State                 : 0
L3 VP-Tunnels in Down State           : 0
L3 PVCs in Down State                 : 0
Cell packing count                    : 0

Received Side Statistics:
    Received Cells                    : 0
    Received Bytes                    : 0
    Received AAL Packets              : 0

Receive Side Cells Dropped:
    Unrecognized VPI/VCI              : 0

Receive Side AAL5 Packets Dropped:
    Unavailable SAR Buffer            : 0
    Non-Resource Exhaustion           : 0
    Reassembly Timeout                : 0
    Zero Length                       : 0
    Unavailable Host Buffer           : 0
    Packet size exceeds MPS           : 0
    AAL5 Trailer Length Errors        : 0

Transmit Side Statistics:
    Transmitted Cells                 : 1899716067
    Transmitted Bytes                 : 0
    Transmitted AAL Packets           : 0

Transmit Side Cells Dropped:
    Unrecognized VPI/VCI              : 0

Transmit Side AAL5 Packets Dropped:
    Unavailable SAR Buffer            : 0
    Non-Resource Exhaustion           : 0
    WRED Threshold                    : 0
    WRED Random                       : 0
```

Table 4: show atm interface atm Field Descriptions

Field	Description
Interface	Interface type and instance. The instance is displayed in the *rack*/*slot*/*module*/*port* format.
Layer2 Transport Port Mode	Displays whether Layer 2 transport mode is enabled or disabled on this interface.
Cell Packing Data Unavailable	Displays whether cell packing is enabled or disabled on this interface.
Received Side Statistics	Displays the following statistical information for the receiving end of this interface: • Received Cells—Total number of cells received from the remote end. • Received Bytes—Total number of bytes received from the remote end. • Received AAL5 Packets—Total number of AAL5 packets received from the remote end.

Field	Description
Receive Side Cells Dropped	Displays the following information about AAL5 packets received from the remote end that were dropped by this end of the interface: • Unavailable SAR Buffer—Total number of AAL5 packets received from the remote end that were dropped because the Segmentation and Reassembly (SAR) buffer was unavailable. • Non-Resource Exhaustion—Total number of packets received from the remote end that were discarded due to events other than resource exhaustion, including raw or non AAL5 cells. • Reassembly Timeout—Number of AAL5 packets received from the remote end that were dropped because the reassembly of those packets took too long and the system timed-out. • CRC-32 Errors—Number of AAL5 packets received from the remote end that were dropped due to CRC-32 errors. • Zero Length—Number of AAL5 packets received from the remote end that were dropped due to • Unavailable Host Buffer—Number of AAL5 packets received from the remote end that were dropped because the host buffer was unavailable. • Packet size exceeds MPS—Number of AAL5 packets received from the remote end that were dropped due to a mismatch between the actual packet length and the reassembled packet length. • AAL5 Trailer Length Errors—Number of AAL5 packets received from the remote end that were dropped because their packet length was bigger than the AAL5 trailer.

Field	Description
Receive Side AAL5 Packets Dropped	Displays the number of received AAL5 packet drops that occurred on this interface due to the following errors: • Unavailable SAR Buffer—Number of AAL5 packets that were dropped because the SAR buffer was unavailable. • Non-Resource Exhaustion— • Reassembly Timeout— • CRC-32 Errors— • Zero Length— • Unavailable Host Buffer— • Packet size exceeds MPS— • AAL5 Trailer Length Errors—
Receive Side Cells Dropped	Number of unrecognized VPI and VCI cells received from the remote end that were dropped.

Field	Description
Receive side AAL5 Packets Dropped:	Displays the following information about AAL5 packets received from the remote end that were dropped by this end of the interface: • Unavailable SAR Buffer—Total number of AAL5 packets received from the remote end that were dropped because the Segmentation and Reassembly (SAR) buffer was unavailable. • Non-Resource Exhaustion—Total number of packets received from the remote end that were discarded due to events other than resource exhaustion, including raw or non AAL5 cells. • Reassembly Timeout—Number of AAL5 packets received from the remote end that were dropped because the reassembly of those packets took too long and the system timed-out. • CRC-32 Errors—Number of AAL5 packets received from the remote end that were dropped due to CRC-32 errors. • Zero Length—Number of AAL5 packets received from the remote end that were dropped due to • Unavailable Host Buffer—Number of AAL5 packets received from the remote end that were dropped because the host buffer was unavailable. • Packet size exceeds MPS—Number of AAL5 packets received from the remote end that were dropped due to a mismatch between the actual packet length and the reassembled packet length. • AAL5 Trailer Length Errors—Number of AAL5 packets received from the remote end that were dropped because their packet length was bigger than the AAL5 trailer.

Field	Description
Transmit Side Statistics	Displays the following statistical information for the transmit side of this interface: • Transmitted Cells—Total number of cells that were transmitted to the remote end. • Transmitted Bytes—Total number of bytes that were transmitted to the remote end. • Transmitted AAL5 Packets—Total number of AAL5 packets that were transmitted to the remote end.
Transmit side Cells Dropped	Number of VPI and VCI cells transmitted to the remote end that were dropped because they were not recognized by the remote end.
Transmit Side AAL5 Packets Dropped	Displays the following information about transmitted AAL5 packets that were dropped by the remote end: • Unavailable SAR Buffer—Number of transmitted AAL5 packets that were dropped by the remote end because the Segmentation and Reassembly (SAR) buffer was unavailable. • Non-Resource Exhaustion—Total number of packets dropped by the remote end due to events other than resource exhaustion, including raw or non AAL5 cells. • WRED Threshold—Gives the value of the packets dropped by WRED QoS mechanism. It is dropped when queue length exceeds the configured WRED max-threshold value. • WRED Random—Gives the value of the early dropped packets by WRED QoS mechanism. It is early dropped when queue length is between WRED min-threshold and max-threshold.
Cell-packing statistics	Displays the following cell packing statistics for the specified interface: • Average number of cells sent—Average number of cells in a packed cell that were packed on this interface. • Average number of cells received—Average number of cells in a packed cell that were received by this interface.

Related Commands

Command	Description
interface atm, on page 26	Configures an ATM interface and enters ATM interface configuration mode.

show atm pvc

To display ATM permanent virtual circuit (PVC) and traffic information for the entire router, or a specific VPI/VCI or ATM interface, use the **show atm pvc** command in EXEC mode.

show atm pvc [*vpi*/*vci*| **interface atm interface-path-id**]

Syntax Description

vpi/*vci*	(Optional) ATM virtual path identifier (VPI) and virtual channel identifier (VCI) numbers. The absence of the slash (/) and a *vpi* value defaults the *vpi* value to 0. **Note** A VPI of 0 is not applicable to VP-tunnels.
interface atm	(Optional) ATM interface for which you want to display information.Use the *interface-path-id* argument to specify the ATM interface.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

Entering the **show atm pvc** command without specifying the *vpi*/*vci* argument or **interface atm** *instance* keyword argument displays ATM PVC and traffic information for the entire router.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.4.1	The **show atm pvc** command output was modified to include Layer 2 VPN parameters when appropriate.

Usage Guidelines

Task ID

Task ID	Operations
atm	read

Examples

The following sample output is from the **show atm pvc** command:

```
RP/0/0/CPU0:router# show atm pvc

                                                Peak  Avg/Min  Burst
Interface          VPI  VCI Type  Encaps  SC   Kbps   Kbps    Cells  Sts
ATM0/1/0/0.230      15  230 PVC   AAL0   UBR  622000    N/A     N/A   UP
ATM0/1/0/3.19       17   19 PVC   SNAP   UBR  622000    N/A     N/A   UP
```

Table 5: show pvc (all PVCs) Field Descriptions

Field	Description
Interface	Interface type and instance. The instance is displayed in the *rack*/*slot*/*module*/*port* format.
VPI	ATM network virtual path identifier (VPI) associated with the specified interface.
VCI	ATM network virtual channel identifier (VCI) associated with the specified interface.
Type	Type of VPI/VCI associated with the specified interface. In this release, only PVCs are supported.

Field	Description
Encaps	Encapsulation type that configured on the specified interface. Possible encapsulation types follow: • ILMI—Interim Local Management Interface. ILMI encapsulation is available for point-to-point PVCs only. • MUX—aal5mux ipv4; IPv4 encapsulation for multiplex (MUX)-type VCs. MUX encapsulation is available for point-to-point PVCs only. • NLPID—aal5nlpid; AAL and encapsulation type that allows ATM interfaces to interoperate with High-Speed Serial Interfaces (HSSIs), which are using an ATM data service unit (ADSU) and running ATM-Data Exchange Interface (DXI). Supported on ATM PVCs only. NLPID encapsulation is available for point-to-point PVCs only. • SNAP—aal5snap; AAL and encapsulation type that supports Inverse ARP. Logical Link Control/Subnetwork Access Protocol precedes the protocol datagram. SNAP encapsulation is available for point-to-point PVCs only. • AAL0— • AAL5— **Note** To disable ILMI on a point-to-point ATM interface, use the **atm ilmi-config disable** command in interface configuration mode for an ATM interface. To configure aal5mux, aal5nlpid, or aal5snap encapsulation on an ATM interface, use the **encapsulation** command in ATM VC-class configuration mode, and then assign that VC-class to the appropriate ATM main interface.

Field	Description
SC	Service class that is assigned to the specified ATM interface. Possible service classes follow: • cbr • ubr • vbr-nrt • vbr-rt **Note** To modify a configured ATM service class, use the **shape** command in the appropriate command mode.
Peak Kbps	Peak output rate for the bit rate in kbps. **Note** To modify the Peak output rate, use the **shape** command.
Avg/Min Kbps	Number of kilobits per second sent at the average (sustained) rate. **Note** To modify the average (or sustained) rate, use the **shape** command.
Burst cells	Identifies the burst cell size in terms of number of cells. This number is the maximum number of ATM cells the VC can send at the peak rate. **Note** To modify the burst cell size, use the **shape** command.
Sts	Status of the PVC. Can be “UP” or “DOWN.”

The following sample output is from the **show atm pvc** command with the *vpi/vci* argument included:

```
RP/0/0/CPU0:router# show atm pvc 10/100

Detailed display of VC(s) with VPI/VCI = 10/100

ATM0/2/0/3.100: VPI: 10 VCI: 100
UBR, PeakRate: 622000 Kbps
AAL5-LLC/SNAP
OAM frequency: 10 second(s), OAM retry frequency: 1 second(s),
OAM up retry count: 3, OAM down retry count: 5,
OAM Keep-vc-up: False, OAM AIS-RDI failure: None,
OAM AIS-RDI down count: 1, OAM AIS-RDI up time: 3 second(s),
OAM Loopback status: No loopback enabled,
OAM VC state: Loopback Not verified,
VC is not managed by OAM,

OAM cells received: 0,
F5 InEndLoop: 0, F5 InSegLoop: 0,
F5 InEndAIS: 0,  F5 InSegAIS: 0,
F5 InEndRDI: 0,  F5 InSegRDI: 0,
OAM cells sent: 0,
F5 OutEndLoop: 0, F5 OutSegLoop: 0,
F5 OutEndAIS: 0,  F5 OutSegAIS: 0,
```

```
F5 OutEndRDI: 0,  F5 OutSegRDI: 0,
OAM cells drops: 0

InPkts: 0                    OutPkts: 0
InBytes: 0                   OutBytes: 0
WRED pkt drop: 0
Non WRED pkt drop: 0

Internal state: READY
Status: UP
```

Table 6: show atm pvc Field Descriptions

Field	Description
Detailed display of VC(s) with VPI/VCI	Displays the following general information for the specified PVC: • VPI and VCI in the *VPI*/*VCI* format • associated interface type and instance in the *type rack*/*slot*/*module*/*port* format. • associated VPI • associated VCI • Service class that is assigned to the specified ATM interface. Possible service classes follow: ◦ cbr ◦ ubr ◦ vbr-nrt ◦ vbr-rt • Peak line rate (bandwidth) required for the specified ATM interface, in kilobits per second. • Whether ILMI is enabled on the interface. **Note** To modify a configured ATM service class, use the **shape** command in the appropriate command mode. **Note** To modify the bandwidth required for an ATM interface (peak line rate), use the **shape** command in interface configuration mode.
OAM frequency	Frequency (in seconds) at which end-to-end F5 OAM loopback cells are transmitted when a change in the up or down state of a PVC is being verified. **Note** To modify the OAM frequency, use the **oam-pvc manage** command in ATM virtual circuit (VC) class configuration mode.

Field	Description
OAM retry frequency	Frequency (in seconds) at which end-to-end F5 OAM loopback cells are transmitted when a change in the up or down state is being verified. **Note** To modify the OAM retry frequency, use the **oam retry** command in the appropriate command mode.
OAM up retry count	Number of consecutive end-to-end F5 OAM loopback cell responses that must be received in order to modify a PVC state to up.
OAM down retry count	Number of consecutive unreceived end-to-end F5 OAM loopback cell responses allowed before a PVC state changes to down.
OAM AIS-RDI down count:	Number of OAM AIS/RDI cells received on a PVC before it is brought down. **Note** To modify the OAM AIS-RDI down count, use the **oam ais-rdi** command in ATM VC-class configuration mode
OAM AIS-RDI up time	Interval after which a PVC is brought up if it has not received any OAM AIS/RDI cells. **Note** To modify the OAM AIS-RDI uptime, use the **oam ais-rdi** command in ATM VC-class configuration mode
OAM Loopback status	Status of end-to-end F5 OAM loopback cell generation for this VC. Possible value follow: • No loopback enabled—No loopback is enabled on this interface. • OAM Disabled—End-to-end F5 OAM loopback cell generation is disabled. • OAM Sent—OAM cell was sent. • OAM Received—OAM cell was received. • OAM Failed—OAM reply was not received within the frequency period or contained bad correlation tag.

Field	Description
OAM VC state	Current state of the specified VC. Possible VC states follow: • AIS/RDI—The VC received AIS/RDI cells. End-to-end F5 OAM loopback cells are not sent in this state. • Down Retry—An OAM loopback failed. End-to-end F5 OAM loopback cells are sent at retry frequency to verify that the VC is really down. After down-count unsuccessful retries, the VC goes to the Not Verified state. • Loopback Not Managed—VC is not being managed by OAM. • Loopback Not Verified—VC has not been verified by end-to-end F5 OAM loopback cells. AIS and RDI conditions are cleared. • Up Retry—An OAM loopback was successful. End-to-end F5 OAM loopback cells are sent at retry frequency to verify the VC is really up. After up-count successive and successful loopback retries, the VC goes to the Verified state. • Loopback Verified—Loopbacks are successful. AIS/RDI cell was not received.
OAM cells received	Number of OAM cells that have been received by this interface.
F5 InEndLoop:	Number of end-to-end F5 OAM loopback cells received by this interface.
F5 InSegLoop	Number of segment F4 OAM loopback cells received by this interface.
F5 InAIS	Number of F4 OAM AIS cells received by this interface.
F5 InRDI	Number of F4 OAM RDI cells received by this interface.
OAM cells sent	Total number of OAM cells sent on this VC.
F5 OutEndLoop	Number of end-to-end F5 OAM loopback cells sent from this interface.

Field	Description
F5 OutSegLoop	Number of segment F5 OAM loopback cells sent from this interface.
F5 OutAIS	Number of F5 OAM AIS cells sent from this interface.
F5 OutRDI	Number of F5 OAM RDI cells sent from this interface.
OAM cells drops	Number of OAM cells dropped (or flushed) by this interface.
InPkts	Total number of packets received on this VC. This number includes all fast-switched and process-switched packets.
OutPkts	Total number of packets sent on this VC. This number includes all fast-switched and process-switched packets.
InBytes	Total number of bytes received on this VC. This number includes all fast-switched and process-switched bytes.
OutBytes	Total number of bytes sent on this VC. This number includes all fast-switched and process-switched bytes.
WRED pkt drop	Total number of AAL5 packets that were dropped by this interface because their size exceeded the maximum threshold set for Weighted Random Early Discard (WRED).
Non WRED pkt drop	Total number of dropped AAL5 packets that did not exceeded the maximum threshold set for Weighted Random Early Discard (WRED).
Internal state	Internal PVC state.
Status	Current status of this PVC. Can be “Up” or “Down.”

Related Commands

Command	Description
pvc (ATM), on page 42	Creates an ATM PVC with ILMI encapsulation and enters ATM virtual circuit configuration mode.

show atm pvp

To display ATM PVP and traffic information for the entire router, or a specific VPI or ATM interface, use the **show atm pvp** command in EXEC mode.

show atm pvp [*vpi*| **interface atm instance**]

Syntax Description

vpi	(Optional) ATM virtual path identifier (VPI) number. Replace *vpi* with the VPI of the PVP whose information you want to display.
interface atm *instance*	(Optional) Displays all PVCs on the specified ATM interface. **Note** To determine the appropriate form of the *instance* argument, see your ATM network module, port adapter, or router documentation.

Command Default

Entering the **show atm pvp** command without specifying the *vpi* argument or **interface atm** *instance* keyword argument displays ATM PVP and traffic information for the entire router.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
atm	read

Examples

The following example shows how to display ATM PVP and traffic information for the entire router:

```
RP/0/0/CPU0:router# show atm pvp interface atm 0/3/0/1

                                  Peak  Avg/Min   Burst
Interface          VPI  SC        Kbps     Kbps   Cells      Sts
ATM0/3/0/1.100     100 UBR      155000    N/A      N/A       UP
```

Table 7: show pvp (all PVPs) Field Descriptions

Field	Description
Interface	Interface type and instance. The instance is displayed in the *rack*/*slot*/*module*/*port* format.
VPI	ATM network virtual path identifier (VPI) associated with the specified interface.
SC	Service class that is assigned to the specified ATM interface. Possible service classes follow: • cbr • ubr • vbr-nrt • vbr-rt **Note** To modify a configured ATM service class, use the **shape** command in the appropriate command mode.
Peak Kbps	Peak output rate for the bit rate in kbps. **Note** To modify the Peak output rate, use the **shape** command.
Avg/Min Kbps	Number of kilobits per second sent at the average (sustained) rate. **Note** To modify the average (or sustained) rate, use the **shape** command.
Burst cells	Identifies the burst cell size in terms of number of cells. This number is the maximum number of ATM cells the PVP can send at the peak rate. **Note** To modify the burst cell size, use the **shape** command.
Sts	Status of the PVP. Can be “UP” or “DOWN.”

The following example shows how to display ATM PVP and traffic information for the a specific VPI:

```
RP/0/0/CPU0:router# show atm pvp 100

Detailed display of L2PVP(s) with VPI = 100

ATM0/3/0/1.100: VPI: 100
UBR, PeakRate: 155000 Kbps
AAL0
OAM frequency: 10 second(s), OAM retry frequency: 1 second(s),
OAM up retry count: 3, OAM down retry count: 5,
OAM AIS-RDI down count: 1, OAM AIS-RDI up time: 3 second(s),
OAM Loopback status: No loopback enabled,
```

```
OAM L2PVP state: Unknown,
L2PVP is not managed by OAM,

OAM cells received: 0,
F4 InEndLoop: 0, F4 InSegLoop: 0,
F4 InEndAIS: 0,  F4 InSegAIS: 0,
F4 InEndRDI: 0,  F4 InSegRDI: 0,
OAM cells sent: 8948,
F4 OutEndLoop: 0, F4 OutSegLoop: 0,
F4 OutEndAIS: 8948,  F4 OutSegAIS: 0,
F4 OutEndRDI: 0,  F4 OutSegRDI: 0,
OAM cells drops: 0

InPkts: 8948                OutPkts: 0
InBytes: 465296             OutBytes: 0

Internal state: READY
Status: UP
```

Table 8: show atm pvp Field Descriptions

Field	Description
ATM0/1/0/0.30	Associated interface type and instance in the *type rack/slot/module/port.subinterface* format. • Service class that is assigned to the specified ATM interface. Possible service classes follow: ◦ cbr ◦ ubr ◦ vbr-nrt ◦ vbr-rt • Peak line rate (bandwidth) required for the specified ATM interface, in kilobits per second. **Note** To modify a configured ATM service class, use the **shape** command in the appropriate command mode. **Note** To modify the bandwidth required for an ATM interface (peak line rate), use the **shape** command in interface configuration mode.
VPI	VPI associated with the specified PVP.

Field	Description
UBR	Service class that is assigned to the specified ATM interface. The example shows that vbr-rt is assigned to the interface that hosts the specified PVP. Possible service classes are: • cbr • ubr • vbr-nrt • vbr-rt
PeakRate	Peak output rate for the bit rate in kbps. **Note** To modify the peak output rate, use the **shape** command.
AAL0	ATM adaptation layer (AAL) and encapsulation type for the PVP. Currently, only AAL0 is the only supported encapsulation type for PVPs.
OAM frequency	Frequency (in seconds) at which end-to-end F5 OAM loopback cells are transmitted when a change in the up or down state of a PVC is being verified. **Note** To modify the OAM frequency, use the **oam-pvc manage** command in ATM virtual circuit (VC) class configuration mode.
OAM retry frequency	Frequency (in seconds) at which end-to-end F5 OAM loopback cells are transmitted when a change in the up or down state is being verified. **Note** To modify the OAM retry frequency, use the **oam retry** command in the appropriate command mode.
OAM up retry count	Number of consecutive end-to-end F5 OAM loopback cell responses that must be received in order to modify a PVC state to up.
OAM down retry count	Number of consecutive unreceived end-to-end F5 OAM loopback cell responses allowed before a PVC state changes to down.
OAM AIS-RDI down count	Number of OAM AIS/RDI cells received on a PVC before it is brought down. **Note** To modify the OAM AIS-RDI down count, use the **oam ais-rdi** command in ATM VC-class configuration mode

Field	Description
OAM AIS-RDI up time	Interval after which a PVC is brought up if it has not received any OAM AIS/RDI cells. **Note** To modify the OAM AIS-RDI uptime, use the **oam ais-rdi** command in ATM VC-class configuration mode
OAM Loopback status	Status of end-to-end F5 OAM loopback cell generation for this VC. Possible value follow: • No loopback enabled—No loopback is enabled on this interface. • OAM Disabled—End-to-end F5 OAM loopback cell generation is disabled. • OAM Sent—OAM cell was sent. • OAM Received—OAM cell was received. • OAM Failed—OAM reply was not received within the frequency period or contained bad correlation tag.
OAM L2PVP state	Current state of the specified VC. **Note** OAM management is not supported on Layer 2 PVPs in the current release of Cisco IOS XR software.
OAM cells received	Number of OAM cells that have been received by this interface.
F4 InEndLoop:	Number of end-to-end F4 OAM loopback cells received by this interface.
F4 InSegLoop	Number of segment F4 OAM loopback cells received by this interface.
F4 InEndAIS	Number of F4 OAM AIS cells received by this interface.
F4 InSegAIS	Number of segment F4 OAM AIS cells received by this interface.
F4 InEndRDI	Number of F4 OAM RDI cells received by this interface.
F4 InSegRDI	Number of F4 segment OAM RDI cells received by this interface.

Field	Description
OAM cells drops	Number of OAM cells dropped (or flushed) by this interface.
InPkts	Total number of packets received on this VC. This number includes all fast-switched and process-switched packets.
OutPkts	Total number of packets sent on this VC. This number includes all fast-switched and process-switched packets.
InBytes	Total number of bytes received on this VC.
OutBytes	Total number of bytes sent on this VC.
Internal state	Internal PVC state.
Status	Current status of this PVC. Can be “Up” or “Down.”

Related Commands

Command	Description
pvp (ATM), on page 46	Creates an ATM PVP and enters ATM layer 2 transport PVP configuration mode.

show atm vc-class

To display information about all ATM virtual circuit (VC) classes on the router or for a specific ATM VC-class, use the **show atm vc-class** command in EXEC mode.

show atm vc-class *vc-class-name*

Syntax Description

vc-class-name	Name of the VC-class whose information you want to display.

Command Default

Entering the **show atm vc-class** command without specifying the *vc-class-name* argument displays ATM PVC and traffic information for the entire router.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.4.1	The **show atm vc-class** command output was modified to include Layer 2 VPN parameters when appropriate.

Usage Guidelines

Task ID

Task ID	Operations
atm	read

Examples

The following sample output is from the **show atm vc-class** command:

```
RP/0/0/CPU0:router# show atm vc-class

ATM vc-class class1

  encapsulation          -    aal5mux ip
  shape                  -    cbr 100000
  oam ais-rdi            -    35
  oam retry              -    300
  oam-pvc                -    manage 300

ATM vc-class class2

  encapsulation          -    aal5nlpid
  shape                  -    ubr 40000
```

```
  oam ais-rdi             -    30
  oam retry               -    30
  oam-pvc                 -    manage 300

ATM vc-class class3

  encapsulation           -    aal5snap
  shape                   -    vbr-nrt 60000 60000 1000
  oam ais-rdi             -    30
  oam retry               -    30
  oam-pvc                 -    manage 300
```

Table 9: show atm vc-class Field Descriptions

Field	Description
encapsulation	Type of ATM adaptation layer (AAL) encapsulation type that is enabled on the specified VC-class. Possible AAL encapsulation types follow: • **aal5mux ipv4—**IPv4 encapsulation for multiplex (MUX)-type VCs • **aal5nlpid—**AAL and encapsulation type that allows ATM interfaces to interoperate with High-Speed Serial Interfaces (HSSIs), which are using an ATM data service unit (ADSU) and running ATM-Data Exchange Interface (DXI). Supported on ATM PVCs only. • **aal5snap—**AAL and encapsulation type that supports Inverse ARP. Logical Link Control/Subnetwork Access Protocol (LLC/SNAP) precedes the protocol datagram. **Note** To modify the AAL encapsulation type on an interface, use the **encapsulation** command in ATM VC-class configuration mode.

Field	Description
shape	Displays traffic shaping information for the service class that is assigned to the specified VC-class. Possible service classes follow: • cbr—command output shows the peak output rate for the bit rate in kbps. • ubr—command output shows the peak output rate for the bit rate in kbps. • vbr-nrt—command output shows the peak output rate, sustained output rate, and burst size for the bit rate in kbps. • vbr-rt—command output shows the peak output rate, sustained output rate, and burst size for the bit rate in kbps. **Note** To modify a configured ATM service class and peak output rate for the bit rate, use the **shape** command in the appropriate command mode.
oam ais-rdi	Displays the maximum number of OAM AIS/RDI cells that can be received on a PVC before it is brought down. **Note** Use the **oam ais-rdi** command in to modify the current configuration for this field.
oam retry	Displays the following information related to F5 OAM loopback cells, if this information was configured for the specified VC-class: • Number of consecutive end-to-end F5 OAM loopback cell responses that must be received to change a connection state to up. (Retry count) • Number of consecutive unreceived end-to-end F5 OAM loopback cells allowed on a PVC before its state changes to down. (down count) • Frequency (in seconds) at which end-to-end F5 OAM loopback cells are transmitted when a change in the up or down state is being verified. (retry frequency) **Note** Use the **oam retry** command to modify the current configuration for this field. **Note** If the **oam retry** command was not use to configure the F5 OAM loopback retry count, down count, or retry frequency, then this information is not displayed in the command output for the **show atm vc-class** command.

Field	Description
oam-pvc	Frequency (in seconds) at which end-to-end F5 OAM loopback cells are transmitted on this PVC. Range is from 0 through 600. **Note** Use the **oam-pvc manage** command to modify the current configuration for this field.

The following sample output is from the **show atm vc-class** command with the *vc-class-name* argument included:

```
RP/0/0/CPU0:router# show atm vc-class class1

ATM vc-class class1

  encapsulation          -    aal5mux ip
  shape                  -    cbr 100000
  oam ais-rdi            -    35
  oam retry              -    300
  oam-pvc                -    manage 300
```

Related Commands

Command	Description
class-vc, on page 19	Attaches a VC class to an ATM PVC.
vc-class atm, on page 94	Creates a VC class for an ATM PVC or an ATM interface and enters VC-class configuration mode.

show atm vp-tunnel

To display virtual path (VP) tunnel information for the entire router or for a specific interface, use the **show atm vp-tunnel** command in EXEC mode.

show atm vp-tunnel [**interface atm** *interface-path-id*]

Syntax Description

interface atm	(Optional) ATM interface for which you want to display information.Use the *interface-path-id* argument to specify the ATM interface.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

Entering the **show atm vp-tunnel** command without specifying the *instance* argument displays ATM VP-tunnel information for the entire router.

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
atm	read

Examples

The following sample output is from the **show atm vp-tunnel** command:

```
RP/0/0/CPU0:router# show atm vp-tunnel

                                 Data       Peak    Avg/Min      Burst
Interface         VPI      SC     VCs       Kbps      Kbps      Cells    Status

ATM0/6/0/0         10     CBR       0     155000       N/A        N/A      DOWN
ATM0/6/0/0         20     CBR       0     155000       N/A        N/A      DOWN
ATM0/6/0/0         30     CBR       0     155000       N/A        N/A      DOWN
```

```
ATM0/6/0/0          40     CBR       0     155000        N/A        N/A      DOWN
ATM0/6/0/1          10 VBR_NRT       0     155000     155000        800      DOWN
ATM0/6/0/1          20 VBR_NRT       0     155000     155000        800      DOWN
```

Table 10: show atm vp-tunnel Command Field Descriptions

Field	Description
Interface	Interface type and instance. The instance is displayed in the *rack*/*slot*/*module*/*port* format.
VPI	ATM network virtual path identifier (VPI) associated with the specified interface.
SC	Service class that is assigned to the specified ATM interface. Possible service classes follow: • cbr • ubr • vbr-nrt • vbr-rt **Note** To modify a configured ATM service class, use the **shape** command in the appropriate command mode
Data VCs	Number of VCs that are attached to the specified VP tunnel.
Peak Kbps	Peak line rate (bandwidth) required for the specified ATM interface, in kilobits per second. **Note** To modify the bandwidth required for an ATM interface (peak line rate), use the **shape** command in interface configuration mode
Avg/Min Kbps	Number of kilobits per second sent at the average rate.
Burst Cells	Identifies the burst cell size in terms of number of cells. This number is the maximum number of ATM cells the VC can send at the peak rate. **Note** To modify the burst cell size, use the **shape** command.
Status	Current state for this interface. Possible states are “Up” or “Down.”

The following sample output is from the **show atm vp-tunnel** command with the **interface atm** *instance* keyword argument included:

```
RP/0/0/CPU0:router# show atm vp-tunnel interface atm 0/6/0/1

Data       Peak    Avg/Min      Burst
Interface         VPI      SC     VCs       Kbps      Kbps       Cells    Status

ATM0/6/0/1         10 VBR_NRT       0     155000     155000         800      DOWN
ATM0/6/0/1         20 VBR_NRT       0     155000     155000         800      DOWN
```

Table 10: show atm vp-tunnel Command Field Descriptions, on page 86 describes the significant fields shown in the display.

Related Commands

Command	Description
vp-tunnel, on page 96	Configures a VP tunnel on an interface and enters ATM VP-tunnel configuration mode.

show controllers atm

To display information about the physical status of the ATM interface, use the **show controllers atm** command in EXEC mode.

show controllers atm *interface-path-id* [**all**| **traffic** {**f4oam**| **port**| **vc** *vpi*/*vci* | **vp** *vpi*}]

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
f4oam	Displays information about the ATM layer f4oam traffic that is transmitted and received on the specified interface.
port	(Optional) Displays information about the ATM layer traffic that is transmitted and received by the ports associated with the specified interface.
vc *vpi*/*vci*	(Optional) Displays information about the ATM layer traffic carried by specific ATM VC (virtual channel). Replace *vpi*/*vci* with the ATM virtual path identifier (VPI) and virtual channel identifier (VCI) of the VC whose information you want to display.
vp *vpi*	(Optional) Displays information about the ATM layer traffic carried by specific ATM virtual path. Replace *vpi* with the ATM virtual path identifier (VPI) whose information you want to display.

Command Default

Entering the **show controllers atm** command without specifying the *instance* argument displays ATM controller status and configuration information for the entire router.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
interface	read

Examples

The following example shows partial output from the **show controllers atm** command:

```
RP/0/0/CPU0:router# show controllers atm 0/6/0/0

SAR Counters:
  tx_packets            :4085                 tx_bytes             :212420

  tx_total_resource_errs:0                    tx_total_other_errs  :0

  tx_wred_thresh_drops  :0                    tx_wred_random_drops :0

  rx_packets            :0                    rx_bytes             :0

  rx_total_resource_errs:0                    rx_total_other_errs  :0

  rx_buffer_exhaust_errs:0                    rx_CRC32_errors      :0

  rx_packet_abort_errs  :0                    rx_trailer_len_errs  :0

  rx_mps_errors         :0                    rx_reassembly_timeout:0

The following are per-SAR counters:
Reassembly SAR:
  sys_rx_unopen_vc_cls  :0                    sys_tx_unopen_vc_cls :0

  sys_ecc_errors        :0                    sys_ecc_and_addr     :         0xf
fffffff
  sys_ecc_or_addr       :         0x0
Segmentation SAR:
  sys_rx_unopen_vc_cls  :0                    sys_tx_unopen_vc_cls:0

  sys_ecc_errors        :0                    sys_ecc_and_addr     :         0xf
fffffff
  sys_ecc_or_addr       :         0x0
RSAR 0: (6.0.2.1c)
RSAR Build ID= E7EE
SSAR 0: (6.0.2.1c)
SSAR Build ID= 570

--More--
```

Table 11: show controllers atm Field Descriptions

Field	Description
SAR Counters	Counters that provide information about the Segmentation and Reassembly (SAR) chip.
tx_packets	Number of AAL5 packets transmitted.
tx_bytes	A 64-bit counter of the bytes transmitted on this interface, including OAM cells and AAL5 header encapsulations (such as AAL5SNAP). This should be approximately the total number of bytes transmitted on each of the VCs.

Field	Description
tx_total_resource_errs	Total number of packets that were not transmitted because of any resource exhaustion error. This does not necessarily imply an error, because this counter includes tx_wred_thresh_drops and tx_wred_random_drops, as well as packet drops due to complete buffer exhaustion on the SAR. This should be equal to the sum of the number of resource errors that occur on all the VCs.
tx_total_other_errs	Total number of packets that were not transmitted because of any error other than resource exhaustion, but not including no-vc drops. This includes malformed packets, CRC errors, and so on. This should be approximately the total number of tx_other_errors that occur on all the VCs on this interface.
tx_wred_thresh_drops	Total number of WRED maximum threshold drops on this interface. This counter is included in the tx_total_resource_errs counter.
tx_wred_random_drops	Total number of WRED random drops on this interface. This counter is included in the tx_total_resource_errs counter.
rx_packets	Total number of packets reassembled on this interface by the SAR, including OAM cells.
rx_bytes	Number of AAL5 packets received on this interface.
rx_total_resource_errs	Total number of packet reassemblies that failed due to resource exhaustion. This error should not occur if the queue thresholds are not oversubscribed. This error includes rx_buffer_exhaust_errs.
rx_total_other_errs	Total number of packet reassemblIes that failed due to errors besides resource exhaustion (not including “no-vc” cells), including rx_crc32_errors, rx_packet_abort_errs, rx_trailer_len_errs, rx_mps_errors, and rx_reassembly_timeout.
rx_buffer_exhaust_errs	Total number of packet reassemblies that failed due to complete buffer exhaustion on the SAR. This error should not occur if the queue thresholds are not oversubscribed. This is included in rx_total_resource_errs.

Field	Description
sys_tx_unopen_vc_cls	Total number of packets transmitted by this endpoint that failed due to an error other than those listed in the show controllers atm command output.
Reassembly SAR	Counters that provide information specific to the reassembly chip.
sys_ecc_and_addr	Total number of single bit end and addressing errors detected on the reassembly SAR.
sys_ecc_errors	Total number of single bit errors detected on the reassembly SAR.
sys_ecc_or_addr	Total number of single bit end or addressing errors detected on the reassembly SAR.
Segmentation SAR	Counters that provide information specific to the segmentation chip.
sys_tx_unopen_vc_cls	Total number of packet reassemblies transmitted by this endpoint that failed due to errors other than those listed in the show controllers atm command output.
sys_rx_unopen_vc_cls	Total number of packet reassemblies received by this endpoint that failed due to errors other than those listed in the show controllers atm command output.
rx_CRC32_errors	Total number of packet reassemblies that failed due to an invalid AAL5 CRC32 trailer. This is included in rx_total_other_errs.
rx_packet_abort_errs	Total number of packet reassemblies that failed due to receiving a trailer length of 0. This is included in rx_total_other_errs.
rx_trailer_len_errs	Total number of packet reassemblies that failed due to a packet whose AAL5 trailer had an invalid trailer length. This is included in rx_total_other_errs.
rx_mps_errors	Total number of packet reassemblies that failed due to a packet size greater than the maximum allowed packet size. This is included in rx_total_other_errs.
rx_reassembly_timeout	Total number of packet reassemblies that failed due to timing out before receiving the last cell of a packet. This is included in rx_total_other_errs.
sys_rx_unopen_vc_cls	Packets received on nonexistent VC.

Field	Description
RSAR 0	RSAR ID.
RSAR Build ID	Unique number that identifies the RSAR build.
SSAR 0	SSAR ID.
SSAR Build ID	Unique number that identifies the SAR build.

Related Commands

Command	Description
show atm interface atm, on page 60	Displays ATM-specific information about an ATM interface.

shutdown (ATM)

To disable an ATM interface, use the **shutdown** command in interface configuration mode. To re-enable an ATM interface, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no keywords or arguments.

Command Default

The ATM interface is up.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

Use the **show interface atm** command in EXEC mode to verify that the ATM interface is administratively up or down.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to bring down an ATM interface:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/2/0/0
RP/0/0/CPU0:router(config-if)# shutdown
```

The following example shows how to re-enable an ATM interface that has been brought down with the **shutdown** command:

```
RP/0/0/CPU0:router# no shutdown
```

Related Commands

Command	Description
show atm interface atm, on page 60	Displays ATM-specific information about an ATM interface.

vc-class atm

To create a virtual circuit (VC) class for an ATM permanent virtual circuit (PVC) or an ATM interface and enter VC-class configuration mode, use the **vc-class atm** command in global configuration mode. To remove a VC-class, use the **no** form of this command.

vc-class atm *name*

no vc-class atm *name*

Syntax Description

name	Name of your VC class.

Command Default

No VC-class is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

When you issue the **vc-class atm** command in global configuration mode, the CLI prompt changes to "config-vc-class-atm," indicating that you have entered the VC-class configuration submode. In the following sample output, the question mark (**?**) online help function displays all the commands available under the VC-class configuration submode:

```
RP/0/0/CPU0:router(config)# vc-class atm classA
RP/0/0/CPU0:router(config-vc-class-atm)# ?

  commit         Commit the configuration changes to running
  describe       Describe a command without taking real actions
  do             Run an exec command
  encapsulation  Configure encapsulation
  exit           Exit from this submode
  no             Negate a command or set its defaults
  oam            Configure OAM parameters
  oam-pvc        OAM PVC management configuration
  shape          ATM Traffic Shaping
  show           Show contents of configuration

RP/0/0/CPU0:router(config-vc-class-atm)#
```

Task ID

Task ID	Operations
atm	read, write

Examples

The following example shows how to create a VC-class. In this example, the class is called “class1.”

```
RP/0/0/CPU0:router(config)# vc-class atm class1
RP/0/0/CPU0:router(config-vc-class-atm)#
```

Related Commands

Command	Description
class-vc, on page 19	Attaches a VC class to an ATM PVC.
show atm vc-class, on page 81	Displays information about all ATM VC classes on the router or for a specific ATM VC-class.

vp-tunnel

To configure a virtual path (VP) tunnel on an interface and enter ATM VP-tunnel configuration mode, use the **vp-tunnel** command in interface configuration mode.

vp-tunnel *vpi*

Syntax Description

vpi	VPI for this tunnel. Range is from 0 through 4095.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

For Vp-tunnels, a VPI of 0 is not supported on the following line cards:

- 4-port OC12
- 4-port OC3

When you issue the **vp-tunnel** command in global configuration mode, the CLI prompt changes to "config-atm-vp-tunnel," indicating that you have entered ATM VP-tunnel configuration submode. In the following sample output, the question mark (**?**) online help function displays all the commands available under the ATM VP-tunnel configuration submode:

```
RP/0/0/CPU0:router(config-if)# vp-tunnel 10
RP/0/0/CPU0:router(config-atm-vp-tunnel)# ?

  commit    Commit the configuration changes to running
  describe  Describe a command without taking real actions
  do        Run an exec command
  exit      Exit from this submode
  f4oam     F4 OAM configuration
  no        Negate a command or set its defaults
  shape     ATM Traffic Shaping
  show      Show contents of configuration

RP/0/0/CPU0:router(config-atm-vp-tunnel)#
```

Task ID

Task ID	Operations
atm	read, write

Examples

The following example shows how to configure a virtual path (VP) tunnel on an interface and enter ATM VP-tunnel configuration mode:

```
RP/0/0/CPU0:router(config-if)# vp-tunnel 10
RP/0/0/CPU0:router(config-atm-vp-tunnel)#
```

Related Commands

Command	Description
show atm vp-tunnel, on page 85	Displays VP tunnel information for the entire router or for a specific interface.

Ethernet Interface Commands on the Cisco IOS XR Software

This module provides command line interface (CLI) commands for configuring Ethernet interfaces on the Cisco XR 12000 Series Router.

carrier-delay

To delay the processing of hardware link down notifications, use the **carrier-delay** command in interface configuration mode.

carrier-delay {**down** *milliseconds* [**up** *milliseconds*]| **up** *milliseconds* [**down** *milliseconds*]}

Syntax Description

down *milliseconds*	Length of time, in milliseconds, to delay the processing of hardware link down notifications. Range is from 0 through 65535.
up *milliseconds*	Length of time, in milliseconds, to delay the processing of hardware link up notifications. Range is from 0 through 65535.

Command Default

No carrier-delay is used, and the upper layer protocols are notified as quickly as possible when a physical link goes down.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.4.0	The **msec** keyword was replaced by the **down** keyword, and the value of the *milliseconds* argument was increased to 0 through 65535. The **up** keyword was added, and the value of the *milliseconds* argument was set at 0 through 65535.

Usage Guidelines

When you delay the processing of hardware link down notifications, the higher layer routing protocols are unaware of a link until that link is stable.

If the **carrier-delay down** *milliseconds* command is configured on a physical link that fails and cannot be recovered, link down detection is increased, and it may take longer for the routing protocols to re-route traffic around the failed link.

In the case of very small interface state flaps, running the **carrier-delay down** *milliseconds* command prevents the routing protocols from experiencing a route flap.

Note Enter the **show interface** command to see the current state of the carrier-delay operation for an interface. No carrier-delay information is displayed if carrier-delay has not been configured on an interface.

Task ID

Task ID	Operations
interface	read, write

Examples

This example shows how to delay the processing of hardware link down notifications:

```
RP/0/0/CPU0:router(config-if)# carrier-delay down 10
```

The following example shows how to delay the processing of hardware link up and down notifications:

```
RP/0/0/CPU0:router(config-if)# carrier-delay up 100 down 100
```

Related Commands

Command	Description
dampening, on page 412	Turns on event dampening.

clear mac-accounting (Ethernet)

To clear Media Access Control (MAC) accounting statistics, use the **clear mac-accounting** command in EXEC mode.

clear mac-accounting {**GigabitEthernet**| **TenGigE**| **FastEthernet**} *interface-path-id* [**location** *node-id*]

Syntax Description

{**GigabitEthernet** | **TenGigE** | **FastEthernet**}	Type of Ethernet interface whose MAC accounting statistics you want to clear. Enter **GigabitEthernet**, **TenGigE** , or **FastEthernet**.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location *node-id*	(Optional) Clears MAC accounting statistics for the designated node. The *node-id* argument is entered in the *rack*/*slot*/*module* notation.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
interface	read, write
basic-services	read, write

Examples

This example shows how to clear all MAC accounting statistics for the TenGigE port at 1/0/0/1:

```
RP/0/0/CPU0:router# clear mac-accounting TenGigE 0/1/5/0 location 1/0/0/1
```

Related Commands

Command	Description
mac-accounting, on page 114	Generates accounting information for IP traffic based on the source and destination MAC addresses on LAN interfaces.
show mac-accounting (Ethernet), on page 120	Displays MAC accounting statistics for an interface.

duplex full (Fast Ethernet)

To configure full-duplex operation on a Fast Ethernet interface, use the **duplex full** command in interface configuration mode. To return the system to the default duplex operation, use the **no** form of the **duplex full** command.

duplex full

no duplex full

Syntax Description

This command has no keywords or arguments.

Command Default

If autonegotiation is disabled on an interface, then the default duplex operation is full duplex.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

The **duplex full** command automatically replaces the **duplex half** command if half duplex was previously configured on your router.

Note The **duplex full** command and the **duplex half** command cannot be configured simultaneously.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to set the Fast Ethernet interface at full duplex:

```
RP/0/RP0/CPU0:router(config)# interface FastEthernet 0/2/0/0
RP/0/RP0/CPU0:router(config-if)# duplex full
```

Related Commands

Command	Description
duplex half (Fast Ethernet), on page 106	Configures half-duplex operation on a Fast Ethernet interface.

Command	Description
negotiation auto	Enables link autonegotiation on Ethernet interfaces.
show interfaces, on page 423	Displays statistics for all interfaces configured on the router or for a specific node.
speed (Fast Ethernet), on page 122	Configures the speed for a Fast Ethernet interface.

duplex half (Fast Ethernet)

To configure half-duplex operation on a Fast Ethernet interface, use the **duplex half** command in interface configuration mode. To return the system to the default duplex operation, use the **no** form of the **duplex half** command.

duplex half

no duplex half

Syntax Description

This command has no keywords or arguments.

Command Default

If autonegotiation is disabled on an interface, then the default duplex operation is full duplex.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

The **duplex half** command automatically replaces the **duplex full** command if full duplex was previously configured on your router.

Note The **duplex half** command and the **duplex full** command cannot be configured simultaneously.

Task ID

Task ID	Operations
interface	read, write

Examples

The following examples shows how to set the Fast Ethernet interface at half duplex:

```
RP/0/RP0/CPU0:router(config)# interface mgmteth 0/RP0/CPU0/0
RP/0/RP0/CPU0:router(config-if)# duplex half
```

Related Commands

Command	Description
duplex full (Fast Ethernet), on page 104	

Command	Description
negotiation auto	Enables link autonegotiation on Ethernet interfaces.
show interfaces, on page 423	Displays statistics for all interfaces configured on the router or for a specific node.
speed (Fast Ethernet), on page 122	Configures the speed for a Fast Ethernet interface.

flow-control

To enable the sending of flow-control pause frames, use the **flow-control** command in interface configuration mode. To disable flow control, use the **no** form of this command.

flow-control {**bidirectional**| **egress**| **ingress**}

no flow-control ingress {**bidirectional**| **egress**| **ingress**}

Syntax Description

bidirectional	Enables flow-control for egress and ingress direction.
egress	Pauses egress traffic if IEEE 802.3x PAUSE frames are received.
ingress	Sends IEEE 802.3x PAUSE frames in case of congestion with ingress traffic.

Command Default

If autonegotiate is enabled on the interface, then the default is negotiated.

If autonegotiate is disabled on the interface, then the sending of flow-control pause frames is disabled for both egress and ingress traffic.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelin

Note When you explicitly enable the sending of flow-control pause frames, the value you configured with the **flow-control** command overrides any autonegotiated value. This prevents a link from coming up if the value you set with the **flow-control** command conflicts with the allowable settings on the other end of the connection.

Note The **flow-control** command is supported on Gigabit Ethernet, TenGigE, and FastEthernet interfaces only; the **flow-control** command is not supported on Management Ethernet Interfaces.

Note The **flow-control** command syntax options may vary, depending on the type of PLIM or SPA that is installed in your router.

Task ID

Task ID	Operations
interface	read, write

Examples

This example shows how to enable the sending of flow-control pause frames for ingress traffic on the TenGigE interface 0/3/0/0:

```
RP/0/0/CPU0:router(config)# interface TenGigE 0/3/0/0
RP/0/0/CPU0:router(config-if)# flow-control ingress
```

Related Commands

Command	Description
show interfaces, on page 423	Displays statistics for all interfaces configured on the router or for a specific node.

interface (Ethernet)

To specify or create an Ethernet interface and enter interface configuration mode, use the **interface (Ethernet)** command in global configuration mode.

interface {**FastEthernet| GigabitEthernet| TenGigE**} *interface-path-id*

no interface {**FastEthernet| GigabitEthernet| TenGigE**} *interface-path-id*

Syntax Description

FastEthernet	Specifies or creates a Fast Ethernet (100 Mbps) interface.
GigabitEthernet	Specifies or creates a Gigabit Ethernet (1000 Mbps) interface.
TenGigE	Specifies or creates a Ten Gigabit Ethernet (10 Gbps) interface.
interface-path-id	Physical interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	This command was modified. The **FastEthernet** keyword was added.

Usage Guidelines

To specify a physical interface, the notation for the *interface-path-id* is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:

- *rack*: Chassis number of the rack.
- *slot*: Physical slot number of the line card.
- *module*: Module number. A physical layer interface module (PLIM) is always 0.
- *port*: Physical port number of the interface.

Task ID

Task ID	Operation
interface	read, write

Examples

This example shows how to enter interface configuration mode for a Ten Gigabit Ethernet interface:

```
RP/0/0/CPU0:router(config)# interface TenGigE 0/4/0/0
RP/0/0/CPU0:router(config-if)#
```

Related Commands

Command	Description
show interfaces, on page 423	Displays statistics for all interfaces configured on the router or for a specific node.

loopback (Ethernet)

To configure an Ethernet controller for loopback mode, use the **loopback** command in interface configuration mode. To disable loopback, use the **no** form of this command.

loopback {**external**| **internal**| **line**}

no loopback

Syntax Description

external	All IPv4 self-ping packets are sent out of the interface and looped back externally before being received on the ingress path.
internal	All packets are looped back internally within the router before reaching an external cable.
line	Incoming network packets are looped back through the external cable.

Command Default

Loopback mode is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

The **loopback** command is available for all Ethernet interface types (Gigabit Ethernet, 10-Gigabit Ethernet, and Fast Ethernet).

Two loopback operation modes are supported for diagnostic purposes: internal and line. In the terminal (internal) loopback, the sent signal is looped back to the receiver. In the facility (line) loopback, the signal received from the far end is looped back and sent on the line. The two loopback modes cannot be active at the same time. In normal operation mode, neither of the two loopback modes is enabled.

Tip Use the **loopback external** command when an external loopback connector is attached to the interface.

Task ID

Task ID	Operations
interface	read, write

Examples

In the following example, all packets are looped back to the TenGigE controller:

```
RP/0/0/CPU0:router(config)# interface TenGigE 0/3/0/0
RP/0/0/CPU0:router(config-if)# loopback internal
```

mac-accounting

To generate accounting information for IP traffic based on the source and destination Media Access Control (MAC) addresses on LAN interfaces, use the **mac-accounting** command in interface configuration mode. To disable MAC accounting, use the **no** form of this command.

mac-accounting {**egress**| **ingress**}

no mac-accounting {**egress**| **ingress**}

Syntax Description

egress	Generates accounting information for IP traffic based on the destination MAC addresses (egress direction).
ingress	Generates accounting information for IP traffic based on the source MAC addresses (ingress direction).

Command Default

MAC accounting is disabled

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

The **mac-accounting** command calculates the total packet and byte counts for a LAN interface that receives or sends IPv4 packets to or from a unique MAC address.

Task ID

Task ID	Operations
interface	read, write

Examples

This example shows how to enable MAC accounting for the source MAC address on the ingress direction:

```
RP/0/0/CPU0:routerconfigure
RP/0/0/CPU0:routerinterface bundle-ether <bundle-id>
RP/0/0/CPU0:router(config-if)# mac-accounting ingress
```

This example shows how to enable MAC accounting for the source MAC address on the egress direction:

```
RP/0/0/CPU0:routerconfigure
```

```
RP/0/0/CPU0:routerinterface bundle-ether <bundle-id>
RP/0/0/CPU0:router(config-if)# mac-accounting egress
```

Note In order to view the mac-accounting statistics for the configured bundle interface, use the **show mac-accounting bundle-ether <bundle id>** command.

Related Commands

Command	Description
clear mac-accounting (Ethernet), on page 102	Clears MAC accounting statistics for an interface.
show mac-accounting (Ethernet), on page 120	Displays MAC accounting statistics for an interface.

mac-address (Ethernet)

To set the MAC layer address of an Ethernet interface, use the **mac-address** command in interface configuration mode. To return the device to its default MAC address, use the **no** form of this command.

mac-address *value1***.***value2***.***value3*

no mac-address

Syntax Description

*value1***.**	High 2 bytes of the MAC address in hexadecimal format. Range is from 0 to ffff.
*value2***.**	Middle 2 bytes of the MAC address in hexadecimal. Range is from 0 to ffff.
value3	Low 2 bytes of the MAC address in hexadecimal. Range is from 0 to ffff.

Command Default

The default MAC address is read from the hardware burned-in address (BIA).

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

The MAC address must be in the form of three 4-digit values (12 digits in dotted decimal notation).

The **mac-address** command is available for all types of line card Ethernet interfaces (Gigabit Ethernet, 10-Gigabit Ethernet, Fast Ethernet) and for the Management Ethernet interface.

Task ID

Task ID	Operations
interface	read, write

Examples

This example shows how to set the MAC address of a Ten Gigabit Ethernet interface located at 0/3/0/0:

```
RP/0/0/CPU0:router(config)# interface TenGigE 0/1/0/0
RP/0/0/CPU0:router(config-if)# mac-address 0001.2468.ABCD
```

packet-gap non-standard

To change the packet interval for traffic on an interface for improved interoperability with Cisco Catalyst 6000 series switches, use the **packet-gap non-standard** command in interface configuration mode. To use the standard packet interval as defined by the IEEE 802.ae specification, use the **no** form of this command.

packet-gap non-standard

no packet-gap non-standard

Syntax Description

This command has no keywords or arguments.

Command Default

The interface uses the standard packet interval as defined by the IEEE 802.ae specification.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

An interface that is connected to a Cisco Catalyst 6000 series switch may experience packet loss problems that can be resolved by changing the packet interval of traffic from standard (as defined by the IEEE 802.ae specification) to nonstandard using the **packet-gap non-standard** command.

Note The **packet-gap non-standard** command is available on 10-Gigabit Ethernet interfaces only.

Task ID

Task ID	Operations
interface	read, write

Examples

This example shows how to change the packet interval for traffic on an interface from standard to nonstandard:

```
RP/0/0/CPU0:router(config)# interface TenGigE 0/3/0/0
RP/0/0/CPU0:router(config-if)# packet-gap non-standard
```

show controllers (Ethernet)

To display status and configuration information about the Ethernet interfaces on a specific node, use the **show controllers command** in EXEC mode.

show controllers {**FastEthernet**| **GigabitEthernet**| **TenGigE**} *interface-path-id* [**all**| **bert**| **internal**| **mac**| **phy**| **stats**| **xgxs**]

Syntax Description

{**FastEthernet** | **GigabitEthernet** | **TenGigE**}	Specifies the type of Ethernet interface whose status and configuration information you want to display. Enter FastEthernet, GigabitEthernet, or TenGigE.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
all	Displays detailed information for the specified interface.
bert	Displays BERT status information for the interface.
internal	Displays internal information for the interface.
mac	Displays mac information for the interface.
phy	Displays physical information for the interface.
stats	Displays statistical information for the interface.
xgxs	Displays information about the 10 Gigabit Ethernet Extended Sublayer (XGXS).

Command Default

No default behavior or values

Command Modes

EXEC (#)

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.5.0	This command was modified. The **GigabitEthernet** and **TenGigE** keywords were added.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.
- If specifying a virtual interface, the number range varies, depending on interface type.

Task ID

Task ID	Operations
cisco-support	read **Note** Required in addition to the interface (read) task ID to use the **control** keyword only.
dwdm	read
interface	read
sonet-sdh	read

show mac-accounting (Ethernet)

To display MAC accounting statistics for an interface, use the **show mac-accounting** command in EXEC mode.

show mac-accounting {**GigabitEthernet| TenGigE| FastEthernet**} *interface-path-id* [**location node-id**]

Syntax Description

{**GigabitEthernet** | **TenGigEHundred GigEbundle-ether** | **FastEthernet**}	Indicates the type of Ethernet interface whose MAC accounting statistics you want to display. Enter **GigabitEthernet**, **TenGigE** , **FastEthernet**, .
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location *node-id*	(Optional) Displays detailed MAC accounting information for the specified interface on the specified node. The *node-id* argument is entered in the *rack*/*slot*/*module*/*port* notation.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use these guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

Task ID

Task ID	Operations
interface	read

Examples

These examples show the outputs from the **show mac-accounting** command, which displays MAC accounting statistics on any specified interface:

```
RP/0/0/CPU0:router# show mac-accounting TenGigE 0/2/0/4 location 0/1/CPU0

TenGigE0/2/0/4
  Input (511 free)
000b.4558.caca: 4 packets, 456 bytes
             Total: 4 packets, 456 bytes
```

Table 12: show mac-accounting Field Descriptions

Field	Description
Interface	The interface from which the statistics are generated.
Input	Heading for the ingress MAC accounting statistics. The number of MAC accounting entries still available is shown in parentheses.
Total	Total statistics for the traffic accounted for by MAC accounting. This excludes any traffic for which there is no MAC address entry, such as non-IP traffic from an unknown MAC source address. This output also excludes any MAC addresses that have 0 packets currently, even if that MAC address was accounted before. Such type of MAC addresses still contribute towards the maximum address limit.

Related Commands

Command	Description
clear mac-accounting (Ethernet), on page 102	Clears MAC accounting statistics for an interface.
mac-accounting, on page 114	Generates accounting information for IP traffic based on the source and destination MAC addresses on LAN interfaces.

speed (Fast Ethernet)

To configure the speed for a Fast Ethernet interface, enter the **speed** command in interface configuration mode. To return the system to autonegotiate speed, use the **no** form of this command.

speed {**10**| **100**| **1000**}

no speed

Syntax Description

10	Configures the interface to transmit at 10 Mbps.
100	Configures the interface to transmit at 100 Mbps.
1000	Configures the interface to transmit at 1000 Mbps (1 Gbps).

Command Default

If autonegotiation is enabled on an interface, the default speed is negotiated.

If autonegotiation is disabled on an interface, the default speed is the maximum speed allowed on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelin

Note The **speed** command is available on Management Ethernet interfaces and Fast Ethernet interfaces only.

Note Keep in mind that both ends of a link must have the same interface speed. A manually configured interface speed overides any autonegotiated speed, which can prevent a link from coming up if the configured interface speed at one end of a link is different from the interface speed on the other end.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure the Fast Ethernet interface to transmit at one gigabit:

```
RP/0/0/CPU0:router(config)# interface FastEthernet 0/0/2/0
RP/0/0/CPU0:router(config-if)# speed 1000
```

Ethernet OAM Commands on the Cisco IOS XR Software

This module provides command line interface (CLI) commands for configuring Ethernet Operations, Administration, and Maintenance (EOAM) on the Cisco XR 12000 Series Router.

action capabilities-conflict

To configure what action is taken on an interface when a capabilities-conflict event occurs, use the **action capabilities-conflict** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of this command.

action capabilities-conflict {**disable**| **efd** | **error-disable-interface**| **log**}

no action capabilities-conflict {**disable**| **efd** | **error-disable-interface**| **log**}

Syntax Description

disable	Performs no action on the interface when a capabilities-conflict event occurs.
efd	Puts the line protocol into the down state for an interface when a capabilities-conflict event occurs. The state is removed when the first packet is received without a conflict.
error-disable-interface	Puts the interface into the error-disable state when a capabilities-conflict event occurs.
log	(Interface Ethernet OAM configuration only) Creates a syslog entry when a capabilities-conflict event occurs. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 4.0.0	This command was introduced.
Release 4.1.0	The **efd** keyword was added.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure that no action is performed on the interface when a capabilities-conflict event occurs.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# action capabilities-conflict disable
```

The following example shows how to configure putting the interface into the line-protocol-down state when a capabilities-conflict event occurs.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# action capabilities-conflict efd
```

The following example shows how to configure that the interface is put into the error-disable state when a capabilities-conflict event occurs.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# action capabilities-conflict error-disable-interface
```

The following example shows how to configure that a syslog entry is created when a capabilities-conflict event occurs. This configuration overrides the interface Ethernet OAM profile.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/0/CPU0:router(config-if)# ethernet oam
RP/0/0/CPU0:router(config-if-eoam)# action capabilities-conflict log
```

Related Commands

Command	Description
ethernet oam profile, on page 199	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 198	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 257	Attaches an Ethernet OAM profile to an interface.

action critical-event

To configure what action is taken on an interface when a critical-event notification is received from the remote Ethernet OAM peer, use the **action critical-event** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of this command.

action critical-event {**disable**| **error-disable-interface**| **log**}

no action critical-event {**disable**| **error-disable-interface**| **log**}

Syntax Description

disable	Performs no action on the interface when a critical-event notification is received.
error-disable-interface	Puts the interface into the error-disable state when a critical-event notification is received.
log	(Interface Ethernet OAM configuration only) Creates a syslog entry when a critical-event notification is received. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure that no action is performed on the interface when a critical-event notification is received.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
```

```
RP/0/0/CPU0:router(config-eoam)# action critical-event disable
```

The following example shows how to configure that the interface is put into the error-disable state when a critical-event notification is received.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# action critical-event error-disable-interface
```

The following example shows how to configure that a syslog entry is created when a critical-event notification is received. This configuration overrides the interface Ethernet OAM profile.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/0/CPU0:router(config-if)# ethernet oam
RP/0/0/CPU0:router(config-if-eoam)# action critical-event log
```

Related Commands

Command	Description
ethernet oam profile, on page 199	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 198	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 257	Attaches an Ethernet OAM profile to an interface.

action discovery-timeout

To configure what action is taken on an interface when a connection timeout occurs, use the **action discovery-timeout** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of this command.

action discovery-timeout {**disable**| **efd error-disable-interface**| **log**}

no action discovery-timeout {**disable**| **efd error-disable-interface**| **log**}

Syntax Description

disable	Performs no action on the interface when a connection timeout occurs.
efd	Puts the line protocol into the down state for an interface when a connection timeout occurs. The state is removed when the session is re-established.
error-disable-interface	Puts the interface into the error-disable state when a connection timeout occurs.
log	(Interface Ethernet OAM configuration only) Creates a syslog entry when a connection timeout occurs. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 4.0.0	This command was introduced.
Release 4.1.0	The **efd** keyword was added.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure that no action is performed on the interface when a connection timeout occurs.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# action discovery-timeout disable
```

The following example shows how to configure putting the interface into the line-protocol-down state when a connection timeout occurs.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# action discovery-timeout efd
```

The following example shows how to configure that the interface is put into the error-disable state when a connection timeout occurs.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# action discovery-timeout error-disable-interface
```

The following example shows how to configure that a syslog entry is created when a connection timeout occurs. This configuration overrides the interface Ethernet OAM profile.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/0/CPU0:router(config-if)# ethernet oam
RP/0/0/CPU0:router(config-if-eoam)# action discovery-timeout log
```

Related Commands

Command	Description
ethernet oam profile, on page 199	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 198	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 257	Attaches an Ethernet OAM profile to an interface.

action dying-gasp

To configure what action is taken on an interface when a dying-gasp notification is received from the remote Ethernet OAM peer, use the **action dying-gasp** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of this command.

action dying-gasp {**disable| error-disable-interface| log**}

no action dying-gasp {**disable| error-disable-interface| log**}

Syntax Description

disable	Performs no action on the interface when a dying-gasp notification is received.
error-disable-interface	Puts the interface into the error-disable state when a dying-gasp notification is received.
log	(Interface Ethernet OAM configuration only) Creates a syslog entry when a dying-gasp notification is received. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure that no action is performed on the interface when a dying-gasp notification is received.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
```

```
RP/0/0/CPU0:router(config-eoam)# action dying-gasp disable
```

The following example shows how to configure that the interface is put into the error-disable state when a dying-gasp notification is received.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# action dying-gasp error-disable-interface
```

The following example shows how to configure that a syslog entry is created when a dying-gasp notification is received. This configuration overrides the interface Ethernet OAM profile.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/0/CPU0:router(config-if)# ethernet oam
RP/0/0/CPU0:router(config-if-eoam)# action dying-gasp log
```

Related Commands

Command	Description
ethernet oam profile, on page 199	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 198	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 257	Attaches an Ethernet OAM profile to an interface.

action high-threshold

To configure what action is taken on an interface when a high threshold is exceeded, use the **action high-threshold** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of this command.

action high-threshold {**disable| error-disable-interface| log**}

no action high-threshold {**disable| error-disable-interface| log**}

Syntax Description

disable	(Interface Ethernet OAM configuration only) Performs no action on the interface when a high threshold is exceeded.
error-disable-interface	Puts the interface into the error-disable state when a high threshold is exceeded.
log	Creates a syslog entry when a high threshold is exceeded. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.

Command Default

The default is that no action is taken when a high threshold is exceeded.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure that a syslog entry is created on the interface when a high threshold is exceeded.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
```

```
RP/0/0/CPU0:router(config-eoam)# action high-threshold log
```

The following example shows how to configure that the interface is put into the error-disable state when a high threshold is exceeded.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# action high-threshold error-disable-interface
```

The following example shows how to configure that no action is taken when a high threshold is exceeded. This configuration overrides the Ethernet OAM profile configuration.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/0/CPU0:router(config-if)# ethernet oam
RP/0/0/CPU0:router(config-if-eoam)# action high-threshold disable
```

Related Commands

Command	Description
ethernet oam profile, on page 199	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 198	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 257	Attaches an Ethernet OAM profile to an interface.

action remote-loopback

To configure what action is taken on an interface when a remote-loopback event occurs, use the **action remote-loopback** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of this command.

action remote-loopback {**disable**| **log**}

no action remote-loopback {**disable**| **log**}

Syntax Description

disable	Performs no action on the interface when a remote-loopback event occurs.
log	(Interface Ethernet OAM configuration only) Creates a syslog entry when a remote-loopback event occurs. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure that no action is performed on the interface when a remote-loopback event occurs.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# action remote-loopback disable
```

The following example shows how to configure that a syslog entry is created when a remote-loopback event occurs. This configuration overrides the interface Ethernet OAM profile.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/0/CPU0:router(config-if)# ethernet oam
RP/0/0/CPU0:router(config-if-eoam)# action remote-loopback log
```

Related Commands

Command	Description
ethernet oam profile, on page 199	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 198	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 257	Attaches an Ethernet OAM profile to an interface.

action session-down

To configure what action is taken on an interface when an Ethernet OAM session goes down, use the **action session-down** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of this command.

action session-down {**disable**| **efd** | **error-disable-interface**| **log**}

no action session-down {**disable**| **efd** | **error-disable-interface**| **log**}

Syntax Description

disable	Performs no action on the interface when a capabilities-conflict event occurs.
efd	Puts the line protocol into the down state for an interface when a capabilities-conflict event occurs. The state is removed when the first packet is received without a conflict.
error-disable-interface	Puts the interface into the error-disable state when a capabilities-conflict event occurs.
log	(Interface Ethernet OAM configuration only) Creates a syslog entry when a capabilities-conflict event occurs. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 4.0.0	This command was introduced.
Release 4.1.0	The **efd** keyword was added.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure that no action is performed on the interface when an Ethernet OAM session goes down.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# action session-down disable
```

The following example shows how to configure putting the interface into the line-protocol-down state when an Ethernet OAM session goes down.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# action session-down efd
```

The following example shows how to configure that the interface is put into the error-disable state when an Ethernet OAM session goes down.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# action session-down error-disable-interface
```

The following example shows how to configure that a syslog entry is created when an Ethernet OAM session goes down. This configuration overrides the interface Ethernet OAM profile.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/0/CPU0:router(config-if)# ethernet oam
RP/0/0/CPU0:router(config-if-eoam)# action session-down log
```

Related Commands

Command	Description
ethernet oam profile, on page 199	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 198	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 257	Attaches an Ethernet OAM profile to an interface.

action session-up

To configure what action is taken on an interface when an Ethernet OAM session is established, use the **action session-up** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of this command.

action session-up {**disable**| **log**}

no action session-up {**disable**| **log**}

Syntax Description

disable	Performs no action on the interface when an Ethernet OAM session is established.
log	(Interface Ethernet OAM configuration only) Creates a syslog entry when an Ethernet OAM session is established. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure that no action is performed on the interface when an Ethernet OAM session is established.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# action session-up disable
```

The following example shows how to configure that a syslog entry is created when an Ethernet OAM session is established. This configuration overrides the interface Ethernet OAM profile.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/0/CPU0:router(config-if)# ethernet oam
RP/0/0/CPU0:router(config-if-eoam)# action session-up log
```

Related Commands

Command	Description
ethernet oam profile, on page 199	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 198	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 257	Attaches an Ethernet OAM profile to an interface.

action uni-directional link-fault

To configure what action is taken on an interface when a link-fault notification is received from the remote Ethernet OAM peer, use the **action uni-directional link-fault** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of this command.

action uni-directional link-fault {**disable**| **efd** | **error-disable-interface**| **log**}

no action uni-directional link-fault {**disable**| **efd** | **error-disable-interface**| **log**}

Syntax Description

disable	Performs no action on the interface when a capabilities-conflict event occurs.
efd	Puts the line protocol into the down state for an interface when a capabilities-conflict event occurs. The state is removed when the first packet is received without a conflict.
error-disable-interface	Puts the interface into the error-disable state when a capabilities-conflict event occurs.
log	(Interface Ethernet OAM configuration only) Creates a syslog entry when a capabilities-conflict event occurs. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 4.0.0	This command was introduced.
Release 4.1.0	The **efd** keyword was added.

Usage Guidelines

This command only determines the action taken when a uni-directional link fault notification is received from the peer; it does not affect the action taken when a fault is detected locally.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure that no action is performed on the interface when a link-fault notification is received.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# action uni-directional link-fault disable
```

The following example shows how to configure putting the interface into the line-protocol-down state when a link-fault notification is received.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# action uni-directional link-fault efd
```

The following example shows how to configure that the interface is put into the error-disable state when a link-fault notification is received.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# action uni-directional link-fault error-disable-interface
```

The following example shows how to configure that a syslog entry is created when a link-fault notification is received. This configuration overrides the interface Ethernet OAM profile.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/0/CPU0:router(config-if)# ethernet oam
RP/0/0/CPU0:router(config-if-eoam)# action uni-directional link-fault log
```

Related Commands

Command	Description
ethernet oam profile, on page 199	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 198	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 257	Attaches an Ethernet OAM profile to an interface.

action wiring-conflict

To configure what action is taken on an interface when a wiring-conflict event occurs, use the **action wiring-conflict** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of this command.

action wiring-conflict {**disable**| **efd** | **error-disable-interface**| **log**}

no action wiring-conflict {**disable**| **efd** | **error-disable-interface**| **log**}

Syntax Description

disable	Performs no action on the interface when a capabilities-conflict event occurs.
efd	Puts the line protocol into the down state for an interface when a capabilities-conflict event occurs. The state is removed when the first packet is received without a conflict.
error-disable-interface	Puts the interface into the error-disable state when a capabilities-conflict event occurs.
log	(Interface Ethernet OAM configuration only) Creates a syslog entry when a capabilities-conflict event occurs. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.

Command Default

The default action is to put the interface into error-disable state.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 4.0.0	This command was introduced.
Release 4.1.0	The **efd** keyword was added.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure that no action is performed on the interface when a wiring-conflict event occurs.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# action wiring-conflict disable
```

The following example shows how to configure putting the interface into the line-protocol-down state when a wiring-conflict event occurs.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# action wiring-conflict efd
```

The following example shows how to configure that a syslog entry is created when a wiring-conflict event occurs.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# action wiring-conflict log
```

The following example shows how to configure that the interface is put into the error-disable state when a wiring-conflict event occurs. This configuration overrides the interface Ethernet OAM profile.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/0/CPU0:router(config-if)# ethernet oam
(config-if-eoam)# action wiring-conflict error-disable-interface
```

Related Commands

Command	Description
ethernet oam profile, on page 199	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 198	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 257	Attaches an Ethernet OAM profile to an interface.

aggregate

To configure the size and number of bins into which to aggregate the results of statistics collection, use the **aggregate** command in SLA profile statistics configuration mode. To return to the default, use the **no** form of this command.

aggregate {**bins** *count* **width** *width*| **none**}

no aggregate {**bins** *count* **width** *width*| **none**}

Syntax Description

bins *count*	Number of bins. The range is 2 to 100.
width *width*	For delay and jitter measurements, the size of each bin in milliseconds (range 1-10000). In addition, the width must be specified if the number of bins is at least 2, regardless of the type of measurement.
none	No aggregation is performed. All samples are stored individually.

Command Default

For delay measurements, all collected statistics are aggregated into one bin.

Command Modes

SLA profile statistics configuration (config-sla-prof-stat-cfg)

Command History

Release 4.1.0	This command was introduced.

Usage Guidelines

Changing the aggregation for a given metric clears all stored data for that metric.

When aggregation is enabled, a number of bins are created, each of which represents a range of values. Instead of storing each individual result, all that is stored is a counter of the number of results that fall within the range for each bin. This uses much less memory than storing each individual result.

For delay and jitter measurements, the first bin starts at 0, each bin covers a range of values defined by the specified width, except for the last bin which ends at infinity. For example, an aggregate bin count of 4 and a width of 20 for delay measurements yields 4 bins of statistics for these sample ranges:

- Bin 1—Samples with delay ranges 0 to < 20 ms.
- Bin 2—Samples with delay ranges greater than or equal to 20 and < 40 ms.
- Bin 3—Samples with delay ranges greater than or equal to 40 and < 60 ms.
- Bin 4—Samples with delay ranges 60 ms or greater (unbounded).

Note The lower bound of each bin is inclusive, while the upper bound is exclusive. Changing the aggregation for a given metric clears all stored data for that metric.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

This example shows how to configure round-trip-delay statistics measurement in 4 bins each with a range of 20 milliseconds:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet sla
RP/0/0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RP/0/0/CPU0:router(config-sla-prof)# statistics measure round-trip-delay
RP/0/0/CPU0:router(config-sla-prof-stat-cfg)# aggregate bins 4 width 20
```

ais transmission

To configure Alarm Indication Signal (AIS) transmission for a Connectivity Fault Management (CFM) domain service, use the **ais transmission** command in CFM domain service configuration mode. To disable AIS transmission in a CFM domain service, use the no form of this command.

ais transmission [**interval 1s**| **1m**] [**cos** *cos*]

no ais transmission [**interval 1s**| **1m**] [**cos** *cos*]

Syntax Description

interval	(Optional) Interval at which AIS packets are transmitted. Valid values are: • **1s –** Interval of 1 second • **1m –** Interval of 1 minute
cos *cos*	(Optional) Specifies the Class of Service (CoS) for the AIS packets. Valid values are 0 to 7.

Command Default

AIS transmission is disabled by default.

If **interval** is not specified, the default interval is 1 second.

IF **cos** is not specified, each MEP uses its own CoS value, inherited from the interface.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

This command enables AIS for all MEPs in the service. AIS messages are triggered by the following events:

- Detection of a CCM defect.
- Detection of a missing peer MEP (when cross-check is configured).
- Receipt of AIS or LCK messages.
- Detection of interface down events (for down MEPs only).

AIS messages are transmitted in the opposite direction of CCMs and other CFM messages that are sent by the MEP. Therefore, up MEPs send AIS messages out of the interface, whereas down MEPs send AIS messages toward the bridging function.

In addition, AIS messages are sent at a higher maintenance level than other CFM messages sent by the MEP:

- If there is a higher-level MEP on the interface in the same direction (up MEP or down MEP), then the AIS messages are passed internally to this higher level MEP. In this case, no AIS messages are actually transmitted (unless the higher-level MEP is also in a service with AIS transmission configured).
- If there is a MIP on the interface, then AIS messages are sent at the level of the MIP.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure Alarm Indication Signal (AIS) transmission for a CFM domain service:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet cfm
RP/0/0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/0/CPU0:router(config-cfm-dmn-svc)# ais transmission interval 1m cos 7
```

Related Commands

Command	Description
log ais, on page 228	Configures AIS logging for a CFM domain service to indicate when AIS or LCK packets are received.
ais transmission up, on page 153	Configures AIS transmission on a CFM interface.
show ethernet cfm interfaces ais, on page 279	Displays the information about interfaces that are currently transmitting AIS.
show ethernet cfm local meps, on page 287	Displays information about local MEPs.

ais transmission up

To configure Alarm Indication Signal (AIS) transmission on a Connectivity Fault Management (CFM) interface, use the **ais transmission up** command in interface CFM configuration mode. To disable AIS transmission on an interface, use the no form of this command.

ais transmission up [**interval 1s**| **1m**] [**cos** *cos*]

no ais transmission up [**interval 1s**| **1m**] [**cos** *cos*]

Syntax Description

interval	(Optional) Interval at which AIS packets are transmitted. Valid values are: • **1s –** Interval of 1 second • **1m –** Interval of 1 minute
cos *cos*	(Optional) Specifies the Class of Service (CoS) for the AIS packets. Valid values are 0 to 7.

Command Default

AIS transmission is disabled by default.

If **interval** is not specified, the default interval is 1 second.

IF **cos** is not specified, each MEP uses its own CoS value, inherited from the interface.

Command Modes

Interface CFM configuration (config-if-cfm)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

AIS transmission packets for CFM can be configured only on interfaces with no down MEPs. AIS packets are transmitted only if a MIP exists on the interface and the line protocol state is down. AIS messages are transmitted up, toward the bridging function (same direction as an up MEP sends CCMs), and they are transmitted at the level of the MIP.

If AIS transmission is configured on an interface with any down MEPs, the configuration is ignored, and an error is displayed in the **show ethernet cfm configuration-errors** command.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure AIS transmission on a CFM interface.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/2
RP/0/0/CPU0:router(config-if)# ethernet cfm
RP/0/0/CPU0:router(config-if-cfm)# ais transmission up interval 1m cos 7
```

Related Commands

Command	Description
ais transmission, on page 151	Configures AIS transmission for a CFM domain service.
log ais, on page 228	Configures AIS logging for a CFM domain service to indicate when AIS or LCK packets are received.
show ethernet cfm interfaces ais, on page 279	Displays the information about interfaces that are currently transmitting AIS.
show ethernet cfm local meps, on page 287	Displays information about local MEPs.

buckets archive

To configure the number of buckets to store in memory, use the **buckets archive** command in SLA profile statistics configuration mode. To return to the default value, use the no form of this command.

buckets archive *number*

Syntax Description

number	Number of buckets to store. The range is 1 to 100.

Command Default

The default number of buckets stored in memory is 100.

Command Modes

SLA profile statistics configuration (config-sla-prof-stat-cfg)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

The results stored in the oldest bucket are discarded when the limit is reached, to make room for new results. If the number of archived buckets for a given metric decreases, the oldest buckets are deleted and the remaining buckets are untouched. If the number archived buckets for a given metric increases, the newest buckets are filled when the data is collected. See the Usage Guidelines in the buckets size, on page 157 command for a description of buckets.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the number of buckets to store in memory:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet sla
RP/0/0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/0/CPU0:router(config-sla-prof)# statistics measure round-trip-delay
RP/0/0/CPU0:router(config-sla-prof-stat-cfg)# buckets archive 50
```

Related Commands

Command	Description
buckets size, on page 157	Configures the size of the buckets in which statistics are collected.

buckets size

To configure the size of the buckets in which statistics are collected, use the **buckets size** command in SLA profile statistics configuration mode. To return the **buckets size** to the default value, use the no form of this command.

buckets size *number* {**probes**}

no buckets size *number* {**probes**}

Syntax Description

number	Specifies the size of each bucket. The number of probes that each buckets may contain. The range is 1 to 100.
probes	Buckets span multiple probes.

Command Default

1 probe per bucket is collected.

Command Modes

SLA profile statistics configuration mode (config-sla-prof-stat-cfg)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

A bucket represents a time period during which statistics are collected. All the results received during that time period are recorded in the corresponding bucket. If aggregation is enabled, each bucket has its own set of bins and counters, and only results received during the time period represented by the bucket are included in those counters.

By default, there is a separate bucket for each probe. The time period is determined by how long the probe lasts (configured by the probe, on page 256, send (SLA), on page 267, and schedule (SLA), on page 263 commands). This command allows you to modify the size of buckets so that you can have more buckets per probe, or fewer buckets per probe (fewer buckets allows the results from multiple probes to be included in the same bucket).

Note Changing the size of the buckets for a given metric clears all stored data for that metric. All existing buckets are deleted and new buckets are created.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

This example shows how to configure the size of the buckets in which statistics are collected.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet sla
RP/0/0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RP/0/0/CPU0:router(config-sla-prof)# statistics measure round-trip-delay
RP/0/0/CPU0:router(config-sla-prof-stat-cfg)# buckets size 100 per-probe
```

Related Commands

Command	Description
buckets archive, on page 155	Configures the number of buckets to store in memory.
probe, on page 256	Enters SLA profile probe configuration mode.
schedule (SLA), on page 263	
send (SLA), on page 267	Configures the number and timing of packets sent by a probe in an operations profile.

clear ethernet cfm ccm-learning-database location

To clear the Continuity Check Message (CCM) learning database, use the **clear ethernet cfm ccm-learning-database location** command in EXEC mode.

clear ethernet cfm ccm-learning-database location {**all**| *node-id*}

Syntax Description

all	Clears the CCM learning database for all interfaces.
node-id	Clears the CCM learning database for the designated node, entered in *rack*/*slot*/*module* notation.

Command Default

No default behavior or values

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to clear all the CFM CCM learning databases on all interfaces:

```
RP/0/0/CPU0:router# clear ethernet cfm ccm-learning-database location all
```

Related Commands

Command	Description
show ethernet cfm ccm-learning-database, on page 275	Displays the CCM learning database.

clear ethernet cfm interface statistics

To clear the counters for an Ethernet CFM interface, use the **clear ethernet cfm interface statistics** command in EXEC mode.

clear ethernet cfm interface *interface-path-id* **statistics** [**location** {**all**| **location**}]

clear ethernet cfm interface statistics location {**all**| *node-id*}

Syntax Description

interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location	(Optional only when used with a specified interface) Clears MAC accounting statistics for a designated interface or for all interfaces.
all	Clears CFM counters for all interfaces.
node-id	Clears CFM counters for a specified interface, using *rack*/*slot*/*module* notation.

Command Default

No default behavior or values

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to clear all the CFM counters from all interfaces:

```
RP/0/0/CPU0:router# clear ethernet cfm interface statistics location all
```

Related Commands

Command	Description
show ethernet cfm interfaces statistics, on page 282	Displays the per-interface counters for CFM.

clear ethernet cfm local meps

To clear the counters for all MEPs or a specified MEP, use the **clear ethernet cfm local meps** command in EXEC mode.

clear ethernet cfm local meps {**all**| **domain** *domain-name* {**all**| **service** *service-name* {**all**| **mep-id** *id*}}| **interface** *interface-name* {**all**| **domain** *domain-name*}}

Syntax Description

all	Clears counters for all local MEPs.
domain *domain-name*	String of a maximum of 80 characters that identifies the domain in which the maintenance points reside. **Note** For more information about the syntax, use the question mark (**?**) online help function.
service *service-name*	String of a maximum of 80 characters that identifies the maintenance association to which the maintenance points belong.
mep-id *id*	Maintenance end point (MEP) ID number. The range for MEP ID numbers is 1 to 8191.
interface *interface-name*	String of a maximum of 80 characters that identifies the Ethernet interface.

Command Default

No default behavior or values

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

The following counters are cleared:

- Number of continuity-check messages (CCMs) sent
- Number of CCMs received
- Number of CCMs received out of sequence
- Number of CCMs received, but discarded due to the **maximum-meps** limit
- Number of loopback messages (LBMs), used for CFM ping
- Number of loopback replies (LBRs), used for CFM ping, sent and received

- Number of LBRs received out of sequence
- Number of LBRs received with bad data (such as LBRs containing padding which does not match the padding sent in the corresponding LBM)
- Number of alarm indication signal (AIS) messages sent and received
- Number of lock (LCK) messages received

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to clear counters for all MEPs:

```
RP/0/0/CPU0:router# clear ethernet cfm local meps all
```

Related Commands

Command	Description
show ethernet cfm local meps, on page 287	Displays information about local MEPs.

clear ethernet cfm peer meps

To clear all peer MEPs or peer MEPs for a specified local MEP, use the **clear ethernet cfm peer meps** command in EXEC mode.

clear ethernet cfm peer meps {**all**| **domain** *domain-name* {**all**| **service** *service-name* {**all**| **local mep-id** *id*}}| **interface** *interface-name* {**all**| **domain** *domain-name*}}

all	Clears counters for all peer MEPs.
domain *domain-name*	String of a maximum of 80 characters that identifies the domain in which the maintenance points reside. **Note** For more information about the syntax, use the question mark (**?**) online help function.
service *service-name*	String of a maximum of 80 characters that identifies the maintenance association to which the maintenance end points belong.
local mep-id *id*	Local maintenance end point (MEP) ID number. The range for MEP ID numbers is 1 to 8191.
interface *interface-name*	String of a maximum of 80 characters that identifies the Ethernet interface.

Command Default

No default behavior or values

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

This command removes all received CCMs and corresponding peer MEPs from the database (other than those configured with cross-check). The peer MEPs will be added again when the next CCM is received.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to clear all peer MEPs:

```
RP/0/0/CPU0:router# clear ethernet cfm peer meps all
```

Related Commands

Command	Description
show ethernet cfm peer meps, on page 293	Displays information about maintenance end points (MEPs) for peer MEPs.

clear ethernet cfm traceroute-cache

To remove the contents of the traceroute cache, use the **clear ethernet cfm traceroute-cache** command in EXEC mode.

clear ethernet cfm traceroute-cache {**all**| **domain** *domain-name* {**all**| **service** *service-name* {**all**| **mep-id** *id*}}| **interface** *interface-name* {**all**| **domain** *domain-name*}}

Syntax Description

domain *domain-name*	String of a maximum of 80 characters that identifies the domain in which the maintenance points reside. **Note** For more information about the syntax, use the question mark (**?**) online help function.
service *service-name*	String of a maximum of 80 characters that identifies the maintenance association to which the maintenance end points belong.
mep-id *id*	Maintenance end point (MEP) ID number. The range for MEP ID numbers is 1 to 8191.
interface *interface-name*	String of a maximum of 80 characters that identifies the Ethernet interface.

Command Default

No default behavior or values

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to clear all ethernet cfm traceroute-cache:

```
RP/0/0/CPU0:router# clear ethernet cfm traceroute-cache all
```

Related Commands

Command	Description
traceroute cache, on page 336	Sets the maximum limit of traceroute cache entries or the maximum time limit to hold the traceroute cache entries.
show ethernet cfm traceroute-cache, on page 300	Displays the contents of the traceroute cache.

clear ethernet oam statistics

To clear the packet counters on Ethernet OAM interfaces, use the **clear ethernet oam statistics** command in EXEC mode.

clear ethernet oam statistics [**interface** *type interface-path-id*| **location** *node-id* **all**]

Syntax Description

interface *type interface-path-id*	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location	Clears the statistics for a specific node. For more information about the syntax for the router, use the question mark (**?**) online help function.
node-id	Path ID of the node.
all	Clears the statistics for all nodes on the router.

Command Default

No parameters clears the packet counters on all Ethernet OAM interfaces.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to clear the packet counters on a specific interface:

```
RP/0/0/CPU0:router# clear ethernet oam statistics interface gigabitethernet 0/1/5/1
```

Related Commands

Command	Description
show ethernet oam statistics, on page 317	Displays the local and remote Ethernet OAM statistics for interfaces.
show ethernet oam interfaces, on page 314	Displays the current state of Ethernet OAM interfaces.

clear ethernet sla statistics all

To delete the contents of buckets containing SLA statistics collected by all operations probes, including on-demand operations, use the **clear ethernet sla statistics all** command in EXEC mode.

clear ethernet sla statistics [**current**| **history**] **all**

Syntax Description

current	(Optional) Clears statistics for buckets currently being filled for all operations.
history	(Optional) Clears statistics for full buckets for all operations.
all	Clears statistics for all operations.

Command Default

When **current** or **history** are not used, all buckets (current, old, new, half empty, and full) for all operations (including on-demand operations) are cleared. This is equivalent to restarting the operation.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

When you clear a bucket for a currently running probe, the remaining statistics are still collected and stored in that bucket.

See the Usage Guidelines in the buckets size, on page 157 command for a description of buckets.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to delete the contents of all buckets containing SLA metrics collected by all probes:

```
RP/0/0/CPU0:router# clear ethernet sla statistics all
```

The following example shows how to delete the contents of all current buckets containing SLA metrics collected by all probes:

```
RP/0/0/CPU0:router# clear ethernet sla statistics current all
```

The following example shows how to delete the contents of all full buckets containing SLA metrics collected by all probes:

```
RP/0/0/CPU0:router# clear ethernet sla statistics history all
```

clear ethernet sla statistics on-demand

To delete the contents of buckets containing SLA statistics collected by on-demand probes, use the **clear ethernet sla statistics on-demand** command in EXEC mode.

clear ethernet sla statistics [**current**| **history**] **on-demand** {**all**| *id*} [**interface** *type interface-path-id* **domain all**| **interface** *type interface-path-id* **domain** *domain-name* **target** {**all**| **mac-address** *H.H.H*| **mep-id** *id*}| **interface all domain** *domain-name*]

Syntax Description

current	(Optional) Clears statistics for all buckets currently being filled.
history	(Optional) Clears statistics for all full buckets.
all	Clears statistics for all on-demand operations.
id	Clears statistics for the on-demand operation of the specified number.
interface *type*	(Optional) Clears statistics for the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
domain all	Clears statistics for on-demand operations for all domains.
domain *domain-name*	Clears statistics for on-demand operations for the specified domain.
target all	Clears statistics for on-demand operations targeted to all MEPs for the specified interface domain.
target mac-address *H.H.H*	Clears statistics for on-demand operations targeted to the specified MAC address.
target mep-id *id*	Clears statistcs for on-demand operations targeted to the specified MEP ID.
interface all	(Optional) Clears statistics for on-demand operations on all interfaces.

Command Default

When **current** or **history** are not used, all buckets for on-demand operations (current, old, new, half empty, and full) are cleared. This is equivalent to restarting the operation.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

When you clear a bucket for a currently running probe, the remaining statistics are still collected and stored in that bucket.

See the Usage Guidelines in the buckets size, on page 157 command for a description of buckets.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to delete the contents of all buckets currently being filled for the on-demand operation with ID 1:

```
RP/0/0/CPU0:router# clear ethernet sla statistics current on-demand 1
```

The following example shows how to delete the contents of all buckets for all on-demand operations:

```
RP/0/0/CPU0:router# clear ethernet sla statistics on-demand all
```

The following example shows how to delete the contents of all buckets for all on-demand operations on a specified interface and domain that is targeted to a specific MEP:

```
RP/0/0/CPU0:router# clear ethernet sla statistics on-demand all interface TenGigE 0/6/1/0
domain D1 target mep-id 3
```

Related Commands

Command	Description
clear ethernet sla statistics all, on page 170	Deletes the contents of buckets containing SLA statistics collected by all operations probes.
ethernet sla on-demand operation type cfm-delay-measurement probe, on page 201	Executes an on-demand Ethernet SLA operation probe for CFM delay measurement.
ethernet sla on-demand operation type cfm-loopback probe, on page 208	Executes an on-demand Ethernet SLA operation probe for CFM loopback measurements
show ethernet sla operations, on page 321	Displays information about configured Ethernet SLA operations.
show ethernet sla statistics, on page 324	Displays the contents of buckets containing Ethernet SLA metrics collected by probes.

clear ethernet sla statistics profile

To delete the contents of buckets containing SLA statistics collected by probes for a profile, use the **clear ethernet sla statistics profile** command in EXEC mode.

clear ethernet sla statistics [**current**| **history**] **profile** {**all**| *profile-name*} [**interface** *type interface-path-id* **domain all**| **interface** *type interface-path-id* **domain** *domain-name* **target** {**all**| **mac-address** *H.H.H*| **mep-id** *id*}| **interface all domain** *domain-name*]

Syntax Description

current	(Optional) Clears statistics for all buckets currently being filled.
history	(Optional) Clears statistics for all full buckets.
profile-name	Clears statistics for the specified profile name.
all	Clears statistics for all profiles.
interface *type*	(Optional) Clears statistics for the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
domain all	Clears statistics for on-demand operations for all domains.
domain *domain-name*	Clears statistics for on-demand operations for the specified domain.
target all	Clears statistics for on-demand operations targeted to all MEPs for the specified interface domain.
target mac-address *H.H.H*	Clears statistics for on-demand operations targeted to the specified MAC address.
target mep-id *id*	Clears statistcs for on-demand operations targeted to the specified MEP ID.
interface all	(Optional) Clears statistics for on-demand operations on all interfaces.

Command Default

When **current** or **history** are not used, all buckets in the profile (current, old, new, half empty, and full) are cleared. This is equivalent to restarting the operation.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

When you clear a bucket for a currently running probe, the remaining statistics are still collected and stored in that bucket.

See the Usage Guidelines in the buckets size, on page 157 command for a description of buckets.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to delete the contents of all buckets currently being filled for a specified profile:

```
RP/0/0/CPU0:router# clear ethernet sla statistics current profile P1
```

The following example shows how to delete the contents of all full buckets for a specified profile:

```
RP/0/0/CPU0:router# clear ethernet sla statistics history profile P2
```

The following example shows how to delete the contents of all buckets for a specified profile:

```
RP/0/0/CPU0:router# clear ethernet sla statistics profile P3
```

The following example shows how to delete the contents of all buckets for all profiles:

```
RP/0/0/CPU0:router# clear ethernet sla statistics profile all
```

The following example shows how to delete the contents of all buckets for all profiles on a specified interface and domain that is targeted to a specific MEP:

```
RP/0/0/CPU0:router# clear ethernet sla statistics profile all interface TenGigE 0/6/1/0
domain D1 target mep-id 3
```

Related Commands

Command	Description
buckets size, on page 157	Configures the size of the buckets in which statistics are collected.

connection timeout

To configure the timeout value for an Ethernet OAM session, use the **connection timeout** command in Ethernet OAM configuration mode.

connection timeout *seconds*

Syntax Description

seconds	Connection timeout period in seconds. The range is 2 to 30.

Command Default

The default value is 5.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

If no packets are received from the OAM peer in the specified time, the OAM session is brought down, and the negotiation phase starts again.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the connection timeout value of an Ethernet OAM session:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# connection timeout 20
```

Related Commands

Command	Description
action discovery-timeout, on page 133	Configures what action is taken on an interface when a connection timeout occurs.

Command	Description
ethernet oam, on page 198	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
ethernet oam profile, on page 199	Creates an EOAM profile and enters EOAM configuration mode.
show ethernet oam configuration, on page 307	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam discovery, on page 310	Displays the current status of Ethernet OAM sessions.
show ethernet oam interfaces, on page 314	Displays the current state of Ethernet OAM interfaces.

continuity-check archive hold-time

To configure the time limit for how long peer maintenance-end-points (MEPs) are held in the continuity-check database after they have timed out (no more CCMs are received), use the **continuity-check archive hold-time** command in CFM domain service configuration mode. To return to the default value, use the no form of this command.

continuity-check archive hold-time *minutes*

no continuity-check archive hold-time *minutes*

Syntax Description

minutes	Time limit (in minutes) that peer MEPs are held in the continuity-check database before they are cleared. Range is 1 to 65535.

Command Default

The default is 100.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Peer MEPs appear in **show ethernet cfm peer meps** command display output after they timeout (no more continuity check messages (CCMs) are received).

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the time limit for how long continuity-check messages are held in the continuity-check archive:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet cfm
RP/0/0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/0/CPU0:router(config-cfm-dmn-svc)# continuity-check archive hold-time 100
```

Related Commands

Command	Description
show ethernet cfm peer meps, on page 293	Displays information about maintenance end points (MEPs) for peer MEPs.

continuity-check interval

To enable continuity check and configure the time interval at which continuity-check messages are transmitted or to set the threshold limit for when a MEP is declared down, use the **continuity-check interval** command in CFM domain service configuration mode. To disable continuity check, use the **no** form of this command.

continuity-check interval *time* [**loss-threshold** *threshold*]

no continuity-check interval *time* [**loss-threshold** *threshold*]

Syntax Description

time	Interval at which continuity-check messages are transmitted. Valid values are: • 100ms: 100 milliseconds • 1s: 1 second • 10s: 10 seconds • 1m: 1 minute • 10m: 10 minutes
loss-threshold *threshold*	(Optional) Specifies the number of continuity-check messages that are lost before CFM declares that a MEP is down (unreachable). Range is 2 to 255. Used in conjunction with **interval**.

Command Default

Continuity check is off by default.

If **loss-threshold** is not specified, the default is 3.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

This example shows how to configure the time interval at which continuity-check messages are transmitted and set the threshold limit for when a MEP is declared down.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet cfm
RP/0/0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/0/CPU0:router(config-cfm-dmn-svc)# continuity-check interval 100ms loss-threshold 10
```

continuity-check loss auto-traceroute

To configure automatic triggering of a traceroute when a MEP is declared down, use the **continuity-check loss auto-traceroute** command in CFM domain service configuration mode. To disable automatic triggering of a traceroute, use the no form of this command.

continuity-check loss auto-traceroute

no continuity-check loss auto-traceroute

This command has no keywords or arguments.

Command Default

Auto-trigger is off.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

The results of the traceroute can be seen using the **show ethernet cfm traceroute-cache** command.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure automatic triggering of a traceroute when a MEP is declared down:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet cfm
RP/0/0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/0/CPU0:router(config-cfm-dmn-svc)# continuity-check loss auto-traceroute
```

Related Commands

Command	Description
show ethernet cfm traceroute-cache, on page 300	Displays the contents of the traceroute cache.

cos (CFM)

To configure the class of service (CoS) for all CFM packets generated by the maintenance end point (MEP) on an interface, use the **cos** command in interface CFM MEP configuration mode. To return to the default CoS, use the no form of this command.

cos *cos*

no cos *cos*

Syntax Description

cos	Class of Service for this MEP. The range is 0 to 7.

Command Default

When not configured, the default CoS value is inherited from the Ethernet interface.

Command Modes

Interface CFM MEP configuration (config-if-cfm-mep)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Configuring the class of service (CoS) on maintenance end points (MEPs) is supported on all Ethernet interfaces.

The specifed CoS value is used for all CFM messages transmitted by the MEP, except for the following:

- Loopback and Linktrace replies—These are transmitted using the CoS value received in the corresponding loopback or linktrace message.
- AIS messages—If a different CoS value is specified in the AIS configuration.
- Ethernet SLA probe messages.

Note For Ethernet interfaces, the CoS is carried as a field in the VLAN tag. Therefore, CoS only applies to interfaces where packets are sent with VLAN tags. If the **cos (CFM)** command is specified for a MEP on an interface that does not have a VLAN encapsulation configured, an error message will be logged and no CFM packets will be sent.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the class of service (CoS) for a maintenance end point (MEP) on an interface.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/1
RP/0/0/CPU0:router(config-if)# ethernet cfm mep domain Dm1 service Sv1 mep-id 1
RP/0/0/CPU0:router(config-if-cfm-mep)# cos 7
```

Related Commands

Command	Description
ethernet cfm (interface), on page 196	Enters interface CFM configuration mode.

debug ethernet cfm packets

To log debug messages about CFM packets that are sent or received by the Ethernet connectivity fault management (CFM) process, use the **debug ethernet cfm packets** command in EXEC mode.

debug ethernet cfm packets [**domain** *domain-name* [**service** *service-name* [**mep-id** *mep-id*]]] [**interface** *type interface-path-id* [**domain** *domain-name*]] [**packet-type** {**ccm**| **linktrace**| **loopback**}] [**remote mac-address** *mac-address*] [**remote mep-id** *mep-id*] [**sent**| **received**] [**brief**| **full**| **hexdump**]**debug ethernet cfm packets** [**domain** *domain-name* [**service** *service-name* [**mep-id** *mep-id*]]] [**interface** *type interface-path-id* [**domain** *domain-name*]] [**packet-type** {**ais**| **ccm**| **delay-measurement**| **linktrace**| **loopback**}] [**remote mac-address** *mac-address*] [**remote mep-id** *mep-id*] [**sent**| **received**] [**brief**| **full**| **hexdump**]

Syntax Description

domain *domain-name*	(Optional) Filters packets for display by the specified CFM maintenance domain, where *domain-name* is a string of up to 80 characters.
service *service-name*	(Optional) Filters packets for display by the specified service name, where *service-name* is a string of up to 80 characters.
mep-id *mep-id*	(Optional) Filters packets for display by the specified maintenance end point (MEP) ID number. The range for MEP ID numbers is 1 to 8191.
interface *type interface-path-id*	(Optional) Filters packets for display by the specified physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
packet-type	(Optional) Filters packets for display by the specified packet type. The following packet types are valid: • **ais** • **ccm** • **delay-measurement** • **linktrace** • loopback
remote mac-address *mac-address*	(Optional) Filters packets for display by the specified MAC address.
remote mep-id *mep-id*	(Optional) Filters packets for display by the remote MEP properties.
sent	(Optional) Displays only sent packets.
received	(Optional) Displays only received packets.

brief	(Optional) Displays brief information about each packet.
full	(Optional) Displays a full decode of each packet.
hexdump	(Optional) Displays a full decode and hexadecimal output of each packet.

Command Default

If no parameters are specified, all CFM packets are debugged and logged.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelin

Caution Enabling packet debugging without filters can have an adverse effect on the performance of the router. To avoid this, filters should always be specified to restrict the output to the domain, service, local MEP, interface, direction and packet type of interest.

Packets can be filtered for debugging by specifying any of the optional parameters.

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows a sample output of the **debug ethernet cfm packets** command with a full decode and hexadecimal output for sent and received CCM packets:

```
RP/0/0/CPU0:router# debug ethernet cfm packets hexdump

RP/0/0/CPU0:May 29 14:15:39.621 : cfmd[150]: PKT-RX: GigabitEthernet0/1/0/0 ingress: CCM
packet rcvd at level 2 for domain foo, service foo: length 91, src MAC 0001.0203.0402, dst
 MAC 0180.c200.0032: Packet processed successfully
RP/0/0/CPU0:May 29 14:15:39.621 : cfmd[150]: PKT-RX:   CCM: Level 2, opcode CCM, version
0, RDI bit unset, interval 10s, seq. num 1, remote MEP ID 16, flags 0x05, first TLV offset
 70, 0 unknown TLVs
RP/0/0/CPU0:May 29 14:15:39.621 : cfmd[150]: PKT-RX:   CCM: MAID: MDID String 'dom4', SMAN
 String 'ser4'
RP/0/0/CPU0:May 29 14:15:39.621 : cfmd[150]: PKT-RX:   CCM: Sender ID: Chassis ID Local
'hpr', Mgmt Addr <none>
RP/0/0/CPU0:May 29 14:15:39.621 : cfmd[150]: PKT-RX:   CCM: Port status: Up, interface
status Up
RP/0/0/CPU0:May 29 14:15:39.622 : cfmd[150]: PKT-RX:   Raw Frame:
RP/0/0/CPU0:May 29 14:15:39.622 : cfmd[150]: PKT-RX:     0x40010546 00000001 00100404
646F6D34 02047365 72340000 00000000 00000000
```

```
RP/0/0/CPU0:May 29 14:15:39.622 : cfmd[150]: PKT-RX:     0x00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000
RP/0/0/CPU0:May 29 14:15:39.622 : cfmd[150]: PKT-RX:     0x00000000 00000000 00000200
01020400 01010100 05030768 707200
RP/0/0/CPU0:May 29 14:15:43.625 : cfmd[150]: PKT-TX: GigabitEthernet0/1/0/0 egress: CCM
packet sent at level 2 for domain foo, service foo: length 91, src MAC 0001.0203.0400, dst
 MAC 0180.c200.0032
RP/0/0/CPU0:May 29 14:15:43.625 : cfmd[150]: PKT-TX:   CCM: Level 2, opcode CCM, version
0, RDI bit set, interval 10s, seq. num 16, remote MEP ID 1, flags 0x85, first TLV offset
70, 0 unknown TLVs
RP/0/0/CPU0:May 29 14:15:43.625 : cfmd[150]: PKT-TX:   CCM: MAID: MDID String 'foo', SMAN
String 'foo'
RP/0/0/CPU0:May 29 14:15:43.625 : cfmd[150]: PKT-TX:   CCM: Sender ID: Chassis ID Local
'ios', Mgmt Addr <none>
RP/0/0/CPU0:May 29 14:15:43.625 : cfmd[150]: PKT-TX:   CCM: Port status: Up, interface
status Up
RP/0/0/CPU0:May 29 14:15:43.625 : cfmd[150]: PKT-TX:   Raw Frame:
RP/0/0/CPU0:May 29 14:15:43.625 : cfmd[150]: PKT-TX:     0x40018546 00000010 00010403
666F6F02 03666F6F 00000000 00000000 00000000
RP/0/0/CPU0:May 29 14:15:43.625 : cfmd[150]: PKT-TX:     0x00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000
RP/0/0/CPU0:May 29 14:15:43.625 : cfmd[150]: PKT-TX:     0x00000000 00000000 00000200
01020400 01010100 05030769 6F7300
```

Related Commands

Command	Description
debug ethernet cfm protocol-state, on page 188	Logs debug messages about CFM state machines and protocol events.

debug ethernet cfm protocol-state

To log debug messages about CFM state machines and protocol events, use the **debug ethernet cfm protocol-state** command in EXEC mode.

debug ethernet cfm protocol-state [**domain** *domain-name* [**service** *service-name* [**mep-id** *mep-id*]]] [**interface** *type interface-path-id* [**domain** *domain-name*]]

Syntax Description

domain *domain-name*	(Optional) Filters information for display by the specified CFM maintenance domain, where *domain-name* is a string of up to 80 characters.
service *service-name*	(Optional) Filters information for display by the specified service name, where *service-name* is a string of up to 80 characters.
mep-id *mep-id*	(Optional) Filters information for display by the specified maintenance end point (MEP) ID number. The range for MEP ID numbers is 1 to 8191.
interface *type interface-path-id*	(Optional) Filters information for display by the specified physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

If no parameters are specified, all CFM state machines and protocol events are debugged and logged.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Debug messages can be filtered by specifying any of the optional parameters.

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows a sample output of the **debug ethernet cfm protocol-state** command.

```
RP/0/0/CPU0:router# debug ethernet cfm protocol-state

RP/0/0/CPU0:May 29 14:41:49.966 : cfmd[150]: CFM: Created 1 local MEPs in PM and Engine
RP/0/0/CPU0:May 29 14:41:49.967 : cfmd[150]: CFM: State changes notification for 1 EFPs
RP/0/0/CPU0:May 29 14:42:14.143 : cfmd[150]: CFM: New remote MEP detected in domain foo,
service foo for local MEP ID 1 on interface GigabitEthernet0/1/0/0; remote MEP ID 16, MAC
0001.0203.0402, errors: set: mismatched MAID; current: mismatched MAID;
RP/0/0/CPU0:May 29 14:42:16.644 : cfmd[150]: CFM: Fault alarm notification for local MEP -
 domain: foo, service: foo, MEP ID: 1, interface: GigabitEthernet0/1/0/0, defect:
cross-connect CCM
RP/0/0/CPU0:May 29 14:43:32.247 : cfmd[150]: CFM: Initiated exploratory linktrace to
ffff.ffff.ffff from MEP in domain foo, service foo, MEP ID 1, interface GigabitEthernet0/1/0/0
 with ttl 64 and transaction ID 65537, reply-filtering Default and directed MAC None
May 29 14:43:49.155 : cfmd[150]: CFM: Remote MEP timed out in domain foo, service foo for
local MEP ID 1 on interface GigabitEthernet0/1/0/0; remote MEP ID 16, MAC 0001.0203.0402,
errors: cleared: mismatched MAID; current: none
```

Related Commands

Command	Description
debug ethernet cfm packets, on page 185	Logs debug messages about CFM packets that are sent or received by the Ethernet CFM process.

domain

To create and name a container for all domain configurations and enter the CFM domain configuration mode, use the **domain** command in CFM configuration mode. To remove the domain, use the no form of this command.

domain *domain-name* **level** *level-value* [**id null** [**dns** *dns-name*][**mac** *H.H.H*][**string** *string*]]

no domain *domain-name* **level** *level-value* [**id null** [**dns** *dns-name*][**mac** *H.H.H*][**string** *string*]]

Syntax Description

domain-name	Administrative name unique to this container, case sensitive ASCII string, up to 80 characters.
level *level-value*	The CFM protocol level of this domain. Range is 0 to 7.
id	(Optional) Maintenance domain identifier (MDID) used in conjunction with one of the following keywords to specify the MDID type and value: • null • **dns** *DNS-name* • **mac** *H.H.H* • **string** *string*
null	(Optional) Null value ID, used with the **id** keyword.
dns *DNS-name*	(Optional) DNS name, up to 43 characters in length, used with the **id** keyword.
mac *H.H.H*	(Optional) Hexadecimal MAC address, used with the **id** keyword.
string *string*	(Optional) Maintenance domain identifier (MDID) value, up to 43 characters in length, used with the **id** keyword. **Note** The domain name may be the used here as the maintenance domain identifier (MDID) if desired.

Command Default

If **id** is not specified, the domain name is used as the MDID.

Command Modes

CFM configuration (config-cfm)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

The level must be specified.

The maintenance domain identifier (MDID) is used as the first part of the maintenance association identifier (MAID) in CFM frames. If the MDID is not specified, the domain name is used as the MDID by default.

Multiple domains may be specified at the same level. If the MDID is specified as NULL, the MAID is constructed as a short maintenance association name.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to create a domain and give it a domain name, level, and maintenance domain identifier (MDID):

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet cfm
RP/0/0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/0/CPU0:router(config-cfm-dmn)#
```

Related Commands

Command	Description
ethernet cfm (global), on page 194	Enters CFM configuration mode.
ethernet cfm (interface), on page 196	Enters interface CFM configuration mode.
mep domain, on page 240	Creates a MEP on an interface.
service, on page 270	
show ethernet cfm configuration-errors, on page 277	Displays information about errors that are preventing configured CFM operations from becoming active, as well as any warnings that have occurred.
show ethernet cfm local maintenance-points, on page 284	Displays a list of local maintenance points.
show ethernet cfm local meps, on page 287	Displays information about local MEPs.

efd

To enable Ethernet Fault Detection (EFD) on all down Maintenance End Points (MEPs) in a down MEPs service, use the **efd** command in CFM domain service configuration mode. To disable EFD, use the no form of this command.

efd{}

no efd

Command Default

EFD is disabled.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

EFD can only be enabled for down MEPs within a down MEPs service.

If the **efd** command is issued when any MEP in the service has any of the following error conditions, the MEP will shut down the interface:

- The MEP appears cross-connected to another MAID.
- The MEP is receiving invalid CCMs, such as receiving its own MAC or MEP-ID.
- All peer MEPs are reporting a state other than UP via the Port Status TLV.
- A peer MEP is reporting a state other than UP in Interface Status TLV.
- When cross-check is configured, and a session with an expected MEP times out, EFD is triggered on the local MEP.
- No CCMs are received from a peer MEP appearing in the configured cross-check list.
- An RDI is being received from a peer MEP.
- The MEP is receiving an AIS/LCK.

The MEP will bring the interface back up when the error condition is no longer detected.

Note When an interface is shut down by a MEP using EFD, the MEP will continue to send and receive CCMs and other CFM messages.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

This example shows how to enable EFD:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet cfm
RP/0/0/CPU0:router(config-cfm)# domain D1 level 1
RP/0/0/CPU0:router(config-cfm-dmn)# service S1 down-meps
RP/0/0/CPU0:router(config-cfm-dmn-svc)# efd
```

Related Commands

Command	Description
log efd, on page 234	Enables logging of EFD state changes to an interface (such as when an interface is shut down or brought up via EFD).
show efd interface, on page 273	Displays all interfaces that are shut down because of EFD.
show ethernet cfm local meps, on page 287	Displays information about local MEPs.

ethernet cfm (global)

To enter Connectivity Fault Management (CFM) configuration mode, use the **ethernet cfm (global)** command in global configuration mode.

ethernet cfm

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enter the CFM configuration mode.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet cfm
RP/0/0/CPU0:router(config-cfm)#
```

Related Commands

Command	Description
domain, on page 190	
ethernet cfm (interface), on page 196	Enters interface CFM configuration mode.
show ethernet cfm configuration-errors, on page 277	Displays information about errors that are preventing configured CFM operations from becoming active, as well as any warnings that have occurred.
show ethernet cfm local maintenance-points, on page 284	Displays a list of local maintenance points.

Command	Description
show ethernet cfm local meps, on page 287	Displays information about local MEPs.

ethernet cfm (interface)

To enter interface CFM configuration mode, use the **ethernet cfm (interface)** command in interface configuration mode.

ethernet cfm

Syntax Description

This command has no keywords or arguments.

Command Default

No MEPs are configured on the interface.

Command Modes

Interface configuration (config-if)

Subinterface configuration (config-subif)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enter interface CFM configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/1
RP/0/0/CPU0:router(config-if)# ethernet cfm
RP/0/0/CPU0:router(config-if-cfm)#
```

Related Commands

Command	Description
cos (CFM), on page 183	Configures the CoS for all CFM packets generated by the MEP on an interface.
ethernet cfm (global), on page 194	Enters CFM configuration mode.
mep domain, on page 240	Creates a MEP on an interface.

Command	Description
show ethernet cfm configuration-errors, on page 277	Displays information about errors that are preventing configured CFM operations from becoming active, as well as any warnings that have occurred.
show ethernet cfm local maintenance-points, on page 284	Displays a list of local maintenance points.
show ethernet cfm local meps, on page 287	Displays information about local MEPs.

ethernet oam

To enable Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode, use the **ethernet oam** command in interface configuration mode. To disable Ethernet Link OAM, use the **no** form of this command.

ethernet oam

no ethernet oam

Syntax Description

This command has no keywords or arguments.

Command Default

When enabled on an interface, the Ethernet Link OAM default values apply.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

When you enable Ethernet Link OAM on an interface, the default Ethernet Link OAM values are applied to the interface. For the default Ethernet Link OAM values, see the related Ethernet Link OAM commands.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enable Ethernet Link OAM and enter interface Ethernet OAM configuration mode.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/5/6
RP/0/0/CPU0:router(config-if)# ethernet oam
RP/0/0/CPU0:router(config-if-eoam)#
```

ethernet oam profile

To create an Ethernet Operations, Administration and Maintenance (EOAM) profile and enter EOAM configuration mode, use the **ethernet oam profile** command in global configuration mode. To delete an EOAM profile, use the **no** form of this command.

ethernet oam profile *profile-name*

no ethernet oam profile *profile-name*

Syntax Description

profile-name	Text string name of the OAM profile. The maximum length is 32 bytes.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Before you can delete an EOAM profile, you must remove the profile from all interfaces to which it is attached.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

This example shows how to create an Ethernet OAM profile and enter Ethernet OAM configuration mode:

```
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)#
```

ethernet sla

To enter the Ethernet Service Level Agreement (SLA) configuration mode, use the **ethernet sla** command in global configuration mode.

ethernet sla

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enter the Ethernet SLA configuration mode.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet sla
RP/0/0/CPU0:router(config-sla)#
```

ethernet sla on-demand operation type cfm-delay-measurement probe

To execute an on-demand Ethernet SLA operation probe for CFM delay measurement, use the **ethernet sla on-demand operation type cfm-delay-measurement probe** command in EXEC mode.

ethernet sla on-demand operation type {**cfm-delay-measurement**} **probe** [**priority** *number*] [**send** {**packet** {**once**| **every** *number* {**milliseconds**| **seconds**| **minutes**| **hours**}}| **burst** {**once**| **every** *number* {**seconds**| **minutes**| **hours**}}} **packet count** *number* **interval** *number* {**milliseconds**| **seconds**}] **packet size** *bytes* [**test pattern** {**hex 0x** *HHHHHHHH*| **pseudo-random**}]**domain** *domain_name* **source interface** *type interface-path-id* **target** {**mac-address H**.**H**.**H**.**H**| **mep-id** *id_number*} **statistics measure** {**one-way-delay-ds**| **one-way-delay-sd**| **one-way-jitter-ds**| **one-way-jitter-sd**| **round-trip-delay**| **round-trip-jitter**} [**aggregate** {**none**| **bins** *number* **width** *milliseconds*}] [**buckets** {**archive** *number*| **size** *number* {**per-probe**| **probes**}}] [**schedule** {**now**| **at** *hh*:*mm* [*.ss*] [*day* [*month* [*year*]]]| **in** *number* {**seconds**| **minutes**| **hours**}} [**for** *duration* {**seconds**| **minutes**| **hours**}] [**repeat every** *number* {**seconds**| **minutes**| **hours**} **count** *probes*]] **[asynchronous]**

Syntax Description

priority *number*	(Optional) Configures the priority of outgoing SLA probe packets. The range is 0 to 7. The default is to use the COS bits for the egress interface.
send packet once	(Optional) Sends one packet one time.
send packet every *number* {**milliseconds** | **seconds** | **minutes** | **hours**}	(Optional) Sends one packet every specified number of milliseconds, seconds, minutes, or hours, where *number* is in the following range: • 1 to 3600 **seconds** • 1 to 1440 **minutes** • 1 to 168 **hours** • 100 to 10000 **milliseconds** (specified in increments of 100)
send burst once	(Optional) Specifies that a burst of packets is sent one time. This is the default.

send burst every *number* {**seconds** | **minutes** | **hours**}}	(Optional) Sends a burst of packets every specified number of seconds, minutes, or hours, where *number* is in the following range: • 1–3600 **seconds** • 1–1440 **minutes** • 1–168 **hours** The default is to send a burst every 10 seconds.
packet count *number*	Specifies the number of packets to be sent in a burst, in the range 2 to 600. The default is 10.
interval *number* {**milliseconds** | **seconds**}	Specifies the time between sending packets in a burst, where *number* is in the following range: • 100 to 30000 **milliseconds** • 1 to 30 **seconds** **Note** The total length of a burst (the packet count multiplied by the interval) must not exceed 1 minute.
packet size*bytes*	Minimum size of the packet including padding when necessary. The range is 1 to 9000 bytes. This value is the total frame size including the Layer 2 or Layer 3 packet header.
test pattern hex 0x *HHHHHHHH*	(Optional) Specifies a 4-byte string (8 hexadecimal characters) to repeat as many times as required to fill the outgoing probe packet to the specified minimum packet size. The default is all 0s.
test pattern pseudo-random	(Optional) Specifies a pseudo-random bit sequence determined by the protocol to fill the outgoing probe packet to the specified minimum packet size.
domain *domain-name*	Specifies the name of the domain for the locally defined CFM MEP.

source interface *type*	Specifies the source interface type of the locally defined CFM MEP. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
target mac-address *H.H.H*	Specifies the MAC address (in dotted hexadecimal format) of the target MEP that is known to the local MEP for the probe.
target mep-id *id-number*	Specifies the ID (from 1 to 8191) of the target MEP that is known to the local MEP for the probe.
statistics measure	(Optional) Specifies the type of statistics to collect: • **one-way-delay-ds—**One-way delay statistics from destination to source. • **one-way-delay-sd—**One-way delay statistics from source to destination. • **one-way-jitter-ds—**One-way delay jitter from destination to source. • **one-way-jitter-sd—**One-way delay jitter from source to destination. • **round-trip-delay—**Round-trip delay statistics. • **round-trip-jitter—**Round-trip jitter statistics. All statistics are collected by default.

aggregate none	(Optional) Specifies that statistics are not aggregated into bins, and each statistic is stored individually. **Caution** This option can be memory-intensive and should be used with care.
aggregate bins *number*	(Optional) Specifies the number of bins (from 2 to 100) within each bucket to store sample packets from the probe. The default is to aggregate into one bin.
width *milliseconds*	Specifies the range of the samples to be collected within each bin in milliseconds, from 1 to 10000. Based on the specified width, bins are established in the following way: • Delay measurements (round-trip or one-way)—The lower bound of the bins is zero and the first bin's upper limit is 0 plus the specified width, and the last bin is unbounded. • Jitter measurements (round-trip or one-way)—The bins are evenly distributed around zero, with both the lowest and highest numbered bins being unbounded. See the Usage Guidelines for more information.
buckets archive *number*	(Optional) Specifies the number of buckets to store in memory from 1 to 100. The default is 100.
buckets size *number*	(Optional) Specifies the number of buckets to be used for probes from 1 to 100. The default is 1.
per-probe	Specifies that probes span multiple buckets.
probes	Specifies that buckets span multiple probes.

schedule now	(Optional) Specifies that the probe begins as soon as you enter the command. This is the default.
schedule at *hh*:*mm*	(Optional) Specifies a specific time at which to start the probe in 24-hour notation.
ss	(Optional) Number of seconds into the next minute at which to start the probe.
day	(Optional) Number in the range 1 to 31 of the day of the month on which to start the probe.
month	(Optional) Name of the month (full word in English) in which to start the probe.
year	(Optional) Year (fully specified as 4 digits) in which to start the probe.
schedule in *number* {**seconds** | **minutes** | **hours**}	(Optional) Specifies a relative time, as a number of seconds, minutes or hours from the current time, at which to start the probe, where *number* is in the following ranges: • 1 to 3600 **seconds** • 1 to 1440 **minutes** • 1 to 24 **hours**
for *duration* {**seconds** | **minutes** | **hours**}	(Optional) Specifies the length of the probe as a number of seconds, minutes, or hours, where *number* is in the following ranges: • 1 to 3600 **seconds** • 1 to 1440 **minutes** • 1 to 24 **hours** **Note** The duration should not exceed the interval specified by the **repeat every** option.

repeat every *number* {**seconds** | **minutes** | **hours**}	(Optional) Specifies the interval at which to restart the probe as a number of seconds, minutes, or hours, where *number* is in the following ranges: • 1 to 90 **seconds** • 1 to 90 **minutes** • 1 to 24 **hours** The default is that probes are not repeated, and there is no default interval.
count *probes*	Specifies the number of probes to run in the range 1–100. There is no default.
asynchronous	(Optional) Specifies that the command displays the on-demand operation ID and exits immediately, with the operation continuing in the background. The default is synchronous and the operation displays the on-demand operation ID and all results on the console when it completes.

Command Default

No on-demand operations are configured or executed.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	execute

Examples

This example shows how to enter the most basic SLA on-demand operation to measure CFM delay statistics. This example implements these defaults:

- Send a burst once for a packet count of 10 and interval of 1 second (10-second probe).
- Use default class of service (CoS) for the egress interface.
- Measure all statistics, including both one-way and round-trip delay and jitter statistics.
- Aggregate statistics into one bin.
- Schedule now.
- Display results on the console.

```
RP/0/0/CPU0:router# ethernet sla on-demand operation type cfm-delay-measurement
probe domain D1 source interface TenGigE 0/6/1/0 target mep-id 100
```

Related Commands

Command	Description
clear ethernet sla statistics all, on page 170	Deletes the contents of buckets containing SLA statistics collected by all operations probes.
clear ethernet sla statistics on-demand, on page 172	Deletes the contents of buckets containing SLA statistics collected by on-demand probes.
show ethernet sla operations, on page 321	Displays information about configured Ethernet SLA operations.
show ethernet sla statistics, on page 324	Displays the contents of buckets containing Ethernet SLA metrics collected by probes.

ethernet sla on-demand operation type cfm-loopback probe

To execute an on-demand Ethernet SLA operation probe for CFM loopback measurement, use the **ethernet sla on-demand operation type cfm-loopback probe** command in EXEC configuration mode.

ethernet sla on-demand operation type cfm-delay-measurement probe [**priority** *number*]**send** {**packet** {**once**| **every** *number* {**milliseconds**| **seconds**| **minutes**| **hours**}}| **burst** {**once**| **every** *number* {**seconds**| **minutes**| **hours**}} **packet count** *number* **interval** *number* {**milliseconds**| **seconds**}}**packet size** *bytes* [**test pattern** {**hex 0x** *HHHHHHHH*| **pseudo-random**}]**domain** *domain_name* **source interface** *type interface-path-id* **target** {**mac-address** *H.H.H.H*| **mep-id** *id_number*}**statistics measure** {**one-way-delay-ds**| **one-way-delay-sd**| **one-way-jitter-ds**| **one-way-jitter-sd**| **round-trip-delay**| **round-trip-jitter**}**aggregate** {**none**| **bins** *number* **width** *milliseconds*}**buckets** {**archive** *number*| **size** *number* {**per-probe**| **probes**}}**schedule** {**now**| **at** *hh*:*mm*:*ss* [*day month year*]| **in** *number* {**seconds**| **minutes**| **hours**}}**for** *duration* {**seconds**| **minutes**| **hours**}**repeat every** *number* {**seconds**| **minutes**| **hours**} **count** *probes***[asynchronous]**

Syntax Description

priority *number*	(Optional) Configures the priority of outgoing SLA probe packets. The range is 0 to 7. The default is to use the COS bits for the egress interface.
send packet once	(Optional) Sends one packet one time.
send packet every *number* {**milliseconds** | **seconds** | **minutes** | **hours**}	(Optional) Sends one packet every specified number of milliseconds, seconds, minutes, or hours, where *number* is in the following range: • 1 to 3600 **seconds** • 1 to 1440 **minutes** • 1 to 168 **hours** • 100 to 10000 **milliseconds** (specified in increments of 100)
send burst once	(Optional) Specifies that a burst of packets is sent one time. This is the default.

send burst every *number* {**seconds** | **minutes** | **hours**}}	(Optional) Sends a burst of packets every specified number of seconds, minutes, or hours, where *number* is in the following range: • 1–3600 **seconds** • 1–1440 **minutes** • 1–168 **hours** The default is to send a burst every 10 seconds.
packet count *number*	Specifies the number of packets to be sent in a burst, in the range 2 to 600. The default is 10.
interval *number* {**milliseconds** | **seconds**}	Specifies the time between sending packets in a burst, where *number* is in the following range: • 100 to 30000 **milliseconds** • 1 to 30 **seconds** **Note** The total length of a burst (the packet count multiplied by the interval) must not exceed 1 minute.
packet size*bytes*	Minimum size of the packet including padding when necessary. The range is 1 to 9000 bytes. This value is the total frame size including the Layer 2 or Layer 3 packet header.
test pattern hex 0x *HHHHHHHH*	(Optional) Specifies a 4-byte string (8 hexadecimal characters) to repeat as many times as required to fill the outgoing probe packet to the specified minimum packet size. The default is all 0s.
test pattern pseudo-random	(Optional) Specifies a pseudo-random bit sequence determined by the protocol to fill the outgoing probe packet to the specified minimum packet size.
domain *domain-name*	Specifies the name of the domain for the locally defined CFM MEP.

source interface *type*	Specifies the source interface type of the locally defined CFM MEP. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
target mac-address *H.H.H.H*	Specifies the MAC address (in dotted hexadecimal format) of the target MEP that is known to the local MEP for the probe.
target mep-id *id-number*	Specifies the ID (from 1 to 8191) of the target MEP that is known to the local MEP for the probe.
statistics measure	(Optional) Specifies the type of statistics to collect: • **one-way-delay-ds**—One-way delay statistics from destination to source. • **one-way-delay-sd**—One-way delay statistics from source to destination. • **one-way-jitter-ds**—One-way jitter statistics from destination to source. • **one-way-jitter-sd**—One-way jitter statistics from source to destination. • **round-trip-delay**—Round-trip delay statistics. • **round-trip-jitter**—Round-trip jitter statistics. All statistics are collected by default.

aggregate none	(Optional) Specifies that statistics are not aggregated into bins, and each statistic is stored individually. **Caution** This option can be memory-intensive and should be used with care.
aggregate bins *number*	(Optional) Specifies the number of bins (from 2 to 100) within each bucket to store sample packets from the probe. The default is to aggregate into one bin.
width *milliseconds*	Specifies the range of the samples to be collected within each bin in milliseconds, from 1 to 10000. Based on the specified width, bins are established in the following way: • Delay measurements (round-trip or one-way)—The lower bound of the bins is zero and the first bin's upper limit is 0 plus the specified width, and the last bin is unbounded. • Jitter measurements (round-trip or one-way)—The bins are evenly distributed around zero, with both the lowest and highest numbered bins being unbounded. See the Usage Guidelines for more information.
buckets archive *number*	(Optional) Specifies the number of buckets to store in memory from 1 to 100. The default is 100.
buckets size *number*	(Optional) Specifies the number of buckets to be used for probes from 1 to 100. The default is 1.
per-probe	Specifies that probes span multiple buckets.
probes	Specifies that buckets span multiple probes.

schedule now	(Optional) Specifies that the probe begins as soon as you enter the command. This is the default.
schedule at *hh*:*mm*:*ss*	(Optional) Specifies a specific time at which to start the probe in 24-hour notation.
day	(Optional) Number in the range 1 to 31 of the day of the month on which to start the probe.
month	(Optional) Name of the month (full word in English) in which to start the probe.
year	(Optional) Year (fully specified as 4 digits) in which to start the probe.
schedule in *number* {**seconds** | **minutes** | **hours**}	(Optional) Specifies a relative time, as a number of seconds, minutes or hours from the current time, at which to start the probe, where *number* is in the following ranges: • 1 to 3600 **seconds** • 1 to 1440 **minutes** • 1 to 24 **hours**
for *duration* {**seconds** | **minutes** | **hours**}	(Optional) Specifies the length of the probe as a number of seconds, minutes, or hours, where *number* is in the following ranges: • 1 to 3600 **seconds** • 1 to 1440 **minutes** • 1 to 24 **hours** **Note** The duration should not exceed the interval specified by the **repeat every** option.

repeat every *number* {**seconds** | **minutes** | **hours**}	(Optional) Specifies the interval at which to restart the probe as a number of seconds, minutes, or hours, where *number* is in the following ranges: • 1 to 90 **seconds** • 1 to 90 **minutes** • 1 to 24 **hours** The default is that probes are not repeated, and there is no default interval.
count *probes*	Specifies the number of probes to run in the range 1–100. There is no default.
asynchronous	(Optional) Specifies that the command displays the on-demand operation ID and exits immediately, with the operation continuing in the background. The default is synchronous and the operation displays the on-demand operation ID and all results on the console when it completes.

Command Default

No on-demand operations are configured or executed.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to enter the most basic SLA on-demand operation to measure CFM loopback statistics. This example implements the following defaults:

- Send a burst once for a packet count of 10 and interval of 1 second (10-second probe).
- Use default test pattern of 0's for padding.
- Use default class of service (CoS) for the egress interface.
- Measure all statistics.
- Aggregate statistics into one bin.
- Schedule now.
- Display results on the console.

```
RP/0/0/CPU0:router# ethernet sla on-demand operation type cfm-loopback
probe packet size 1500 domain D1 source interface TenGigE 0/6/1/0 target mep-id 100
```

Related Commands

Command	Description
clear ethernet sla statistics all, on page 170	Deletes the contents of buckets containing SLA statistics collected by all operations probes.
clear ethernet sla statistics on-demand, on page 172	Deletes the contents of buckets containing SLA statistics collected by on-demand probes.
show ethernet sla operations, on page 321	Displays information about configured Ethernet SLA operations.
show ethernet sla statistics, on page 324	Displays the contents of buckets containing Ethernet SLA metrics collected by probes.

frame-period threshold

To configure the thresholds that trigger an Ethernet OAM frame-period error event, use the **frame-period threshold** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the threshold to the default value, use the **no** form of this command.

frame-period threshold low *threshold* [**high** *threshold*]

no frame-period threshold low *threshold* [**high** *threshold*]

Syntax Description

low *threshold*	Low threshold, in frames, that triggers a frame-period error event. The range is 0 to 1000000.
high *threshold*	(Optional) High threshold, in frames, that triggers a frame-period error event. The range is 0 to 1000000. The high threshold value can be configured only in conjunction with the low threshold value.

Command Default

The default low threshold is 1.

Command Modes

Ethernet OAM link monitor configuration (config-eoam-lm)

Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

When the low threshold is passed, a frame-period error event notification is generated and transmitted to the OAM peer. Additionally, any registered higher level OAM protocols, such as Connectivity Fault Management (CFM), are also notified. When the high threshold is passed, the configured high threshold action is performed in addition to the low threshold actions. The high threshold is optional and is configurable only in conjunction with the low threshold.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the low and high thresholds that trigger a frame-period error event.

```
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# link-monitor
RP/0/0/CPU0:router(config-eoam-lm)# frame-period threshold low 100 high 600000
```

frame-period window

To configure the window size for an Ethernet OAM frame-period error event, use the **frame-period window** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the window size to the default value, use the **no** form of this command.

frame-period window *window*

no frame-period window *window*

Syntax Description

window	Size of the window for a frame-period error in milliseconds. The range is 100 to 60000.

Command Default

The default value is 1000.

Command Modes

Ethernet OAM link monitor configuration (config-eoam-lm)

Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the window size for a frame-period error.

```
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# link-monitor
RP/0/0/CPU0:router(config-eoam-lm)# frame-period window 60000
```

frame-seconds threshold

To configure the thresholds that trigger a frame-seconds error event, use the **frame-seconds threshold** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the threshold to the default value, use the **no** form of this command.

frame-seconds threshold low *threshold* [**high** *threshold*]

no frame-seconds threshold low *threshold* [**high** *threshold*]

Syntax Description

low *threshold*	Low threshold, in seconds, that triggers a frame-seconds error event. The range is 0 to 900.
high *threshold*	(Optional) High threshold, in seconds, that triggers a frame-seconds error event. The range is 1 to 900. The high threshold value can be configured only in conjunction with the low threshold value.

Command Default

The default value is 1.

Command Modes

Ethernet OAM link monitor configuration (config-eoam-lm)

Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

When the low threshold is passed, a frame-seconds error event notification is generated and transmitted to the OAM peer. Additionally, any registered higher level OAM protocols, such as Connectivity Fault Management (CFM), are also notified. When the high threshold is passed, the configured high threshold action is performed in addition to the low threshold actions. The high threshold is optional and is configurable only in conjunction with the low threshold.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the low and high thresholds that trigger a frame-seconds error event:

```
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# link-monitor (config-eoam)#  link-monitor
RP/0/0/CPU0:router(config-eoam-lm)# frame-seconds threshold low 10 high 900
```

Related Commands

Command	Description
ethernet oam profile, on page 199	Creates an EOAM profile and enters EOAM configuration mode.
link-monitor, on page 227	Enters Ethernet OAM link monitor configuration mode.

frame-seconds window

To configure the window size for the OAM frame-seconds error event, use the **frame-seconds window** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the window size to the default value, use the **no** form of this command.

frame-seconds window *window*

no frame-seconds window *window*

Syntax Description

window	Size of the window for a frame-seconds error in milliseconds. The range is 10000 to 900000.

Command Default

The default value is 60000.

Command Modes

Ethernet OAM link monitor configuration (config-eoam-lm)

Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the window size for a frame-seconds error.

```
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# link-monitor
RP/0/0/CPU0:router(config-eoam-lm)# frame-seconds window 900000
```

Related Commands

Command	Description
ethernet oam profile, on page 199	Creates an EOAM profile and enters EOAM configuration mode.

Command	Description
link-monitor, on page 227	Enters Ethernet OAM link monitor configuration mode.

frame threshold

To configure the thresholds that triggers an Ethernet OAM frame error event, use the **frame threshold** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the threshold to the default value, use the **no** form of this command.

frame threshold low *threshold* [**high** *threshold*]

no frame threshold low *threshold* [**high** *threshold*]

Syntax Description

low *threshold*	Low threshold, in symbols, that triggers a frame error event. The range is 0 to 12000000.
high *threshold*	(Optional) High threshold, in symbols, that triggers a frame error event. The range is 0 range is 0 to 12000000. The high threshold value can be configured only in conjunction with the low threshold value.

Command Default

The default low threshold is 1.

Command Modes

Ethernet OAM link monitor configuration (config-eoam-lm)

Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

When the low threshold is passed, a frame error event notification is generated and transmitted to the OAM peer. Additionally, any registered higher level OAM protocols, such as Connectivity Fault Management (CFM), are also notified. When the high threshold is passed, the configured high threshold action is performed in addition to the low threshold actions. The high threshold is optional and is configurable only in conjunction with the low threshold.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the low and high thresholds that trigger a frame error event:

```
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# link-monitor
RP/0/0/CPU0:router(config-eoam-lm)# frame threshold low 100 high 60000
```

Related Commands

Command	Description
ethernet oam profile, on page 199	Creates an EOAM profile and enters EOAM configuration mode.
link-monitor, on page 227	Enters Ethernet OAM link monitor configuration mode.

frame window

To configure the frame window size of an OAM frame error event, use the **frame window** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the window size to the default value, use the **no** form of this command.

frame window *window*

no frame window *window*

Syntax Description

window	Size of the window for a frame error in seconds. The range is 1000 to 60000.

Command Default

The default value is 1000.

Command Modes

Ethernet OAM link monitor configuration (config-eoam-lm)

Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the window size for a frame error.

```
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# link-monitor
RP/0/0/CPU0:router(config-eoam-lm)# frame window 60
```

Related Commands

Command	Description
ethernet oam profile, on page 199	Creates an EOAM profile and enters EOAM configuration mode.
link-monitor, on page 227	Enters Ethernet OAM link monitor configuration mode.

hello-interval

To specify the time interval between hello packets for an Ethernet OAM session, use the **hello-interval** command in Ethernet OAM or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of the command.

hello-interval {**100ms**| **1s**}

no hello-interval {**100ms**| **1s**}

Syntax Description

100ms	Specifies a 100-millisecond interval between hello packets.
1s	(Interface Ethernet OAM configuration mode only) Specifies a 1-second interval between hello packets. This is the default.

Command Default

The default is 1 second.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

If a profile exists on the interface, setting the mode with this command overrides the mode setting in the profile on an interface.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to set the hello interval to 100 milliseconds on a Gigabit Ethernet interface:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/5/6
RP/0/0/CPU0:router(config-if)# ethernet oam
RP/0/0/CPU0:router(config-if-eoam)# profile Profile_1
RP/0/0/CPU0:router(config-if-eoam)# hello-interval 100ms
```

Related Commands

Command	Description
ethernet oam profile, on page 199	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 198	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 257	Attaches an Ethernet OAM profile to an interface.
show ethernet oam configuration, on page 307	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam interfaces, on page 314	Displays the current state of Ethernet OAM interfaces.

link-monitor

To enter Ethernet OAM link monitor configuration mode, use the **link-monitor** command in Ethernet OAM configuration mode. To enter interface Ethernet OAM link monitor configuration mode, use the **link-monitor** command in interface Ethernet OAM configuration mode.

link-monitor

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

This example shows how to enter the Ethernet OAM link monitor configuration mode.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# link-monitor
RP/0/0/CPU0:router(config-eoam-lm)#
```

The following example shows how to enter the link monitor configuration mode from interface Ethernet OAM configuration mode.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/5/6
RP/0/0/CPU0:router(config-if)# ethernet oam
RP/0/0/CPU0:router(config-if-eoam)# link-monitor
```

log ais

To configure AIS logging for a Connectivity Fault Management (CFM) domain service to indicate when AIS or LCK packets are received, use the **log ais** command in CFM domain service configuration mode. To disable AIS logging, use the no form of this command.

log ais

no log ais

Syntax Description

This command has no keywords or arguments.

Command Default

Logging is disabled.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure AIS logging for a Connectivity Fault Management (CFM) domain service to indicate when AIS or LCK packets are received:

log continuity-check errors

To enable logging of continuity-check errors, use the **log continuity-check errors** command in CFM domain service configuration mode. To disable logging of continuity-check errors, use the no form of this command.

log continuity-check errors

no log continuity-check errors

Syntax Description

This command has no keywords or arguments.

Command Default

Logging is disabled.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

The following types of continuity-check errors are logged:

- Incorrect level (cross-connect)
- Incorrect interval
- Incorrect MA-ID (cross-connect)
- Local MAC address received (loop)
- Local MEP-ID received (mis-config)
- Invalid source MAC received
- RDI received

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enable logging of continuity check errors:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet cfm
RP/0/0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
```

```
RP/0/0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/0/CPU0:router(config-cfm-dmn-svc)# log continuity-check errors
```

log continuity-check mep changes

To enable logging of peer maintenance-end-point (MEP) state changes, use the **log continuity-check mep changes** command in CFM domain service configuration mode. To disable logging of peer MEP state changes, use the no form of this command.

log continuity-check mep changes

no log continuity-check mep changes

Syntax Description

This command has no keywords or arguments.

Command Default

Logging is disabled

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

This command enables logging of state changes that occur in MEPs for a particular service, such as:

- New peer MEP detected.
- Peer MEP time out (loss of continuity) detected.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enable logging of continuity-check mep changes:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet cfm
RP/0/0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/0/CPU0:router(config-cfm-dmn-svc)# log continuity-check mep changes
```

log crosscheck errors

To enable logging of crosscheck error events, use the **log crosscheck errors** command in CFM domain service configuration mode. To disable logging of crosscheck error events, use the no form of this command.

log crosscheck errors

no log crosscheck errors

Syntax Description

This command has no keywords or arguments.

Command Default

Logging is disabled.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

This command enables logging of crosscheck errors, such as:

- MEPs missing
- Additional peer MEPs detected

Note Crosscheck errors are only detected and logged when crosscheck is configured using the **mep crosscheck** and **mep-id** commands.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enable logging of crosscheck errors:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet cfm
RP/0/0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/0/CPU0:router(config-cfm-dmn-svc)# log crosscheck errors
```

Related Commands

Command	Description
mep crosscheck, on page 237	Enters CFM MEP crosscheck configuration mode.
mep-id, on page 238	Enables crosscheck on a MEP.

log efd

To enable logging of Ethernet Fault Detection (EFD) state changes to an interface (such as when an interface is shut down or brought up via EFD), use the **log efd** command in CFM domain service configuration mode. To disable EFD logging, use the no form of this command.

log efd

no log efd

Syntax Description

This command has no keywords or arguments.

Command Default

EFD logging is disabled.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

When EFD logging is enabled, a syslog is generated whenever the EFD state of an interface changes.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enable EFD logging:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet cfm
RP/0/0/CPU0:router(config-cfm)# domain D1 level 1
RP/0/0/CPU0:router(config-cfm-dmn)# service S1 down-meps
RP/0/0/CPU0:router(config-cfm-dmn-svc)# log efd
```

Related Commands

Command	Description
efd, on page 192	Enables EFD on all down MEPs in a down MEPs service.
show efd interface, on page 273	Displays all interfaces that are shut down because of EFD.

maximum-meps

To configure the maximum number of maintenance end points (MEPs) for a service, use the **maximum-meps** command in CFM domain service configuration mode. To return to the default value, use the no form of this command.

maximum-meps *number*

Syntax Description

number	Maximum number of MEPs allowed for this service. The range is 2 to 8190.

Command Default

The default is 100.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

This command configures the maximum number of peer maintenance end points (MEPs). It does not limit the number of local MEPs. The configured **maximum-meps** *number* must be at least as great as the number of configured crosscheck MEPs.

The **maximum-meps** *number* limits the number of peer MEPs, for which local MEPs store continuity-check messages (CCMs). When the limit is reached, CCMs from any new peer MEPs are ignored, but CCMs from existing peer MEPs continue to be processed normally.

The **maximum-meps** *number* also limits the size of the CCM learning database.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the maximum number of maintenance end points (MEPs) for a service:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet cfm
RP/0/0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
```

```
RP/0/0/CPU0:router(config-cfm-dmn-svc)# maximum-meps 4000
```

Related Commands

Command	Description
domain, on page 190	
ethernet cfm (global), on page 194	Enters CFM configuration mode.
ethernet cfm (interface), on page 196	Enters interface CFM configuration mode.
service, on page 270	
show ethernet cfm configuration-errors, on page 277	Displays information about errors that are preventing configured CFM operations from becoming active, as well as any warnings that have occurred.
show ethernet cfm local maintenance-points, on page 284	Displays a list of local maintenance points.
show ethernet cfm local meps, on page 287	Displays information about local MEPs.
show ethernet cfm peer meps, on page 293	Displays information about maintenance end points (MEPs) for peer MEPs.

mep crosscheck

To enter CFM MEP crosscheck configuration mode, use the **mep crosscheck** command in CFM domain service configuration mode.

mep crosscheck

Syntax Description

This command has no keywords or arguments.

Command Default

Not configured, in which case no crosscheck is performed on the MEP.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enter CFM MEP crosscheck configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet cfm
RP/0/0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/0/CPU0:router(config-cfm-dmn-svc)# mep crosscheck
RP/0/0/CPU0:router(config-cfm-xcheck)#
```

mep-id

To enable crosscheck on a maintenance end point (MEP), use the **mep-id** command in CFM MEP crosscheck configuration mode. To disable crosscheck on a MEP, use the **no** form of this command.

mep-id *mep-id-number* [**mac-address** *mac-address*]

no mep-id *mep-id-number* [**mac-address** *mac-address*]

Syntax Description

mac *mac-address*	(Optional) MAC address of the interface upon which the MEP resides, in standard hexadecimal format, hh:hh:hh:hh:hh:hh.

Command Default

Not configured, in which case no crosscheck is performed on the MEP.

Command Modes

CFM MEP crosscheck configuration (config-cfm-xcheck)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

This command enables Crosscheck on the maintenance end point (MEP) specified by the MEP ID number (*mep-id-number*). The range for MEP ID numbers is 1 to 8191. Crosscheck is enabled when the first crosscheck MEP is entered.

Repeat this command for every MEP that you want to include in the expected set of MEPs for crosscheck.

Crosscheck detects the following two additional defects for continuity-check messages (CCMs) on peer MEPs:

- Peer MEP missing—A crosscheck MEP is configured, but has no corresponding peer MEP from which to receive CCMs.
- Peer MEP unexpected—A peer MEP is sending CCMs, but no crosscheck MEP is configured for it.

Note If more than one local MEP is configured for a service, all the local MEPs must be included in the list of configured crosscheck MEPs.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to statically define a maintenance end point (MEP) under a service, so that it can be crosschecked.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet cfm
RP/0/0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/0/CPU0:router(config-cfm-dmn-svc)# mep crosscheck
RP/0/0/CPU0:router(config-cfm-xcheck)# mep-id 10
```

mep domain

To create a maintenance end point (MEP) on an interface, use the **mep domain** command in interface CFM configuration mode. To remove the MEP from the interface, use the **no** form of this command.

mep domain *domain-name* **service** *service-name* **mep-id** *id-number*

no mep domain *domain-name* **service** *service-name* **mep-id** *id-number*

Syntax Description

domain *domain-name*	Domain in which to create the maintenance end point (MEP).
service *service-name*	Operation service in which to create the maintenance end point (MEP).
mep-id *id-number*	Maintenance end points (MEP) identifier to assign to this MEP. The range is 1 to 8191.

Command Default

No MEPs are configured on the interface.

Command Modes

Interface CFM configuration (config-if-cfm)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

CFM Maintenance end points (MEPs) are supported on all Ethernet interfaces and VLAN subinterfaces.

This command creates MEPs in the UP MEP state, unless the specified **service** is configured with MEPs in the DOWN MEP state. See the service, on page 270 command.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to create a MEP using an ID of 1 on the CFM domain named DM1 and service named Sv1:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/1
RP/0/0/CPU0:router(config-if)# ethernet cfm
```

```
RP/0/0/CPU0:router(config-if-cfm)# mep domain Dm1 service Sv1 mep-id 1
```

Related Commands

Command	Description
ethernet cfm (interface), on page 196	Enters interface CFM configuration mode.
show ethernet cfm configuration-errors, on page 277	Displays information about errors that are preventing configured CFM operations from becoming active, as well as any warnings that have occurred.

mib-retrieval

To enable MIB retrieval in an Ethernet OAM profile or on an Ethernet OAM interface, use the **mib-retrieval** command in Ethernet OAM or interface Ethernet OAM configuration mode. To return the interface to the default (disabled), use the **disable** keyword.

mib-retrieval [disable]

Syntax Description

disable	Disables MIB retrieval the Ethernet OAM interface.

Command Default

MIB retrieval is disabled by default.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

When MIB retrieval is enabled on an Ethernet OAM interface, the OAM client advertises support for MIB retrieval to the peer.

When MIB retrieval is disabled (the default), only the enable form of the **mib-retrieval** command is available in interface Ethernet OAM configuration mode. The **disable** keyword is provided to override the profile when needed.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enable MIB retrieval on a Gigabit Ethernet interface:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/5/6
RP/0/0/CPU0:router(config-if)# ethernet oam
RP/0/0/CPU0:router(config-if-eoam)# mib-retrieval
```

Related Commands

Command	Description
ethernet oam profile, on page 199	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 198	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 257	Attaches an Ethernet OAM profile to an interface.
show ethernet oam configuration, on page 307	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam interfaces, on page 314	Displays the current state of Ethernet OAM interfaces.

mip auto-create

To enable the automatic creation of Maintenance Intermediate Points (MIPs) in a cross-connect, use the **mip auto-create** command in CFM domain service configuration mode. To disable automatic creation of MIPs, use the **no** form of this command.

mip auto-create {**all**| **lower-mep-only**}{}

no mip auto-create {**all**| **lower-mep-only**}

Syntax Description

all	Enables automatic creation of MIPs on all interfaces.
lower-mep-only	[Optional] Enables automatic creation of MIPs only on interfaces with a MEP at a lower level.

Command Default

None

Command Modes

CFM domain service configuration (config-cfm-dmn-svc) mode

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

The MIP auto-creation feature is configured only for services associated with cross-connects.

Unlike MEPs, MIPs are not explicitly configured on each interface. MIPs are created automatically according to the algorithm specified in the CFM 802.1ag standard. For each interface, the algorithm, in brief, operates in this manner:

- The cross-connect for the interface is found, and all services associated with that cross-connect are considered for MIP auto-creation.
- The level of the highest-level MEP on the interface is found. From among the services considered above, the service in the domain with the lowest level that is higher than the highest MEP level is selected. If there are no MEPs on the interface, the service in the domain with the lowest level is selected.
- The MIP auto-creation configuration for the selected service is examined to determine whether a MIP should be created.

Note Configuring a MIP auto-creation policy for a service does not guarantee that a MIP will automatically be created for that service. The policy is only considered if that service is first selected by the algorithm.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

This example shows how to enable the automatic creation of MIPs for all interfaces in a cross-connect:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet cfm
RP/0/0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/0/CPU0:router(config-cfm-dmn-svc)# mip auto-create all
```

Related Commands

Command	Description
domain, on page 190	
ethernet cfm (global), on page 194	Enters CFM configuration mode.
service, on page 270	
show ethernet cfm configuration-errors, on page 277	Displays information about errors that are preventing configured CFM operations from becoming active, as well as any warnings that have occurred.
show ethernet cfm local maintenance-points, on page 284	Displays a list of local maintenance points.
show ethernet cfm local meps, on page 287	Displays information about local MEPs.
show ethernet cfm peer meps, on page 293	Displays information about maintenance end points (MEPs) for peer MEPs.

mode (Ethernet OAM)

To configure the Ethernet OAM mode on an interface, use the **mode** command in Ethernet OAM or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of the command.

mode {**active**| **passive**}

Syntax Description

passive	Specifies that the interface operates in passive mode, where it cannot initiate the discovery process, generate a retrieval PDU, or request loopback.
active	(Interface Ethernet OAM configuration only) Specifies that the interface operates in active mode to initiate processes and make requests.

Command Default

The default is active.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

If a profile exists on the interface, setting the mode with this command overrides the mode setting in the profile on an interface.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enable Ethernet OAM passive mode on a Gigabit Ethernet interface:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/5/6
RP/0/0/CPU0:router(config-if)# ethernet oam
RP/0/0/CPU0:router(config-if-eoam)# profile Profile_1
RP/0/0/CPU0:router(config-if-eoam)# mode passive
```

Related Commands

Command	Description
ethernet oam profile, on page 199	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 198	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 257	Attaches an Ethernet OAM profile to an interface.
show ethernet oam configuration, on page 307	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam interfaces, on page 314	Displays the current state of Ethernet OAM interfaces.

monitoring

To enable Ethernet OAM link monitoring, use the **monitoring** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return link monitoring to its default state of enabled, use the **no** form of this command.

monitoring [disable]

no monitoring [disable]

Syntax Description

disable	(Optional) Disables Ethernet OAM link monitoring.

Note When configuring on a profile, only the **monitoring disable** form of the command is supported.

Command Default

Link monitoring is enabled by default.

Command Modes

Ethernet OAM link monitor configuration (config-eoam-lm)

Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Monitoring is enabled by default. To disable it either on a profile or an interface, use the **monitoring disable** form of the command.

If monitoring is disabled on a profile, but you want to override the configuration and enable it for an interface, use the **monitoring** command in interface Ethernet OAM link monitor configuration mode.

You cannot configure the **monitoring** command without the **disable** keyword on a profile.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to disable link-monitoring on an Ethernet OAM interface:

```
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# link-monitor
```

```
RP/0/0/CPU0:router(config-eoam-lm)# monitoring disable
```

Related Commands

Command	Description
ethernet oam profile, on page 199	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 198	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
link-monitor, on page 227	Enters Ethernet OAM link monitor configuration mode.
profile (EOAM), on page 257	Attaches an Ethernet OAM profile to an interface.
show ethernet oam configuration, on page 307	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam statistics, on page 317	Displays the local and remote Ethernet OAM statistics for interfaces.
show ethernet oam interfaces, on page 314	Displays the current state of Ethernet OAM interfaces.

packet size

To configure the minimum size (in bytes) for outgoing probe packets, including padding when necessary, use the **packet size** command in SLA profile probe configuration mode. To remove this configuration, use the no form of this command.

packet size *bytes* [**test pattern** {**hex 0x** *HHHHHHHH*| **pseudo-random**}]

no packet size *bytes* [**test pattern** {**hex 0x** *HHHHHHHH*| **pseudo-random**}]

Syntax Description

bytes	Minimum size of the packet including padding when necessary. The range is 1 to 9000 bytes. This value is the total frame size including the Layer 2 or Layer 3 packet header.
test pattern hex 0x *HHHHHHHH*	(Optional) Specifies a 4-byte string (8 hexadecimal characters) to repeat as many times as required to fill the outgoing probe packet to the specified minimum packet size. The default is all 0s.
test pattern pseudo-random	(Optional) Specifies a pseudo-random bit sequence determined by the protocol to fill the outgoing probe packet to the specified minimum packet size.

Command Default

The minimum packet size is not configured. When a minimum packet size is configured and padding is required, the default padding is all 0s.

Command Modes

SLA profile probe configuration (config-sla-prof-pb)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

For supported packet types, this configuration determines the minimum size of all outgoing SLA probe packets, including the size to which they are padded. The amount of padding that is added to a packet depends on the type of frame that is sent and the amount of data in the frame.

When the packet size is not configured, packets are sent at the minimum size required to fit all the required information. Even when the packet size is configured, the packets may be larger than the configured size if the required information exceeds the configured value.

Note If a probe packet is too large, it may get dropped somewhere in the network.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the minimum size of outgoing probe packets using default padding of all 0s as needed:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet sla
RP/0/0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/0/CPU0:router(config-sla-prof)# probe
RP/0/0/CPU0:router(config-sla-prof-pb)# packet size 9000
RP/0/0/CPU0:router(config-sla-prof-pb)# commit
```

The following example shows how to configure a hexadecimal test pattern to pad packets with to reach the minimum packet size:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet sla
RP/0/0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/0/CPU0:router(config-sla-prof)# probe
RP/0/0/CPU0:router(config-sla-prof-pb)# packet size 9000 test pattern hex 0xabcdabcd
RP/0/0/CPU0:router(config-sla-prof-pb)# commit
```

ping ethernet cfm

To send Ethernet connectivity fault management (CFM) loopback messages to a maintenance end point (MEP) or MAC address destination from the specified source MEP, and display a summary of the responses, use the **ping ethernet cfm** command in EXEC mode.

ping ethernet cfm domain *domain-name* **service** *service-name* {**mac-address** *mac*| **mep-id** *id*} **source** [**mep-id** *source-id*] **interface** *interface-path-id* [**cos** *cos-val*] [**count** *n*] [**frame-size** *size*] [**data-pattern** *hex*] [**interval** *seconds*] [**timeout** *time*]

Syntax Description

domain *domain-name*	String of a maximum of 80 characters that identifies the domain in which the maintenance points reside. **Note** For more information about the syntax, use the question mark (**?**) online help function.
service *service-name*	String of a maximum of 80 characters that identifies the maintenance association to which the maintenance points belong.
mac-address *mac*	6-byte ID number of the MAC address of the destination MEP.
mep-id *id*	Maintenance end point (MEP) ID number of the destination MEP. The range for MEP ID numbers is 1 to 8191.
source	Source information.
mep-id *source-id*	(Optional) Maintenance end point (MEP) ID number of the source MEP. The range for MEP ID numbers is 1 to 8191.
interface *interface-path-id*	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
cos *cos-val*	(Optional) Class of Service (CoS) value that identifies the class of traffic of the source MEP. The valid values are from 0 to 7.
count *n*	(Optional) Number of pings as an integer value. The default is 5.
frame-size *size*	(Optional) Size, as an integer, of the ping frames. Frames are padded to reach the specified size. The default is 0 (no padding).
data-pattern *hex*	(Optional) Hexadecimal value to be used as the data pattern for padding within a ping frame, when padding is required due to the **frame-size** configuration. The default is 0.
interval *seconds*	(Optional) Specifies, in seconds, the time between pings. The *n* argument is entered in seconds. The default is 1 second.

timeout *time*	(Optional) Timeout, in seconds, for the ping packet. The default is 2.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Before you can use this command, a local MEP must be configured for the domain and the interface.

The command displays the following infomation:

- Number of loopback message being sent
- Timeout period
- Domain name
- Domain level
- Service name
- Source MEP ID
- Interface
- Target MAC address
- MEP ID – If no MEP ID is specified, "No MEP ID specified" is displayed.
- Running time for the current ping operation to complete

Note The remaining information is not displayed until the current ping operation is complete. If the user interrupts the operation during this time (by pressing control-C), the prompt is returned and no further information is displayed. However, all loopback messages continue to be sent.

- Success rate of responses received – displayed as a percentage followed by the actual number of responses
- The round trip time minimum/maximum/average in milliseconds
- Out-of-sequence responses – displayed as a percentage followed by the actual number of out-of-sequence responses when at least one response is received. An out-of-sequence response occurs if the first response does not correspond with the first message sent, or a subsequent response is not the expected next response after a previously received response.
- Bad data responses – displayed as a percentage followed by the actual number of bad data responses when at least one response is received. A bad data response occurs if the padding data in the response does not match the padding data that in the sent message. This can only happen if the sent message is padded using the **frame-size** option.

- Received packet rate – displayed in packets per second when at least two responses are received. This approximate rate of response is the time between the first response received and the last response received, divided by the total number of responses received.

Task ID

Task ID	Operations
basic-services	execute
ethernet-services	execute

Examples

The following example shows how to send an Ethernet CFM loopback message:

```
RP/0/0/CPU0:router# ping ethernet cfm domain D1 service S1 mep-id 16 source
interface GigabitEthernet 0/0/0/0

Type escape sequence to abort.
Sending 5 CFM Loopbacks, timeout is 2 seconds -
Domain foo (level 2), Service foo
Source: MEP ID 1, interface GigabitEthernet0/0/0/0
Target: 0001.0002.0003 (MEP ID 16):
  Running (5s) ...
Success rate is 60.0 percent (3/5), round-trip min/avg/max = 1251/1349/1402 ms
Out-of-sequence: 0.0 percent (0/3)
Bad data: 0.0 percent (0/3)
Received packet rate: 1.4 pps
```

priority (SLA)

To configure the priority of outgoing SLA probe packets, use the **priority** command in SLA profile probe configuration mode. To return the priority to the default value, use the no form of this command.

priority *priority*

no priority *priority*

Syntax Description

priority	Priority level. The range is 0 to 7.

Command Default

When the priority is not configured by SLA, the default is the Class of Service (CoS) priority for the egress interface.

Command Modes

SLA profile probe configuration (config-sla-prof-pb)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

The default priority for all CFM operation types is the Class of Service (CoS) priority for the egress interface. SLA operations that are configured on Maintenance End Points (MEPs) do not use the Class of Service (CoS) settings that are configured independently on Maintenance End Points (MEPs). Use this command to change the priority level of SLA probe packets.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the priority of outgoing SLA probe packets.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet sla
RP/0/0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/0/CPU0:router(config-sla-prof)# probe
RP/0/0/CPU0:router(config-sla-prof-pb)# priority 7
```

probe

To enter SLA profile probe configuration mode, use the **probe** command in SLA profile configuration mode. To exit to the previous mode, use the no form of this command.

probe

no probe

Syntax Description

This command has no keywords or arguments.

Command Default

If no items are configured in the probe mode, all items in the probe mode use their default values.

Command Modes

SLA profile configuration (config-sla-prof)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

Each profile may optionally have 1 probe submode.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enter the SLA profile probe configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet sla
RP/0/0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/0/CPU0:router(config-sla-prof)# probe
RP/0/0/CPU0:router(config-sla-prof-pb)#
```

profile (EOAM)

To attach an Ethernet OAM profile to an interface, use the **profile** command in interface Ethernet OAM configuration mode. To remove the profile from the interface, use the no form of this command.

profile *name*

no profile *name*

Syntax Description

name	Text name of the Ethernet OAM profile to attach to the interface.

Command Default

No profile is attached.

Command Modes

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

When an Ethernet OAM profile is attached to an interface using this command, all of the parameters configured for the profile are applied to the interface.

Individual parameters that are set by the profile configuration can be overridden by configuring them directly on the interface.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to attach an Ethernet OAM profile to a Gigabit Ethernet interface.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/5/6
RP/0/0/CPU0:router(config-if)# ethernet oam
RP/0/0/CPU0:router(config-if-eoam)# profile Profile_1
```

Related Commands

Command	Description
ethernet oam profile, on page 199	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 198	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
show ethernet oam configuration, on page 307	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam interfaces, on page 314	Displays the current state of Ethernet OAM interfaces.

profile (SLA)

To create an SLA operation profile and enter the SLA profile configuration mode, use the **profile** command in SLA configuration mode. To remove the profile, use the **no** form of this command.

profile *profile-name* **type** {{**cfm-delay-measurement**}| **cfm-loopback**}

no profile *profile-name*

Syntax Description

profile-name	Profile name, case-sensitive string up to 31 characters in length. The name “all” cannot be used.
type	Specifies the type of packets sent by operations in this profile. Valid types are: • **cfm-delay-measurement**: CFM delay measurement packets • **cfm-loopback**: CFM loopback packets

Command Default

No default behavior or values

Command Modes

Ethernet SLA configuration (config-sla)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelin

Note Each profile is uniquely identified by its name. Changing the packet **type** for the profile removes all stored data from the profile and is equivalent to deleting the profile and creating a new profile.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

This example shows how to configure an SLA operation profile and enter the SLA profile configuration mode:

```
RP/0/0/CPU0:router# configure
```

```
RP/0/0/CPU0:router(config)# ethernet sla
RP/0/0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/0/CPU0:router(config-sla-prof)#
```

require-remote

To require that certain features are enabled before an OAM session can become active, or to disable a requirement that is part of an active OAM profile, use the **require-remote** command in Ethernet OAM configuration or interface Ethernet OAM configuration mode. To remove the configuration and return to the default, use the **no** form of this command.

require-remote {**mode** {**active**| **passive**}| **mib-retrieval**| **link-monitoring [disabled]**}

no require-remote {**mode** {**active**| **passive**}| **mib-retrieval**| **link-monitoring [disabled]**}

Syntax Description

mode {**active** | **passive**}	Requires that active or passive mode is configured on the peer device before the OAM profile can become active.
mib-retrieval	Requires that MIB-retrieval is configured on the peer device before the OAM profile can become active.
link-monitoring	Requires that link-monitoring feature is configured on the peer device before the OAM profile can become active.
disabled	(Optional—Interface Ethernet OAM configuration only) Overrides the Ethernet OAM profile configuration for this option and disables the feature at the specified interface.

Command Default

No default behavior or values

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

The **disabled** keyword is available only when you are configuring Ethernet OAM on an interface, and is used to override the configuration that is part of an active OAM profile.

The **disabled** keyword does not remove the configuration of the command. Use the **no** form of this command to do that.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to require that specific features are enabled before an OAM session can become active

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/0/CPU0:router(config-eoam)# require-remote mode active
RP/0/0/CPU0:router(config-eoam)# require-remote mib-retrieval
RP/0/0/CPU0:router(config-eoam)# require-remote link-monitoring
```

The following example shows how to disable requirements on a particular interface that is part of an active OAM profile:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/6/5/0
RP/0/0/CPU0:router(config-if)# ethernet oam
RP/0/0/CPU0:router(config-if-eoam)# require-remote mode active disabled
RP/0/0/CPU0:router(config-if-eoam)# require-remote mib-retrieval disabled
RP/0/0/CPU0:router(config-if-eoam)# require-remote link-monitoring disabled
```

Related Commands

Command	Description
ethernet oam profile, on page 199	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 198	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 257	Attaches an Ethernet OAM profile to an interface.
action capabilities-conflict, on page 129	Configures what action is taken on an interface when a capabilities-conflict event occurs.
show ethernet oam configuration, on page 307	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam discovery, on page 310	Displays the current status of Ethernet OAM sessions.
show ethernet oam interfaces, on page 314	Displays the current state of Ethernet OAM interfaces.

schedule (SLA)

To schedule an operation probe in a profile, use the **schedule** command in SLA profile configuration mode. To disable a schedule, use the **no** form of this command.

Hourly Scheduling

schedule every number {**hours**| **minutes**} [**first at hh:mm**[**:ss**]] [**for duration** {**seconds**| **minutes**| **hours**}]

no schedule every number {**hours**| **minutes**} [**first at hh:mm**[**:ss**]] [**for duration** {**seconds**| **minutes**| **hours**}]

Daily Scheduling

schedule every day [**at hh:mm**] [**for duration** {**seconds**| **minutes**| **hours**| **days**}]

no schedule every day [**at hh:mm**] [**for duration** {**seconds**| **minutes**| **hours**| **days**}]

Weekly Scheduling

schedule every week on day [**at hh:mm**] [**for duration** {**seconds**| **minutes**| **hours**| **days**| **week**}]

no schedule every week on day [**at hh:mm**] [**for duration** {**seconds**| **minutes**| **hours**| **days**| **week**}]

Syntax Description

every week on *day* [**at** *hh:mm*][**f** or *duration* {**seconds** | **minutes** | **hours** | **days** | **week**}]	Schedules a probe one day per week, on the specified *day*, at the specified time (*hh:mm*), for the specified *duration*.
every day [**at** *hh:mm*][**f** or *duration* {**seconds** | **minutes** | **hours** | **days**}	Schedules a probe every day, at the specified time (*hh:mm*), for the specified *duration*.
every *number* {**hours** | **minutes**} **first at** *hh:mm*[*.ss*]	Schedules a probe every specified *number* of **hours** or **minutes**, starting at the specified time after midnight (*hh:mm*[*.ss*]).
every *number* {**hours** | **minutes**} [**f** or *duration* {**seconds** | **minutes** | **hours**}]	Schedules a probe every specified *number* of **hours** or **minutes**, for the specified *duration*.

day	Day of the week. Valid values are: • Monday • Tuesday • Wednesday • Thursday • Friday • Saturday • Sunday
hh:mm hh:mm[*:s s*]	Time of day in 24 hour time: • *hh:mm* = hour:minutesexample: 22:30 • *hh:mm:ss* = hour:minutes:seconds example: 12:30:10(seconds are optional)
duration	Duration of probe. The ranges are : • 1 to 3600 seconds • 1 to 1440 minutes • 1 to 24 hours • 1 day • 1 week
number	Number of **hours** or **minutes**. • Valid values for hours are the factors of 24: 1, 2, 3, 4, 6, 8, 12 • Valid values for minutes are the factors of 1440 (up to 90): 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 30, 32, 36, 40, 45, 48, 60, 80, 90

Command Default

The default is every hour. If the **at** keyword is not specified, the start time of each operation is distributed uniformly within the duration of the probe. If the **for** keyword is not specified, only one single burst is sent.

Command Modes

SLA profile configuration (config-sla-prof)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

Schedules are optional, but a profile may contain only one schedule.

Note Any change to a schedule causes all stored data for that operation to be deleted.

Changing a schedule is equivalent to deleting an operation and creating a new operation.

The **for** *duration* option must be specified if (and only if) the probe is configured to send multiple packets (or bursts of packets), using the **send packet every** or **send burst every** configuration of the **send (SLA)** command. If the **send (SLA)** command is not configured for the probe, or if **send burst once** is configured, the **for** *duration* option must not be used. If it is used in those cases, an error is returned.

The **for** *duration* option must not exceed the **schedule every** {**week | day | number**} option.

When the "**first at** *hh*:*hh*[:*ss*]" option is used, the configured time is used to calculate an offset after midnight when the first probe should be sent each day. The offset is calculated by taking the configured time plus the interval. Thus, probes may be sent before the configured time.

For example, if you configure "**schedule every 6 hours first at 11:15**," then the offset after midnight will be 5:15 (11:15 plus 6:00) and probes will be sent each day at 05:15, 11:15, 17:15 and 23:15.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following examples show how to schedule operation probes in a profile:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet sla
RP/0/0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/0/CPU0:router(config-sla-prof)# schedule every week on Monday at 23:30 for 1 hour


RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet sla
RP/0/0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/0/CPU0:router(config-sla-prof)# schedule every day at 11:30 for 5 minutes


RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet sla
RP/0/0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/0/CPU0:router(config-sla-prof)# schedule every 2 hours first at 13:45:01


RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet sla
RP/0/0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/0/CPU0:router(config-sla-prof)# schedule every 6 hours for 2 hours
```

Related Commands

Command	Description
send (SLA), on page 267	Configures the number and timing of packets sent by a probe in an operations profile.

send (SLA)

To configure the number and timing of packets sent by a probe in an operations profile, use the **send** command in SLA profile probe configuration mode. To return to the default, use the **no** form of the command.

send burst {**every** *number* {**seconds**| **minutes**| **hours**}| **once**} **packet count** *packets* **interval** *number* {**seconds**| **milliseconds**}

no send burst {**every** *number* {**seconds**| **minutes**| **hours**}| **once**} **packet count** *packets* **interval** *number* {**seconds**| **milliseconds**}

send packet {**every** *number* {**milliseconds**| **seconds**| **minutes**| **hours**}| **once**}

no send packet {**every** *number* {**milliseconds**| **seconds**| **minutes**| **hours**}| **once**}

Syntax Description

burst every *number* {**seconds** | **minutes** | **hours**}	Sends a burst of packets every specified number of seconds, minutes, or hours, where *number* is in the following range: • 1–3600 **seconds** • 1–1440 **minutes** • 1–168 **hours**
burst once	Sends a single burst one time.
packet count *packets*	Specifies the number of *packets* in each burst. The range is 2 to 600.
interval *number* {**seconds** | **milliseconds**}	Specifies the time interval (in seconds or milliseconds) between each packet in a burst, where *number* is in the following range: • 1–30 **seconds** • 50–30000 **milliseconds**
packet every *number* {**milliseconds** | **seconds** | **minutes** | **hours**}	Sends one packet every specified number of milliseconds, seconds, minutes, or hours, where *number* is in the following range: • 1–3600 **seconds** • 1–1440 **minutes** • 1–168 **hours** • 50–10000 **milliseconds**
packet once	Sends a single packet one time.

Command Default

If the operation is configured to measure jitter or data packet loss, the default is to send a single burst of 2 packets with a second interval between the packets.

If the operation is configured to measure synthetic packet loss, the default is to send a single burst of 10 packets with a 100 millisecond interval between the packets.

If the operation does not calculate jitter, data, or synthetic packet loss, the default is to send a single packet one time.

Command Modes

SLA profile probe configuration (config-sla-prof-pb)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelin

Note The total length of a burst is the packet count multiplied by the interval and must not exceed 1 minute.

The minimum **interval** supported is platform and packet-type dependent, so certain a configuration may cause an error even if it falls within the specified limits. In the case of Ethernet SLA, the shortest interval for packet types not used for synthetic loss measurement is 100ms.

When **burst once** is sent, a single burst is sent at the start of the probe. If the schedule defines a duration for the probe, a configuration warning is flagged. The same is true if the default is in effect.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

These examples show how to configure the types of packets sent by a probe in an operations profile:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet sla
RP/0/0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/0/CPU0:router(config-sla-prof)# probe
RP/0/0/CPU0:router(config-sla-prof-pb)# send burst every 60 seconds packet count 30 interval
 1 second
RP/0/0/CPU0:router(config-sla-prof-pb)#
```

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet sla
RP/0/0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/0/CPU0:router(config-sla-prof)# probe
RP/0/0/CPU0:router(config-sla-prof-pb)# send burst once packet count 2 interval 1 second
RP/0/0/CPU0:router(config-sla-prof-pb)#
```

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet sla
RP/0/0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/0/CPU0:router(config-sla-prof)# probe
```

```
RP/0/0/CPU0:router(config-sla-prof-pb)# send packet every 1 second
```

service

To associate a service with a domain and enter CFM domain service configuration mode, use the **service** command in CFM domain configuration mode. To remove a service from a domain, use the **no** form of this command.

service *service-name* {**down-meps**| **xconnect group** *xconnect-group-name* **p2p** *xconnect-name*} [**id** | [**string** *text*]| [**number** *number*]| [**vlan-id** *id-number*]| [**vpn-id** *oui-vpnid*]]

no service *service-name* {**down-meps**| **xconnect group** *xconnect-group-name* **p2p** *xconnect-name*} [**id** | [**string** *text*]| [**number** *number*]| [**vlan-id** *id-number*]| [**vpn-id** *oui-vpnid*]]

Syntax Description

service-name	Administrative name for the service. Case sensitive ASCII string up to 80 characters. Used in conjunction with one of the following service types: • **down-meps** • xconnect
down-meps	Specifies that all MEPs are down and no MIPs are permitted.
xconnect	Specifies the use of a cross connect. Used in conjunction with **group** and p2p. **Note** When **xconnect** is specified, all MEPs are up and MIPs are permitted.
group *xconnect-group-name*	Specifies the name of the cross connect group.
p2p *xconnect-name*	Specifies the name of the point-to-point cross connect and enters the Ethernet CFM domain service mode.
id	(Optional) Service identifier. Valid service identifiers are: • **number** *number*—Number from 0 to 65535. • **string** *text*—String length no longer than 46 minus MDID length. • **vlan-id** *id-number*—Number from 1 to 4094. • **vpn-id** *oui-vpnid* —VPN ID in RFC 2685 format (HHH:HHHH)

Command Default

If **id** is not specified, the service name is used as the Short MA name.

Command Modes

CFM domain configuration (config-cfm-dmn)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

The Short MA Name is the second part of the Maintenance Assoication Identifier (MAID) in CFM frames. If the Short MA Name (service id) is not specified, the service administrative name is used by default.

When configuring the **service** command, consider the following restrictions:

- The **bridge group** and **bridge-domain** keyword options appear in the software, but they are unsupported.
- The **service xconnect group p2p** form of the command is not supported for L2TPv3 cross-connect types. The following example shows a sample L2TPv3 configuration that is not supported when used with the **service xconnect group** command:

```
l2vpn
 pw-class l2tpv3_class2
  encapsulation l2tpv3
   protocol l2tpv3
   ipv4 source 10.110.110.110
!
!
 xconnect group 1
  p2p 1
   interface GigabitEthernet0/2/5/6.1
   neighbor 10.120.120.120 pw-id 1
    pw-class l2tpv3_class2
```

In this example, a corresponding CFM configuration of the **service xconnect group 1 p2p 1** command will not work.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to specify that all MEPs are down and no MIPs are permitted, and enter CFM domain service configuration mode.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet cfm
RP/0/0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/0/CPU0:router(config-cfm-dmn)# service Serv_1 down-meps
RP/0/0/CPU0:router(config-cfm-dmn-svc)#
```

The following example shows how to associate a cross connect service to a domain and enter CFM domain service configuration mode.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet cfm
RP/0/0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
```

```
RP/0/0/CPU0:router(config-cfm-dmn-svc)#
```

Related Commands

Command	Description
domain, on page 190	Creates and names a container for all domain configurations and enter the CFM domain configuration mode.
ethernet cfm (global), on page 194	Enters Ethernet CFM configuration mode.
p2p	Enters p2p configuration mode to configure point-to-point cross-connects.
show ethernet cfm configuration-errors, on page 277	Displays information about errors that are preventing configured cfm operations from becoming active, as well as any warnings that have occurred.
show ethernet cfm local maintenance-points, on page 284	Displays all the maintenance points that have been created.
show ethernet cfm local meps, on page 287	Displays information about local MEPs.
show ethernet cfm peer meps, on page 293	Displays other MEPs detected by a local MEP.
xconnect group	Configures a cross-connect group.

show efd interface

To display all interfaces that are shut down because of Ethernet Fault Detection (EFD), or to display whether a specific interface is shut down because of EFD, use the **show efd interface** command in EXEC mode.

show efd interface [*type interface-path-id*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

If no parameters are specified, all interfaces that are shut down because of EFD are displayed.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

If this command is issued when no EFD errors are detected, the system displays the following message:

```
< date time >
No matching interfaces with EFD-shutdown triggered
```

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to display all interfaces that are shut down because of Ethernet Fault Detection (EFD):

```
RP/0/0/CPU0:router# show efd interfaces
```

```
Server VLAN MA
==============
Interface          Clients
-------------------------
GigE0/0/0/0.0      CFM
```

Related Commands

Command	Description
efd, on page 192	Enables EFD on all down MEPs in a down MEPs service.
log efd, on page 234	Enables logging of EFD state changes to an interface (such as when an interface is shut down or brought up via EFD).

show ethernet cfm ccm-learning-database

To display the Continuity Check Message (CCM) learning database, use the **show ethernet cfm ccm-learning-database** command in EXEC configuration mode.

show ethernet cfm ccm-learning-database [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays the CFM CCM learning database for the designated node. The *node-id* argument is entered in the *rack*/*slot*/*module* notation.

Command Default

All CFM ccm-learning-databases on all interfaces are displayed.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

The CCM Learning Database is populated by MEPs and MIPs that have received continuity-check messages (CCMs). The information in the CCM Learning Database is used to reply to traceroutes when no applicable entries are found in the main MAC learning table.

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows how to display all the CFM CCM learning databases on all interfaces:

```
RP/0/0/CPU0:router# show ethernet cfm ccm-learning-database

Location 0/0/CPU0:

Domain/Level           Service              Source MAC     Interface
---------------------- -------------------- -------------- ------------------
foo/2                  foo                  0001.0203.0401 Gi0/0/0/0
foo/2                  foo                  0001.0203.0402 PW

Location 0/1/CPU0:

Domain/Level           Service              Source MAC     Interface
---------------------- -------------------- -------------- ------------------
```

```
foo/2                   foo                   0001.0203.0401 XC ID: 0xff000002
```

Table 13: show ethernet cfm ccm-learning-database Field Descriptions

Domain/Level	The domain name and the level of the domain for the maintenance point that received the CCM that caused this entry to be created. This entry will be used to respond to traceroute messages received by maintenance points in this domain.
Service	The name of the service for the maintenance point that received the CCM that caused this entry to be created. This entry will be used to respond to traceroute messages received by maintenance points in this domain.
Source MAC	Source MAC address in the CCM that caused this entry to be created. This entry will be used to respond to traceroute messages targeted at this MAC address.
Interface	The interface through which the CCM entered the router. This will be one of the following: • An interface or sub-interface name • A pseudowire identification (neighbor address and PW ID) • PW – Indicates the CCM was received through the PW in a cross-connect • XC ID – the internal cross-connect ID value, indicating that the CCM was received through an interface that no longer exists, or is no longer in L2 mode.

show ethernet cfm configuration-errors

To display information about errors that are preventing configured CFM operations from becoming active, as well as any warnings that have occurred, use the **show ethernet cfm configuration-errors** command in EXEC mode.

show ethernet cfm configuration-errors [**domain** *domain-name*] [**interface** *type interface-path-id*]

Syntax Description

domain *domain-name*	(Optional) Displays information about the specified CFM domain name.
interface *type*	(Optional) Displays information about the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

All CFM configuration errors on all domains are displayed.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read

Examples

```
RP/0/0/CPU0:router# show ethernet cfm configuration-errors

Domain fig (level 5), Service bay
 * MIP creation configured using bridge-domain blort, but bridge-domain blort does not
exist.
 * An Up MEP is configured for this domain on interface GigabitEthernet0/1/2/3.234 and an
Up MEP is also configured for domain blort, which is at the same level (5).
```

```
 * A MEP is configured on interface GigabitEthernet0/3/2/1.1 for this domain/service, which
 has CC interval 100ms, but the lowest interval supported on that interface is 1s.
```

The following example shows how to display all the CFM configuration errors on all domains:

```
RP/0/0/CPU0:router# show ethernet cfm configuration-errors

Domain fig (level 5), Service bay
 * An Up MEP is configured for this domain on interface GigabitEthernet0/1/2/3.234 and an
Up MEP is also configured for domain blort, which is at the same level (5).
 * A MEP is configured on interface GigabitEthernet0/3/2/1.1 for this domain/service, which
 has CC interval 100ms, but the lowest interval supported on that interface is 1s.
```

Related Commands

Command	Description
ethernet cfm (global), on page 194	Enters CFM configuration mode.
ethernet cfm (interface), on page 196	Enters interface CFM configuration mode.
traceroute ethernet cfm, on page 338	Sends Ethernet CFM traceroute messages to generate a basic.

show ethernet cfm interfaces ais

To display the information about interfaces that are currently transmitting Alarm Indication Signal (AIS), use the **show ethernet cfm interfaces ais** command in EXEC mode.

show ethernet cfm interfaces [*type interface-path-id*] **ais** [**location** *node-id*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location *node-id*	(Optional) Displays information about the node location specified as *rack* / *slot* / *module*. Location cannot be specified if you configure an interface type.

Command Default

If no parameters are specified, information for all AIS interfaces is displayed.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

Note The **location** keyword cannot be specified if an interface has been specified.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to display the information published in the Interface AIS table:

```
RP/0/0/CPU0:router# show ethernet cfm interfaces ais

Defects (from at least one peer MEP):
 A - AIS received                I - Wrong interval
 R - Remote Defect received      V - Wrong Level
 L - Loop (our MAC received)     T - Timed out (archived)
 C - Config (our ID received)    M - Missing (cross-check)
 X - Cross-connect (wrong MAID)  U - Unexpected (cross-check)
 P - Peer port down              D - Local port down

                                Trigger                  Transmission
                         AIS  ---------    Via    ----------------------------
Interface (State)        Dir  L Defects  Levels   L Int Last started  Packets
------------------------ ---  - -------  -------  - --- ------------ --------
Gi0/1/0/0.234 (Up)       Dn   5 RPC      6        7 1s  01:32:56 ago     5576
Gi0/1/0/0.567 (Up)       Up   0 M        2,3      5 1s  00:16:23 ago      983
Gi0/1/0/1.1 (Dn)         Up     D                7 60s 01:02:44 ago     3764
Gi0/1/0/2 (Up)           Dn   0 RX       1!
```

Table 14: show ethernet cfm interfaces ais Field Descriptions

Interface (State)	The name and state of the interface.
AIS dir	The direction that the AIS packets are transmitted, up or down.
Trigger L	The level of the lowest MEP that is transmitting AIS.The field is blank if there are no down MEPs on the interface, and AIS is being transmitted due to configuration on the interface itself.
Trigger Defects	Defects detected by the lowest MEP transmitting AIS.
Via Levels	The levels of any MEPs on the interface that are receiving AIS from a lower MEP, and potentially re-transmitting the signal. If the highest MEP is not re-transmitting the signal, the list of levels is ended using an exclamation point.
Transmission L	The level at which AIS is being transmitted outside of the interface, via a MIP. The field is blank if this is not occurring.
Transmission Int	The interval at which AIS is being transmitted outside of the interface via a MIP. The field is blank if this is not occurring.
Transmission last started	If AIS is being transmitted outside of the interface, the time that the signal started. The field is blank if this is not occurring.

Transmission packets	If AIS is being transmitted outside of the interface, the number of packets sent by the transmitting MEP since it was created or since its counters were last cleared. The field is blank if this is not occurring.

Related Commands

Command	Description
ais transmission, on page 151	Configures AIS transmission for a CFM domain service.
log ais, on page 228	Configures AIS logging for a CFM domain service to indicate when AIS or LCK packets are received.
ais transmission up, on page 153	Configures AIS transmission on a CFM interface.
show ethernet cfm local meps, on page 287	Displays information about local MEPs.

show ethernet cfm interfaces statistics

To display the per-interface counters for Ethernet Connectivity Fault Management (CFM), use the **show ethernet cfm interfaces statistics** command in EXEC mode.

show ethernet cfm interfaces [*type interface-path-id*] **statistics** [**location** *node-id*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location *node-id*	(Optional) Displays information about the node location specified as *rack* / *slot* / *module*. Location cannot be specified if you configure an interface type.

Command Default

All CFM counters from all interfaces are displayed.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelin

Note The location cannot be specified if a particular interface is specified.

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows all the CFM counters on all interfaces:

```
RP/0/0/CPU0:router# show ethernet cfm interfaces statistics
Location 0/1/CPU0:

Interface          Malformed   Dropped Last Malformed Reason
------------------ --------- --------- ---------------------
Gi0/1/0/3.185              0         0
Gi0/1/0/7.185              0         0
Gi0/1/0/7.187              0         0
```

Table 15: show ethernet cfm statistics Field Descriptions

Interface	Name of the interface.
Malformed	Number of packets that have been received at this interface that have been found to be non-compliant with the packet formats specified in IEEE 802.1ag and ITU-T Y.1731.
Dropped	Number of valid (well-formed) packets that have been received at this interface, that have been dropped in software. Packets may be dropped for the following reasons: • Packet has an unknown operation code, and reached a MEP. • Packet dropped at a MEP because it has a lower CFM level than the MEP. • Packet could not be forwarded because the interface is STP blocked. • Packet could not be forwarded because it is destined for this interface.
Last Malformed Reason	Operation code for the last malformed packet received, and the reason that it was found to be malformed. If no malformed packets have been received, this field is blank.

Related Commands

Command	Description
clear ethernet cfm interface statistics, on page 160	Clears the counters for an Ethernet CFM interface.

show ethernet cfm local maintenance-points

To display a list of local maintenance points, use the **show ethernet cfm local maintenance-points** command in EXEC mode.

show ethernet cfm local maintenance-points [**domain** *domain-name* [**service** *service-name*]| **interface** *type interface-path-id*] [**mep**| **mip**]

Syntax Description

domain *domain-name*	(Optional) Displays information about the specified domain, where *domain-name* is a string of a maximum of 80 characters that identifies the domain in which the maintenance points reside.
service *service-name*	(Optional) Displays information about the specified service, where *service-name* is a string of a maximum of 80 characters that identifies the maintenance association to which the maintenance points belong.
interface *type*	(Optional) Displays information about the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
mep	(Optional) Displays information about maintenance end points (MEPs).
mip	(Optional) Displays information about maintenance intermediate points (MIPs).

Command Default

All maintenance points from all interfaces are displayed.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read

Examples

This example shows how to display maintenance points:

```
RP/0/0/CPU0:router# show ethernet cfm local maintenance-points

Domain/Level         Service             Interface         Type    ID   MAC
-------------------- ------------------- ----------------- ------ ---- --------
bar/0                bar                 Gi0/0/0/0         Dn MEP    1 03:04:00
baz/4                baz                 Gi0/0/0/1.1       MIP         03:04:01
baz/4                baz                 Gi0/0/0/2         MIP         03:04:02
foo/?                foo                 Gi0/0/0/3         MEP       1 03:04:03!
qux/2                qux                 Gi0/0/0/1.1       Up MEP   10 03:04:01
qux/2                qux                 Gi0/0/0/2         Up MEP   11 03:04:02
```

Table 16: show ethernet cfm local maintenance-points Field Descriptions

Domain/Level	The domain name and the level of the domain. If the domain is not configured globally, a question mark (?) is displayed for the Level.
Service	The name of the service.
Interface	The interface containing the maintenance point.
Type	The type of maintenance point: • MIP • Up MEP • Down MEP • MEP–If the MEP belongs to a service that is not configured globally, the type cannot be determined and just MEP is displayed.
ID	The configured MEP ID. **Note** Since MIPs do not have an ID, this column is blank for MIPs.
MAC	The last 3 octets of the interface MAC address. **Note** The first three octets are typically the Cisco OUI.

Note	If the MEP has a configuration error, a exclamation point (!) is displayed at the end of the line in the display output.

Related Commands

Command	Description
show ethernet cfm local meps, on page 287	Displays information about local MEPs.
show ethernet cfm peer meps, on page 293	Displays information about maintenance end points (MEPs) for peer MEPs.
traceroute cache, on page 336	Sets the maximum limit of traceroute cache entries or the maximum time limit to hold the traceroute cache entries.
traceroute ethernet cfm, on page 338	Sends Ethernet CFM traceroute messages to generate a basic.

show ethernet cfm local meps

To display information about local maintenance end points (MEPs), use the **show ethernet cfm local meps** command in EXEC mode.

show ethernet cfm local meps [**domain** *domain-name* [**service** *service-name* [**mep-id** *id*]]| **interface** *type interface-path-id* [**domain** *domain-name*]] [**errors** [**detail**| **verbose**]| **detail**| **verbose**]

Syntax Description

domain *domain-name*	(Optional) Displays information about the specified CFM domain, where *domain-name* is a string of a maximum of 80 characters that identifies the domain in which the maintenance points reside.
service *service-name*	(Optional) Displays information about the specified service, where *service-name* is a string of a maximum of 80 characters that identifies the maintenance association to which the maintenance points belong.
interface *type*	(Optional) Displays information about the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
mep-id *id*	(Optional) Displays information about the specified MEP, where *id* is a number of a local maintenance end point (MEP). The range is 1 to 8191.
errors	(Optional) Displays information about peer MEPs with errors.
detail	(Optional) Displays detailed information.
verbose	(Optional) Displays detailed information, plus counters for each type of CFM packet.

Command Default

Brief information is displayed for all local MEPs.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

All MEPs are displayed in the **show ethernet cfm local meps** command output, unless they have configuration errors.

Task ID

Task ID	Operations
ethernet-services	read

Examples

This example shows sample output of the default statistics for local MEPs without any filtering:

```
RP/0/0/CPU0:router# show ethernet cfm local meps

 A - AIS received                I - Wrong interval
 R - Remote Defect received      V - Wrong Level
 L - Loop (our MAC received)     T - Timed out (archived)
 C - Config (our ID received)    M - Missing (cross-check)
 X - Cross-connect (wrong MAID)  U - Unexpected (cross-check)
 P - Peer port down

Domain foo (level 6), Service bar
   ID Interface (State)        Dir MEPs/Err RD Defects AIS
----- ------------------------ --- -------- -- ------- ---
  100 Gi1/1/0/1.234 (Up)       Up     0/0   N  A       L7

Domain fred (level 5), Service barney
   ID Interface (State)        Dir MEPs/Err RD Defects AIS
----- ------------------------ --- -------- -- ------- ---
    2 Gi0/1/0/0.234 (Up)       Up     3/2   Y  RPC     L6

RP/0/0/CPU0:router# show ethernet cfm local meps

 A - AIS received                I - Wrong interval
 R - Remote Defect received      V - Wrong Level
 L - Loop (our MAC received)     T - Timed out (archived)
 C - Config (our ID received)    M - Missing (cross-check)
 X - Cross-connect (wrong MAID)  U - Unexpected (cross-check)
 P - Peer port down

Domain foo (level 6), Service bar
   ID Interface (State)        Dir MEPs/Err RD Defects AIS
----- ------------------------ --- -------- -- ------- ---
  100 Gi1/1/0/1.234 (Up)       Up     0/0   N  A

Domain fred (level 5), Service barney
   ID Interface (State)        Dir MEPs/Err RD Defects AIS
----- ------------------------ --- -------- -- ------- ---
    2 Gi0/1/0/0.234 (Up)       Up     3/2   Y  RPC
```

Table 17: show ethernet cfm local meps Field Descriptions

ID	Configured MEP ID of the MEP.

Interface (State)	Interface that the MEP is configured under, and the state of the interface. The states are derived from the interface state, the Ethernet Link OAM interworking state, and the Spanning Tree Protocol (STP) state. The following states are reported: • Up – Interface Up, Ethernet Link OAM Up, STP Up • Down – Interface Down or Admin Down • Test – Interface Up, Ethernet Link OAM loopback mode • Blkd – Interface Up, Ethernet Link OAM Up, STP Blocked • Otherwise, the interface state.
Dir	Direction of the MEP.
RD	Remote Defect. Y (yes) indicates that a remote defect is detected on at least one peer MEP. In which case, the RDI bit is set in outgoing CCM messages. Otherwise, N (no).
MEPs	Total number of peer MEPs sending CCMs to the local MEP.
Err	Number of peer MEPs for which at least one error has been detected.
Defects	Types of errors detected. Each error is listed as a single character. Multiple errors are listed if they are from the same MEP. Possible errors are listed at the top of the display output of the command.
AIS	Alarm Indication Signal. If AIS is configured for the service, the configured level is displayed when an alarm is signaled. If AIS is not configured for the service, or if no alarm is currently signaled, this field is blank. **Note** In Cisco IOS XR Release 4.0, AIS is not supported, so this field will always be blank.

This example shows sample output of the statistics for MEPs in a specified domain and service:

```
RP/0/0/CPU0:router# show ethernet cfm local meps domain foo service bar

 A - AIS received                I - Wrong interval
 R - Remote Defect received      V - Wrong Level
 L - Loop (our MAC received)     T - Timed out (archived)
```

```
 C - Config (our ID received)    M - Missing (cross-check)
 X - Cross-connect (wrong MAID)  U - Unexpected (cross-check)
 P - Peer port down

Domain foo (level 6), Service bar
   ID Interface (State)        Dir MEPs/Err RD Defects AIS
----- ----------------------- --- -------- -- ------- ---
  100 Gi1/1/0/1.234 (Up)       Up     0/0   N  A       L7

RP/0/0/CPU0:router# show ethernet cfm local meps domain foo service bar

 A - AIS received                I - Wrong interval
 R - Remote Defect received      V - Wrong Level
 L - Loop (our MAC received)     T - Timed out (archived)
 C - Config (our ID received)    M - Missing (cross-check)
 X - Cross-connect (wrong MAID)  U - Unexpected (cross-check)
 P - Peer port down

Domain foo (level 6), Service bar
   ID Interface (State)        Dir MEPs/Err RD Defects AIS
----- ----------------------- --- -------- -- ------- ---
  100 Gi1/1/0/1.234 (Up)       Up     0/0   N  X
```

This example shows sample output of detailed statistics for local MEPs:

Note The Discarded CCMs field is not displayed when the number is zero (0). It is unusual for the count of discarded CCMs to be anything other than zero, since CCMs are only discarded when the limit on the number of peer MEPs is reached. The Peer MEPs field is always displayed, but the counts are always zero when continuity check is not enabled.

```
RP/0/0/CPU0:router# show ethernet cfm local meps detail

Domain foo (level 6), Service bar
Up MEP on GigabitEthernet0/1/0/0.234, MEP-ID 100
================================================================================
  Interface state: Up      MAC address: 1122.3344.5566
  Peer MEPs: 0 up, 0 with errors, 0 timed out (archived)

  CCM generation enabled:  No
  AIS generation enabled:  Yes (level: 7, interval: 1s)
  Sending AIS:             Yes (started 01:32:56 ago)
  Receiving AIS:           Yes (from lower MEP, started 01:32:56 ago)

Domain fred (level 5), Service barney
Up MEP on GigabitEthernet0/1/0/0.234, MEP-ID 2
================================================================================
  Interface state: Up      MAC address: 1122.3344.5566
  Peer MEPs: 3 up, 2 with errors, 0 timed out (archived)
  Cross-check defects: 0 missing, 0 unexpected

  CCM generation enabled:  Yes (Remote Defect detected: Yes)
  CCM defects detected:    R - Remote Defect received
                           P - Peer port down
                           C - Config (our ID received)
  AIS generation enabled:  Yes (level: 6, interval: 1s)
  Sending AIS:             Yes (to higher MEP, started 01:32:56 ago)
  Receiving AIS:           No

RP/0/0/CPU0:router# show ethernet cfm local meps detail

Domain foo (level 5), Service bar
Down MEP on GigabitEthernet0/1/0/0.123, MEP-ID 20
================================================================================
  Interface state: Up      MAC address: 1122.3344.5566
  Peer MEPs: 1 up, 0 with errors, 0 timed out (archived)
  Cross-check errors: 0 missing, 0 unexpected
```

```
  CCM generation enabled:  Yes, 10ms
                           CCM processing offloaded to high-priority software
  AIS generation enabled:  No
  Sending AIS:             No
  Receiving AIS:           No


RP/0/0/CPU0:router# show ethernet cfm local meps verbose

Domain foo (level 6), Service bar
Up MEP on GigabitEthernet0/1/0/0.234, MEP-ID 100
================================================================================
  Interface state: Up      MAC address: 1122.3344.5566
  Peer MEPs: 0 up, 0 with errors, 0 timed out (archived)

  CCM generation enabled:  No
  AIS generation enabled:  Yes (level: 7, interval: 1s)
  Sending AIS:             Yes (started 01:32:56 ago)
  Receiving AIS:           Yes (from lower MEP, started 01:32:56 ago)

  Packet        Sent      Received
  ------  ----------  ----------------------------------------------------
  CCM              0             0  (out of seq: 0)
  LBM              0             0
  LBR              0             0  (out of seq: 0, with bad data: 0)
  AIS           5576             0
  LCK              -             0

Domain fred (level 5), Service barney
Up MEP on GigabitEthernet0/1/0/0.234, MEP-ID 2
================================================================================
  Interface state: Up      MAC address: 1122.3344.5566
  Peer MEPs: 3 up, 2 with errors, 0 timed out (archived)
  Cross-check defects: 0 missing, 0 unexpected

  CCM generation enabled:  Yes (Remote Defect detected: Yes)
  CCM defects detected:    R - Remote Defect received
                           P - Peer port down
                           C - Config (our ID received)
  AIS generation enabled:  Yes (level: 6, interval: 1s)
  Sending AIS:             Yes (to higher MEP, started 01:32:56 ago)
  Receiving AIS:           No

  Packet        Sent      Received
  ------  ----------  ----------------------------------------------------------
  CCM          12345         67890  (out of seq: 6, discarded: 10)
  LBM              5             0
  LBR              0             5  (out of seq: 0, with bad data: 0)
  AIS              0         46910
  LCK              -             0
```

This example shows sample output of detailed statistics for local MEPs:

```
RP/0/0/CPU0:router# show ethernet cfm local meps verbose

Domain foo (level 6), Service bar
Up MEP on GigabitEthernet0/1/0/0.234, MEP-ID 100
================================================================================
  Interface state: Up      MAC address: 1122.3344.5566
  Peer MEPs: 0 up, 0 with errors, 0 timed out (archived)

  CCM generation enabled:  No
  AIS generation enabled:  No
  Sending AIS:             No
  Receiving AIS:           No

  Packet        Sent      Received
  ------  ----------  ----------------------------------------------------
  CCM              0             0  (out of seq: 0)
  LBM              0             0
```

```
  LBR              0             0  (out of seq: 0, with bad data: 0)
  AIS              -             -
  LCK              -             -

Domain fred (level 5), Service barney
Up MEP on GigabitEthernet0/1/0/0.234, MEP-ID 2
================================================================================
  Interface state: Up      MAC address: 1122.3344.5566
  Peer MEPs: 3 up, 2 with errors, 0 timed out (archived)
  Cross-check defects: 0 missing, 0 unexpected

  CCM generation enabled:  Yes (Remote Defect detected: Yes)
  CCM defects detected:    R - Remote Defect received
                           P - Peer port down
                           C - Config (our ID received)
  AIS generation enabled:  No
  Sending AIS:             No
  Receiving AIS:           No

  Packet        Sent      Received
  ------  ----------  ------------------------------------------------------------
  CCM          12345         67890  (out of seq: 6, discarded: 10)
  LBM              5             0
  LBR              0             5  (out of seq: 0, with bad data: 0)
  AIS              -             -
  LCK              -             -
```

Related Commands

Command	Description
show ethernet cfm local maintenance-points, on page 284	Displays a list of local maintenance points.
show ethernet cfm peer meps, on page 293	Displays information about maintenance end points (MEPs) for peer MEPs.
traceroute ethernet cfm, on page 338	Sends Ethernet CFM traceroute messages to generate a basic.

show ethernet cfm peer meps

To display information about maintenance end points (MEPs) for peer MEPs, use the **show ethernet cfm peer meps** command in EXEC mode.

show ethernet cfm peer meps [**domain** *domain-name* [**service** *service-name* [**local mep-id** *id* [**peer** {**mep-id** *id*| **mac-address** *H . H . H*}]]]| **interface** *type interface-path-id* [**domain** *domain-name* [**peer** {**mep-id** *id*| **mac-address** *H . H . H*}]]] [**cross-check** [**missing| unexpected**]| **errors**] **[detail]**

Syntax Description

cross-check	(Optional) Displays information about peer MEPs with cross-check errors.
detail	(Optional) Displays detailed information.
domain *domain-name*	(Optional) Displays information about a CFM domain, where *domain-name* is a string of a maximum of 80 characters that identifies the domain in which the maintenance points reside.
errors	(Optional) Displays information about peer MEPs with errors.
interface *type*	(Optional) Displays information about the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
local mep-id *id*	(Optional) Displays information about a local MEP, where *id* is the number of the MEP.
missing	(Optional) Displays information about peer MEPs that are missing.
peer mep-id *id*	(Optional) Displays information about a peer MEP, where *id* is the number of the MEP.
peer mac-address *H.H.H*	(Optional) Displays information about a peer MEP, where *H.H.H* is the hexadecimal address of the MEP.
service *service-name*	(Optional) Displays information about a CFM service, where *service-name* is a string of a maximum of 154 characters that identifies the maintenance association to which the maintenance points belong.
unexpected	(Optional) Displays information about unexpected peer MEPs.

Command Default

Peer MEPs for all domains are displayed.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows sample output of MEPs detected by a local MEP:

```
RP/0/0/CPU0:router# show ethernet cfm peer meps

Flags:
> - Ok                          I - Wrong interval
R - Remote Defect received      V - Wrong level
L - Loop (our MAC received)     T - Timed out
C - Config (our ID received)    M - Missing (cross-check)
X - Cross-connect (wrong MAID)  U - Unexpected (cross-check)
* - Multiple errors received

Domain dom3 (level 5), Service ser3
Down MEP on GigabitEthernet0/0/0/0 MEP-ID 1
================================================================================
St     ID MAC Address    Port    Up/Downtime   CcmRcvd SeqErr   RDI Error
-- ----- -------------- ------- ------------ --------- ------ ----- -----
V      10 0001.0203.0403 Up      00:01:35            2      0     0     2

Domain dom4 (level 2), Service ser4
Down MEP on GigabitEthernet0/0/0/0 MEP-ID 1
================================================================================
St     ID MAC Address    Port    Up/Downtime   CcmRcvd SeqErr   RDI Error
-- ----- -------------- ------- ------------ --------- ------ ----- -----
 >     20 0001.0203.0402 Up      00:00:03            4      1     0     0
 >     21 0001.0203.0403 Up      00:00:04            3      0     0     0

Domain dom5 (level 2), Service dom5
```

Table 18: show ethernet cfm peer meps Field Descriptions

St	Status: one or two characters, representing the states listed at the top of the output.
ID	Peer MEP ID

MAC address	Peer MAC Address. If this entry is a configured cross-check MEP, with no MAC address specified, and no CCMs are currently being received from a peer MEP with a matching MEP ID, then this field is blank.
Port	Port state of the peer, based on the Port Status and Interface Status TLVs. If no TLVs or CCMs have been received, this field is blank. Otherwise, the port status is displayed—unless it is Up. If the port status is Up, then the interface status is displayed.
Up/Downtime	Time since the peer MEP last came up or went down. If CCMs are currently being received, it is the time since the peer MEP last came up, which is the time since the first CCM was received. If CCMs are not currently being received, it is the time since the peer MEP last went down, which is the time since the loss threshold was exceeded and a loss of continuity was detected.
CcmRcvd	Total number of CCMs received from this peer MEP.
SeqErr	Number of CCMs received out-of-sequence.
RDI	Number of CCMs received with the RDI bit set.
Error	Number of CCMs received with CCM defects, such as: • Invalid level error • Maintenance Association Identifier (MAID) error • Interval error • Received with out MEP ID error • Invalid source MAC error

This example shows sample detailed output of MEPs detected by a local MEP:

```
RP/0/0/CPU0:router# show ethernet cfm peer meps detail

Domain dom3 (level 5), Service ser3
Down MEP on GigabitEthernet0/0/0/0 MEP-ID 1
================================================================================
Peer MEP-ID 10, MAC 0001.0203.0403
   CFM state: Wrong level, for 00:01:34
   Port state: Up
   CCM defects detected:    V - Wrong Level
   CCMs received: 5
```

```
     Out-of-sequence:             0
     Remote Defect received:      5
     Wrong Level:                 0
     Cross-connect (wrong MAID):  0
     Wrong Interval:              5
     Loop (our MAC received):     0
     Config (our ID received):    0
Last CCM received
     Level: 4, Version: 0, Interval: 1min
     Sequence number: 5, MEP-ID: 10
     MAID: String: dom3, String: ser3
     Port status: Up, Interface status: Up


Domain dom4 (level 2), Service ser4
Down MEP on GigabitEthernet0/0/0/0 MEP-ID 1
================================================================================
Peer MEP-ID 20, MAC 0001.0203.0402
   CFM state: Ok, for 00:00:04
   Port state: Up
   CCMs received: 7
     Out-of-sequence:             1
     Remote Defect received:      0
     Wrong Level:                 0
     Cross-connect (wrong MAID):  0
     Wrong Interval:              0
     Loop (our MAC received):     0
 Config (our ID received):    0
Last CCM received
     Level: 2, Version: 0, Interval: 10s
     Sequence number: 1, MEP-ID: 20
     MAID: String: dom4, String: ser4
     Chassis ID: Local: ios; Management address: 'Not specified'
     Port status: Up, Interface status: Up

Peer MEP-ID 21, MAC 0001.0203.0403
   CFM state: Ok, for 00:00:05
   Port state: Up
   CCMs received: 6
     Out-of-sequence:             0
     Remote Defect received:      0
     Wrong Level:                 0
     Cross-connect (wrong MAID):  0
     Wrong Interval:              0
     Loop (our MAC received):     0
     Config (our ID received):    0
Last CCM received 00:00:05 ago:
     Level: 2, Version: 0, Interval: 10s
     Sequence number: 1, MEP-ID: 21
     MAID: String: dom4, String: ser4
     Port status: Up, Interface status: Up


Domain dom5 (level 2), Service ser5
Up MEP on Standby Bundle-Ether 1 MEP-ID 1
================================================================================
Peer MEP-ID 600, MAC 0001.0203.0401
   CFM state: Ok (Standby), for 00:00:08, RDI received
   Port state: Down
   CCM defects detected:    Defects below ignored on local standby MEP
                            I - Wrong Interval
                            R - Remote Defect received
   CCMs received: 5
     Out-of-sequence:             0
     Remote Defect received:   5
 Wrong Level:                  0
     Cross-connect W(wrong MAID): 0
     Wrong Interval:              5
     Loop (our MAC received):     0
     Config (our ID received):    0
   Last CCM received 00:00:08 ago:
     Level: 2, Version: 0, Interval: 10s
     Sequence number: 1, MEP-ID: 600
```

```
     MAID: DNS-like: dom5, String: ser5
     Chassis ID: Local: ios; Management address: 'Not specified'
     Port status: Up, Interface status: Down

Peer MEP-ID 601, MAC 0001.0203.0402
   CFM state: Timed Out (Standby), for 00:15:14, RDI received
   Port state: Down
   CCM defects detected:    Defects below ignored on local standby MEP
                            I - Wrong Interval
                            R - Remote Defect received
                            T - Timed Out
                            P - Peer port down
   CCMs received: 2
     Out-of-sequence:             0
     Remote Defect received:      2
     Wrong Level:                 0
     Cross-connect (wrong MAID):  0
     Wrong Interval:              2
     Loop (our MAC received):     0
     Config (our ID received):    0
   Last CCM received 00:15:49 ago:
     Level: 2, Version: 0, Interval: 10s
     Sequence number: 1, MEP-ID: 600
     MAID: DNS-like: dom5, String: ser5
     Chassis ID: Local: ios; Management address: 'Not specified'
     Port status: Up, Interface status: Down
```

Table 19: show ethernet cfm peer meps detail Field Descriptions

CFM state	State of the peer MEP, how long it has been up or down, and whether the RDI bit was set in the last received CCM. The following possible states are shown if CCMs are currently being received: • Missing • Timed out—No CCMs have been received for the loss time • Ok • Indication of a defect
Port state	Port state of the peer, based on the Port Status and Interface Status TLVs. If no TLVs or CCMs have been received, this field is blank. Otherwise, the port status is displayed—unless it is Up. If the port status is Up, then the interface status is displayed.

CCM defects detected	Types of CCM defects that have been detected. The possible defects are: • Remote Defect re ceived—The last CCM received from the peer had the RDI bit set. • Loop (our MAC received)—CCMs were received from a peer with the same MAC address as the local MEP. • Config (our ID received)—CCMs were received from a peer with the same MEP ID as the local MEP. • Cross-connect (wrong MAID)—The last CCM received from the peer contained a domain/service identified that did not match the locally configured domain/service identifier. • Peer port down—The last CCM received from the peer contained an Interface Status indicating that the interface on the peer was not up. • Wrong interval—The last CCM received contained a CCM interval that did not match the locally configured CCM interval. • Wrong level—The last CCM received was for a lower level than the level of the local MEP. • Timed out—No CCMs have been received within the loss time. • Missing (cross-check)—Cross-check is configured and lists this peer MEP, but no CCMs have been received within the loss time. • Unexpected (cross-check)—Cross check is configured for this service and does not list this peer MEP, but CCMs have been received from it within the loss time.
CCMs received	Number of CCMs received in total, by defect type.
Last CCM received	How long ago the last CCM was received, and a full decode of its contents. Any unknown TLVs are displayed in hexadecimal.

Related Commands

Command	Description
show ethernet cfm local maintenance-points, on page 284	Displays a list of local maintenance points.

Command	Description
show ethernet cfm local meps, on page 287	Displays information about local MEPs.
traceroute ethernet cfm, on page 338	Sends Ethernet CFM traceroute messages to generate a basic.

show ethernet cfm traceroute-cache

To display the contents of the traceroute cache, use the **show ethernet cfm traceroute-cache** command in EXEC mode.

{**show ethernet cfm traceroute-cache** [[**domain** *domain-name*] [**service** *service-name*] [**local mep-id** *id*] [**transaction-id** *id*]]| **interface** *type interface-path-id* [[**domain** *domain-name*] [**transaction-id** *id*]] [**exploratory**| **targeted**] [**status** {**complete**| **incomplete**}] **[detail]**}

Syntax Description

domain *domain-name*	(Optional) Displays information about a CFM domain, where *domain-name* is a string of a maximum of 80 characters that identifies the domain in which the maintenance points reside.
service *service-name*	(Optional) Displays information about a CFM service, where *service-name* is a string of a maximum of 80 characters that identifies the maintenance association to which the maintenance points belong.
local mep-id *id*	(Optional) Displays information for the specified local maintenance end point (MEP). The range for MEP ID numbers is 1 to 8191.
transaction-id *id*	(Optional) Displays information for the specified transaction.
interface *type*	(Optional) Displays information about the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
exploratory	(Optional) Displays information for exploratory traceroutes.
targeted	(Optional) Displays information for traceroutes that are not exploratory, but explicitly mapped.
status	(Optional) Displays status information.
complete	(Optional) Displays status information for traceroutes that have received all replies.
incomplete	(Optional) Displays status information for traceroutes that are still receiving replies.
detail	(Optional) Displays detailed information.

Command Default Shows output for the default traceroute.

Command Modes EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines Use the **show ethernet cfm traceroute-cache** command to display the contents of the traceroute cache; for example, to see the maintenance intermediate points (MIPs) and maintenance end points (MEPs) of a domain as they were discovered. The data is historic. The traceroute cache stores entries from previous traceroute operations.

In the output, the traceroutes sourced from each local MEP are listed. The heading for the local MEP contains the domain name and level, service name, MEP ID and interface name.

Task ID

Task ID	Operations
ethernet-services	read

Examples The following example shows sample output for the **show ethernet cfm traceroute-cache** command:

```
RP/0/0/CPU0:router# show ethernet cfm traceroute-cache

Traceroutes in domain bar (level 4), service bar
Source: MEP-ID 1, interface GigabitEthernet0/0/0/0
================================================================================
Traceroute at 2009-05-18 12:09:10 to 0001.0203.0402,
TTL 64, Trans ID 2:

Hop Hostname/Last            Ingress MAC/name       Egress MAC/Name        Relay
--- ------------------------ ---------------------- ---------------------- -----
  1 ios                      0001.0203.0400 [Down]                         FDB
      0000-0001.0203.0400    Gi0/0/0/0
  2 abc                                             0001.0203.0401 [Ok]    FDB
      ios                                           Not present
  3 bcd                      0001.0203.0402 [Ok]                           Hit
      abc                    GigE0/0
Replies dropped: 0


Traceroutes in domain foo (level 2), service foo
Source: MEP-ID 1, interface GigabitEthernet0/0/0/0
================================================================================
Traceroute at 2009-05-18 12:03:31 to 0001.0203.0403,
TTL 64, Trans ID 1:

Hop Hostname/Last            Ingress MAC/name       Egress MAC/Name        Relay
--- ------------------------ ---------------------- ---------------------- -----
  1 abc                      0001.0203.0401 [Ok]                           FDB
```

```
     0000-0001.0203.0400    Not present
  2 bob                     0001.0203.0402 [Ok]                           MPDB
     abc                    Gi0/1/0/2.3
  3 cba                                            0001.0203.0403 [Ok]    Hit
     bob                                           Gi0/2/0/3.45
Replies dropped: 0


Traceroute at 2009-05-18 12:15:47 to 0001.0203.0409,
TTL 64, Trans ID 3, automatic:
00:00:05 remaining


Traceroute at 2009-05-18 12:20:10 explore to ffff.ffff.ffff,
TTL 64, Trans ID 4, Timeout auto, Reply Filter Default:

Hop               Hostname/Last            Ingr/Egr MAC/name               Relay
----------------- ------------------------ -------- ---------------------- -----
1                 abc                      Ingress  0015.0000.323f [Ok]    FDB
                    0000-0001.0203.0400             Gi0/0/0/0.1
 2                abc                      Egress   0015.0000.323e [Ok]    FDB
                    abc                             Te0/1/0/0.1
  3               0002-0016.eeee.1234      Ingress  0016.eeee.1234 [Ok]    FDB
                    abc                             Te0/4.23
   4              0000-0016.eeee.4321      Egress   0016.eeee.4321 [Ok]    FDB
                    0002-0016.eeee.1234             Gi1/2.23
    5             rtr                      Ingress  0015.0000.f123 [Ok]    FDB
                    0002-00.16.eeee.4321            Gi0/0/0/0
 2                abc                      Egress   0015.0000.323d [Ok]    FDB
                    abc                             Te0/1/0/1.1
  3               pe2                      Ingress  0017.0000.cf01 [Ok]    FDB
                    abc                             Te0/0/2/0/1.450
   4              pe2                      Egress   0017.0000.cf01 [Ok]    Drop
                    pe2                             Gi0/0/0/0.451
   4              pe2                      Egress   0017.0000.cf01 [Ok]    FDB
                    pe2                             Gi0/0/0/1.452
    5             ce2                      Ingress  0015.0000.8830 [Ok]    FDB
                    pe2                             Gi0/1/0/0
Replies dropped: 0
```

Table 20: show ethernet cfm traceroute-cache Field Descriptions

Field	Description
Traceroute at	Date and time the traceroute was started.
to	Destination MAC address.
explore to	(Exploratory traceroutes) MAC address of the target for the exploratory traceroute.
TTL	Initial Time To Live used for the traceroute operation.
Trans ID	Transaction ID
Timeout	(Exploratory traceroutes) If no timeout was configured, “Timeout auto” is shown.
Reply Filter	(Exploratory traceroutes) Type of filter.

Field	Description
automatic	Indicates that the traceroute was triggered automatically (for example, as a result of a peer MEP exceeding the loss threshold, or if Continuity-Check Auto-traceroute is configured).
00:00:00 remaining	If the traceroute is in progress, the time remaining until it completes.
No replies received	Traceroute has completed but no replies were received.
Replies dropped	Number of replies dropped.
FDB only	Indicates FDB-only was configured for a standard traceroute.
Hop	Number of hops between the source MEP and the Maintenance Point that sent the reply. (Exploratory traceroutes) The display is indented by an extra character as the hop increases, so that the tree of responses can be seen.
Hostname/Last	On the first line, the hostname of the Maintenance Point that sent the reply. On the second line, the hostname of the previous Maintenance Point in the path. If either of the hostnames is unknown, the corresponding Egress ID is displayed instead.
Ingr/Egr	(Exploratory traceroutes) Indicates whether the reply is for an ingress or egress interface, but never both.
Ingress MAC/Name	If the reply includes information about the ingress interface, then the first line displays the ingress interface MAC address and the ingress action. The ingress interface name, if known, is displayed on the second line.
Egress MAC/Name	If the reply includes information about the egress interface, then the first line displays the egress interface MAC address and the egress action. The egress interface name, if known, is displayed on the second line.

Field	Description
MAC/Name	(Exploratory traceroutes) The MAC address of the interface from which the reply was sent, and the ingress/egress action, are displayed on the first line. If the interface name was present in the reply, it is displayed on the second line.
Relay	Type of relay action performed. For standard traceroutes, the possible values are: • Hit—The target MAC address was reached. • FDB—The target MAC address was found in the Filtering Database (the MAC learning table on the switch) and will be forwarded by the interface. • MPDB—The target MAC address was found in the MP Database (the CCM Learning database on the switch). In addition, "MEP" is displayed on the second line if a terminal MEP was reached. For exploratory traceroutes, the possible values are: • Hit—The target MAC address was reached. • FDB—The target MAC address was found in the Filtering Database and will be forwarded at this interface. • Flood—The target MAC address was not found in the Filtering database, and will be flooded at this interface. • Drop—The target MAC address will not be forwarded at this interface.

The following example shows sample output for the **show ethernet cfm traceroute-cache detail** command:

```
RP/0/0/CPU0:router# show ethernet cfm traceroute-cache domain bar detail

Traceroutes in domain bar (level 4), service bar
Source: MEP-ID 1, interface GigabitEthernet0/0/0/0
================================================================================
Traceroute at 2009-05-18 12:09:10 to 0001.0203.0402,
TTL 64, Trans ID 2:

Hop Hostname                Ingress MAC            Egress MAC             Relay
--- ----------------------- ---------------------- ---------------------- -----
  1 ios                     0001.0203.0400 [Down]                         FDB
        Level: 4, version: 0, Transaction ID: 2
        TTL: 63, Relay Action: RlyFDB
        Forwarded, Terminal MEP not reached
        Last egress ID: 0000-0001.0203.0400
```

```
        Next egress ID: 0000-0001.0203.0400
        Ingress interface:
          Action: IngDown, MAC: 0001.0203.0400
          ID: Local: Gi0/0/0/0
        Hostname: Local: ios, address Not specified

  2 abc                                                 0001.0203.0401 [Ok]    FDB
        Level: 4, version: 0, Transaction ID: 2
        TTL: 62, Relay Action: RlyFDB
        Forwarded, Terminal MEP not reached
        Last egress ID: 0000-0001.0203.0400
        Next egress ID: 0000-0001.0203.0401
        Egress interface:
          Action: EgOk, MAC: 0001.0203.0401
          ID: Not present
        Hostname: Local: abc, address Not specified

  3 bcd                      0001.0203.0402 [Ok]                          Hit
        Level: 4, version: 0, Transaction ID: 2
        TTL: 61, Relay Action: RlyHit
        Not Forwarded, Terminal MEP not reached
        Last egress ID: 0000-0001.0203.0401
        Next egress ID: Not Forwarded
        Ingress interface:
          Action: IngOk, MAC: 0001.0203.0402
          ID: Local: GigE0/0
        Hostname: Local: bcd, address Not specified

Replies dropped: 0


Traceroute at 2009-05-18 12:30:10 explore to ffff.ffff.ffff from 0204.0608.0a0c,
TTL 255, Trans ID 5, Timeout auto, Reply Filter Spanning Tree:

Hop Hostname                            Ingr/Egr MAC                    Relay
--- ----------------------------------- -------- ---------------------- -----
  1 0000-0015.0000.fffe                 Ingress  0015.0000.fffe [Ok]    FDB
        Level: 2, version: 0, Transaction ID: 5
        TTL: 254, Relay Action: RlyFDB
        Forwarded, Terminal MEP not reached
        Next-Hop Timeout: 5 seconds
        Delay Model: Logarithmic
        Last egress ID: 0000-0002.0002.0002
        Next egress ID: 0000-0015.0000.fffe
        Ingress interface:
          Action: ELRIngOk, MAC: 0015.0000.fffe
          ID: Local: Gi0/0/0/0.1

  2 0001-0030.0000.fffd                 Egress   0030.0000.fffd [Ok]    Drop
        Level: 2, version: 0, Transaction ID: 5
        TTL: 253, Relay Action: RlyDrop
        Not Forwarded, Terminal MEP not reached
        Next-Hop Timeout: 5 seconds
        Delay Model: Logarithmic
        Last egress ID: 0000-0015.0000.fffe
        Next egress ID: 0030-0000.0000.fffd
        Egress interface:
          Action: ELREgrOk, MAC: 0030.0000.fffd
          ID: Local: Gi0/1/0/1.2
```

Related Commands

Command	Description
traceroute cache, on page 336	Sets the maximum limit of traceroute cache entries or the maximum time limit to hold the traceroute cache entries.
clear ethernet cfm traceroute-cache, on page 166	Removes the contents of the traceroute cache.

Command	Description
traceroute ethernet cfm, on page 338	Sends Ethernet CFM traceroute messages to generate a basic.

show ethernet oam configuration

To display the current active Ethernet OAM configuration on an interface, use the **show ethernet oam configuration** command in EXEC mode.

show ethernet oam configuration [**interface** *type interface-path-id*]

Syntax Description

interface *type*	(Optional) Displays information about the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

If no parameters are specified, the configurations for all Ethernet OAM interfaces is displayed.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced. The "Uni-directional link-fault detection enabled" field is not supported in this release. Therefore, the field will always display "N."

Usage Guidelines

This command displays the Ethernet OAM configuration information for all interfaces, or a specified interface.

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows how to display Ethernet OAM configuration information for a specific interface:

```
RP/0/0/CPU0:router# show ethernet oam configuration interface gigabitethernet 0/4/0/0
Thu Aug  5 21:54:34.050 DST
GigabitEthernet0/4/0/0:
  Hello interval:                                    1s
```

```
  Link monitoring enabled:                                Y
  Remote loopback enabled:                                N
  Mib retrieval enabled:                                  N
  Uni-directional link-fault detection enabled:           N
  Configured mode:                                   Active
  Connection timeout:                                     5
  Symbol period window:                                   0
  Symbol period low threshold:                            1
  Symbol period high threshold:                        None
  Frame window:                                        1000
  Frame low threshold:                                    1
  Frame high threshold:                                None
  Frame period window:                                 1000
  Frame period low threshold:                             1
  Frame period high threshold:                         None
  Frame seconds window:                               60000
  Frame seconds low threshold:                            1
  Frame seconds high threshold:                        None
  High threshold action:                               None
  Link fault action:                                    Log
  Dying gasp action:                                    Log
  Critical event action:                                Log
  Discovery timeout action:                             Log
  Capabilities conflict action:                         Log
  Wiring conflict action:                     Error-Disable
  Session up action:                                    Log
  Session down action:                                  Log
  Remote loopback action:                               Log
  Require remote mode:                               Ignore
  Require remote MIB retrieval:                           N
  Require remote loopback support:                        N
  Require remote link monitoring:                         N
```

The following example shows how to display the configuration for all EOAM interfaces:

```
RP/0/0/CPU0:router# show ethernet oam configuration
Thu Aug  5 22:07:06.870 DST
GigabitEthernet0/4/0/0:
  Hello interval:                                        1s
  Link monitoring enabled:                                Y
  Remote loopback enabled:                                N
  Mib retrieval enabled:                                  N
  Uni-directional link-fault detection enabled:           N
  Configured mode:                                   Active
  Connection timeout:                                     5
  Symbol period window:                                   0
  Symbol period low threshold:                            1
  Symbol period high threshold:                        None
  Frame window:                                        1000
  Frame low threshold:                                    1
  Frame high threshold:                                None
  Frame period window:                                 1000
  Frame period low threshold:                             1
  Frame period high threshold:                         None
  Frame seconds window:                               60000
  Frame seconds low threshold:                            1
  Frame seconds high threshold:                        None
  High threshold action:                               None
  Link fault action:                                    Log
  Dying gasp action:                                    Log
  Critical event action:                                Log
  Discovery timeout action:                             Log
  Capabilities conflict action:                         Log
  Wiring conflict action:                     Error-Disable
  Session up action:                                    Log
  Session down action:                                  Log
  Remote loopback action:                               Log
  Require remote mode:                               Ignore
  Require remote MIB retrieval:                           N
  Require remote loopback support:                        N
  Require remote link monitoring:                         N
```

Related Commands

Command	Description
show ethernet oam discovery, on page 310	Displays the current status of Ethernet OAM sessions.
show ethernet oam statistics, on page 317	Displays the local and remote Ethernet OAM statistics for interfaces.
show ethernet oam interfaces, on page 314	Displays the current state of Ethernet OAM interfaces.

show ethernet oam discovery

To display the currently configured OAM information of Ethernet OAM sessions on interfaces, use the **show ethernet oam discovery** command in EXEC mode.

show ethernet oam discovery [**brief**| **interface** *type interface-path-id* **[remote]**]

Syntax Description

brief	Displays minimal, currently configured OAM information in table form.
interface *type*	(Optional) Displays information about the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
remote	(Optional) Retrieves and displays information from a remote device, as if the command was run on the remote device.

Command Default

Displays detailed information for Ethernet OAM sessions on all interfaces.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows how to display the minimal, currently configured OAM information for Ethernet OAM sessions on all interfaces:

```
RP/0/0/CPU0:router# show ethernet oam discovery brief
```

```
Sat Jul  4 13:52:42.949 PST
Flags:
    L - Link Monitoring support
    M - MIB Retrieval support
    R - Remote Loopback support
    U - Unidirectional detection support
    * - data is unavailable

Local                  Remote         Remote
Interface              MAC Address    Vendor Mode    Capability
---------------------- -------------- ------ ------- ----------
Gi0/1/5/1              0010.94fd.2bfa 00000A Active  L
Gi0/1/5/2              0020.95fd.3bfa 00000B Active  M
Gi0/1/6/1              0030.96fd.6bfa 00000C Passive L R
Fa0/1/3/1              0080.09ff.e4a0 00000C Active  L R
```

The following example shows how to display detailed, currently configured OAM information for the Ethernet OAM session on a specific interface:

```
RP/0/0/CPU0:router# show ethernet oam discovery interface gigabitethernet 0/1/5/1

Sat Jul  4 13:56:49.967 PST
GigabitEthernet0/1/5/1:
Local client
------------
  Administrative configuration:
    PDU revision:                         1
    Mode:                            Active
    Unidirectional support:               N
    Link monitor support:                 Y
    Remote loopback support:              N
    MIB retrieval support:                N
    Maximum PDU size:                  1500
    Mis-wiring detection key:          5E9D

Operational status:
    Port status:                Active send
    Loopback status:                  None
    Interface mis-wired:                 N

Remote client
-------------
  MAC address:               0030.96fd.6bfa
  Vendor (OUI):            00.00.0C (Cisco)

  Administrative configuration:
    PDU revision:                         5
    Mode:                           Passive
    Unidirectional support:               N
    Link monitor support:                 Y
    Remote loopback support:              Y
    MIB retrieval support:                N
    Maximum PDU size:                  1500
```

Related Commands

Command	Description
show ethernet oam configuration, on page 307	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam statistics, on page 317	Displays the local and remote Ethernet OAM statistics for interfaces.
show ethernet oam interfaces, on page 314	Displays the current state of Ethernet OAM interfaces.

show ethernet oam event-log

To display the most recent OAM event logs per interface, use the **show ethernet oam event-log** command in EXEC mode.

show ethernet oam event-log [**interface** <*interface* >]**[detail]**

Syntax Description

interface *interface*	Filters the output to only include events for the specified interface.
detail	Displays additional details like threshold value, breaching value, total running errors and window size of a particular interface.

Command Default

This command displays event logs for all interfaces which have OAM configured.

Command Modes

EXEC mode

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows how to display the event logs for all interfaces which have OAM configured:

```
RP/0/0/CPU0:router# show ethernet oam event-log
Wed Jan 23 06:16:46.684 PST
Local Action Taken:
    N/A    - No action needed         EFD    - Interface brought down using EFD
    None   - No action taken          Err.D  - Interface error-disabled
    Logged - System logged

GigabitEthernet0/1/0/0
================================================================================
Time                      Type           Loc'n  Action Threshold Breaching Value
------------------------- -------------- ------ ------ --------- ---------------
Wed Jan 23 06:13:25 PST   Symbol period  Local  N/A            1               4
Wed Jan 23 06:13:33 PST   Frame          Local  N/A            1               6
Wed Jan 23 06:13:37 PST   Frame period   Local  None           9              12
Wed Jan 23 06:13:45 PST   Frame seconds  Local  N/A            1              10
Wed Jan 23 06:13:57 PST   Dying gasp     Remote Logged       N/A             N/A
```

```
GigabitEthernet0/1/0/1
================================================================================
Time                      Type           Loc'n  Action Threshold Breaching Value
------------------------- -------------- ------ ------ --------- ---------------
Wed Jan 23 06:26:14 PST   Dying gasp     Remote Logged       N/A             N/A
Wed Jan 23 06:33:25 PST   Symbol period  Local  N/A            1               4
Wed Jan 23 06:43:33 PST   Frame period   Remote N/A            9              12
Wed Jan 23 06:53:37 PST   Critical event Remote Logged       N/A             N/A
Wed Jan 23 07:13:45 PST   Link fault     Remote EFD          N/A             N/A
Wed Jan 23 07:18:23 PST   Dying gasp     Local  Logged       N/A             N/A
```

Related Commands

Command	Description
show ethernet oam configuration, on page 307	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam discovery, on page 310	Displays the current status of Ethernet OAM sessions.
show ethernet oam interfaces, on page 314	Displays the current state of Ethernet OAM interfaces.

show ethernet oam interfaces

To display the current state of Ethernet OAM interfaces, use the **show ethernet oam interfaces** command in EXEC mode.

show ethernet oam interfaces [**interface** *type interface-path-id*]

Syntax Description

interface *type*	(Optional) Displays information about the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No parameters displays the current state for all Ethernet OAM interfaces.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows how to display the current state of a specific Ethernet OAM interface.

```
RP/0/0/CPU0:router# show ethernet oam interfaces interface gigabitethernet 0/1/5/1

Sat Jul  4 15:01:21.625 PST
GigabitEthernet0/1/5/1
In ACTIVE_SEND_LOCAL state
Local MWD key: 005E9D


RP/0/0/CPU0:router# show ethernet oam interfaces
```

```
GigabitEthernet0/0/0/0
In REMOTE_OK state
Local MWD key: 80081234
Remote MWD key: 8F08ABCC
EFD triggered: Yes (link-fault)
```

Table 21: show ethernet oam interfaces Field Descriptions

Field	Description
In *type* state	The possible discovery state *type* values are: • ACTIVE_SEND_LOCAL—The interface is configured in active mode (the default), but no Information PDUs have been received from the peer (except possibly link-fault PDUs). Information PDUs are sent. • FAULT—A local unidirectional link fault has been detected. Link-fault PDUs are sent. • INACTIVE—The interface is down. • PASSIVE_WAIT—The interface is configured in passive mode (**mode passive** command) but no Information PDUs have been received from the peer (except possibly link-fault PDUs). No PDUs are sent. • REMOTE—(Also known as SEND_LOCAL_REMOTE). Information PDUs are being sent and received, but the local device is not satisfied with the remote peer's capabilities (for example, because there is a 'require-remote' configuration and the peer does not have the required capabilities). • REMOTE_OK—(Also known as SEND_LOCAL_REMOTE_OK). Information PDUs are being sent and received, and the local device is satisfied with the peer's capabilities, but the remote peer is not satisfied with the local device capabilities (for example, because there is a 'require-remote' configuration on the peer device). • SEND_ANY—The discovery process has completed, both devices are satisfied with the configuration and the session is up. All types of PDU can be sent and received.

Related Commands

Command	Description
show ethernet oam configuration, on page 307	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam discovery, on page 310	Displays the current status of Ethernet OAM sessions.
show ethernet oam statistics, on page 317	Displays the local and remote Ethernet OAM statistics for interfaces.

show ethernet oam statistics

To display the local and remote Ethernet OAM statistics for interfaces, use the **show ethernet oam statistics** command in EXEC mode.

show ethernet oam statistics [**interface** *type interface-path-id* **[remote]**]

Syntax Description

interface *type*	(Optional) Displays information about the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
remote	(Optional) Retrieves and displays information from a remote device, as if the command was run on the remote device.

Command Default

No parameters displays statistics for all Ethernet OAM interfaces.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows how to display Ethernet OAM statistics for a specific interface:

```
RP/0/0/CPU0:router# show ethernet oam statistics interface gigabitethernet 0/1/5/1

GigabitEthernet0/1/5/1:
Counters
--------
```

```
    Information OAMPDU Tx                       161177
    Information OAMPDU Rx                       151178
    Unique Event Notification OAMPDU Tx              0
    Unique Event Notification OAMPDU Rx              0
    Duplicate Event Notification OAMPDU Tx           0
    Duplicate Event Notification OAMPDU Rx           0
    Loopback Control OAMPDU Tx                       0
    Loopback Control OAMPDU Rx                       0
    Variable Request OAMPDU Tx                       0
    Variable Request OAMPDU Rx                       0
    Variable Response OAMPDU Tx                      0
    Variable Response OAMPDU Rx                      0
    Organization Specific OAMPDU Tx                  0
    Organization Specific OAMPDU Rx                  0
    Unsupported OAMPDU Tx                           45
    Unsupported OAMPDU Rx                            0
    Frames Lost due to OAM                          23
    Fixed frames Rx                                  1

Local event logs
----------------
    Errored Symbol Period records                    0
    Errored Frame records                            0
    Errored Frame Period records                     0
    Errored Frame Second records                     0

Remote event logs
-----------------
    Errored Symbol Period records                    0
    Errored Frame records                            0
    Errored Frame Period records                     0
    Errored Frame Second records                     0
```

Related Commands

Command	Description
show ethernet oam configuration, on page 307	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam discovery, on page 310	Displays the current status of Ethernet OAM sessions.
show ethernet oam interfaces, on page 314	Displays the current state of Ethernet OAM interfaces.

show ethernet sla configuration-errors

To display information about errors that are preventing configured Ethernet Service Level Agreement (SLA) operations from becoming active, as well as any warnings that have occurred, use the **show ethernet sla configuration-errors** command in EXEC mode.

show ethernet sla configuration-errors [**domain** *domain-name*] [**interface** *type interface-path-id*] [**profile** *profile-name*]

Syntax Description

domain *domain-name*	Displays information for the specified domain, where *domain-name* is a string of a maximum of 80 characters that identifies the domain where the SLA operation is configured.
interface *type*	(Optional) Displays information for the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
profile *profile-name*	(Optional) Displays information for the specified profile name.

Command Default

No default behavior or values

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to display information about errors that are preventing configured SLA operations from becoming active:

```
RP/0/0/CPU0:router# show ethernet sla configuration-errors

Errors:
-------
  Profile 'gold' is not defined but is used on Gi0/0/0/0.0
  Profile 'red' defines a test-pattern, which is not supported by the type
```

show ethernet sla operations

To display information about configured Ethernet Service Level Agreement (SLA) operations, use the **show ethernet sla operations** command in EXEC mode.

show ethernet sla operations [detail] [**domain** *domain-name*] [**interface** *type interface-path-id*] [**on-demand** {**all**| *id*}| **profile** {*profile-name*| **all**}]

Syntax Description

detail	(Optional) Displays detailed information.
domain *domain-name*	(Optional) Displays information for the specified domain, where *domain-name* is a string of a maximum of 80 characters that identifies the domain where the SLA operation is configured.
interface *type*	(Optional) Displays information for the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Displays information for the specified interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
on-demand all	(Optional) Displays information for all on-demand operations.
on-demand *id*	(Optional) Displays information for the specified on-demand operation, where *id* is the number of the operation.
profile *profile-name*	(Optional) Displays information for the specified profile name.
profile all	(Optional) Displays information for all profiles.

Command Default

No default behavior or values

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to display information about configured SLA operations in brief:

```
RP/0/0/CPU0:router# show ethernet sla operations

Profile               Instance
--------------------  ------------------------------------------------------------
business-gold         Gi0/0/0/0, dom mydom, to 00ab.cdef.1234
business-gold         Gi0/0/0/0, dom mydom, to MEP-ID 2
```

The following example shows how to display information about configured SLA operations in detail:

```
RP/0/0/CPU0:router# show ethernet sla operations detail

Source: Interface GigabitEthernet0/0/0/0, Domain mydom
Destination: Target MAC Address 00ab.cdef.1234
================================================================================
Profile 'business-gold'
Probe type 'cfm-delay-measurement':
    burst sent every 1min, each of 20 packets sent every 100ms
Measures RT Delay: 5 bins; 1 buckets/probe; 75 of 100 archived
Measures RT Jitter (interval 1): no aggregation; 5 probes/bucket; 10 of 10 archived
Scheduled to run every 5min first at 00:02:00 UTC for 2min (2 bursts)
    last run at 07:32:00 PST Tue 19 January 2010

Source: Interface GigabitEthernet0/0/0/0, Domain mydom
Destination: Target MEP-ID 2
================================================================================
Profile 'business-gold'
Probe type 'cfm-delay-measurement':
    burst sent every 1min, each of 20 packets sent every 100ms
Measures RT Delay: 5 bins; 1 buckets/probe; 75 of 100 archived
Measures RT Jitter (interval 1): no aggregation; 5 probes/bucket; 10 of 10 archived
Scheduled to run every 5min first at 00:02:00 UTC for 2min (2 bursts)
    last run at 07:32:00 PST Tue 19 January 2010
```

The following example shows how to display information about on-demand SLA operations in detail:

```
RP/0/0/CPU0:router# show ethernet sla operations detail on-demand

Source: Interface GigabitEthernet0/0/0/0.0, Domain mydom
Destination: Target MAC Address 00ab.cdef.1234
================================================================================
On-demand operation ID #6
Probe type 'cfm-loopback':
    burst sent every 10s, each of 10 packets sent every 1s
    packets padded to 1024 bytes with pattern 0xabcd56ef
    packets use priority value of 3
Measures RT Delay: no aggregation; 1 buckets/probe; 1 of 100 archived
Started at 12:01:49 GMT Tue 02 March 2010, runs every 1hr for 1hr (360 bursts)
    repeats 10 times, ends at 22:01:49 GMT Tue 02 March 2010
```

The following example shows how to display information about configured and on-demand SLA operations on a specific interface:

```
RP/0/0/CPU0:router# show ethernet sla operations interface gigabitethernet 0/0/0/0.0 detail

Interface GigabitEthernet 0/0/0/0.0
Domain mydom Service myser to 00AB.CDEF.1234
--------------------------------------------------------------------------------
Profile 'business-gold'
Probe type CFM-delay-measurement:
    bursts sent every 1min, each of 20 packets sent every 100ms
    packets padded to 1500 bytes with zeroes
    packets use priority value of 7
Measures RTT: 5 bins 20ms wide; 2 buckets/ probe; 75/100 archived
Measures Jitter (interval 1): 3 bins 40ms wide; 2 buckets/probe; 50 archived
Scheduled to run every Sunday at 4am for 2 hours:
    last run at 04:00 25/05/2008
```

show ethernet sla statistics

To display the contents of buckets containing Ethernet Service Level Agreement (SLA) metrics collected by probes, use the **show ethernet sla statistics** command in EXEC mode.

show ethernet sla statistics [**current**| **history**] **[detail]** [**domain** *domain-name*] [**interface** *type interface-path-id*] [**on-demand** {**all**| *id*}| **profile** {*profile-name*| **all**}] [**statistic** *stat-type*]

Syntax Description

current	(Optional) Displays the content of buckets currently being filled.
history	(Optional) Displays the content of all full buckets.
detail	(Optional) Displays detailed content of buckets.
domain *domain-name*	(Optional) Displays the content of buckets for the specified domain, where *domain-name* is a string of a maximum of 80 characters that identifies the domain where the SLA operation is configured.
interface *type*	(Optional) Displays the content of buckets for the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Displays the content of buckets for the specified interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
on-demand all	(Optional) Displays the content of buckets for all on-demand operations.
on-demand *id*	(Optional) Displays the content of buckets for the specified on-demand operation, where *id* is the number of the operation.
profile *profile-name*	(Optional) Displays the content of buckets for the specified profile name.
profile all	(Optional) Displays the content of buckets for all profiles.
statistic *stat-type*	(Optional) Displays only the specified type of statistic. Valid values are: • **one-way-delay-ds—**Displays only one-way (destination-to-source) delay. • **one-way-delay-sd—**Displays only one-way (source-to-destination) delay. • **one-way-jitter-ds—**Displays only one-way (destination-to-source) jitter. • **one-way-jitter-sd—**Displays only one-way (source-to-destination) jitter. • **round-trip-delay—**Displays only round-trip delay. • **round-trip-jitter—**Displays only round-trip jitter.

Command Default No default behavior or values

Command Modes EXEC (#)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines See the Usage Guidelines in the **buckets size** command for a description of buckets.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples This example shows how to display the current contents of buckets containing SLA metrics collected by probes in brief:

```
RP/0/0/CPU0:router# show ethernet sla statistics

Source: Interface GigabitEthernet0/0/0/0, Domain mydom
Destination: Target MEP-ID 2
================================================================================
Profile 'business-gold', packet type 'cfm-delay-measurement'
Scheduled to run every 5min first at 00:02:00 UTC for 2min

Round Trip Delay
~~~~~~~~~~~~~~~~
1 buckets per probe

Bucket started at 07:47:00 PST Tue 19 January 2010 lasting 2min
    Pkts sent: 20; Lost: 0 (0.0%); Corrupt: 0 (0.0%); Misordered: 0 (0.0%)
    Min: 0.24ms; Max: 0.49ms; Mean: 0.34ms; StdDev: 0.05ms

Bucket started at 07:52:00 PST Tue 19 January 2010 lasting 2min
    Pkts sent: 20; Lost: 0 (0.0%); Corrupt: 0 (0.0%); Misordered: 0 (0.0%)
    Min: 0.24ms; Max: 0.69ms; Mean: 0.34ms; StdDev: 0.12ms


Round Trip Jitter
~~~~~~~~~~~~~~~~~
1 buckets per probe

Bucket started at 07:47:00 PST Tue 19 January 2010 lasting 2min
    Pkts sent: 20; Lost: 0 (0.0%); Corrupt: 0 (0.0%); Misordered: 0 (0.0%)
    Min: -0.25ms; Max: 0.13ms; Mean: -0.01ms; StdDev: 0.08ms

Bucket started at 07:52:00 PST Tue 19 January 2010 lasting 2min
    Pkts sent: 20; Lost: 0 (0.0%); Corrupt: 0 (0.0%); Misordered: 0 (0.0%)
    Min: -0.38ms; Max: 0.38ms; Mean: -0.02ms; StdDev: 0.14ms
```

This example shows how to display the current contents of buckets containing SLA metrics collected by probes in detail:

Note In this example, the round-trip-delay measurement is configured with aggregation (and hence bins are displayed), whereas the round-trip-jitter measurement is configured with no aggregation (and hence individual samples are displayed).

```
RP/0/0/CPU0:router# show ethernet sla statistics detail
Source: Interface GigabitEthernet0/0/0/0, Domain mydom
Destination: Target MEP-ID 2
================================================================================
Profile 'business-gold', packet type 'cfm-delay-measurement'
Scheduled to run every 5min first at 00:02:00 UTC for 2min

Round Trip Delay
~~~~~~~~~~~~~~~~
1 buckets per probe

Bucket started at 07:47:00 PST Tue 19 January 2010 lasting 2min
    Pkts sent: 20; Lost: 0 (0.0%); Corrupt: 0 (0.0%); Misordered: 0 (0.0%)
    Min: 0.24ms, occurred at 07:47:29 on Tue 19 Jan 2010 UTC
    Max: 0.49ms, occurred at 07:48:04 on Tue 19 Jan 2010 UTC
    Mean: 0.34ms; StdDev: 0.05ms

    Bins:
    Range            Samples   Cum. Count   Mean
    -----------  -----------  -----------  -----
     0 to 20 ms  20 (100.0%)  20 (100.0%)  0.34ms
    20 to 40 ms   0   (0.0%)  20 (100.0%)      -
    40 to 60 ms   0   (0.0%)  20 (100.0%)      -
    60 to 80 ms   0   (0.0%)  20 (100.0%)      -
    > 80     ms   0   (0.0%)  20 (100.0%)      -

Bucket started at 07:52:00 PST Tue 19 January 2010 lasting 2min
    Pkts sent: 20; Lost: 0 (0.0%); Corrupt: 0 (0.0%); Misordered: 0 (0.0%)
    Min: 0.24ms, occurred at 07:53:10 on Tue 19 Jan 2010 UTC
    Max: 0.69ms, occurred at 07:53:42 on Tue 19 Jan 2010 UTC
    Mean: 0.34ms; StdDev: 0.12ms

    Bins:
    Range            Samples   Cum. Count   Mean
    -----------  -----------  -----------  -----
     0 to 20 ms  20 (100.0%)  20 (100.0%)  0.34ms
    20 to 40 ms   0   (0.0%)  20 (100.0%)      -
    40 to 60 ms   0   (0.0%)  20 (100.0%)      -
    60 to 80 ms   0   (0.0%)  20 (100.0%)      -
    > 80     ms   0   (0.0%)  20 (100.0%)      -


Round Trip Jitter
~~~~~~~~~~~~~~~~~
1 buckets per probe

Bucket started at 07:47:00 PST Tue 19 January 2010 lasting 2min
    Pkts sent: 20; Lost: 0 (0.0%); Corrupt: 0 (0.0%); Misordered: 0 (0.0%)
    Min: -0.25ms, occurred at 07:47:53 on Tue 19 Jan 2010 UTC
    Max: 0.13ms, occurred at 07:48:11 on Tue 19 Jan 2010 UTC
    Mean: -0.01ms; StdDev: 0.08ms

    Samples:
    Time sent   Result  Notes
    ----------  ------  ----------
    07:47:00.0     ...
    07:47:00.1  -0.12ms
    07:47:00.2  0.06ms
    07:47:00.3  0.00ms
    07:47:00.4  -0.06ms
```

```
    07:47:00.5  0.00ms
    07:47:00.6  0.00ms
    07:47:00.7  0.00ms
    07:47:00.8  0.06ms
    07:47:00.9  0.00ms
    07:48:00.0  0.11ms
    07:48:00.1  -0.25ms
    07:48:00.2  0.13ms
    07:48:00.3  0.00ms
    07:48:00.4  -0.06ms
    07:48:00.5  0.00ms
    07:48:00.6  0.06ms
    07:48:00.7  -0.06ms
    07:48:00.8  0.00ms
    07:48:00.9  0.00ms

Bucket started at 07:52:00 PST Tue 19 January 2010 lasting 2min
    Pkts sent: 20; Lost: 0 (0.0%); Corrupt: 0 (0.0%); Misordered: 0 (0.0%)
    Min: -0.38ms, occurred at 07:52:13 on Tue 19 Jan 2010 UTC
    Max: 0.38ms, occurred at 07:53:26 on Tue 19 Jan 2010 UTC
    Mean: -0.02ms; StdDev: 0.14ms

    Samples:
    Time sent   Result  Notes
    ----------  ------  ----------
    07:52:00.0     ...
    07:52:00.1  -0.38ms
    07:52:00.2  0.00ms
    07:52:00.3  -0.05ms
    07:52:00.4  0.00ms
    07:52:00.5  0.05ms
    07:52:00.6  0.00ms
    07:52:00.7  0.00ms
    07:52:00.8  0.00ms
    07:52:00.9  0.00ms
    07:53:00.0  0.38ms
    07:53:00.1  -0.32ms
    07:53:00.2  0.00ms
    07:53:00.3  -0.13ms
    07:53:00.4  0.06ms
    07:53:00.5  0.00ms
    07:53:00.6  0.00ms
    07:53:00.7  0.00ms
    07:53:00.8  0.06ms
    07:53:00.9  0.00ms
```

This example shows how to display the current contents of buckets containing SLA metrics collected by probes on a specific interface:

```
RP/0/0/CPU0:router# show ethernet sla statistics current interface GigabitEthernet 0/0/0/0.0


Interface GigabitEthernet 0/0/0/0.0
Domain mydom Service myser to 00AB.CDEF.1234
------------------------------------------------------------------------------
Profile 'business-gold', packet type 'cfm-superpacket'
Scheduled to run every Sunday at 4am for 2 hours

Round Trip Delay
~~~~~~~~~~~~~~~~
2 buckets per probe

Bucket started at 04:00 Sun 17 Feb 2008 lasting 1 hour:
    Pkts sent: 2342; Lost 2 (0%); Corrupt: 0 (0%); Misordered: 0 (0%)
    Min: 13ms; Max: 154ms; Mean: 28ms; StdDev: 11ms

Round Trip Jitter
~~~~~~~~~~~~~~~~~
2 buckets per probe

Bucket started at 04:00 Sun 17 Feb 2008 lasting 1 hour:
```

```
    Pkts sent: 2342; Lost: 2 (0%); Corrupt: 0 (0%); Misordered: 0 (0%)
    Min: -5ms; Max: 8ms; Mean: 0ms; StdDev: 3.6ms
```

This example shows how to display a history detail of buckets containing SLA metrics collected by probes on a specific interface:

```
RP/0/0/CPU0:router# show ethernet sla history detail GigabitEthernet 0/0/0/0.0

Interface GigabitEthernet 0/0/0/0.0
Domain mydom Service myser to 00AB.CDEF.1234
================================================================================
Profile 'business-gold', packet type 'cfm-loopback'
Scheduled to run every Sunday at 4am for 2 hours

Round Trip Delay
~~~~~~~~~~~~~~~~
2 buckets per probe

Bucket started at 04:00 Sun 17 Feb 2008 lasting 1 hour:
    Pkts sent: 2342; Lost: 2 (0%); Corrupt: 0 (0%); Misordered: 0 (0%)
    Min: 13ms, occurred at 04:43:29 on Sun 22 Aug 2010 UTC
    Max: 154ms, occurred at 05:10:32 on Sun 22 Aug 2010 UTC
    Mean: 28ms; StdDev: 11ms

    Results suspect as more than 10 seconds time drift detected
    Results suspect as scheduling latency prevented some packets being sent

    Samples:
    Time sent       Result  Notes
    ------------  --------  ----------
    04:00:01.324      23ms
    04:00:01.425      36ms
    04:00:01.525         -  Timed Out
    ...

Round Trip Jitter
~~~~~~~~~~~~~~~~~
2 buckets per probe

Bucket started at 04:00 Sun 17 Feb 2008, lasting 1 hour:
    Pkts sent: 2342; Lost: 2 (0%); Corrupt: 0 (0%); Misordered: 0 (0%)
    Min: -5ms, occurred at 04:15:03 on Sun 22 Aug 2010 UTC
    Max: 10ms, occurred at 05:29:15 on Sun 22 Aug 2010 UTC
    Mean: 0ms; StdDev: 3.6ms

    Samples:
    Time sent       Result  Notes
    ------------  --------  ----------
    04:00:01.324         -
    04:00:01.425      13ms
    04:00:01.525         -  Timed out
    ...
```

This example shows how to display statistics for all full buckets for on-demand operations in detail:

```
RP/0/0/CPU0:router# show ethernet sla statistics history detail on-demand

Interface GigabitEthernet0/0/0/0.1
Domain mydom Service myser to 0123.4567.890A
================================================================================
On-demand operation ID #1, packet type 'cfm-delay-measurement'
Started at 15:38 on 06 July 2010 UTC, runs every 1 hour for 1 hour

Round Trip Delay
~~~~~~~~~~~~~~~~
1 bucket per probe

Bucket started at 15:38 on Tue 06 Jul 2010 UTC, lasting 1 hour:
    Pkts sent: 1200; Lost: 4 (0%); Corrupt: 600 (50%); Misordered: 0 (0%)
    Min: 13ms, occurred at 15:43:29 on Tue 06 Jul 2010 UTC
```

```
    Max: 154ms, occurred at 16:15:34 on Tue 06 Jul 2010 UTC
    Mean: 28ms; StdDev: 11ms

    Bins:
    Range              Samples    Cum. Count      Mean
    ------------  ------------  ------------  --------
     0 - 20 ms       194 (16%)     194 (16%)      17ms
    20 - 40 ms       735 (61%)     929 (77%)      27ms
    40 - 60 ms       212 (18%)    1141 (95%)      45ms
    > 60    ms        55  (5%)    1196            70ms

Bucket started at 16:38 on Tue 01 Jul 2008 UTC, lasting 1 hour:
    Pkts sent: 3600; Lost: 12 (0%); Corrupt: 1800 (50%); Misordered: 0 (0%)
    Min: 19ms, occurred at 17:04:08 on Tue 06 Jul 2010 UTC
    Max: 70ms, occurred at 16:38:00 on Tue 06 Jul 2010 UTC
    Mean: 28ms; StdDev: 11ms

    Bins:
    Range              Samples    Cum. Count      Mean
    ------------  ------------  ------------  --------
     0 - 20 ms       194 (16%)     194 (16%)      19ms
    20 - 40 ms       735 (61%)     929 (77%)      27ms
    40 - 60 ms       212 (18%)    1141 (95%)      45ms
    > 60    ms        55  (5%)    1196            64ms
```

Related Commands

Command	Description
buckets size, on page 157	Configures the size of the buckets in which statistics are collected.

sla operation

To create an operation instance from a maintenance end point (MEP) to a specified destination, use the **sla operation** command in interface CFM MEP configuration mode. To remove the operation, use the **no** form of this command.

sla operation profile *profile-name* **target** {**mep-id** *id*| **mac-address** *mac-address*}

no sla operation profile *profile-name* **target** {**mep-id** *id*| **mac-address** *mac-address*}

Syntax Description

profile *profile-name*	Name of the profile to assign this operation.
target mep-id *id*	Destination MEP ID. The range is 1 to 8191.
mac-address *mac-address*	Destination MAC address in standard hexadecimal format, hh:hh:hh:hh:hh:hh.

Command Default

No operations are configured

Command Modes

Interface CFM MEP configuration (config-if-cfm-mep)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

The **sla operation** command is supported on all Ethernet interfaces.

Multiple SLA operation instances may be configured under each MEP, and may have different targets, and may be assigned to different profiles.

If an operation is assigned to a nonexistent profile, a warning message is issued, and the offending configuration is shown in the output of the related show commands.

Changing the configuration of an SLA operation is equivalent to deleting the operation and creating a new operation. All stored data for the operation is discarded.

When **target mep-id** is specified, the operation is activated only if that MEP is in the peer MEP database. You can verify that a MEP is in the database, using the **show ethernet cfm peer meps** command.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to create an SLA operation instance using a profile named “Profile_1” to a destination MEP with the specified MAC address:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/1
RP/0/0/CPU0:router(config-if)# ethernet cfm
RP/0/0/CPU0:router(config-if-cfm)# mep domain Dm1 service Sv1 mep-id 1
RP/0/0/CPU0:router(config-if-cfm-mep)# sla operation profile Profile_1 target mac-address
01:23:45:67:89:ab
```

Related Commands

Command	Description
show ethernet cfm peer meps, on page 293	Displays information about maintenance end points (MEPs) for peer MEPs.

snmp-server traps ethernet cfm

To enable SNMP traps for Ethernet Connectivity Fault Management (CFM), use the **snmp-server traps ethernet cfm** command in global configuration mode.

snmp-server traps ethernet cfm

Syntax Description

This command has no keywords or arguments.

Command Default

Ethernet OAM event traps are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to enable SNMP server traps on an Ethernet OAM interface.

```
RP/0/0/CPU0:router #configure
RP/0/0/CPU0:router(config)# snmp-server traps ethernet cfm
```

snmp-server traps ethernet oam events

To enable SNMP traps for Ethernet OAM events, use the **snmp-server traps ethernet oam events** command in global configuration mode.

snmp-server traps ethernet oam events

Syntax Description

This command has no keywords or arguments.

Command Default

Ethernet OAM event traps are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to enable SNMP server traps on an Ethernet OAM interface.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# snmp-server traps ethernet oam events
```

statistics measure

To enable the collection of Ethernet Service Level Agreement (SLA) statistics, and enter the SLA profile statistics configuration mode, use the **statistics measure** command in SLA profile configuration mode. To disable statistics collection, use the **no** form of this command.

statistics measure {**one-way-delay-ds**| **one-way-delay-sd**| **one-way-jitter-ds**| **one-way-jitter-sd**| **round-trip-delay**| **round-trip-jitter**}

no statistics measure {**one-way-delay-ds**| **one-way-delay-sd**| **one-way-jitter-ds**| **one-way-jitter-sd**| **round-trip-delay**| **round-trip-jitter**}

Syntax Description

one-way-delay-ds	(CFM delay measurement profile type only) Enables the collection of statistics that measure delay in one direction, from destination to source.
one-way-delay-sd	(CFM delay measurement profile type only) Enables the collection of statistics that measure delay in one direction, from source to destination.
one-way-jitter-ds	(CFM delay measurement profile type only) Enables the collection of statistics that measure delay variance in one direction, from destination to source.
one-way-jitter-sd	(CFM delay measurement profile type only) Enables the collection of statistics that measure delay variance in one direction, from source to destination.
round-trip-delay	(CFM delay measurement and CFM loopback profile types only) Enables the collection of statistics that measure the delay in the round trip of a packet.
round-trip-jitter	(CFM delay measurement and CFM loopback profile types only) Enables the collection of statistics that measure the amount of delay variance in the round trip of a packet.

Command Default

No statistics are collected

Command Modes

SLA profile configuration (config-sla-prof)

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

For statistics to be collected, at least one statistics entry must be present in each profile. To measure more than one type of statistic, this command may be configured more than once in a single profile.

The one-way delay and jitter statistics are available for CFM delay measurement profile types only (**profile (SLA)** command with the **type cfm-delay-measurement** keywords).

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

This example shows how to enable the collection of round-trip-delay statistics, and enter the SLA profile statistics configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ethernet sla
RP/0/0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RP/0/0/CPU0:router(config-sla-prof)# statistics measure round-trip-delay
RP/0/0/CPU0:router(config-sla-prof-stat-cfg)#
```

Related Commands

Command	Description
ethernet sla, on page 200	Enters the Ethernet SLA configuration mode.
profile (SLA), on page 259	Creates an SLA operation profile and enter the SLA profile configuration mode.

traceroute cache

To set the maximum limit of traceroute cache entries or the maximum time limit to hold the traceroute cache entries, use the **traceroute cache** command in CFM configuration mode. To return the traceroute cache to its default limits, use the **no** form of this command.

traceroute cache hold-time *minutes* **size** *entries*

no traceroute cache hold-time *minutes* **size** *entries*

Syntax Description

hold-time *minutes*	Timeout value in minutes that entries are held in the Ethernet CFM traceroute cache table before being cleared. Range is 1 minute or greater.
size *entries*	Maximum number of entries that are stored in the Ethernet CFM traceroute cache table. An entry is a single traceroute reply. Range is 1 to 5000.

Command Default

hold-time: 100

size: 100

Command Modes

CFM configuration (config-cfm)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

A separate cache is managed for each node that sends a traceroute request. All replies to a single traceroute request are cached at once. The **hold-time** begins when the last reply to a request is received. When the **hold-time** limit is reached, all replies to that request are cleared. The size of each traceroute reply is limited by the MTU of the interface.

When the maximum number of entries (**size** *entries*) is exceeded, all replies for the oldest request are deleted.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to set the **hold-time** and the **size** of a traceroute cache.

```
RP/0/0/CPU0:router# configure
```

```
RP/0/0/CPU0:router(config)# ethernet cfm
RP/0/0/CPU0:router(config-cfm)# traceroute cache hold-time 1 size 3000
```

Related Commands

Command	Description
ethernet cfm (global), on page 194	Enters CFM configuration mode.
traceroute ethernet cfm, on page 338	Sends Ethernet CFM traceroute messages to generate a basic.

traceroute ethernet cfm

To send Ethernet connectivity fault management (CFM) traceroute messages to generate a basic, targeted, or exploratory traceroute, use the **traceroute ethernet** command in EXEC mode.

traceroute ethernet cfm domain *domain-name* **service** *service-name* {**mac-address** *target-mac-address*| **mep-id** *target-mep-id*| **explore [all-ports]** [**from** *from-mac-address*]} **source** [**mep-id** *source-mep-id*] **interface** *type interface-path-id* **[asynchronous]** [**timeout** *seconds*] **[filtering-db-only]** [**cos** *cos-no*] [**ttl** *ttl*] **[detail]**

Syntax Description

domain *domain-name*	String of a maximum of 80 characters that identifies the domain in which the destination MEP resides. (Basic traceroute)
service *service-name*	String of a maximum of 80 characters that identifies the maintenance association to which the destination MEP belongs. (Basic traceroute)
mac-address *target-mac-address*	Identifies the 6-byte MAC address (in hexadecimal H.H.H format) of the destination MEP. (Targeted traceroute)
mep-id *target-mepid*	Destination maintenance end point (MEP) ID number. The range for MEP ID numbers is 1 to 8191. (Targeted traceroute)
explore	(Optional) Specifies that an exploratory traceroute is performed.
all-ports	(Optional) Specifies an exploratory traceroute of all ports.
from *from-mac-address*	(Optional) Specifies an exploratory traceroute beginning at the specified MAC address (in hexadecimal H.H.H format).
source	Specifies source information for the traceroute.
mep-id *source-mep-id*	(Optional) Source maintenance end point (MEP) ID number. The range for MEP ID numbers is 1 to 8191.
interface *type*	Source interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
asynchronous	(Optional) Specifies that the traceroute is performed asynchronously, where control is returned to the command prompt immediately, and no results are displayed. The results can be displayed later using the **show ethernet cfm traceroute-cache** command.

timeout *seconds*	(Optional) Timeout value (in seconds) for the specified interface. For a basic traceroute, the timeout is a fixed value that defaults to 5 seconds. For an exploratory traceroute, a logarithmic algorithm is used unless this value is specified.
filtering-db-only	(Optional) Sets whether or not the remote maintenance points should base their responses on the filtering database only. The default is no—use both the filtering and MIP-CCM databases. **Note** The **filtering-db-only** option is only available for basic traceroute (when the MAC address or MEP ID is specified). It is not available with the **explore** option.
cos *cos-no*	(Optional) Identifies the class of traffic of the source MEP by setting a Class of Service (CoS) value. The valid values are from 0 to 7.
ttl *ttl*	Specifies the initial time-to-live (TTL) value (from 1 to 255) for the traceroute message. The default is 64.
detail	(Optional) Specifies that details are displayed in the output for the traceroute.

Command Default

No default behavior or values

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

By default, this command pauses until the traceroute operation is complete, then displays the results. If the **asynchronous** option is used, this command returns immediately and no results are displayed. Results are placed placed the traceroute cache and can be retrieved using the **show ethernet cfm traceroute-cache** command.

An exploratory traceroute, by default uses a **timeout** value that is calculated by a logarithmic delay algorithm. If the **timeout** value is specified, the specified value is used.

The display output of this command is similar to the output of the **show ethernet cfm traceroute-cache** command.

Task ID

Task ID	Operations
interface	read

Examples

The following example shows how generate a basic traceroute:

```
RP/0/0/CPU0:router# traceroute ethernet cfm domain bar service bar mep-id 1 source interface
 gigabitethernet 0/0/0/0

Traceroutes in domain bar (level 4), service bar
Source: MEP-ID 1, interface GigabitEthernet0/0/0/0
================================================================================
Traceroute at 2009-05-18 12:09:10 to 0001.0203.0402,
TTL 64, Trans ID 2:

Hop Hostname/Last            Ingress MAC/name       Egress MAC/Name        Relay
--- ---------------------- ---------------------- ---------------------- -----
  1 ios                      0001.0203.0400 [Down]                        FDB
      0000-0001.0203.0400    Gi0/0/0/0
  2 abc                                             0001.0203.0401 [Ok]    FDB
      ios                                           Not present
  3 bcd                      0001.0203.0402 [Ok]                          Hit
      abc                    GigE0/0
Replies dropped: 0
```

Related Commands

Command	Description
traceroute cache, on page 336	Sets the maximum limit of traceroute cache entries or the maximum time limit to hold the traceroute cache entries.
clear ethernet cfm traceroute-cache, on page 166	Removes the contents of the traceroute cache.
show ethernet cfm traceroute-cache, on page 300	Displays the contents of the traceroute cache.

Frame Relay Commands on the Cisco IOS XR Software

This module provides CLI commands for configuring Frame Relay services on the Cisco XR 12000 Series Router.

clear frame-relay multilink interface

To clear the multilink frame-relay (MFR) statistics for the given interface or location, use the **clear frame-relay multilink interface** command in EXEC mode.

clear frame-relay multilink interface {*type interface-path-id*| **all** [**location** *node id*]}

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
all	Clears MFR statistics for all interfaces
location *node-id*	(Optional) Clears MFR statistics for all interfaces at the location specified by *node-id*. The *node-id* argument is entered in the *rack*/*slot*/*module* notation.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
fr	execute

Examples

The following example shows how to use the **clear frame-relay multilink interface** command to clear the multilink frame-relay protocol and internal statistics on an interface:

```
RP/0/0/CPU0:router# clear frame-relay multilink interface serial 0/1/0/0
```

Related Commands

Command	Description
show frame-relay lmi-info, on page 381	Displays Frame Relay information for the LMI.
show interfaces multilink, on page 525	Displays information about a multilink interface.

clear frame-relay lmi interface

To clear the LMI statistics for the given interface or location, use the **clear frame-relay lmi** command in EXEC mode.

clear frame-relay lmi interface {*type interface-path-id*| **all** [**location** *node id*]}

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
all	Clears LMI statistics for all interfaces
location *node-id*	(Optional) Clears LMI statistics for all interfaces at the location specified by *node-id*. The *node-id* argument is entered in the *rack*/*slot*/*module* notation.

Command Default

No default behavior or values

Command Modes

EXEC (#)

Command History

Release	Modification
Release 3.5.0	This command was introduced.
Release 3.6.0	The keyword **all** was added.

Usage Guidelines

Task ID

Task ID	Operations
fr	execute

Examples

The following example shows how to use the **clear frame-relay lmi** command to clear the LMI counters on an interface:

```
RP/0/0/CPU0:router# clear frame-relay lmi interface pos 0/1/0/0
```

Related Commands

Command	Description
show frame-relay lmi, on page 378	Displays Frame Relay statistics for the LMI.

encap (PVC)

To change the encapsulation for a Frame Relay permanent virtual circuit (PVC), use the **encap** command in Frame Relay PVC configuration mode. To restore default encapsulation from the Frame Relay main interface, use the **no** form of this command.

encap {**cisco**| **ietf**}

no encap {**cisco**| **ietf**}

Syntax Description

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

Command Default

The default encapsulation keyword is Cisco.

When this command is not configured, encapsulation is inherited from the Frame Relay main interface.

Command Modes

Frame Relay PVC configuration (config-fr-vc)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

Use the **encap** command to configure encapsulation for a Frame Relay PVC. If this command is not configured, encapsulation is inherited from the Frame Relay subinterface.

This command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows how to set encapsulation on PVC data-link connection identifier (DLCI) 16 for Packet-over-SONET/SDH (POS) subinterface 0/4/0/1.1:

```
RP/0/0/CPU0:router(config)# interface POS 0/4/0/1.1 l2transport
RP/0/0/CPU0:router(config-subif)# pvc 16
RP/0/0/CPU0:router(config-fr-vc)# encap ietf
```

Related Commands

Command	Description
encapsulation frame-relay, on page 349	Enables Frame Relay encapsulation.

encapsulation frame-relay

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

encapsulation frame-relay [ietf]

no encapsulation frame-relay [ietf]

Syntax Description

ietf	(Optional) Sets the encapsulation method to comply with the Internet Engineering Task Force (IETF) standard (RFC 1490). Use this keyword when connecting to equipment from another vendor across a Frame Relay network.

Command Default

The default encapsulation method is Cisco.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

Use the **encapsulation frame-relay** command to connect an interface to a Frame Relay network. When this command is configured, outgoing packets are encapsulated with a Frame Relay header and Frame Relay headers are removed from incoming packets to the interface.

A Cisco or IETF encapsulation method controls the Network Layer Protocol Identifier (NLPID) that is added to outgoing packets on the interface. The encapsulation method enabled for an outgoing packet can be changed for each data-link connection identifier (DLCI) per subinterface by using the **encap (PVC)** command in Frame Relay PVC configuration mode.

When the **encapsulation frame-relay** command is configured, LMI is enabled by default. To disable LMI use the **frame-relay lmi disable** command.

The following restrictions apply to the **encapsulation frame-relay** command upon configuration or removal of the command on an interface:

- When configuring this command, Layer 3 and Layer 2 configurations are not allowed on the interface.
- Before removing this command, all Frame Relay subinterfaces and LMI configuration should be deleted from the interface.

The **encapsulation frame-relay** command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

Task ID

Task ID	Operations
interface	read, write
fr	read, write

Examples

The following example shows Frame Relay encapsulation configured on Packet-over-SONET/SDH (POS) 0/3/0/1:

```
RP/0/0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/0/CPU0:router(config-if)# encapsulation frame-relay ietf
```

Related Commands

Command	Description
encap (PVC), on page 347	Changes the encapsulation for a Frame Relay PVC.
frame-relay lmi disable, on page 352	Disables the Frame Relay LMI.

frame-relay intf-type

To configure the interface type of the User-Network Interface (UNI), use the **frame-relay intf-type** command in interface configuration mode. To change the configuration, use the **no** form of this command.

frame-relay intf-type {**dce**| **dte**}

no frame-relay intf-type {**dce**| **dte**}

Syntax Description

dce	Router functions as a switch connected to a router.
dte	Router is connected to a Frame Relay network.

Command Default

DTE

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

The **frame-relay intf-type** command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows how to configure a DCE switch type on the interface:

```
RP/0/0/CPU0:router(config)# interface pos 0/4/0/0
RP/0/0/CPU0:router(config-if)# frame-relay intf-type dce
```

frame-relay lmi disable

To disable the Frame Relay Local Management Interface (LMI), use the **frame-relay lmi disable** command in interface configuration mode. To reenable LMI, use the **no** form of this command.

frame-relay lmi disable

no frame-relay lmi disable

Syntax Description

This command has no keywords or arguments.

Command Default

LMI is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

The **frame-relay lmi disable** command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows how to configure a DCE switch type on the interface:

```
RP/0/0/CPU0:router(config)# interface pos 0/4/0/0
RP/0/0/CPU0:router(config-if)# frame-relay lmi disable
```

frame-relay lmi-n391dte

To set the full status polling interval, use the **frame-relay lmi-n391dte** command in interface configuration mode. To restore the default interval value, use the **no** form of this command.

frame-relay lmi-n391dte *polling-cycles*

no frame-relay lmi-n391dte *polling-cycles*

Syntax Description

polling-cycles	Number of Line Integrity Verification (LIV) exchanges performed before requesting a full status message. Range is from 1 to 255. The default is 6.

Command Default

The full status polling interval is 6.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

Use the **frame-relay lmi-n391dte** command to set the full status message polling interval. This command is relevant only when the interface type is data terminal equipment (DTE).

Two message types are supported: status inquiry and status. Status inquiry messages are sent from DTE to DCE. Status messages are sent from DCE to DTE (in response to a status inquiry). The Status (Full) and LIV report types are contained within these messages, and typically there is one status transaction for every five LIV transactions.

This command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows that one out of every four status inquiries generated requests a full status response from the DCE on the interface:

```
RP/0/0/CPU0:router(config)# interface pos 0/1/0/1
RP/0/0/CPU0:router(config-if)# frame-relay intf-type dte
RP/0/0/CPU0:router(config-if)# frame-relay lmi-n391dte 4
```

frame-relay lmi-n392dce

To set the error threshold on a DCE interface, use the **frame-relay lmi-n392dce** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

frame-relay lmi-n392dce *threshold*

no frame-relay lmi-n392dce *threshold*

Syntax Description

threshold	Error threshold value. Range is from 1 to 10. Default is 3.

Command Default

The DCE error threshold is 3.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

N392 errors must occur within the number defined by the N393 event count for the link to be declared down. Therefore, the threshold value for this command must be less than the count value defined in the **frame-relay lmi-n393dce** command.

The **frame-relay lmi-n392dce** command is relevant only when the interface type is data communication equipment (DCE).

This command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows how to set the Local Management Interface (LMI) failure threshold to 4. The router acts as a Frame Relay DCE switch:

```
RP/0/0/CPU0:router(config)# interface pos 0/1/0/1
RP/0/0/CPU0:router(config-if)# frame-relay intf-type dce
RP/0/0/CPU0:router(config-if)# frame-relay lmi-n392dce 4
```

Related Commands

Command	Description
frame-relay lmi-n393dce, on page 357	Sets the DCE monitored events count.

frame-relay lmi-n392dte

To set the error threshold on a DTE interface, use the **frame-relay lmi-n392dte** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

frame-relay lmi-n392dte *threshold*

no frame-relay lmi-n392dte *threshold*

Syntax Description

threshold	Error threshold value. Range is from 1 to 10. The default is 3.

Command Default

The DTE error threshold is 3.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

The **frame-relay lmi-n392dte** command is relevant only when the interface type is data terminal equipment (DTE).

This command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows how to set the Local Management Interface (LMI) failure threshold to 4. The router acts as a Frame Relay DTE switch.

```
RP/0/0/CPU0:router(config)# interface pos 0/1/0/1
RP/0/0/CPU0:router(config-if)# frame-relay intf-type dte
RP/0/0/CPU0:router(config-if)# frame-relay lmi-n392dte 4
```

frame-relay lmi-n393dce

To set the DCE monitored events count, use the **frame-relay lmi-n393dce** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

frame-relay lmi-n393dce *events*

no frame-relay lmi-n393dce *events*

Syntax Description

events	Monitored events count. Range is from 1 to 10. The default is 4.

Command Default

The number of DCE monitored events is 4.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

The **frame-relay lmi-n393dce** command is used along with the **frame-relay lmi-n392dce** command to define the condition that causes the link to be declared down.

N392 errors must occur within the *events* argument count in order for the link to be declared down. Therefore, the events value defined in this command must be greater than the threshold value defined in the **frame-relay lmi-n392 dce** command.

The **frame-relay lmi-n393dce** command is relevant only when the interface type is data communication equipment (DCE).

This **frame-relay lmi-n393dce** command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows how to set the Local Management Interface (LMI) monitored events count to 5.

```
RP/0/0/CPU0:router(config)# interface pos 0/1/0/1
RP/0/0/CPU0:router(config-if)# frame-relay intf-type dce
```

```
RP/0/0/CPU0:router(config-if)# frame-relay lmi-n393dce 5
```

Related Commands

Command	Description
frame-relay lmi-n392dce, on page 354	Sets the error threshold on a DCE interface.

frame-relay lmi-n393dte

To set the monitored event count on a DTE interface, use the **frame-relay lmi-n393dte** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

frame-relay lmi-n393dte *events*

no frame-relay lmi-n393dte *events*

Syntax Description

events	Monitored events count. Range is from 1 to 10. The default is 4.

Command Default

The number of DTE monitored events is 4.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

The **frame-relay lmi-n393dte** command is relevant only when the interface type is data terminal equipment (DTE).

This **frame-relay lmi-n393dte** command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows how to set the Local Management Interface (LMI) monitored events count to 5.

```
RP/0/0/CPU0:router(config)# interface pos 0/1/0/1
RP/0/0/CPU0:router(config-if)# frame-relay intf-type dte
RP/0/0/CPU0:router(config-if)# frame-relay lmi-n393dte 5
```

frame-relay lmi-t391dte

To set the Local Management Interface (LMI) polling interval, use the **frame-relay lmi-t391dte** command in interface configuration mode. To restore the default interval value, use the **no** form of this command.

frame-relay lmi-t391dte *seconds*

no frame-relay lmi-t391dte *seconds*

Syntax Description

seconds	Polling interval between each status inquiry from the DTE end, in seconds. Range is from 5 to 30. The default is 10.

Command Default

The LMI polling interval is 10 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

This **frame-relay lmi-t391dte** command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

The *seconds* value defined in this command must be less than the polling verification timer defined in the **frame-relay lmi-t392 dce** command.

The **frame-relay lmi-t391dte** command is relevant only when the interface type is data terminal equipment (DCE).

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows how to set the LMI polling timer interval to 15 seconds:

```
RP/0/0/CPU0:router(config)# interface pos 0/1/0/1
RP/0/0/CPU0:router(config-if)# frame-relay intf-type dte
RP/0/0/CPU0:router(config-if)# frame-relay lmi-t391dte 15
```

frame-relay lmi-t392dce

To set the Local Management Interface (LMI) polling verification timer on the DCE, use the **frame-relay lmi-t392dce** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

frame-relay lmi-t392dce *seconds*

no frame-relay lmi-t392dce *seconds*

Syntax Description

seconds	Polling verification timer, in seconds. The range is from 5 to 30. The default is 15.

Command Default

The LMI polling verification timer is 15 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

The **frame-relay lmi-t392dce** command is used along with the **frame-relay lmi-t391dte** command to define the condition that causes the link to be declared down.

The *seconds* value defined in this command must be greater than the polling verification timer defined in the **frame-relay lmi-t391 dte** command.

This **frame-relay lmi-n392dce** command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows how to set the Local Management Interface (LMI) polling timer interval to 30 seconds:

```
RP/0/0/CPU0:router(config)# interface pos 0/1/0/1
RP/0/0/CPU0:router(config-if)# frame-relay intf-type dce
```

```
RP/0/0/CPU0:router(config-if)# frame-relay lmi-t392dce 30
```

frame-relay lmi-type

To select the Local Management Interface (LMI) type, use the **frame-relay lmi-type** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

frame-relay lmi-type [**ansi**| **cisco**| **q933a**]

no frame-relay lmi-type [**ansi**| **cisco**| **q933a**]

Syntax Description

ansi	(Optional) Uses LMI as defined by ANSI T1.617a-1994 Annex D.
cisco	(Optional) Uses LMI as defined by Cisco (not standard).
q933a	(Optional) Uses LMI as defined by ITU-T Q.933 (02/2003) Annex A.

Command Default

The default is **cisco**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.5.0	The **ccitt** keyword was replaced with the **q933a** keyword.

Usage Guidelines

If the DTE is not explicitly configured or the **no** form is not used after explicit configuration, then the DTE automatically senses the LMI type of the DCE and use that type of LMI.

This **frame-relay lmi-type** command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows how to set the Local Management Interface (LMI) type to Q.933, Annex A:

```
RP/0/0/CPU0:router(config)# interface pos 0/1/0/1
RP/0/0/CPU0:router(config-if)# frame-relay lmi-type q933a
```

frame-relay multilink ack

To configure the MFR acknowledge timeout value for a Frame Relay multilink bundle link, use the **frame-relay multilink ack** command in interface configuration mode. To revert to the default settings, use the **no** form of this command.

frame-relay multilink ack *ack-timeout*

no frame-relay multilink ack

Syntax Description

ack-timeout	Ack timeout value, in seconds. The range is from 1 to 10.

Command Default

The default MFR acknowledge timeout value is 4 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

Note The **frame-relay multilink ack** command is supported only on serial interfaces. The **frame-relay multilink ack** command is not supported on Packet-over-SONET/SDH (POS) or multilink frame relay interfaces.

The **frame-relay multilink ack** command can be configured only on bundle link interfaces that have been associated with a bundle using the **encapsulation frame-relay mfr** command.

Note You can enter the **frame-relay multilink ack** command at any time without affecting the current state of the interface; however, the configured timeout value does not go into effect until the interface has gone from the down state to the up state. One way to bring the interface down and back up again is by using the **shutdown** and **no shutdown** commands in interface configuration mode.

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows how to configure the MFR acknowledge timeout value as 2 seconds. for the serial interface 0/3/1/0:

```
RP/0/0/CPU0:router(config)# interface serial 0/3/1/0
RP/0/0/CPU0:router(config-if)# frame-relay multilink ack 2
```

Related Commands

Command	Description
encapsulation frame-relay, on page 349	Enables Frame Relay encapsulation.
frame-relay multilink bid, on page 368	Assigns a BID name to a multilink Frame Relay bundle.
show frame-relay lmi-info, on page 381	Displays frame relay information for the LMI.
shutdown (interface)	Disables an interface.

frame-relay multilink bandwidth-class

To configure the bandwidth class for a Frame Relay multilink bundle interface, use the **frame-relay multilink bid bandwidth-class** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

frame-relay multilink bandwidth-class {**a**| **b**| **c** *threshold*}

no frame-relay multilink bandwidth-class

Syntax Description

a	Configures bandwidth class A. When one or more member links are up, the bundle interface is up. When all the member links are down, the bundle interface is down.
b	Configures bandwidth class B. When all the member links are up, the bundle interface is up. When any member link is down, the bundle interface is down.
c	Configures bandwidth class C. The bundle link *threshold* must be configured.
threshold	Minimum number of links that must be up for the bundle interface to be up. The range is 1 to 255.

Command Default

The default is a (Bandwidth Class A).

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

Bandwidth class is configurable only under Frame Relay Forum 16.1 (FRF 16.1).

Note The **frame-relay multilink bandwidth-class** command is supported only on multilink frame relay interfaces. The **frame-relay multilink bandwidth-class** command is not supported on Packet-over-SONET/SDH (POS) or serial interfaces.

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows how to set a multilink frame relay interface to bandwidth Class C with a threshold of 3:

```
RP/0/0/CPU0:router(config)# interface Multilink 0/3/1/0/100
RP/0/0/CPU0:router(config-if)# frame-relay multilink bandwidth-class c 3
```

Related Commands

Command	Description
show frame-relay lmi-info, on page 381	Displays Frame Relay information for the LMI.

frame-relay multilink bid

To create a name for a Frame Relay multilink bundle interface, use the **frame-relay multilink bid** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

frame-relay multilink bid bundle-id-name

no frame-relay multilink bid

Syntax Description

bundle-id-name	Name for the Frame Relay multilink bundle. The bundle identifier (**bid**) name identifies the bundle interface at both endpoints. The **bid** name is exchanged in the information elements to ensure consistent link assignments. The **bid** name can be up to 50 characters including the null termination character. The **bid** name is configured at the bundle interface level and is applied to each member link.

Command Default

By default, the interface name, for example, Multilink 0/4/1/0/1, is used as the bundle identifier.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelin

Note The **frame-relay multilink bid** command is supported only on multilink frame relay interfaces. The **frame-relay multilink bid** command is not supported on Packet-over-SONET/SDH (POS) or serial interfaces.

Regardless of whether you create a bundle identifier name using the **frame-relay multilink bid** command or whether the system uses the default name for the interface, each bundle should have a unique name.

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows how to create a Frame Relay multilink interface bundle identifier name:

```
RP/0/0/CPU0:router(config)# interface Multilink 0/3/1/0/100
```

```
RP/0/0/CPU0:router(config-if)# frame-relay multilink bid MFRBundle
```

Related Commands

Command	Description
show frame-relay lmi-info, on page 381	Displays Frame Relay information for the LMI.

frame-relay multilink hello

To configure the hello interval used by a Frame Relay multilink bundle link, use the **frame-relay multilink hello** command in interface configuration mode. To reset the name to the default, use the **no** form of this command.

frame-relay multilink hello *hello-interval*

no frame-relay multilink hello

Syntax Description

hello-interval	Hello interval for the Frame Relay multilink bundle link, in seconds. The range is from 1 to 180.

Command Default

The default hello interval is 10 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

Note The **frame-relay multilink hello** command is supported only on serial interfaces. The **frame-relay multilink hello** command is not supported on Packet-over-SONET/SDH (POS) or multilink frame relay interfaces.

The **frame-relay multilink hello** command can be configured only on bundle link interfaces that have been associated with a bundle using the **encapsulation frame-relay mfr** command.

Note You can enter the **frame-relay multilink hello** command at any time without affecting the current state of the interface; however, the configured hello interval value does not go into effect until the interface has gone from the down state to the up state. One way to bring the interface down and back up again is by using the **shutdown** and **no shutdown** commands in interface configuration mode.

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows how to configure the hello interval value as 10 seconds. for the serial interface 0/3/1/0:

```
RP/0/0/CPU0:router(config)# interface serial 0/3/1/0
RP/0/0/CPU0:router(config-if)# frame-relay multilink hello 10
```

Related Commands

Command	Description
encapsulation frame-relay, on page 349	Enables Frame Relay encapsulation.
frame-relay multilink bid, on page 368	Assigns a BID name to a multilink Frame Relay bundle.
show frame-relay lmi-info, on page 381	Displays frame relay information for the LMI.
shutdown (interface)	Disables an interface.

frame-relay multilink lid

To create a name for a Frame Relay multilink bundle link, use the **frame-relay multilink lid** command in interface configuration mode. To reset the name to the default, use the **no** form of this command.

frame-relay multilink lid *link-id name*

no frame-relay multilink lid

Syntax Description

link-id name	Specifies the name for the Frame Relay multilink bundle link. The link identifier (lid) name can be up to 49 characters long.

Command Default

The name of the physical interface, for example, Serial 0/3/0/0/1/2:0, is used as the lid.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelin

Note The **frame-relay multilink lid** command is supported only on serial interfaces. The **frame-relay multilink lid** command is not supported on Packet-over-SONET/SDH (POS) or multilink frame relay interfaces.

The **frame-relay multilink lid** command can be configured only on bundle link interfaces that have been associated with a bundle using the **encapsulation frame-relay mfr** command.

Note You can enter the **frame-relay multilink lid** command at any time without affecting the current state of the interface; however, the link identifier name does not go into effect until the interface has gone from the down state to the up state. One way to bring the interface down and back up again is by using the **shutdown** and **no shutdown** commands in interface configuration mode.

Thelid name is used to identify the bundle link to peer devices and to enable the devices to identify which bundle links are associated with which bundles. The lid name can also be assigned when the bundle link is created using the **encapsulation frame-relay mfr** command with the *name* argument. If a lid name is not assigned, the default lid is the name of the physical interface.

The local and peer lid names do not have to be unique. However, regardless of whether you create a lid name using the **frame-relay multilink lid** command or the systems uses the default name for the bundle link, each

link within a bundle must have a unique name. If the same name is used by different links in the same bundle, the bundles will flap indefinitely.

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows how to configure the lid name as 'BL1' for the serial interface 0/3/1/0:

```
RP/0/0/CPU0:router(config)# interface serial 0/3/1/0
RP/0/0/CPU0:router(config-if)# frame-relay multilink lid BL1
```

Related Commands

Command	Description
encapsulation frame-relay, on page 349	Enables Frame Relay encapsulation.
frame-relay multilink bid, on page 368	Assigns a BID name to a multilink Frame Relay bundle.
show frame-relay lmi-info, on page 381	Displays frame relay information for the LMI.
shutdown (interface)	Disables an interface.

frame-relay multilink retry

To configure the retry count for retransmissions for a Frame Relay multilink bundle link, use the **frame-relay multilink retry** command in interface configuration mode. To reset the name to the default, use the **no** form of this command.

frame-relay multilink retry *retry-count*

no frame-relay multilink retry

Syntax Description

retry-count	Retry count for retransmissions. The range is from 1 to 5.

Command Default

The default retry count for retransmissions is 2.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

Note The **frame-relay multilink retry** command is supported only on serial interfaces. The **frame-relay multilink retry** command is not supported on Packet-over-SONET/SDH (POS) or multilink frame relay interfaces.

The **frame-relay multilink retry** command can be configured only on bundle link interfaces that have been associated with a bundle using the **encapsulation frame-relay mfr** command.

Note You can enter the **frame-relay multilink retry** command at any time without affecting the current state of the interface; however, the configured retry count value does not go into effect until the interface has gone from the down state to the up state. One way to bring the interface down and back up again is by using the **shutdown** and **no shutdown** commands in interface configuration mode.

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows how to configure the retry count for retransmissions as 2 on the serial interface 0/3/1/0:

```
RP/0/0/CPU0:router(config)# interface serial 0/3/1/0
RP/0/0/CPU0:router(config-if)# frame-relay multilink retry 2
```

Related Commands

Command	Description
encapsulation frame-relay, on page 349	Enables Frame Relay encapsulation.
frame-relay multilink bid, on page 368	Assigns a BID name to a multilink Frame Relay bundle.
show frame-relay lmi-info, on page 381	Displays frame relay information for the LMI.
shutdown (interface)	Disables an interface.

pvc (frame relay)

To associate a data-link connection identifier (DLCI) number to a permanent virtual circuit (PVC), and to enter Frame Relay PVC configuration mode, use the **pvc** command in subinterface configuration mode. To delete the PVC, use the **no** form of this command.

pvc *dlci-number*

no pvc *dlci-number*

Syntax Description

dlci-number	DLCI number used to identify the PVC. The range is from 16 to 1007.

Command Default

No PVC is defined.

Command Modes

Subinterface configuration (config-subif)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

Commands available in Frame Relay PVC configuration mode are:

```
RP/0/0/CPU0:router(config-fr-vc)# ?

  commit    Commit the configuration changes to running
  describe  Describe a command without taking real actions
  do        Run an exec command
  encap     Set the Encapsulation of this PVC
  exit      Exit from this submode
  no        Negate a command or set its defaults
  show      Show contents of configuration
```

The **pvc** command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows how to create a PVC with DLCI 16:

```
RP/0/0/CPU0:router(config)# interface pos 0/4/0/0.1 l2transport
RP/0/0/CPU0:router(config-subif)# pvc 16
```

```
RP/0/0/CPU0:router(config-fr-vc)#
```

show frame-relay lmi

To display Frame Relay statistics for the Local Management Interface (LMI), use the **show frame-relay lmi** EXEC command.

show frame-relay lmi [**interface** *type interface-path-id*| **location** *node-id*]

Syntax Description

interface	(Optional) Interface for which information is to be displayed.Use the *interface-path-id* argument to specify the interface.
type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location *node-id*	(Optional) Displays information about all interfaces on the specified node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

Frame Relay LMI statistics are displayed for all interfaces enabled for LMI.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

The **show frame-relay lmi** command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

This command is used to check the status enquiry and status message between DCE and DTE.

Task ID

Task ID	Operations
fr	read

Examples

The following example shows the output from the **show frame-relay lmi** command:

```
RP/0/0/CPU0:router# show frame-relay lmi

LMI Statistics for interface POS0/1/0/0/ (Frame Relay DCE) 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 9
  Invalid Information ID 0              Invalid Report IE Len 0
  Invalid Report Request 0              Invalid Keep IE Len 0
  Num Status Enq. Rcvd 9444             Num Status Msgs Sent 9444
  Num Full Status Sent 1578             Num St Enq. Timeouts 41
  Num Link Timeouts 7

LMI Statistics for interface POS0/1/0/1/ (Frame Relay DCE) 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 9481             Num Status Msgs Sent 9481
  Num Full Status Sent 1588             Num St Enq. Timeouts 16
  Num Link Timeouts 4
```

Table 22: show frame-relay lmi Field Descriptions

Field	Description
LMI Statistics	Signaling or LMI specification: CISCO, ANSI, or CCITT. **Note** CCITT is LMI as defined by ITU-T Q.933 (02/2003) Annex A.
Invalid Unnumbered Info	Number of received LMI messages with invalid unnumbered information field.
Invalid Dummy Call	Number of received LMI messages with invalid dummy calls.
Invalid Status Message	Number of received LMI messages with invalid status message.
Invalid Information ID	Number of received LMI messages with invalid information identifier.
Invalid Report Request	Number of received LMI messages with invalid report request.
Num Status Enq. Rcvd	Number of LMI status enquiry messages received.
Num Link Timeouts	Number of link timeouts.
Invalid Prot Disc	Number of received LMI messages with invalid protocol discriminator.

Field	Description
Invalid Msg Type	Number or received LMI messages with invalid message type.
Invalid Lock Shift	Number of received LMI messages with invalid lock shift type.
Invalid Report IE Len	Number of received LMI messages with invalid report IE Length.
Invalid Keep IE Len	Number of received LMI messages with invalid report request.
Num Status Msgs Sent	Number of LMI status enquiry messages sent.
Num St Enq. Timeouts	Number of times the status enquiry message was not received within the T392 DCE timer value.

show frame-relay lmi-info

To display Frame Relay information for the Local Management Interface (LMI), use the **show frame-relay lmi -info** command in EXEC mode.

show frame-relay lmi-info [**interface** *type interface-path-id*| **location** *node-id*] **[detail]**

Syntax Description

interface	(Optional) Displays information on the the interface specified by the *type interface-path-id* argument.
type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location *node-id*	(Optional) Displays information about all interfaces on the specified node. The *node-id* argument is entered in the *rack/slot/module* notation.
detail	(Optional) Displays managed dcli list.

Command Default

Displays LMI information for all Frame Relay interfaces enabled for LMI.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

The **show frame-relay lmi-info** command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

This command is used to check the status enquiry and status message between DCE and DTE.

Task ID

Task ID	Operations
fr	read

Examples

The following example shows sample output for the **show frame-relay lmi-info** command:

```
RP/0/0/CPU0:router# show frame-relay lmi-info

LMI IDB Info for interface Multilink0/3/0/0/2
  ifhandle:             0x6176840
  Interface type:       DTE
  Interface state:      UP
  Line Protocol:        UP
  LMI type (cnf/oper):  AUTO/CISCO
  LMI type autosense:   OFF
  Interface MTU:        1504
  -------------- DTE -------------
  T391:                 10s
  N391: (cnf/oper):     6/5
  N392: (cnf/oper):     3/0
  N393:                 4
  My seq#:              83
  My seq# seen:         83
  Your seq# seen:       82
  -------------- DCE -------------
  T392:                 15s
  N392: (cnf/oper):     3/0
  N393:                 4
  My seq#:              0
  My seq# seen:         0
  Your seq# seen:       0
LMI IDB Info for interface Multilink0/3/0/0/1
  ifhandle:             0x6186240
  Interface type:       DTE
  Interface state:      UP
  Line Protocol:        UP
  LMI type (cnf/oper):  AUTO/CISCO
  LMI type autosense:   OFF
  Interface MTU:        1504
  -------------- DTE -------------
  T391:                 10s
  N391: (cnf/oper):     6/5
  N392: (cnf/oper):     3/0
  N393:                 4
  My seq#:              83
  My seq# seen:         83
  Your seq# seen:       82
  -------------- DCE -------------
  T392:                 15s
  N392: (cnf/oper):     3/0
  N393:                 4
  My seq#:              0
  My seq# seen:         0
  Your seq# seen:       0
```

Table 23: show frame-relay lmi-info Field Descriptions

Field	Description
DTE	
T391	Local Management Interface polling interval
N391	Full status polling interval
N392	Error threshold value

Field	Description
N393	DTE monitored events count
DCE	
T392	Local Management Interface polling verification timer
N392	Error threshold value
N393	DCE monitored events count

show frame-relay multilink

To display the multilink Frame-Relay (MFR) information about the given interface along with MFR protocol and internal statistics, use the **show frame-relay multilink interface** command in EXEC mode.

show frame-relay multilink [**detail** [**location** *node id*]| **interface** *type interface-path-id* [**detail**| **verbose**]| **location** *node id*| **verbose** [**location** *node id*]]

Syntax Description

detail	(Optional) Displays Interface Descriptor Block (IDB) information and Feasible Successor Metrics (FSM) statistics.
location *node-id*	(Optional) Displays information about all interfaces on the specified node. The *node-id* argument is entered in the *rack*/*slot*/*module* notation.
interface	(Optional) Interface for which you want to display information.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
verbose	(Optional) Displays IDB information, FSM statistics and internal statistics.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.6.0	This command was introduced.
Release 3.7.0	The **verbose** keyword was added.

Usage Guidelines

Task ID

Task ID	Operations
fr	read

Examples

The following example shows how to display the multilink Frame-Relay information for all interfaces:

```
RP/0/0/CPU0:router# show frame-relay multilink

Bundle interface: Multilink0/3/0/0/1, ifhandle 0x060322c0
    Member Links: 2 active, 0 inactive
    State = Up,   BW Class = A

    Member Links:
    Serial0/3/0/0/1/2:0,   HW state = Up, link state = Up
    Serial0/3/0/0/1/1:0,   HW state = Up, link state = Up


Bundle interface: Multilink0/3/0/0/2, ifhandle 0x06032280
    Member Links: 2 active, 0 inactive
    State = Up,   BW Class = A

    Member Links:
    Serial0/3/0/0/1/4:0,   HW state = Up, link state = Up
    Serial0/3/0/0/1/3:0,   HW state = Up, link state = Up


Member interface: Serial0/3/0/0/1/1:0, ifhandle 0x060323c0
  HW state = Up, link state = Up
  Member of bundle interface Multilink0/3/0/0/1 with ifhandle 0x060322c0


Member interface: Serial0/3/0/0/1/2:0, ifhandle 0x06032380
  HW state = Up, link state = Up
  Member of bundle interface Multilink0/3/0/0/1 with ifhandle 0x060322c0


Member interface: Serial0/3/0/0/1/3:0, ifhandle 0x06032340
  HW state = Up, link state = Up
  Member of bundle interface Multilink0/3/0/0/2 with ifhandle 0x06032280


Member interface: Serial0/3/0/0/1/4:0, ifhandle 0x06032300
  HW state = Up, link state = Up
  Member of bundle interface Multilink0/3/0/0/2 with ifhandle 0x06032280
```

The following example shows how to display detailed multilink Frame-Relay information for all interfaces, including IDB information and FSM statistics:

```
RP/0/0/CPU0:router# show frame-relay multilink detail

Bundle interface: Multilink0/3/0/0/1, ifhandle 0x060322c0
    Member Links: 2 active, 0 inactive
    State = Up,   BW Class = A
      nodeid:             0x838
      group:              1
      my_bid:             Multilink0/3/0/0/1
      peer_bid:           Multilink0/6/0/0/1
      magic:              0x696d8a95
      flags:              0x0
      im_state:           3  [Up]
      fsm_req_state:      3  [Up]
      is_owned_resource:  Y
      is_zombie:          N
      active_mbr_count:   2
      cfg_bid:
      bw_class:           1
      bw_class_threshold: 0


    =============== Member Links ===============
```

```
Serial0/3/0/0/1/2:0,   HW state = Up, link state = Up
  my_lid:         Serial0/3/0/0/1/2:0
  peer_lid:       Serial0/6/0/0/1/2:0
  flags:          0x0
  fsm_state:      3  [Up]
  im_state:       3  [Up]
  fsm_req_state:  3  [Up]
  cause:          0  [None]
  retry_count:    0
  in_loopback:    No
  bc_init_rcvd:   Yes
  bc_owned_res:   Yes
  cc_owned_res:   Yes
  is_parent_up:   Yes
  Last Packet Tx: 00:00:09 ago
  Round trip:     00:00.000 (0 secs 999997 nsecs)
  Min Round trip: 00:00.000 (0 secs 999997 nsecs)
  Max Round trip: 00:00.003 (0 secs 3999988 nsecs)
  cfg_lid:
  mfr_t_hello:    10
  mfr_t_ack:      4
  mfr_retry_max:  2
  --------------- Member Link Statistics ---------------
  Add Link Tx:                3     Add Link Rx:                2
  Add Link Ack Tx:            2     Add Link Ack Rx:            1
  Add Link Rej Tx:            0     Add Link Rej Rx:            0
  Remove Link Tx:             0     Remove Link Rx:             0
  Remove Link Ack Tx:         0     Remove Link Ack Rx:         0
  Hello Tx:                6235     Hello Rx:                6236
  Hello Ack Tx:            6236     Hello Ack Rx:            6235
  Loopback Detected:          0     Invalid Pkts Rx:            0
  Bundle Mismatch:            0     Expired Ack Rx:             0
  Hello Timer expiry:      6236     Ack Timer expiry:           1

Serial0/3/0/0/1/1:0,   HW state = Up, link state = Up
  my_lid:         Serial0/3/0/0/1/1:0
  peer_lid:       Serial0/6/0/0/1/1:0
  flags:          0x0
  fsm_state:      3  [Up]
  im_state:       3  [Up]
  fsm_req_state:  3  [Up]
  cause:          0  [None]
  retry_count:    0
  in_loopback:    No
  bc_init_rcvd:   Yes
  bc_owned_res:   Yes
  cc_owned_res:   Yes
  is_parent_up:   Yes
  Last Packet Tx: 00:00:01 ago
  Round trip:     00:00.000 (0 secs 999997 nsecs)
  Min Round trip: 00:00.000 (0 secs 999997 nsecs)
  Max Round trip: 00:00.004 (0 secs 4999985 nsecs)
  cfg_lid:
  mfr_t_hello:    10
  mfr_t_ack:      4
  mfr_retry_max:  2
  --------------- Member Link Statistics ---------------
  Add Link Tx:                3     Add Link Rx:                2
  Add Link Ack Tx:            2     Add Link Ack Rx:            1
  Add Link Rej Tx:            0     Add Link Rej Rx:            0
  Remove Link Tx:             0     Remove Link Rx:             0
  Remove Link Ack Tx:         0     Remove Link Ack Rx:         0
  Hello Tx:                6234     Hello Rx:                6237
  Hello Ack Tx:            6237     Hello Ack Rx:            6234
  Loopback Detected:          0     Invalid Pkts Rx:            0
  Bundle Mismatch:            0     Expired Ack Rx:             0
  Hello Timer expiry:      6235     Ack Timer expiry:           1


Bundle interface: Multilink0/3/0/0/2, ifhandle 0x06032280
    Member Links: 2 active, 0 inactive
```

```
State = Up,   BW Class = A
  nodeid:             0x838
  group:              2
  my_bid:             Multilink0/3/0/0/2
  peer_bid:           Multilink0/6/0/0/2
  magic:              0x303c008f
  flags:              0x0
  im_state:           3  [Up]
  fsm_req_state:      3  [Up]
  is_owned_resource:  Y
  is_zombie:          N
  active_mbr_count:   2
  cfg_bid:
  bw_class:           1
  bw_class_threshold: 0


=============== Member Links ===============

Serial0/3/0/0/1/4:0,   HW state = Up, link state = Up
  my_lid:         Serial0/3/0/0/1/4:0
  peer_lid:       Serial0/6/0/0/1/4:0
  flags:          0x0
  fsm_state:      3  [Up]
  im_state:       3  [Up]
  fsm_req_state:  3  [Up]
  cause:          0  [None]
  retry_count:    0
  in_loopback:    No
  bc_init_rcvd:   Yes
  bc_owned_res:   Yes
  cc_owned_res:   Yes
  is_parent_up:   Yes
  Last Packet Tx: 00:00:00 ago
  Round trip:     00:00.000 (0 secs 999997 nsecs)
  Min Round trip: 00:00.000 (0 secs 999997 nsecs)
  Max Round trip: 00:00.004 (0 secs 4999985 nsecs)
  cfg_lid:
  mfr_t_hello:    10
  mfr_t_ack:      4
  mfr_retry_max:  2
  --------------- Member Link Statistics ---------------
  Add Link Tx:                3     Add Link Rx:                2
  Add Link Ack Tx:            2     Add Link Ack Rx:            1
  Add Link Rej Tx:            0     Add Link Rej Rx:            0
  Remove Link Tx:             0     Remove Link Rx:             0
  Remove Link Ack Tx:         0     Remove Link Ack Rx:         0
  Hello Tx:                6236     Hello Rx:                6235
  Hello Ack Tx:            6235     Hello Ack Rx:            6236
  Loopback Detected:          0     Invalid Pkts Rx:            0
  Bundle Mismatch:            0     Expired Ack Rx:             0
  Hello Timer expiry:      6237     Ack Timer expiry:           1

Serial0/3/0/0/1/3:0,   HW state = Up, link state = Up
  my_lid:         Serial0/3/0/0/1/3:0
  peer_lid:       Serial0/6/0/0/1/3:0
  flags:          0x0
  fsm_state:      3  [Up]
  im_state:       3  [Up]
  fsm_req_state:  3  [Up]
  cause:          0  [None]
  retry_count:    0
  in_loopback:    No
  bc_init_rcvd:   Yes
  bc_owned_res:   Yes
  cc_owned_res:   Yes
  is_parent_up:   Yes
  Last Packet Tx: 00:00:01 ago
  Round trip:     00:00.000 (0 secs 999997 nsecs)
  Min Round trip: 00:00.000 (0 secs 999997 nsecs)
  Max Round trip: 00:00.003 (0 secs 3999988 nsecs)
  cfg_lid:
  mfr_t_hello:    10
```

```
      mfr_t_ack:      4
      mfr_retry_max:  2
      --------------- Member Link Statistics ---------------
      Add Link Tx:                3     Add Link Rx:                2
      Add Link Ack Tx:            2     Add Link Ack Rx:            1
      Add Link Rej Tx:            0     Add Link Rej Rx:            0
      Remove Link Tx:             0     Remove Link Rx:             0
      Remove Link Ack Tx:         0     Remove Link Ack Rx:         0
      Hello Tx:                6236     Hello Rx:                6237
      Hello Ack Tx:            6237     Hello Ack Rx:            6236
      Loopback Detected:          0     Invalid Pkts Rx:            0
      Bundle Mismatch:            0     Expired Ack Rx:             0
      Hello Timer expiry:      6237     Ack Timer expiry:           1

Member interface: Serial0/3/0/0/1/1:0, ifhandle 0x060323c0
  HW state = Up, link state = Up
  Member of bundle interface Multilink0/3/0/0/1 with ifhandle 0x060322c0
  Local bid: Multilink0/3/0/0/1  Peer bid: Multilink0/6/0/0/1
      my_lid:         Serial0/3/0/0/1/1:0
      peer_lid:       Serial0/6/0/0/1/1:0
      flags:          0x0
      fsm_state:      3  [Up]
      im_state:       3  [Up]
      fsm_req_state:  3  [Up]
      cause:          0  [None]
      retry_count:    0
      in_loopback:    No
      bc_init_rcvd:   Yes
      bc_owned_res:   Yes
      cc_owned_res:   Yes
      is_parent_up:   Yes
      Last Packet Tx: 00:00:00 ago
      Round trip:     00:00.000 (0 secs 999997 nsecs)
      Min Round trip: 00:00.000 (0 secs 999997 nsecs)
      Max Round trip: 00:00.004 (0 secs 4999985 nsecs)
      cfg_lid:
      mfr_t_hello:    10
      mfr_t_ack:      4
      mfr_retry_max:  2
      --------------- Member Link Statistics ---------------
      Add Link Tx:                3     Add Link Rx:                2
      Add Link Ack Tx:            2     Add Link Ack Rx:            1
      Add Link Rej Tx:            0     Add Link Rej Rx:            0
      Remove Link Tx:             0     Remove Link Rx:             0
      Remove Link Ack Tx:         0     Remove Link Ack Rx:         0
      Hello Tx:                6235     Hello Rx:                6237
      Hello Ack Tx:            6237     Hello Ack Rx:            6235
      Loopback Detected:          0     Invalid Pkts Rx:            0
      Bundle Mismatch:            0     Expired Ack Rx:             0
      Hello Timer expiry:      6236     Ack Timer expiry:           1

Member interface: Serial0/3/0/0/1/2:0, ifhandle 0x06032380
  HW state = Up, link state = Up
  Member of bundle interface Multilink0/3/0/0/1 with ifhandle 0x060322c0
  Local bid: Multilink0/3/0/0/1  Peer bid: Multilink0/6/0/0/1
      my_lid:         Serial0/3/0/0/1/2:0
      peer_lid:       Serial0/6/0/0/1/2:0
      flags:          0x0
      fsm_state:      3  [Up]
      im_state:       3  [Up]
      fsm_req_state:  3  [Up]
      cause:          0  [None]
      retry_count:    0
      in_loopback:    No
      bc_init_rcvd:   Yes
      bc_owned_res:   Yes
      cc_owned_res:   Yes
      is_parent_up:   Yes
      Last Packet Tx: 00:00:00 ago
      Round trip:     00:00.000 (0 secs 999997 nsecs)
      Min Round trip: 00:00.000 (0 secs 999997 nsecs)
      Max Round trip: 00:00.003 (0 secs 3999988 nsecs)
      cfg_lid:
```

```
      mfr_t_hello:    10
      mfr_t_ack:      4
      mfr_retry_max:  2
      --------------- Member Link Statistics ---------------
      Add Link Tx:                3     Add Link Rx:                2
      Add Link Ack Tx:            2     Add Link Ack Rx:            1
      Add Link Rej Tx:            0     Add Link Rej Rx:            0
      Remove Link Tx:             0     Remove Link Rx:             0
      Remove Link Ack Tx:         0     Remove Link Ack Rx:         0
      Hello Tx:                6236     Hello Rx:                6237
      Hello Ack Tx:            6237     Hello Ack Rx:            6236
      Loopback Detected:          0     Invalid Pkts Rx:            0
      Bundle Mismatch:            0     Expired Ack Rx:             0
      Hello Timer expiry:      6237     Ack Timer expiry:           1

Member interface: Serial0/3/0/0/1/3:0, ifhandle 0x06032340
  HW state = Up, link state = Up
  Member of bundle interface Multilink0/3/0/0/2 with ifhandle 0x06032280
  Local bid: Multilink0/3/0/0/2  Peer bid: Multilink0/6/0/0/2
      my_lid:         Serial0/3/0/0/1/3:0
      peer_lid:       Serial0/6/0/0/1/3:0
      flags:          0x0
      fsm_state:      3  [Up]
      im_state:       3  [Up]
      fsm_req_state:  3  [Up]
      cause:          0  [None]
      retry_count:    0
      in_loopback:    No
      bc_init_rcvd:   Yes
      bc_owned_res:   Yes
      cc_owned_res:   Yes
      is_parent_up:   Yes
      Last Packet Tx: 00:00:02 ago
      Round trip:     00:00.000 (0 secs 999997 nsecs)
      Min Round trip: 00:00.000 (0 secs 999997 nsecs)
      Max Round trip: 00:00.003 (0 secs 3999988 nsecs)
      cfg_lid:
      mfr_t_hello:    10
      mfr_t_ack:      4
      mfr_retry_max:  2
      --------------- Member Link Statistics ---------------
      Add Link Tx:                3     Add Link Rx:                2
      Add Link Ack Tx:            2     Add Link Ack Rx:            1
      Add Link Rej Tx:            0     Add Link Rej Rx:            0
      Remove Link Tx:             0     Remove Link Rx:             0
      Remove Link Ack Tx:         0     Remove Link Ack Rx:         0
      Hello Tx:                6236     Hello Rx:                6237
      Hello Ack Tx:            6237     Hello Ack Rx:            6236
      Loopback Detected:          0     Invalid Pkts Rx:            0
      Bundle Mismatch:            0     Expired Ack Rx:             0
      Hello Timer expiry:      6237     Ack Timer expiry:           1

Member interface: Serial0/3/0/0/1/4:0, ifhandle 0x06032300
  HW state = Up, link state = Up
  Member of bundle interface Multilink0/3/0/0/2 with ifhandle 0x06032280
  Local bid: Multilink0/3/0/0/2  Peer bid: Multilink0/6/0/0/2
      my_lid:         Serial0/3/0/0/1/4:0
      peer_lid:       Serial0/6/0/0/1/4:0
      flags:          0x0
      fsm_state:      3  [Up]
      im_state:       3  [Up]
      fsm_req_state:  3  [Up]
      cause:          0  [None]
      retry_count:    0
      in_loopback:    No
      bc_init_rcvd:   Yes
      bc_owned_res:   Yes
      cc_owned_res:   Yes
      is_parent_up:   Yes
      Last Packet Tx: 00:00:01 ago
      Round trip:     00:00.000 (0 secs 999997 nsecs)
      Min Round trip: 00:00.000 (0 secs 999997 nsecs)
      Max Round trip: 00:00.004 (0 secs 4999985 nsecs)
```

```
    cfg_lid:
    mfr_t_hello:    10
    mfr_t_ack:      4
    mfr_retry_max:  2
    --------------- Member Link Statistics ---------------
    Add Link Tx:                3     Add Link Rx:                2
    Add Link Ack Tx:            2     Add Link Ack Rx:            1
    Add Link Rej Tx:            0     Add Link Rej Rx:            0
    Remove Link Tx:             0     Remove Link Rx:             0
    Remove Link Ack Tx:         0     Remove Link Ack Rx:         0
    Hello Tx:                6236     Hello Rx:                6235
    Hello Ack Tx:            6235     Hello Ack Rx:            6236
    Loopback Detected:          0     Invalid Pkts Rx:            0
    Bundle Mismatch:            0     Expired Ack Rx:             0
    Hello Timer expiry:      6237     Ack Timer expiry:           1
```

The following example shows how to display the multilink Frame-Relay information for the interface at location 0/3/0/0/1:

```
RP/0/0/CPU0:router# show frame-relay multilink interface multilink 0/3/0/0/1

Bundle interface: Multilink0/3/0/0/1, ifhandle 0x060322c0
    Member Links: 2 active, 0 inactive
    State = Up,   BW Class = A

    Member Links:
    Serial0/3/0/0/1/2:0,   HW state = Up, link state = Up
    Serial0/3/0/0/1/1:0,   HW state = Up, link state = Up
```

Related Commands

Command	Description
interface multilink, on page 512	Configures a multilink interface and enters multilink interface configuration mode.
frame-relay multilink bid, on page 368	Creates a name for a Frame Relay multilink bundle interface.

show frame-relay pvc

To display statistics about Frame Relay permanent virtual circuits (PVCs), use the **show frame-relay pvc** command in EXEC mode.

show frame-relay pvc [**interface** *type interface-path-id*| **location** *node-id*] [*dlci-number*]

Syntax Description

interface	(Optional) Interface for which information is to be displayed. Use the *type* and *interface-path-id* arguments to specify the interface.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location *node-id*	(Optional) Displays information about all interfaces on the specified node. The *node-id* argument is entered in the *rack/slot/module* notation.
dlci-number	(Optional) DLCI number used to identify the PVC. The range is from 16 to 1007.

Command Default

Information for all Frame Relay interfaces and PVCs is displayed.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 4.0.0	The Fragmentation Statistics section of output and counters was added.

Usage Guidelines

The **show frame-relay pvc** command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

This command is used to check the status of PVCs on interfaces.

Task ID

Task ID	Operations
fr	read

Examples

The following example shows the output from the **show frame-relay pvc** command:

```
RP/0/0/CPU0:router# show frame-relay pvc

PVC Statistics for interface POS0/3/2/0 (Frame Relay DCE)

              Active     Inactive      Deleted       Static
  Local          4           0            0             0
  Switched       0           0            0             0
  Dynamic        0           0            0             0

DLCI = 612, DLCI USAGE = LOCAL, ENCAP = CISCO, INHERIT = TRUE, PVC STATUS = ACT
VE, INTERFACE = POS0/3/2/0.1
  input pkts 0          output pkts 0           in bytes 0
  out bytes 0           dropped pkts 0          in FECN packets 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 00:00:00      last time pvc status changed 00:00:00

DLCI = 613, DLCI USAGE = LOCAL, ENCAP = CISCO, INHERIT = TRUE, PVC STATUS = ACT
VE, INTERFACE = POS0/3/2/0.2
  input pkts 0          output pkts 0           in bytes 0
  out bytes 0           dropped pkts 0          in FECN packets 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 00:00:00      last time pvc status changed 00:00:00

DLCI = 614, DLCI USAGE = LOCAL, ENCAP = CISCO, INHERIT = TRUE, PVC STATUS = ACT
VE, INTERFACE = POS0/3/2/0.3
  input pkts 0          output pkts 0           in bytes 0
  out bytes 0           dropped pkts 0          in FECN packets 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 00:00:00      last time pvc status changed 00:00:00

DLCI = 615, DLCI USAGE = LOCAL, ENCAP = CISCO, INHERIT = TRUE, PVC STATUS = ACT
VE, INTERFACE = POS0/3/2/0.4
  input pkts 0          output pkts 0           in bytes 0
  out bytes 0           dropped pkts 0          in FECN packets 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 00:00:00      last time pvc status changed 00:00:00
```

The following example shows the output for a specific frame-relay PVC:

```
RP/0/0/CPU0:router# show frame-relay pvc 613

DLCI = 613, DLCI USAGE = LOCAL, ENCAP = CISCO, INHERIT = TRUE, PVC STATUS = ACTI
VE, INTERFACE = POS0/3/2/0.2
  input pkts 0          output pkts 0           in bytes 0
  out bytes 0           dropped pkts 0          in FECN packets 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 00:00:00      last time pvc status changed 00:00:00
```

The following example shows the output for a specific frame-relay PVC with fragment counters enabled:

```
RP/0/0/CPU0:router# show frame-relay pvc interface serial 0/3/2/0/1/1:0 16

Tue Jul 28 11:03:11.646 UTC

DLCI = 16, DLCI USAGE = LOCAL, ENCAP = CISCO, INHERIT = TRUE, PVC STATUS = ACTIVE, INTERFACE
 = Serial0/3/2/0/1/1:0.1 (Frame Relay DTE)
  input pkts 100        output pkts 100         in bytes 80400
  out bytes 80800       dropped pkts 0          in FECN packets 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 Tue Jul 28 11:01:25 2009
  last time pvc status changed Tue Jul 28 11:02:14 2009


  Fragmentation Statistics

  fragment type end-to-end              fragment size 256
  Input Fragmented packets 400          Input Fragmented bytes 0
  Output Fragmented packets 400         Output Fragmented bytes 0
  Input Unfragmented packets 0          Input Unfragmented bytes 0
  Output Unfragmented packets 0         Output Unfragmented bytes 0
  Input Reassembled packets 100         Input Reassembled bytes 0
  Fragment Counters Enabled
```

Table 24: 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.
ENCAP	Type of encapsulation.
INHERIT	Encapsulation type for the PVC is inherited from the main interface.
PVC STATUS	Status of the PVC: ACTIVE, INACTIVE, or DELETED.
INTERFACE	Specific subinterface associated with this DLCI.
input pkts	Number of packets received on this PVC.
output pkts	Number of packets sent on this PVC.
in bytes	Number of bytes received on this PVC.
out bytes	Number of bytes sent on this PVC.

Field	Description
dropped pkts	Number of incoming and outgoing packets dropped by the router at the Frame Relay level.
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.
pvc create time	Time at which the PVC was created.
last time pvc status changed	Time at which the PVC changed status.
shaping drops	Number of packets dropped by the traffic-shaping process.
Fragment Counters	Displays whether fragment counters are enabled or disabled on the PVC. Fragment counters are disabled by default. Use the **fragment-counter** command to enable collection of these statistics.

show frame-relay vcm-info interface

To display Virtual Circuit (VC) manager information for a given interface, use the **show frame-relay vcm-info interface** command in EXEC mode.

show frame-relay vcm-info interface *type interface-path-id* [**vc** *dlci*]

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
vc	(Optional) Specifies a VC on the interface.
dlci	(Optional) Data-link Connection Identifier number. Range is from 0 to 1023.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
fr	read

Examples

The following example shows how to display Virtual Circuit (VC) manager information for the multilink interface 0/1/0/0:

```
RP/0/0/CPU0:router# show frame-relay vcm-info interface multilink 0/3/0/0/1

VCM IDB:Multilink0_3_0_0_1
==================================
```

```
IDB type:               IFT_MAIN
<main specific>
  i/f term type:        L3
  i/f handle:           0x06186240
  BW:                   0x00000c00
  OIR insert:           F
VC chkpt oid:           0x00000000
proto info:             500323c8 [ptr]
proto fn table:         500323d4 [ptr]
i/f type:               0x00000037 [IFT_MULTILINK]
i/f state:              0x00000003 [up]
i/f basecaps num:       0x0000004c [fr]
i/f basecaps state:     0x00000003 [up]
VCM states:             5002c708 [ptr]
in db:                  T
chkpt:                  F
datapath info           0 [0 bytes]
partner info            50016d98 [16 bytes]
  encaps type:          IETF
  intf type:            DTE
non chkptd info         0 [0 bytes]
```

Related Commands

Command	Description
interface multilink, on page 512	Configures a multilink interface and enters multilink interface configuration mode.
frame-relay multilink bid, on page 368	Creates a name for a Frame Relay multilink bundle interface.

show interfaces (frame relay)

To display statistics about Frame Relay interfaces, use the **show interfaces** command in EXEC mode.

show interfaces [**summary**| [*type interface-path-id*] [**brief**| **description**| **detail**| **accounting [rates]**]] [**location** *node-id*]

Syntax Description

summary	(Optional) Displays a summary of interface information by interface type.
type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
brief	(Optional) Displays brief information about each interface (one line per interface).
description	(Optional) Displays an interface description.
detail	(Optional) Displays detailed information about each interface. This is the default.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
rates	(Optional) Displays interface accounting rates.
location *node-id*	(Optional) Displays information about all interfaces on the specified node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

EXEC (#)

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

The **show interfaces** (Frame Relay) command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows the output from the **show interfaces** command when the interface is configured with Frame Relay encapsulation:

```
RP/0/0/CPU0:router# show interfaces pos 0/1/0/0

POS0/1/0/0 is up, line protocol is up
  Hardware is Packet over SONET/SDH
  Internet address is Unknown
  MTU 4474 bytes, BW 622080 Kbit
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, crc 32, controller loopback not set,
  LMI enq sent  0, LMI stat recvd 0, LMI upd recvd 0
  LMI enq recvd 9463, LMI stat sent  9463, LMI upd sent  0, DCE LMI up
  LMI DLCI 0  LMI type is ANSI Annex D  frame relay DCE
  Last clearing of "show interface" counters never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     20934 packets input, 1508069 bytes, 1151 total input drops
     0 drops for unrecognized upper-level protocol
     Received 0 broadcast packets, 0 multicast packets
              0 runts, 0 giants, 0 throttles, 0 parity
     1151 input errors, 1058 CRC, 0 frame, 0 overrun, 93 ignored, 0 abort
     19590 packets output, 990924 bytes, 0 total output drops
     Output 0 broadcast packets, 0 multicast packets
     0 output errors, 0 underruns, 0 applique, 0 resets
     0 output buffer failures, 0 output buffers swapped out
```

Table 25: show interfaces Field Descriptions

Field	Description
Interface name	Displays the name of the current interface. In the example, the interface name is POS0/1/0/0.
Interface state	Displays the state of the interface. In the example, the interface is in the administratively up state.

Field	Description
Line protocol state	Displays the state of the Layer 2 line protocol. This field may be different from the interface state if, for example, a keepalive failure has brought down the Layer 2. **Note** The line protocol state is not the same as the protocol state displayed in the **show ip interfaces** command, because it is the state of Layer 2 (media) rather than Layer 3 (IP protocol).
Hardware	Displays the current hardware type.
Internet address is *n.n.n.n/n*	Displays the Layer 2 address (MAC address for Ethernet interfaces). **Note** Enter the **mac-address** command to configure the hardware address.
MTU	Displays the maximum transmission unit (MTU) for the interface. The MTU is the maximum packet size that can be transmitted over the interface. **Note** The MTU field indicates the interface MTU. Enter the **mtu** command to configure a lower MTU value at the layer 3 level.
BW	Displays the bandwidth of the interface in kbps.
reliability	Displays the proportion of packets that are not dropped and do not have errors. **Note** The reliability is shown as a fraction of 255.
txload	Indicates the traffic flowing out of the interface as a proportion of the bandwidth. **Note** The txload is shown as a fraction of 255.
rxload	Indicates the traffic flowing into the interface as a proportion of the bandwidth. **Note** The rxload is shown as a fraction of 255.
Encapsulation	Layer 2 encapsulation installed on the interface.
CRC	Indicates the length of the cyclic redundancy check (CRC), in bytes. **Note** Enter the **pos crc** command to configure the CRC.

Field	Description
controller loopback	Indicates that the hardware was configured as controller loopback.
LMI enq sent	Number of LMI enquiry messages sent.
LMI stat recvd	Number of LMI status messages received.
LMI upd recvd	Number of LMI updated messages received.
LMI enq recvd	Number of LMI enquiry messages received.
LMI stat sent	Number of LMI status messages sent.
LMI upd sent	Number of LMI updated messages sent.
DCE LMI	Displays the state of the DCE LMI.
LMI DLCI	Displays the LMI DLCI identifier.
LMI type	Displays the LMI type.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing for example, load and reliability) are not cleared when the counters are cleared.
5 minute input rate5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average is within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
Received...broadcasts	Total number of broadcast or multicast packets received by the interface

Field	Description
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.
CRC	Cyclic redundancy checksum generated by the originating station or far-end device does not match the checksum calculated from the data received. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
abort	Illegal sequence of one bits on a serial interface. This usually indicates a clocking problem between the serial interface and the data link equipment.
carrier transitions	Number of times the carrier detect signal of a serial interface has changed state. For example, if data carrier detect (DCD) goes down and comes up, the carrier transition counter will increment two times. Indicates modem or line problems if the carrier detect line is changing state often.

snmp-server traps frame-relay pvc

To enable Simple Network Management Protocol (SNMP) trap notifications for a Frame Relay permanent virtual circuit (PVC), use the **snmp-server traps frame-relay pvc** command in global configuration mode. To disable SNMP notifications for a FR PVC, use the **no** form of this command.

snmp-server traps frame-relay pvc [**interval** *seconds*]

no snmp-server traps frame-relay pvc [**interval** *seconds*]

Syntax Description

interval *seconds*	(Optional) Minimum period between successive traps. The range is from 1 to 3600.

Command Default

seconds: 30

Command Modes

Global configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

Use the **snmp-server traps frame-relay pvc** command to enable trap requests for a Frame Relay PVC. This command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

See *Implementing SNMP on Cisco IOS XR Software* in *Cisco IOS XR System Management Configuration Guide for the Cisco XR 12000 Series Router* for detailed information about SNMP configuration tasks and commands.

Task ID

Task ID	Operations
snmp	read, write
fr	read, write

Examples

The following example shows how to configure the router to send SNMP trap notifications for a Frame Relay PVC:

```
RP/0/0/CPU0:router(config)# snmp-server host 12.26.25.61 traps public udp-port 5000
```

```
RP/0/0/CPU0:router(config)# snmp-server community public RW
RP/0/0/CPU0:router(config)# snmp-server traps frame-relay pvc interval 50
```

Related Commands

Command	Description
snmp-server community	Configures the community access string to permit access to the SNMP.
snmp-server host	Specifies the recipient of an SNMP notification operation.

Global Interface Commandsonthe Cisco IOS XR Software

This module describes the global command line interface (CLI) commands for configuring interfaces on the Cisco XR 12000 Series Router.

bandwidth (global)

To configure the bandwidth of an interface, use the **bandwidth** command in interface configuration mode.

bandwidth *rate*

Syntax Description

rate	Amount of bandwidth to be allocated on the interface, in Kilobits per second (kbps). Range is from 0 through 4294967295.

Command Default

The default bandwidth depends on the interface type.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Note To obtain the default bandwidth for a specific interface, use the **show interfaces** command after you first bring up the interface. The default interface bandwidth is displayed in the **show interfaces** command output.

Task ID

Task ID	Operations
interface	execute
basic-services	read, write

Examples

This example shows how to configure the bandwidth on a Ten Gigabit Ethernet interface:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router# interface TenGigE 0/4/1/0
RP/0/0/CPU0:router# bandwidth 4000000
```

Related Commands

Command	Description
interface (global), on page 414	Configures an interface or creates or configures a virtual interface.
shutdown (global), on page 434	Disables an interface (forces an interface to be administratively down).

clear interface

To clear interface statistics or packet counters, use the **clear interface** command in EXEC mode.

clear interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use these guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.
- If specifying a virtual interface, the number range varies, depending on interface type.

Task ID

Task ID	Operations
interface	execute

Task ID	Operations
basic-services	read, write

Examples

This example shows how to use the **clear interface** command to clear the loopback interface 2:

```
RP/0/0/CPU0:router# clear interface loopback 2
```

Related Commands

Command	Description
interface (global), on page 414	Configures an interface or creates or configures a virtual interface.
shutdown (global), on page 434	Disables an interface (forces an interface to be administratively down).

controller SYSCLOCK

To configure a system clock (telecom-bus clock) controller, use the **controller sysclock** command in global configuration mode. This command does not have a no form.

controller sysclock *location*

Syntax Description

location	Fully qualified location in the notation is *rack/slot/module*. A slash is required between values as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the modular services card or line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure a system clock (telecom-bus clock) controller:

```
RP/0/0/CPU0:Router(config)# controller sysclock 0/0/1
RP/0/0/CPU0:Router(config)#
```

Related Commands

Command	Description
controller t3, on page 780	Configures a T3 controller and enters T3 configuration mode.
clock source (T3/E3), on page 772	Sets clocking for individual T3 or E3 links.
show controllers t3, on page 837	Displays information about the T3 links and hardware and software drivers for the T3 controller.

dampening

To limit propagation of transient or frequently changing interface states on Interface Manager (IM) clients, turn on event dampening by using the **dampening** command in interface configuration mode. To turn dampening off, use the **no** form of this command.

dampening [*half-life* [*reuse suppress max-suppress-time*]]

no dampening [*half-life* [*reuse suppress max-suppress-time*]]

Syntax Description

half-life	(Optional) Time (in minutes) after which a penalty is decreased. Once the interface has been assigned a penalty, the penalty is decreased by half after the half-life period. The process of reducing the penalty happens every 5 seconds. The range of the half-life period is 1 to 45 minutes. The default is 1 minute.
reuse	(Optional) Penalty value below which a stable interface is unsuppressed. Range is from 1 through 20000. Default value is 750.
suppress	(Optional) Limit at which an interface is suppressed when its penalty exceeds that limit. Range is from 1 through 20000, and must be greater than the reuse threshold. The default value is 2000.
max-suppress-time	(Optional) Maximum time (in minutes) that an interface can be suppressed. This value effectively acts as a ceiling that the penalty value cannot exceed. Default value is four times the half-life period.

Command Default

Dampening is turned off by default. When you use the **dampening** command, the following default values are enabled for any optional parameters that you do not enter:

- *half-life*: 1 minute
- *reuse*: 750
- *suppress*: 2000
- *max-suppress-time*: Four times the half-life

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced

Usage Guidelines

Event dampening suppresses a constantly unstable interface until it remains stable for a period of time. Enabling dampening on an interface that already has dampening configured has the effect of resetting the penalty associated with that interface to zero. The reuse threshold must always be less than the suppress threshold.

Consider the following guidelines when configuring event dampening:

- Configuring dampening on both a subinterface and its parent is usually unnecessary because their states are almost always the same and dampening would be triggered at the same time on each interface.
- If all subinterfaces require dampening, then apply dampening to the main interface only. Applying configuration to large numbers of subinterfaces requires an abundance of memory and increases the time required to process the configuration during boot and failover.
- When dampening is enabled, an interface has a penalty value associated with it. The value starts at 0 and is increased by 1000 whenever the underlying state of the interface changes from up to down.
- The penalty value decreases exponentially while the interface state is stable. If the penalty value exceeds a configured suppress threshold, then the state of the interface is suppressed and IM will not notify upper layers of further state transitions. The suppressed state remains until the penalty value decreases past a configured reuse threshold.

Task ID

Task ID	Operations
interface	read, write

Examples

This example shows how to enable dampening with default values on an interface:

```
RP/0/0/CPU0:router(config)# interface TenGigE 0/4/0/0
RP/0/0/CPU0:router(config-if))# dampening
```

Related Commands

Command	Description
show im dampening, on page 419	Displays the state of all interfaces on which dampening has been configured.

interface (global)

To configure an interface or to create or configure a virtual interface, use the **interface** command in global configuration mode. To delete the interface configuration, use the **no** form of this command.

interface *type interface-path-id*

no interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No interfaces are configured

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.
- If specifying a virtual interface, the number range varies, depending on interface type.

The **interface** command enters interface configuration mode to allow you to configure interfaces. If a virtual interface is configured, then the interface is created if it did not already exist.

The **no** form of this command applies only to virtual interfaces or to subinterfaces (that is, interfaces that have been created in global configuration mode).

Task ID

Task ID	Operations
interface	read, write

Examples

In the following example, the **interface** command is given for the POS card in location 0/2/0/1, and interface configuration mode is entered for that interface:

```
RP/0/0/CPU0:router(config)# interface POS 0/2/0/1
```

Related Commands

Command	Description
clear interface, on page 408	Clears interface statistics or packet counters.
shutdown (global), on page 434	Disables an interface (forces an interface to be administratively down).

mtu

To adjust the maximum transmission unit (MTU) value for packets on the interface, use the **mtu** command in interface configuration mode. To return the interface to the default MTU for the interface type, use the **no** form of this command.

mtu *bytes*

no mtu

Syntax Description

bytes	Maximum number of bytes in a Layer 2 frame. Range is from 64 through 65535.

Command Default

The default MTU for each interface is as follows:

- Ethernet—1514 bytes
- POS—4474 bytes
- Tunnel—1500 bytes
- Loopback—1514 bytes
- ATM—4470 bytes

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **mtu** command to set a specific MTU value for an interface, or use the **no mtu** command to return the interface to the default MTU value for that interface type. The MTU value can be increased or decreased using the **mtu** command, subject to minimum and maximum MTU limits for the interface type.

If the MTU value is not configured, then each interface will have a default MTU value that is specific to the interface type. The default MTU value is generally the largest Layer 2 frame size possible for the interface type.

The default/configured MTU value on an atm interface includes the L2 header.

The MTU size consists of L2 header that includes either SNAP(8bytes)/MUX(0)/NLPID(2) header or the AAL5 SDU. The AAL5 SDU includes the L3 datagram and the optional Logical Link Control/Subnetwork Access Protocol (LLC/SNAP) header.

The Ethernet interface is the Layer 3 datagram plus 14 bytes. For ATM main interface, the MTU is L3 datagram + 0 bytes.

For ATM L3 sub interface, mtu is as follows:

- SNAP - L3 datagram + 8 bytes
- NLPID - L3 datagram + 2 bytes
- MUX - L3datagram + 0 bytes
- When no pvc is configured under sub interface - L3datagram + 0 bytes

Note All serial links in a Multilink Point-to-Point Protocol (MLPPP) bundle or a Multilink Frame Relay (MFR) bundle inherit the default MTU value from the multilink bundle. If a serial interface has a nondefault MTU value, the Cisco IOS XR software blocks that serial interface from being added to an MLPPP or MFR bundle. Therefore, you must not configure the MTU value on a serial interface until you have added that serial interface to an MLPPP or MFR bundle.

You can use the **show interfaces** command to determine if the MTU value has been changed. The **show interfaces** command output displays the MTU size for each interface in the MTU (byte) field.

Note You can use the **show interfaces** command to determine if the MTU value has been changed. The **show interfaces** command output displays the MTU size for each interface in the MTU (byte) field. Note that the MTU size that is displayed includes the Layer 2 header bytes used for each encapsulation type.

Note Changing the MTU on an interface triggers a change on the protocols and capsulations configured on that interface, although some protocol-specific configurations can override the interface MTU. For example, specifically changing the interface MTU configuration does not affect the IP MTU configuration, but may affect the resulting MTU on that node.

Task ID

Task ID	Operations
interface	read, write

Examples

In the following example, the MTU value for all interfaces is verified. The MTU value is shown in the next-to-last column:

```
RP/0/0/CPU0:router# show interfaces all brief

                 Intf        Intf         LineP              Encap  MTU       BW
                 Name        State        State               Type (byte)    (Kbps)
--------------------------------------------------------------------------------
                  Nu0          up           up               Null  1500   Unknown
           TenGigE6/0/0/0      up           up               HDLC  4474   2488320
           TenGigE6/0/0/1      up           up               HDLC  4474   2488320
           TenGigE6/0/0/2   admin-down   admin-down          HDLC  4474   2488320
           TenGigE6/0/0/3   admin-down   admin-down          HDLC  4474   2488320
      Mg0/RP0/CPU0/0           up           up               ARPA  1514    100000
```

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface TenGigE 6/0/0/0
RP/0/0/CPU0:router(config-if)# mtu 1000
```

After the **mtu** command is used to decrease the MTU Layer 2 frame size for the POS interface on 6/0/0/0 to 1000 bytes, the **show interfaces all brief** command is used again to verify that the MTU Layer 2 frame size has been changed:

```
RP/0/0/CPU0:router# show interfaces all brief

                Intf        Intf         LineP              Encap  MTU       BW
                Name        State        State               Type (byte)    (Kbps)
--------------------------------------------------------------------------------
                 Nu0          up           up                Null  1500   Unknown
           PO6/0/0/0          up           up                HDLC  1000   2488320
           PO6/0/0/1          up           up                HDLC  4474   2488320
           PO6/0/0/2   admin-down   admin-down              HDLC  4474   2488320
           PO6/0/0/3   admin-down   admin-down              HDLC  4474   2488320
 Mg0/RP0/CPU0/0           up           up              ARPA  1514    100000
```

Related Commands

Command	Description
shutdown (global), on page 434	Disables an interface (forces an interface to be administratively down).

show im dampening

To display the state of all interfaces on which dampening has been configured, use the **show im dampening** command in EXEC mode.

show im dampening [**interface** *type*| **ifhandle** *handle*]

Syntax Description

interface *type*	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
ifhandle *handle*	(Optional) Identifies the caps node whose Interface Manager (IM) dampening information you want to display.

Command Default

If you do not specify an interface, then the system displays brief details about all dampened interfaces.

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

If you do not specify an interface, then the system displays brief details about all dampened interfaces.

The physical hardware (layer 1) is not the only part of an interface that can change state. L2 keepalive failure event is one of the many instances that can have a similar impact on routing protocols despite the underlying interface state staying UP. To take account of such events, when dampening is configured on an interface, it is applied independently to every layer. They all use the same parameters as the interface but they have their own penalty value which is incremented when that layer changes state.

Capsulations that may be dampened in this way include these:

- L2 basecaps, such as HDLC and PPP, which may flap if keepalives are not received due to events such as intermittent packet loss.
- L3 capsulations (for example ipv4, ipv6). These may be brought down if another link has a conflicting IP address configured.
- Other locations where negotiation takes place with a peer router, as in the case of PPP control protocols such as IPCP. If the negotiation fails, then the caps is brought down.

Task ID

Task ID	Operations
interface	read

Examples

This example shows the output from the **show im dampening** command issued with default values:

```
RP/0/0/CPU0:router(config)# interface TenGigE 0/4/0/0
RP/0/0/CPU0:router(config-if)# no shutdown
RP/0/0/CPU0:router(config-if)# dampening
RP/0/0/CPU0:router# show im dampening

Interface               Proto              Caps               Penalty Suppressed

---------               -----              ----               ----------------
TenGigE0/4/0/0              0                  0                   0       NO

RP/0/0/CPU0:router# show im dampening interface TenGigE 0/4/0/0

TenGigE0/4/0/0 (0x05000d00)
Dampening enabled: penalty 0, not suppressed
  underlying state: Up
  half_life: 1        reuse:             750
  suppress:  3000     max-suppress-time: 4
  restart-penalty:   0

RP/0/0/CPU0:router# show interfaces TenGigE 0/4/0/0

TenGigE0/4/0/0 is up, line protocol is down
  Dampening enabled: penalty 0, not suppressed
    half_life: 1        reuse:             750
    suppress:  3000     max-suppress-time: 4
    restart-penalty:  0
  Hardware is Ten Gigabit Ethernet
  Description: ensoft-gsr5 TenGigE 4\2
  Internet address is Unknown
  MTU 4474 bytes, BW 155520 Kbit
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, controller loopback not set, keepalive set (10 sec)
  Last clearing of "show interface" counters never
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 total input drops
     0 drops for unrecognized upper-level protocol
     Received 0 broadcast packets, 0 multicast packets
              0 runts, 0 giants, 0 throttles, 0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     48 packets output, 1504 bytes, 0 total output drops
     Output 0 broadcast packets, 0 multicast packets
     0 output errors, 0 underruns, 0 applique, 0 resets
     0 output buffer failures, 0 output buffers swapped out
```

This sample output shows a POS interface with PPP basecaps and IPCP. The subsequent output for **show im dampening interface <ifname>** contains a table of any capsulations which have their own penalty as shown below:

```
RP/0/0/CPU0:router# show im dampening

Interface                 Protocol           Capsulation          Pen   Sup
------------------------- ------------------ -------------------- ----- ---
GigabitEthernet0/0/0/0                                            629 NO
```

```
GigabitEthernet0/0/0/1                                                  2389 YES
POS0/2/0/0                                                                 0 NO
POS0/2/0/0                  <base>            ppp                          0 NO
POS0/2/0/0                  ipv4              ipcp                         0 NO
```

```
RP/0/0/CPU0:router# show im dampening interface TenGigaE 0/1/0/0

TenGigE 0/1/0/0 (0x01180020)
Dampening enabled: Penalty 1625, SUPPRESSED (42 secs remaining)
  Underlying state: Down
  half-life: 1        reuse:             1000
  suppress:  1500     max-suppress-time: 4
  restart-penalty:  0

Protocol       Capsulation        Pen   Suppression              U-L State
-------------- ------------------ ----- ---------------------- -------------
 ipv6           ipv6               1625  YES    42s  remaining         Down
```

Note When dampening is configured on an interface it is also applied independently to all capsulations on that interface. For example, the ppp or hdlc basecaps state can flap even while the interface stays up and if keepalives fail. The **show im dampening interface** command contains one line for each such capsulation as well as the interface itself.

Table 26: show im dampening Field Descriptions

Field	Description
Dampening	Indicates the dampening state and penalty value: not suppressed, suppressed.
underlying state	Underlying state of the interface: up, down, administratively down (if an interface has been configured to be “shutdown”).
half_life	This is the time (in minutes) at which the penalty on the interface would be half that of the original penalty (of 1000) when the interface transitions from UP to DOWN. It ranges from 1 to 45 minutes and the default is 1 minute.
reuse	Penalty value below which a stable interface is unsuppressed. It ranges from 1 to 20000 and the default value is 750.
suppress	Limit at which an unstable interface is suppressed when the penalty value exceeds the suppress value. It ranges from 1 to 20000 and the default value is 2000.
max-suppress-time	Maximum time (in minutes) that an interface can be suppressed. The default is 4 minutes.
restart-penalty	Penalty assigned to the interface when it flaps.

Related Commands

Command	Description
dampening, on page 412	Turns on event dampening.
shutdown (global), on page 434	Disables an interface (forces an interface to be administratively down).

show interfaces

To display statistics for all interfaces configured on the router or for a specific node, use the **show interfaces** command in EXEC mode.

show interfaces [*type interface-path-id*| **all**| **local**| **location** *node-id*] [**accounting**| **brief**| **description**| **detail**| **summary**]

Syntax Description

type	(Optional) Specifies the type of interface for which you want to display statistics. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
all	(Optional) Displays interface information for all interfaces .This is the default.
local	(Optional) Displays interface information for all interfaces in the local card.
location *node-id*	(Optional) Displays information about all interfaces on the specified node. The *node-id* argument is entered in the *rack/slot/module* notation.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
brief	(Optional) Displays brief information of each interface (one line per interface).

description	(Optional) Displays the status, protocol, and description of each interface (one line per interface).
detail	(Optional) Displays detailed information about each interface. This is the default.
summary	(Optional) Displays a summary of interface information by interface type.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.8.4	The err-disable interface state was added as a possible interface state output value for bundle member links that have been administratively shut down.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.
- If specifying a virtual interface, the number range varies, depending on interface type.

The **show interfaces** command displays statistics for the network interfaces. The resulting display shows the interface processors in slot order.

For example, if you type the **show interfaces** command without an interface type, you receive information for all the interfaces installed in the networking device. Only by specifying the interface *type*, *slot*, and *port* arguments can you display information for a particular interface.

If you enter a **show interfaces** command for an interface type that has been removed from the networking device, an error message is displayed: “Interface not found.”

The output displayed depends on the network for which an interface has been configured.

Beginning in Cisco IOS XR Release 3.8.4, when you shut down a bundle interface, the member links are put into err-disable link interface status and admin-down line protocol state.

Note The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average is within 2 percent of the instantaneous rate of a uniform stream of traffic over that period.

Task ID

Task ID	Operations
interface	read

Examples

The following example shows the output from the **show interfaces** command. The output displayed depends on the type and number of interface cards in the networking device.

```
RP/0/0/CPU0:router# show interfaces tenGigE 0/0/0/1

TenGigE0/0/0/1 is administratively down, line protocol is administratively down
  Hardware is TenGigE, address is 0800.4539.d909 (bia 0800.4539.d909)
  Description: user defined string
  Internet address is Unknown
  MTU 1514 bytes, BW 10000000 Kbit
     reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation ARPA,
  Full-duplex, 10000Mb/s, LR
  output flow control is off, input flow control is off
  loopback not set
  ARP type ARPA, ARP timeout 01:00:00
  Last clearing of "show interface" counters never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 total input drops
     0 drops for unrecognized upper-level protocol
     Received 0 broadcast packets, 0 multicast packets
              0 runts, 0 giants, 0 throttles, 0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 total output drops
     Output 0 broadcast packets, 0 multicast packets
     0 output errors, 0 underruns, 0 applique, 0 resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

In the following sample output, instance 1 is specified on a Packet-over-SONET/SDH (POS) card:

```
RP/0/0/CPU0:router# show interfaces POS 0/1/0/1

POS0/1/0/1 is administratively down, line protocol is administratively down
  Hardware is Packet over SONET
  Internet address is n.n.n.n/n
  MTU 4474 bytes, BW 9953280 Kbit
     reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation HDLC, crc 32, controller loopback not set, keepalive not set
  Last clearing of "show interface" counters never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

```
     0 packets input, 0 bytes, 0 total input drops
     0 drops for unrecognized upper-level protocol
     Received 0 broadcast packets, 0 multicast packets
              0 runts, 0 giants, 0 throttles, 0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 total output drops
     Output 0 broadcast packets, 0 multicast packets
     0 output errors, 0 underruns, 0 applique, 0 resets
     0 output buffer failures, 0 output buffers swapped out
```

The following example shows sample output for ATM subinterface 0/4/2/0/1.1:

```
RP/0/0/CPU0:router# show interfaces ATM0/4/2/0/1.1

ATM0/4/2/0/1.1 is up, line protocol is up
  Interface state transitions: 1
  Hardware is ATM network sub-interface(s)
  Description: Connected to PE22_C12406 ATM 0/4/0/0/1.1
  Internet address is 10.212.4.21/24
  MTU 4486 bytes, BW 1544 Kbit
     reliability Unknown, txload Unknown, rxload Unknown
  Encapsulation AAL5/SNAP, controller loopback not set,
  Last clearing of "show interface" counters Unknown
  Datarate information unavailable.
  Interface counters unavailable.
```

Note The **show interfaces atm** *interface-path-id* command does not display data rates and counters for an ATM subinterface. Alternatively, you can use the **show interfaces atm** *interface-path-id* **accounting** command to view packet and character counters for each protocol, and the **show atm pvc** *vpi*/*vci* command to view cell, packet, and byte counters.

The following example shows bundle member links whose link interface status is “err-disable” and line protocol state is “admin-down” after the bundle interface has been administratively shut down using the **shutdown** command:

```
RP/0/0/CPU0:router# show interfaces brief

Thu May  6 06:30:55.797 DST

               Intf       Intf        LineP              Encap  MTU        BW
               Name       State       State               Type (byte)    (Kbps)
--------------------------------------------------------------------------------
               BE16  admin-down  admin-down               ARPA  9216    1000000
          BE16.160          up          up        802.1Q VLAN  9220    1000000
          BE16.161          up          up        802.1Q VLAN  9220    1000000
          BE16.162          up          up        802.1Q VLAN  9220    1000000
          BE16.163          up          up        802.1Q VLAN  9220    1000000
               Lo0          up          up           Loopback  1500    Unknown
               Nu0          up          up               Null  1500    Unknown
           tt44190          up          up             TUNNEL  1500    Unknown
           tt44192          up          up             TUNNEL  1500    Unknown
           tt44194          up          up             TUNNEL  1500    Unknown
           tt44196          up          up             TUNNEL  1500    Unknown
      Mg0/0/CPU0/0          up          up               ARPA  1514     100000
      Mg0/0/CPU0/1  admin-down  admin-down               ARPA  1514      10000

         Gi0/1/0/0  admin-down  admin-down               ARPA  1514    1000000
         Gi0/1/0/1  admin-down  admin-down               ARPA  1514    1000000
         Gi0/1/0/2          up          up               ARPA  9014    1000000
         Gi0/1/0/3          up          up               ARPA  9014    1000000
     Gi0/1/0/3.160          up          up        802.1Q VLAN  9022    1000000
     Gi0/1/0/3.161          up          up        802.1Q VLAN  9018    1000000
     Gi0/1/0/3.185          up          up        802.1Q VLAN  9022    1000000
     Gi0/1/0/3.189          up          up        802.1Q VLAN  9022    1000000
     Gi0/1/0/3.215          up          up        802.1Q VLAN  9022    1000000
```

```
      Gi0/1/0/4  admin-down  admin-down              ARPA  1514    1000000
      Gi0/1/0/5  admin-down  admin-down              ARPA  1514    1000000
      Gi0/1/0/6  admin-down  admin-down              ARPA  1514    1000000
      Gi0/1/0/7          up          up              ARPA  9014    1000000
  Gi0/1/0/7.185          up          up       802.1Q VLAN  9022    1000000
  Gi0/1/0/7.187          up          up       802.1Q VLAN  9014    1000000
  Gi0/1/0/7.189          up          up       802.1Q VLAN  9022    1000000
  Gi0/1/0/7.210          up          up       802.1Q VLAN  9022    1000000
  Gi0/1/0/7.211          up          up       802.1Q VLAN  9022    1000000
  Gi0/1/0/7.215          up          up       802.1Q VLAN  9022    1000000
      Gi0/1/0/8          up          up              ARPA  9014    1000000
      Gi0/1/0/9  admin-down  admin-down              ARPA  1514    1000000
     Gi0/1/0/10  admin-down  admin-down              ARPA  1514    1000000
     Gi0/1/0/11  admin-down  admin-down              ARPA  1514    1000000
     Gi0/1/0/12          up          up              ARPA  9216    1000000
     Gi0/1/0/13  admin-down  admin-down              ARPA  1514    1000000
     Gi0/1/0/14  admin-down  admin-down              ARPA  1514    1000000
     Gi0/1/0/15  admin-down  admin-down              ARPA  1514    1000000
     Gi0/1/0/16          up          up              ARPA  9216    1000000
     Gi0/1/0/17          up          up              ARPA  1514    1000000
     Gi0/1/0/18          up          up              ARPA  9216    1000000
     Gi0/1/0/19          up          up              ARPA  9014    1000000
Gi0/1/0/19.2127          up          up       802.1Q VLAN  9022    1000000
Gi0/1/0/19.2130          up          up       802.1Q VLAN  9022    1000000
     Gi0/1/0/20          up          up              ARPA  9014    1000000
Gi0/1/0/20.2125          up          up       802.1Q VLAN  9022    1000000
     Gi0/1/0/21  admin-down  admin-down              ARPA  1514    1000000
     Gi0/1/0/22  admin-down  admin-down              ARPA  1514    1000000
     Gi0/1/0/23          up          up              ARPA  9216    1000000
     Gi0/1/0/24  admin-down  admin-down              ARPA  1514    1000000
     Gi0/1/0/25  admin-down  admin-down              ARPA  1514    1000000
     Gi0/1/0/26  admin-down  admin-down              ARPA  1514    1000000
     Gi0/1/0/27          up          up              ARPA  1514    1000000
     Gi0/1/0/28  admin-down  admin-down              ARPA  1514    1000000
     Gi0/1/0/29  admin-down  admin-down              ARPA  1514    1000000
     Gi0/1/0/30          up          up              ARPA  9014    1000000
 Gi0/1/0/30.215          up          up       802.1Q VLAN  9018    1000000
     Gi0/1/0/31          up          up              ARPA  9014    1000000
     Gi0/1/0/32  admin-down  admin-down              ARPA  1514    1000000
     Gi0/1/0/33  admin-down  admin-down              ARPA  1514    1000000
     Gi0/1/0/34  admin-down  admin-down              ARPA  1514    1000000
     Gi0/1/0/35  admin-down  admin-down              ARPA  1514    1000000
     Gi0/1/0/36  admin-down  admin-down              ARPA  1514    1000000
     Gi0/1/0/37  admin-down  admin-down              ARPA  1514    1000000
     Gi0/1/0/38  admin-down  admin-down              ARPA  1514    1000000
     Gi0/1/0/39  admin-down  admin-down              ARPA  1514    1000000
      Te0/4/0/0  err-disable admin-down              ARPA  1514   10000000
      Te0/4/0/1  err-disable admin-down              ARPA  1514   10000000
      Te0/4/0/2  err-disable admin-down              ARPA  1514   10000000
      Te0/4/0/3  err-disable admin-down              ARPA  1514   10000000
      Te0/4/0/4  err-disable admin-down              ARPA  1514   10000000
      Te0/4/0/5  err-disable admin-down              ARPA  1514   10000000
      Te0/4/0/6  err-disable admin-down              ARPA  1514   10000000
      Te0/4/0/7  err-disable admin-down              ARPA  1514   10000000
      Te0/6/0/0  admin-down  admin-down              ARPA  1514   10000000
      Te0/6/0/1  admin-down  admin-down              ARPA  1514   10000000
      Te0/6/0/2  admin-down  admin-down              ARPA  1514   10000000
      Te0/6/0/3  admin-down  admin-down              ARPA  1514   10000000
```

Table 27: show interfaces Field Descriptions

Field	Description
Interface name	Displays the name of the current interface. For example, TenGigE 0/1/0/1.
Interface state	Displays the state of the interface. For example, the interface is in the administratively up state.

Field	Description
Interface state transitions	Displays the number of times since the last reload that the interface transitioned from the administratively up state to the administrative down state and from the administratively down state to the administratively up state.
line protocol state	Displays the state of the Layer 2 line protocol. This field may be different from the interface state if, for example, a keepalive failure has brought down the Layer 2. **Note** The line protocol state is not the same as the protocol state displayed in the **show ip interfaces** command, because it is the state of Layer 2 (media) rather than Layer 3 (IP protocol).
Hardware	Displays the current hardware type.
Internet address is *n.n.n.n/n*	Displays the Layer 2 address (MAC address for Ethernet interfaces). **Note** Enter the **mac-address** command to configure the hardware address.
bia	Displays the burned-in address (BIA) for the interface. The BIA is the default L2 (MAC) address for the interface. **Note** The BIA is not configurable.
description	Displays the user-defined string that is associated with the interface. **Note** Enter the **description** command to configure the description associated with the interface.
Internet Address	Displays the Layer 3 (IP) address for the interface. **Note** Enter the **ipv4 address** command to configure the internet address for the interface.
MTU	Displays the maximum transmission unit (MTU) for the interface. The MTU is the maximum packet size that can be transmitted over the interface. **Note** The MTU field indicates the interface MTU. Enter the **mtu** command to configure a lower MTU value at the Layer 3 level.
BW	Displays the bandwidth of the interface in kbps.

Field	Description
reliability	Displays the proportion of packets that are not dropped and do not have errors. **Note** The reliability is shown as a fraction of 255.
txload	Indicates the traffic flowing out of the interface as a proportion of the bandwidth. **Note** The txload is shown as a fraction of 255.
rxload	Indicates the traffic flowing into the interface as a proportion of the bandwidth. **Note** The rxload is shown as a fraction of 255.
Encapsulation	Layer 2 encapsulation installed on the interface.
CRC	Indicates the length of the cyclic redundancy check (CRC), in bytes. **Note** The CRC is not present for all interface types. **Note** Enter the **pos crc** command to configure the CRC.
loopback or controller loopback	Indicates whether the hardware has been configured to be looped back. **Note** Enter the **loopback** command to configure the loopback or controller loopback.
keepalive	Displays the configured keepalive value, in seconds. **Note** Enter the **keepalive** command to configure the value of the keepalive field. **Note** The *keepalive* field may not be present if it is not applicable to the interface type.
Duplexity	Displays the duplexity of the link. **Note** This field is present only for shared media. **Note** For some interface types, you can configure the duplexity by entering the **full-duplex** and **half-duplex** commands.
Speed	Speed and bandwidth of the link in Mbps. This field is present only when other parts of the media info line are also displayed (see duplexity and media type).
Media Type	Media type of the interface.

Field	Description
output flow control	Whether output flow control is enabled on the interface.
input flow control	See output flow control.
ARP type	Address Resolution Protocol (ARP) type used on the interface. This value is not displayed on interface types that do not use ARP.
ARP timeout	ARP timeout in *hours*:*mins*:*secs*. This value is configurable using the **arp timeout** command.
Last clearing of counters	Time since the following counters were last cleared using the **clear counters** exec command in *hours*:*mins*:*secs*.
5 minute input rate	Average number of bits and packets received per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic that it sends and receives (rather than all network traffic). **Note** The 5-minute period referenced in the command output is a load interval that is configurable under the interface. The default value is 5 minutes. **Note** The 5-minute input should be used only as an approximation of traffic per second during a given 5-minute period. This rate is exponentially weighted average with a time constant of 5 minutes. A period of four time constants must pass before the average is within two percent of the instantaneous rate of a uniform stream of traffic over that period.

Field	Description
5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic that it sends and receives (rather than all network traffic). **Note** The 5-minute period referenced in the command output is a load interval that is configurable under the interface. The default value is 5 minutes. **Note** The 5-minute output should be used only as an approximation of traffic per second during a given 5-minute period. This rate is exponentially weighted average with a time constant of 5 minutes. A period of four time constants must pass before the average is within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Number of packets received on the interface that were successfully delivered to higher layers.
bytes input	Total number of bytes successfully received on the interface
total input drops	Total number of packets that were dropped after they were received. This includes packets that were dropped due to configured quality of service (QoS) or access control list (ACL) policies. QoS drops include policer drops, WRED drops, and tail drops. This does not include drops due to unknown Layer 3 protocol.
drops for unrecognized upper-level protocol	Total number of packets that could not be delivered because the necessary protocol was not configured on the interface.
Received broadcast packets	Total number of Layer 2 broadcast packets received on the interface. This is a subset of the total input packet count.
Received multicast packets	Total number of Layer 2 multicast packets received on the interface. This is a subset of the total input packet count.
runts	Number of received packets that were too small to be handled. This is a subset of the input errors count.
giants	Number of received packets that were too large to be handled. This is a subset of the input errors count.

Field	Description
throttles	Number of packets dropped due to throttling (because the input queue was full).
parity	Number of packets dropped because the parity check failed.
input errors	Total number of received packets that contain errors and hence cannot be delivered. Compare this to total input drops, which counts packets that were not delivered despite containing no errors.
CRC	Number of packets that failed the CRC check.
frame	Number of packets with bad framing bytes.
overrun	Number of overrun errors experienced by the interface. Overruns represent the number of times that the receiver hardware is unable to send received data to a hardware buffer because the input rate exceeds the receiver's ability to handle the data.
ignored	Total number of ignored packet errors. Ignored packets are those that are discarded because the interface hardware does not have enough internal buffers. Broadcast storms and bursts of noise can result in an increased number of ignored packets.
abort	Total number of abort errors on the interface.
packets output	Number of packets received on the interface that were successfully delivered to higher layers.
bytes output	Total number of bytes successfully received on the interface.
total output drops	Number of packets that were dropped before being transmitted. This includes packets that were dropped due to configured quality of service (QoS), (policer drops, WRED drops, and tail drops).
Received broadcast packets	Number of Layer 2 broadcast packets transmitted on the interface. This is a subset of the total input packet count.
Received multicast packets	Total number of Layer 2 multicast packets transmitted on the interface. This is a subset of the total input packet count.

Field	Description
output errors	Number of times that the receiver hardware was unable to handle received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
underruns	Number of underrun errors experienced by the interface. Underruns represent the number of times that the hardware is unable to transmit data to a hardware buffer because the output rate exceeds the transmitter’s ability to handle the data.
applique	Number of applique errors.
resets	Number of times that the hardware has been reset. The triggers and effects of this event are hardware-specifc.
output buffer failures	Number of times that a packet was not output from the output hold queue because of a shortage of MEMD shared memory.
output buffers swapped out	Number of packets stored in main memory when the output queue is full; swapping buffers to main memory prevents packets from being dropped when output is congested. The number is high when traffic is bursty.
carrier transitions	Number of times the carrier detect (CD) signal of a serial interface has changed state.

Related Commands

Command	Description
show controller interface	Displays information that is specific to the interface hardware statistics for all interfaces configured on the networking device.

shutdown (global)

To disable an interface (to force an interface to be administratively down), use the **shutdown** command in interface configuration mode. To enable an interface that has been shut down, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no keywords or arguments.

Command Default

The interface is enabled by default and is disabled only when shutdown is configured.

Note When you add an interface to the system, or when all the configuration for an interface is lost or deleted, the interface is put in the shutdown state by the system adding the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **shutdown** command to move the state of an interface to administratively down, which stops traffic flowing through the interface. This state does not stop other action from happening on the interface such as changes in configuration, protocols, capsulations, and so forth.

The **shutdown** command also marks the interface as unavailable. To check whether the state of an interface is down, use the **show interfaces** command in EXEC mode, which displays the current state of the interface. An interface that has been shut down is shown as administratively down in the display from the **show interfaces** command.

Task ID

Task ID	Operations
interface	read, write

Examples

In this example, TenGigE interface 0/4/0/2 is turned off:

```
RP/0/0/CPU0:router(config)# interface TenGigE 0/4/0/2
```

```
RP/0/0/CPU0:router(config-if)# shutdown
```

Related Commands

Command	Description
show interfaces, on page 423	Displays statistics for all interfaces configured on the router or on a specific node.
show ip interface	Displays IPv4 interface status and configuration.

Link Bundling Commandsonthe Cisco IOS XR Software

This module provides command line interface (CLI) commands for configuring Link Bundle interfaces on the Cisco XR 12000 Series Router.

bundle-hash

To display the source and destination IP addresses for the member links, distributed by the load balancing feature, in a multilink interface bundle, use the **bundle-hash** command in EXEC mode.

bundle-hash {**Bundle-Ether** *bundle-id*| **Bundle-POS bundle-id**| **members** {**GigabitEthernet**| **POS**} *interface-path-id*}

Syntax Description

Bundle-Ether *bundle-id*	Specifies an Ethernet bundle for which you want to calculate load balancing. Range is 1- 65535.
Bundle-POS *bundle-id*	Specifies a POS bundle for which you want to calculate load balancing. Range is 1- 65535.
members	Identifies specific bundle member links for which you want to calculate load balancing.
GigabitEthernet	Specifies the Gigabit Ethernet interface for which you want to calculate load balancing.
POS	Specifies the POS interface for which you want to calculate load balancing.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

Bundle interface traffic is distributed over the various member links of a bundle according to a hash function. The **bundle-hash** command allows you to determine which bundle member link will carry a particular flow of traffic.

You can use the **bundle-hash** command to get these information:

- Which members are used for a specified source/destination address pair,
- such as 10.10.10.1 20.20.20.1
- The destination IP address for a specified source IP address on a specified member.
- The load balancing distribution–how many times the members of a bundle are used for a specified range of IP addresses.

The **bundle-hash** command does not display all possible IP addresses in an entire series. It stops displaying addresses after all the addresses for all the members of the bundle have been displayed once.

The **bundle-hash** command invokes a utility that initially prompts you to select some options. Based on the options you select, the utility prompts you more options to select. The initial options to select are as follows:

- L3/3-tuple
- Single pair or Range
- IPv4 or IPv6

The **bundle-hash** command utility prompts you for these options as follows:

- Specify load-balance configuration (L3/3-tuple) (L3,L4):
- Single SA/DA pair (IPv4,IPv6) or range (IPv4 only): S/R [S]:
- Enter bundle type IP V4 (1) or IP V6 (2):
- Enter source IP V4 address:
- Enter destination IP V4 address:
- Compute destination address set for all members? [y/n]:
- Enter subnet prefix for destination address set:
- Enter bundle IP V4 address [10.10.10.10]:

You may also be prompted to make further option choices depending on your selections.

You can use the **show bundle** command to get IP address information.

Table 28: bundle-hash Command Options, on page 439 provides a general summary of the options and the information you need to provide for each selected option. The actual information that you need to provide depends on the selections you make and may vary from the information provided in Table 28: bundle-hash Command Options, on page 439.

Table 28: bundle-hash Command Options

Option	Information You Need to Provide
L3/3-tuple	L3 information: • Source IP address • Destination IP address • Destination subnet prefix • Bundle IP address

Option	Information You Need to Provide
Single pair	Information for a single source port and destination port. The utility uses this information to calculate the hash and display the bundle load-balance distribution among the user-provided physical/bundle links. The default is single mode. While in single mode, you may receive the following prompt:
Range	Information for sets of source and destination addresses to generate a packet flow for each set. The utility uses this information to calculate the hash for the generated packet flows and display the user-provided egress member links/bundle interfaces and the number of packet flows on each link.
IPv4	IPv4 addresses

```
  Compute destination address set for all members [y|n]:
```

If you enter y(es), several sample IPv4 addresses in the destination subnet are generated, and the link is calculated for each sample address. During this calculation, the destination network address is derived from the destination IPv4 address and the subnet prefix.

Task ID

Task ID	Operations
bundle	read

Examples

The following example shows the **members** keyword prompts and options:

```
RP/0/0/CPU0:router# bundle-hash members pos  0/2/0/1

Thu Aug 20 20:19:21.241 DST
Single SA/DA pair or range: S/R [S]: s
Enter source IP V4 address: 10.10.10.10
Enter source IP V4 address: 10.10.10.10
Enter destination IP V4 address: 20.20.20.20
Compute destination address set for all members? [y/n]: y
Enter subnet prefix for destination address set: 8
Enter bundle IP V4 address [10.10.10.10]: 10.10.10.11

Link hashed [hash:0] to is POS0/2/0/1 member id 0 ifh 0x3000f00

Destination address set for subnet 20.0.0.0:
  20.0.0.1 [hash:4] hashes to link POS0/2/0/1

Another? [y]:
```

The following example shows how to calculate load balancing across the members of a link bundle (bundle-ether 2) using a single source and destination:

```
RP/0/0/CPU0:router# bundle-hash bundle-ether 2
Single SA/DA pair or range: S/R [S]: s
Enter source IP V4 address: 10.23.23.23
Enter destination IP V4 address: 10.12.12.12
Compute destination address set for all members? [y/n]: y
Enter subnet prefix for destination address set: 24
Enter bundle IP V4 address [10.23.23.23]: 10.1.1.2

Link hashed [hash:0] to is GigabitEthernet0/2/1/1 member id 0 ifh 0x3000b00

Destination address set for subnet 10.12.12.0:
  10.12.12.2 [hash:6] hashes to link GigabitEthernet0/2/1/1
  10.12.12.1 [hash:5] hashes to link GigabitEthernet0/2/1/0
```

The following example shows how to calculate load balancing across the members of a link bundle (bundle-ether 2) using a range of source and destinations:

```
RP/0/0/CPU0:router# bundle-hash bundle-ether 2

Single SA/DA pair or range: S/R [S]: r
Enter first source IP address: 10.1.1.1
Enter subnet prefix for source address set: 24
Enter number of source addresses (1-65536): 100
Enter source address modifier (1-167114) [1]: 1
Enter destination IP address: 10.4.4.4
Enter subnet prefix for destination address set: 24
Enter number of destination addresses (1-655): 10
Enter destination address modifier (1-1651404) [1]: 1
.
Total number of hits 1000
Member GigabitEthernet0/2/1/1 has 500 hits
Member GigabitEthernet0/2/1/0 has 500 hits
```

The following example shows how to calculate load balancing across specified members of a link bundle (bundle-ether 2) using a single source and destination:

```
RP/0/0/CPU0:router# bundle-hash members gigabitEthernet 0/2/1/1 gigabitEthernet 0/2/1/0
Single SA/DA pair or range: S/R [S]: s
Enter source IP V4 address: 10.1.1.1
Enter destination IP V4 address: 10.2.1.1
Compute destination address set for all members? [y/n]: y
Enter subnet prefix for destination address set: 16
Enter bundle IP V4 address [10.1.1.1]: 10.1.1.2

Link hashed [hash:6] to is GigabitEthernet0/2/1/1 member id 0 ifh 0x3000b00

Destination address set for subnet 10.2.1.0:
10.2.1.1 [hash:6] hashes to link GigabitEthernet0/2/1/1
10.2.1.2 [hash:5] hashes to link GigabitEthernet0/2/1/0
```

Related Commands

Command	Description
show bundle, on page 464	Displays information about configured bundles.

bundle id

To add a port to an aggregated interface (or bundle), enter the **bundle id** command in interface configuration mode.

bundle id *bundle-id* [**mode** {**active**| **on**| **passive**}]

no bundle id *bundle-id*

Syntax Description

bundle-id	Number of the bundle (from 1 to 65535) on which you want to add a port.
mode	(Optional) Specifies the mode of operation, as follows: • **active—**Use the **mode active** keywords to run Link Aggregation Control Protocol (LACP) in active mode over the port. When you specify **active**, the port joins the bundle and is activated if LACP determines that it is compatible. • **on—**Use the **mode on** keywords to configure an Etherchannel link over the port (no LACP running over the port). • **passive—**Use the **mode passive** keywords to run LACP in passive mode over the port. When you specify **passive**, LACP packets are sent only if the other end of the link is using active LACP. The link joins the bundle and is activated if LACP packets are exchanged and the port is compatible.

Command Default

The default setting is **mode on**.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

If you enter the **bundle id** command and specify a port that is already bound to a bundle, the port unbinds from the original bundle and becomes attached to the new bundle. If the bundle numbers are the same, then the port does not unbind, but the mode changes to mode you specified with the **bundle id** command.

Task ID

Task ID	Operations
bundle	read, write

Examples

This example shows how to add a port onto a bundle:

```
RP/0/0/CPU0:router(config)# interface GigabitEthernet 0/1/5/0
RP/0/0/CPU0:router(config-if)# bundle id 1
```

This example shows how to add an active LACP port onto an aggregated interface (or bundle):

```
RP/0/0/CPU0:router(config)# interface GigabitEthernet 0/6/5/7
RP/0/0/CPU0:router(config-if)# bundle id 5 mode active
```

Related Commands

Command	Description
show bundle, on page 464	Displays information about configured bundles.
show interfaces, on page 423	Displays statistics for all interfaces configured on the router or for a specific node.
show lacp bundle, on page 480	Displays detailed information about LACP ports and their peers.
show lacp port, on page 491	

bundle maximum-active links

To designate one active link and one link in standby mode that can take over immediately for a bundle if the active link fails, use the **bundle maximum-active links** command in interface configuration mode. To return to the default maximum active links value, use the **no** form of this command.

bundle maximum-active links *links* **[hot-standby]**

no bundle maximum-active links *links*

Syntax Description

links	Number of active links you want to bring up in the specified bundle, up to the maximum supported on the platform.
hot-standby	(Optional) Determines how a switchover between active and standby links is implemented. This option is available only on links with LACP enabled. By default, a switchover is implemented per an IEEE standard approach. If you optionally specify the **hot-standby** keyword, a switchover is implemented per a faster proprietary optimization.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.
Release 3.8.0	The **hot-standby** keyword was added.

Usage Guidelin

Note 1:1 link protection is not supported.

By default, multiple links can actively carry traffic for a bundle. However, if one of the links fails, there is no dedicated standby link to take its place. The **bundle maximum-active links** command enables you to implement the optional 1:1 link protection, which means for the specified bundle, you designate one active link and one or more standby links that can take over immediately if the active link fails.

By setting the **bundle maximum-active links** command to 1, the highest-priority link within the bundle becomes active (distributing state) and the remaining links are in standby mode. If a standby link meets one of the following criteria, it is in the collecting state:

- Running Link Aggregation Control Protocol (LACP), and the **hot-standby** option is implemented.

- Not running LACP.

If a standby link does not meet either of these criteria, it is in the waiting state.

The second highest-priority link within the bundle becomes the standby link that takes over immediately if the active link fails. The priority is based on the value from the **bundle port-priority** command, where a lower value is a higher priority. Therefore, you must configure the highest priority (lowest value) for the link that you want to be active and the second-highest priority for the link that you want to act as a backup to the active link.

Note We recommend designating only one backup link to the active link. Although you can designate an additional backup link, maintaining two backup links consumes more bandwidth and offsets any benefits that may be gained.

Note If a link is not running LACP, the configuration of the **bundle maximum-active links** and **bundle port-priority** commands or equivalent commands must be the same on both ends of the link. If a link is running LACP, the configuration of the **bundle maximum-active links** command only must be the same on both ends of the link.

The **hot-standby** option of using an IEEE standard-based switchover (the default) or a faster proprietary optimized switchover is available only for active and standby links running LACP. For links not running LACP, the proprietary optimized switchover option is used.

When using one of the **hot-standby** options on a Cisco IOS XR device, the peer device must have a standby link configured and be one of the following:

- Another Cisco IOS XR device using the same option.
- Another device using an IEEE standard-based switchover. (Cisco does not recommend using this option because unexpected behavior, such as the peer sending traffic on the standby link, can occur.)

Task ID

Task ID	Operations
bundle	read, write

Examples

In the following example, the user implements 1:1 link protection for Ethernet bundle 5 and specifies that the proprietary optimization is used for the LACP-enabled active and standby links:

```
RP/0/0/CPU0:router(config)# interface bundle-ether 5
RP/0/0/CPU0:router(config-if)# bundle maximum-active links 1 hot-standby
```

The following example shows how to display information about Ethernet bundle 5:

```
RP/0/0/CPU0:router# show bundle bundle-ether 5

State: 0 - Port is Detached. 1 - Port is Waiting.
       2 - Port is Attached. 3 - Port is Collecting.
       4 - Port is Distributing.
```

```
Bundle-Ether 5
                                Minimum active     Maximum active
  B/W (Kbps)   MAC address      Links  B/W (Kbps)  Links
  ----------   --------------   -----  ----------  -----
10000000001d.e5eb.2898111

  Port           State  Port ID          B/W (Kbps)  MAC address
  ------------   -----  --------------   ----------  ---------------
  Te0/1/0/1      4      0x8000, 0x0001     10000000  0000.abab.0001
  Te0/1/0/0      3      0x8000, 0x0002     10000000  0000.abab.0000
```

In the **show bundle bundle-ether 5** command output, the state of the active link is 4, which indicates that the port is distributing. The state of the standby link is 3, which indicates that the port is collecting.

In the following example, the user implements 1:1 link protection for Ethernet bundle 5 and does not specify the **hot-standby** keyword, because the user wants to use the default IEEE standard-based switchover on the LACP-enabled active and standby links:

```
RP/0/0/CPU0:router(config)# interface bundle-ether 5
RP/0/0/CPU0:router(config-if)# bundle maximum-active links 1
```

The following example shows how to display information about Ethernet bundle 5:

```
RP/0/0/CPU0:router# show bundle bundle-ether 5

State: 0 - Port is Detached. 1 - Port is Waiting.
       2 - Port is Attached. 3 - Port is Collecting.
       4 - Port is Distributing.

Bundle-Ether 5
                                Minimum active     Maximum active
  B/W (Kbps)   MAC address      Links  B/W (Kbps)  Links
  ----------   --------------   -----  ----------  -----
10000000001d.e5eb.2898111

  Port           State  Port ID          B/W (Kbps)  MAC address
  ------------   -----  --------------   ----------  ---------------
  Te0/1/0/1      4      0x8000, 0x0001     10000000  0000.abab.0001
  Te0/1/0/0      10x8000, 0x0002     10000000  0000.abab.0000
```

In the **show bundle bundle-ether 5** command output, the state of the active link is 4, which indicates that the port is distributing. The state of the standby link is 1, which indicates that the port is waiting.

In the following example, the user implements 1:1 link protection for Ethernet bundle 5 and does not specify the **hot-standby** keyword, because the LACP-disabled link automatically uses the proprietary optimized switchover:

```
RP/0/0/CPU0:router(config)# interface bundle-ether 5
RP/0/0/CPU0:router(config-if)#bundle maximum-active links 1
```

The following example shows how to display information about Ethernet bundle 5:

```
RP/0/0/CPU0:router# show bundle bundle-ether 5

State: 0 - Port is Detached. 1 - Port is Waiting.
       2 - Port is Attached. 3 - Port is Collecting.
       4 - Port is Distributing.

Bundle-Ether 5
                                Minimum active     Maximum active
  B/W (Kbps)   MAC address      Links  B/W (Kbps)  Links
  ----------   --------------   -----  ----------  -----
10000000001d.e5eb.2898111

  Port           State  Port ID          B/W (Kbps)  MAC address
  ------------   -----  --------------   ----------  ---------------
```

```
Te0/1/0/1       4       0x8000, 0x0001     10000000  0000.abab.0001
Te0/1/0/0       3       0x8000, 0x0002     10000000  0000.abab.0000
```

In the **show bundle bundle-ether 5** command output, the state of the active link is 4, which indicates that the port is distributing. The state of the standby link is 3, which indicates that the port is collecting.

Related Commands

Command	Description
bundle minimum-active links, on page 449	Sets the number of active links required to bring up a specific bundle.
show bundle, on page 464	Displays information about configured bundles.
show lacp bundle, on page 480	Displays detailed information about LACP ports and their peers.

bundle minimum-active bandwidth

To set the minimum amount of bandwidth required before a user can bring up a specific bundle, use the **bundle minimum-active bandwidth** command in interface configuration mode.

bundle minimum-active bandwidth *kbps*

Syntax Description

kbps	Minimum bandwidth required before you can bring up a bundle. Range is from 1 through a number that varies depending on the platform and the bundle type.

Command Default

kbps: 1

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
bundle	read, write

Examples

This example shows how to set the minimum amount of bandwidth required before a user can bring up a specific bundle. In this example, the user sets the minimum amount of bandwidth required to bring up Ethernet bundle 1 to 620000:

```
RP/0/0/CPU0:router(config)# interface Bundle-Ether 1
RP/0/0/CPU0:router(config-if)# bundle minimum-active bandwidth 620000
```

Related Commands

Command	Description
show bundle, on page 464	Displays information about configured bundles.

bundle minimum-active links

To set the number of active links required to bring up a specific bundle, use the **bundle minimum-active links** command in interface configuration mode.

bundle minimum-active links *links*

Syntax Description

links	Minimum number of active links allowed in the specified bundle. The range is from 1 through 8.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
bundle	read, write

Examples

The following example shows how to set the number of active links required to bring up a specific bundle. In this example, the user configures Ethernet bundle 5 so that two links must be active before the bundle can be brought up:

```
RP/0/0/CPU0:router(config)# interface Bundle-Ether 5
RP/0/0/CPU0:router(config-if)# bundle minimum-active links 2
```

Related Commands

Command	Description
bundle maximum-active links, on page 444	
show bundle, on page 464	Displays information about configured bundles.

bundle port-priority

To configure a port priority for a bundle member link, enter the **bundle port-priority** command in interface configuration mode. To return to the default priority value, use the **no** form of this command.

bundle port-priority *priority*

no bundle port-priority *priority*

Syntax Description

priority	Priority for this port, where a lower value equals a higher priority. Replace the *priority* argument with a number. Range is from 1 through 65535.

Command Default

priority: 32768

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

The **bundle port-priority** command enables you to determine whether or not similar ports, for example, Gigabit Ethernet ports with Link Aggregation Control Protocol (LACP) enabled or with LACP disabled, are aggregated based on the priority of the port.

In cases where LACP is enabled on aggregated ports, the port priority forms part of the port ID, which is transmitted within a packet when a device exchanges packets with its peer. The peers use the port ID within the packets to determine whether a given port should carry traffic for the bundle.

In cases where LACP is disabled, the port priority is used locally, and a device does not communicate its priority to a peer. Therefore, the peers should have the same priority configured to avoid a mismatch in which links are used for carrying traffic. For example, you could set up the port priorities so that a device would use links 1, 3, and 4 for carrying traffic, and its peer would use links 1, 2, and 3, where links use the same numbering sequence at both ends.

Note A lower value is a higher priority for the port.

Task ID

Task ID	Operations
bundle	read, write

Examples

The following example shows how to configure the priority of a port:

```
RP/0/0/CPU0:router# config
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/1
RP/0/0/CPU0:router(config-if)# bundle port-priority 1
```

Related Commands

Command	Description
bundle id, on page 442	Adds a port to an aggregated interface or bundle.
show lacp bundle, on page 480	Displays detailed information about LACP ports and their peers.
show lacp port, on page 491	
show lacp system-id, on page 494	Displays the local system ID used by the LACP.

clear lacp counters

To clear Link Aggregation Control Protocol (LACP) counters for all members of all bundles, all members of a specific bundle, or for a specific port, enter the **clear lacp counters** command in EXEC mode.

clear lacp counters [**bundle** {**Bundle-Ether** *bundle-id*| **Bundle-POS** *bundle-id*}| **port** {**GigabitEthernet** *interface-path-id*| **TenGigE** *interface-path-id*| **POS** *interface-path-id*}]

Syntax Description

bundle	(Optional) Clears LACP counters for all members of a bundle.
Bundle-Ether *node-id*	(Optional) Ethernet bundle. Use the *node-id* argument to specify the node ID number of the LACP counters you want to clear. Range is 1 through 65535.
Bundle-POS *bundle-id*	(Optional) POS bundle. Use the *bundle-id* argument to specify the bundle ID number of the LACP counters you want to clear. Range is from 1 through 65535.
port	(Optional) Clears all LACP counters on the specified bundle or interface.
GigabitEthernet	(Optional) Gigabit Ethernet interface. Use the *interface-path-id* argument to specify the Gigabit Ethernet interface whose LACP counters you want to clear.
TenGigE	(Optional) Ten Gigabit Ethernet interface. Use the *interface-path-id* argument to specify the Ten Gigabit Ethernet interface whose LACP counters you want to clear.
POS	(Optional) Packet-over-SONET/SDH (POS) interface. Use the *interface-path-id* argument to specify the POS interface whose LACP counters you want to clear.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.
- If specifying a virtual interface, the number range varies, depending on interface type.

Task ID

Task ID	Operations
bundle	execute
basic-services	read, write

Examples

The following example shows how to clear LACP counters:

```
RP/0/0/CPU0:router# clear lacp counters
```

Related Commands

Command	Description
show lacp counters, on page 483	Displays LACP statistics.

interface (bundle)

To create a new bundle and enter interface configuration mode for that bundle, use the **interface (bundle)** command in global configuration mode. To delete a bundle, use the **no** form of this command.

interface {**Bundle-Ether | Bundle-POS** }*bundle-id*

no interface {**Bundle-Ether | Bundle-POS** }*bundle-id*

Syntax Description

Bundle-Ether	Specifies or creates an Ethernet bundle interface.
Bundle-POS	Specifies or creates a POS bundle interface.
bundle-id	Number from 1 to 65535 that identifies a particular bundle.

Command Default

No bundle interface is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Release 3.6.0	This command was introduced.
Release 3.9.0	The **Bundle-POS** keyword was added.

Usage Guidelines

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
bundle	read, write

Examples

This example shows how to create an Ethernet bundle and enter interface configuration mode:

```
RP/0/0/CPU0:router# config
RP/0/0/CPU0:router(config)# interface Bundle-Ether 3
RP/0/0/CPU0:router(config-if)#
```

This example shows how to create a new POS bundle and enter interface configuration mode:

```
RP/0/0/CPU0:router(config)# interface Bundle-POS 10
RP/0/0/CPU0:router(config-if)#
```

Related Commands

Command	Description
show bundle, on page 464	Displays information about configured bundles.

lacp packet-capture

To capture LACP packets so that their information can be displayed by the **show lacp packet-capture** command, use the **lacp packet-capture** command in EXEC mode.

{**lacp packet-capture gigabitethernet** *interface-path-id*| **pos interface-path-id** | **tengige** *interface-path-id number-of-packets*}

To stop capturing LACP packets or to clear captured LACP packets, use the **lacp packet-capture stop** or **lacp packet-capture clear** command in EXEC mode.

{**lacp packet-capture** [**bundle-ether** *bundle-id*] [**bundle-pos bundle-id**] [**gigabitethernet** *interface-path-id*] [**pos interface-path-id**] [**tengige** *interface-path-id*] **clear**| **stop**}

Syntax Description

bundle-ether	Ethernet bundle interface specified by *bundle-id*.
bundle-pos	Packet-over-SONET (POS) bundle interface specified by *bundle-id*.
GigabitEthernet	Gigabit Ethernet interface specified by *interface-path-id*.
POS	Packet-over-SONET (POS) interface specified by *interface-path-id*.
TenGigE	Ten Gigabit Ethernet interface specified by *interface-path-id*.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
bundle-id	Number specifying the bundle interface. The range is 1 to 65535.
number-of-packets	Number of packets to capture.
clear	Clears all currently captured packets.
stop	Stops capturing packets.

Command Default

The default (no parameters) executes globally for all interfaces on the line card.

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

The **lacp packet-capture** command captures transmitted and received LACP packets on a single bundle member interface. The contents of these packets can then be displayed by the **show lacp packet-capture** command. If the **lacp packet-capture** command is not issued, the **show lacp packet-capture** command does not display any information.

The **lacp packet-capture** command continues capturing LACP packets until the **stop** keyword is issued for that port or that bundle. Captured packets are stored and continue to be displayed until the **clear** keyword is issued for that port or that bundle.

LACP packets can only be captured for one port on a line card at a time. Starting a packet capture on a port implicitly stops and clears all packet-captures on all other ports on that line card.

To **stop** capturing LACP packets before the specified number of packets have been captured, issue the **stop** keyword.

If **stop** is specified for a single interface, packet capturing is stopped only on that interface.

If **stop** is specified for a bundle interface, packet capturing is stopped on all members of that bundle.

If **stop** is specified globally (the default - no parameters), packet capturing is stopped on all bundle interfaces on the router.

To **clear** all captured LACP packets that are stored for an interface, issue the **clear** keyword.

If **clear** is specified for a single interface, packets are cleared only on that interface.

If **clear** is specified for a bundle interface, packets are cleared on all members of that bundle.

If **clear** is specified globally (the default - no parameters), packets are cleared on all bundle interfaces on the router.

Task ID

Task ID	Operations
bundle	read

Examples

The following example shows how to capture LACP packets on a POS interface:

```
RP/0/0/CPU0:router# lacp packet-capture pos 0/1/0/0 100
```

The following example shows how to stop capturing LACP packets on a POS interface:

```
RP/0/0/CPU0:router# lacp packet-capture pos 0/1/0/0 stop
```

The following example shows how to clear all captured LACP packets on a POS interface:

```
RP/0/0/CPU0:router# lacp packet-capture pos 0/1/0/0 clear
```

The following example shows how to capture LACP packets on a Gigabit Ethernet interface:

```
RP/0/0/CPU0:router# lacp packet-capture gigabitethernet 0/2/0/0 100
```

The following example shows how to stop capturing LACP packets on a Gigabit Ethernet interface:

```
RP/0/0/CPU0:router# lacp packet-capture gigabitethernet 0/2/0/0 stop
```

Related Commands

Command	Description
show lacp io, on page 485	Displays the LACP transmission information that used by the transmitting device for sending packets on an interface.
show lacp packet-capture, on page 488	Displays the contents of LACP packets that are sent and received on an interface.
lacp period short, on page 459	Enables a short period time interval for the transmission and reception of LACP packets.

lacp period short

To enable a short period time interval for the transmission and reception of Link Aggregation Control Protocol (LACP) packets, use the **lacp period short** command in interface configuration mode. To return to the default short period, use the **no** form of this command.

lacp period short [**receive** *interval*] [**transmit** *interval*]

no lacp period short [**receive** *interval*] [**transmit** *interval*]

Syntax Description

receive *interval*	Time interval (in milliseconds) for receiving LACP packets when LACP short period is enabled. The range is 100 to 1000 and must be multiples of 100, such as 100, 200, 300, and so on.
transmit *interval*	Time interval (in milliseconds) for transmitting LACP packets when LACP short period is enabled. The range is 100 to 1000 and must be multiples of 100, such as 100, 200, 300, and so on.

Command Default

The default is 1000.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.
Release 3.9.0	The keywords **transmit** and **receive** were added.

Usage Guidelin

Note Only the default short period (1 second) is supported.

When you configure a custom LACP short period *transmit* interval at one end of a link, you must configure the same time period for the *receive* interval at the other end of the link.

Note You must always configure the *transmit* interval at both ends of the connection before you configure the *receive* interval at either end of the connection. Failure to configure the *transmit* interval at both ends first results in route flapping (a route going up and down continuously). When you remove a custom LACP short period, you must do it in reverse order. You must remove the *receive* intervals first and then the *transmit* intervals.

Task ID

Task ID	Operations
bundle	read, write

Examples

The following example shows how to enable a default Link Aggregation Control Protocol (LACP) short period on a Gigabit Ethernet interface:

```
RP/0/0/CPU0:router# config
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/0/CPU0:router(config-if)# lacp period short
RP/0/0/CPU0:router(config-if)# commit
```

The following example shows how to configure custom Link Aggregation Control Protocol (LACP) short period transmit and receive intervals at both ends of a connection:

```
RP/0/0/CPU0:router# config
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/0/CPU0:router(config-if)# lacp period short
RP/0/0/CPU0:router(config-if)# commit

RP/0/0/CPU0:router# config
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/0/CPU0:router(config-if)# lacp period short
RP/0/0/CPU0:router(config-if)# commit

RP/0/0/CPU0:router# config
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/0/CPU0:router(config-if)# lacp period short transmit 500
RP/0/0/CPU0:router(config-if)# commit

RP/0/0/CPU0:router# config
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/0/CPU0:router(config-if)# lacp period short transmit 500
RP/0/0/CPU0:router(config-if)# commit

RP/0/0/CPU0:router# config
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/0/CPU0:router(config-if)# lacp period short receive 500
RP/0/0/CPU0:router(config-if)# commit

RP/0/0/CPU0:router# config
RP/0/0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/0/CPU0:router(config-if)# lacp period short receive 500
RP/0/0/CPU0:router(config-if)# commit
```

Related Commands

Command	Description
show lacp io, on page 485	Displays the LACP transmission information that used by the transmitting device for sending packets on an interface.

Command	Description
show lacp packet-capture, on page 488	Displays the contents of LACP packets that are sent and received on an interface.
lacp packet-capture, on page 456	Captures LACP packets so that their information can be displayed.

lacp system priority

To configure the priority for the current system, enter the **lacp system priority** command in global configuration mode. To return to the default LACP system priority value, use the **no** form of this command.

lacp system priority *priority*

no lacp system priority *priority*

Syntax Description

s	Priority for this system. Replace *priority* with a number. Range is from 1 through 65535. A lower value is higher priority.

Command Default

priority: 32768

Command Modes

Global configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

The system priority value forms part of the LACP system ID, which is transmitted within each LACP packet. The system ID, port ID and key combine to uniquely define a port within a LACP system.

Task ID

Task ID	Operations
bundle	read, write

Examples

The following example shows how to configure an LACP priority of 100 on a router:

```
RP/0/0/CPU0:router(config)# lacp system priority 100
```

Related Commands

Command	Description
show lacp system-id, on page 494	Displays the local system ID used by the LACP.
show lacp bundle, on page 480	Displays detailed information about LACP ports and their peers.

Command	Description
show lacp port, on page 491	

show bundle

To display information about all bundles or a specific bundle of a particular type, use the **show bundle** command in EXEC configuration mode.

show bundle [{**Bundle-Ether | Bundle-POS** }*bundle-id*]

Syntax Description

Bundle-Ether	Displays information for the specified Ethernet bundle.
Bundle-POS	Displays information for the specified POS bundle.
bundle-id	Number from 1 to 65535 that identifies a particular bundle.

Command Default

Information is displayed for all configured bundles.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 3.6.0	This command was introduced.
Release 3.8.0	The **reasons** keyword was removed.
Release 4.0.0	The output for this command was replaced with a new format.
Release 4.1.0	The following output fields were added: • Load-balancing • Cisco extensions

Usage Guidelines

To see information for all bundles configured on the router, use the **show bundle**form of the command.

To see information for a specific bundle, use the **show bundle Bundle-Ether***bundle-id*or **show bundle Bundle-POS***bundle-id* form of the command with the number of the configured bundle.

Task ID

Task ID	Operation
bundle	read

Examples

The following example shows output for all bundle interfaces that are configured on the router:

```
RP/0/0/CPU0:router# show bundle
Sun Mar  6 12:16:25.601 PST

Bundle-Ether10
  Status:                                  Up
  Local links <active/standby/configured>:   1 / 1 / 2
  Local bandwidth <effective/available>:     1000000 (1000000) kbps
  MAC address (source):                    f866.f213.25a8 (Gi0/1/0/16)
  Minimum active links / bandwidth:        1 / 1 kbps
  Maximum active links:                    1
  Wait while timer:                        2000 ms
  Load balancing:                          Default
  LACP:                                    Operational
    Flap suppression timer:                Off
    Cisco extensions:                      Disabled
  mLACP:                                   Not configured
  IPv4 BFD:                                Not operational
    State:                                 Off
    Fast detect:                           Enabled
    Start timer:                           Off
    Neighbor-unconfigured timer:           Off
    Preferred min interval:                150 ms
    Preferred multiple:                    3
    Destination address:                   Not Configured

  Port                Device           State        Port ID         B/W, kbps
  ------------------  ---------------  -----------  --------------  ----------
  Gi0/1/0/9           Local            Active       0x0001, 0x0001     1000000
      Link is Active
  Gi0/1/0/10          Local            Standby      0x0002, 0x0002     1000000
      Link is Standby due to maximum-active links configuration
```

Table 29: show bundle Field Descriptions

Field	Description
Bundle-*typenumber*	Full name of the bundle interface, where *type* is Ether (Ethernet) or POS, followed by the configured *number* of the bundle.

Field	Description
Status:	State of the bundle on the local device, with one of the following possible values: • Admin down—The bundle has been configured to be shut down. • Bundle shut—The bundle is holding all links in Standby state and will not support any traffic. • Down—The bundle is operationally down. It has no Active members on the local device. • • • Nak—The local and peer devices cannot resolve a configuration error. • Partner down—The partner system indicates that the bundle is unable to forward traffic at its end. • PE isolated—The bundle is isolated from the core. • Up—The bundle has Active members on this device.
Local links <active/standby/configured>:	The number of links on the device (from 0 to the maximum number of supported links for the bundle) in the format *x / y / z*, with the following values: • *x*—Number of links in Active state on the bundle. • *y*—Number of links in Standby state on the bundle. • *z*—Total number of links configured on the bundle.
Local bandwidth <effective/available>:	Bandwidth characteristics on the bundle in kilobits per second (kbps) in the format *x / y*, with the following values: • *x*—Current bandwidth of the bundle (this effective bandwidth might be limited by configuration). • *y*—Available bandwidth of the bundle that is the sum of the bandwidths of all of the locally active links.

Field	Description
MAC address (source):	Layer 2 MAC address on the bundle interface in the format xxxx.xxxx.xxxx. The (*source*) of the address is shown in parentheses with the following possible values: • Interface name—The MAC address is from the displayed member interface type and path. • Configured—The MAC address is explicity configured. • Chassis pool—The MAC address is from the available pool of addresses for the chassis. • [unknown MAC source 0]—No MAC address could be assigned to the bundle. (You might see this display if you have not completed your bundle configuration.)
Minimum active links / bandwidth:	Displays the following information in the format *x / y* kbps, with the following values: • *x*—Minimum number of active links (from 1 to the maximum number of links supported on the bundle) that are required for the bundle to be operative. • *y*—Minimum total bandwidth on active links (in kbps) that is required for the bundle to be operative. • (partner)—Shows that the peer system's value is in use.
Maximum active links:	Maximum number of links (from 1 to the maximum supported on a bundle) that can be active on the bundle.
Wait-while timer:	Amount of time (in milliseconds) that the system allows for the Link Aggregation Control Protocol (LACP) to negotiate on a “working”link, before moving a “protect”or backup link to Standby state.
Load balancing:	The default load balancing method for the system is used on the bundle.

Field	Description
LACP:	Displays whether or not Link Aggregation Control Protocol (LACP) is active on the bundle, with the following possible values: • Operational—All required configuration has been committed and LACP is in use on active members. • Not operational—LACP is not working because some mandatory configuration is missing on the bundle or on the active members of the bundle. • Not configured—None of the mandatory configuration for LACP has been committed on the bundle, and the LACP sub-fields are not displayed.
Flap suppression timer:	Displays the status of the flap suppression timer, with the following possible values: • Off—The flap suppression timer is not configured using the **lacp switchover suppress-flaps** command. • *x* ms—Amount of time allowed (in milliseconds) for standby links to activate after a working link fails, before putting the link in Down state.
Cisco extensions:	Displays whether or not the Cisco-specific TLVs for LACP are enabled. The possible values are Enabled or Disabled.
mLACP:	mLACP is not supported on the platform.

Field	Description
IPv4 BFD:	Displays whether or not IPv4-based bidirectional forwarding (BFD) is operating on the bundle interface, with the following possible values: • Operational—All required configuration has been committed for IPv4 BFD, and it is in use on the bundle. • Not operational—IPv4 BFD is not working because some mandatory configuration is missing on the bundle or on the active members of the bundle. • Not configured—None of the mandatory configuration for IPv4 BFD has been committed on the bundle, and the BFD sub-fields are not displayed.
State:	When BFD is enabled, displays the state of BFD sessions on the bundle from the sessions running on bundle members that is communicated to interested protocols, with the following possible values: • Down—The configured minimim threshold for active links or bandwidth for BFD bundle members is not available so BFD sessions are down. • Off—BFD is not configured on bundle members. • Up—BFD sessions on bundle members are up because the minimum threshold for the number of active links or bandwidth is met.
Fast detect:	Displays whether or not BFD fast detection is configured on the bundle, with the following possible values: • Enabled—The**bfd fast-detect** command is configured on the bundle. • Disabled—The **bfd fast-detect** command is not configured on the bundle.

Field	Description
Start timer:	Displays status of the BFD start timer that is configured using the **bfd address-family ipv4 timers start** command, with the following possible values: • *x* s—Number of seconds (from 60 to 3600) after startup of a BFD member link session to wait for the expected notification from the BFD peer to be received, so that the session can be declared up. If the SCN is not received after that period of time, the BFD session is declared down. • Off—The start timer is not configured, and a BFD session is only declared Down upon notification from the BFD server.
Neighbor-unconfigured timer:	Displays status of the BFD start timer that is configured using the **bfd address-family ipv4 timers nbr-unconfig** command, with the following possible values: • *x* s—Number of seconds (from 60 to 3600) to wait after receipt of notification that the BFD configuration has been removed by a BFD neighbor, so that any configuration inconsistency between the BFD peers can be fixed. If the BFD configuration issue is not resolved before the specified timer is reached, the BFD session is declared down. • Off—The neighbor-unconfigured timer is not configured, and a BFD session is only declared Down upon notification from the BFD server.
Preferred min interval:	Number of milliseconds (in the format *x* ms) as the minimum control packet interval for BFD sessions. The range is 15 to 30000.
Preferred multiple:	Value of the multiplier (from 2 to 50) that is used for echo failure detection, which specifies the maximum number of echo packets that can be missed before a BFD session is declared Down.
Destination address:	Destination IP address for BFD sessions on bundle member links that is configured using the **bfd address-family ipv4 destination** command. “Not configured” is displayed when no destination IP address is configured.

Field	Description
Port	Name of the local interface port that is configured to be a bundle member The possible values are the shortened interface name or a text string.
Device	Label Distribution Protocol (LDP) address of the device where the interface port is located, with the following possible values: • *address*—IP address of the device. • Local—Interface port is on the local device.
State	Status of the port, with one of the following possible values • Active—Link can send and receive traffic. • BFD Running—Link is inactive because BFD is down or has not been fully negotiated. • Configured—Link is not operational or remains down due to a configuration mismatch. The link is not available for switchover from failure of an active link. • Hot Standby—Link is ready to take over if an active link fails and can immediately transition to Active state without further exchange of LACP protocol data units (PDUs). • Negotiating—Link is in the process of LACP negotiation and is being held in a lower LACP state by the peer (for example, because the link is Standby on the peer.) • Standby—Link is not sending or receiving traffic, but is available for swithchover from failure of an active link.
Port ID	ID of the interface port in the format *x/y*, with the following values: • *x*—Port priority as a 2-byte hexadecimal value. • *y*—Link ID as a 2-byte hexadecimal value.
B/W, kbps	Bandwidth of the interface port in kilobits per second.
State reason	Text string that is displayed beneath the bundle member listing explaining why a link has not reached Active state.

Table 30: State Reasons

Reason	Description
BFD session is unconfigured on the remote end	The link is in BFD Running state because LACP is negotiated but the BFD session from the remote device has been unconfigured.
BFD state of this link is Down	The link is in BFD Running state because LACP is negotiated but the BFD session between the local system and the remote device is Down.
Bundle has been shut down	The link is in Configured state because the bundle it is configured as a member of is administratively down.
Bundle interface is not present in configuration	The link is in Configured state because the bundle it is configured as a member of has not itself been configured.
Bundle is in the process of being created	The link is in Configured state because the bundle it is configured as a member of is still being created.
Bundle is in the process of being deleted	The link is in Configured state because the bundle it is configured as a member of is being deleted.
Bundle is in the process of being replicated to this location	The link is in Configured state because the bundle it is configured as a member of is still being replicated to the linecard where the link is located.
Forced switchover to the mLACP peer	The link is in Configured state because it has been brought down as part of a forced switchover to the mLACP peer PoA. This happens only when brute force switchovers are configured.
ICCP group is isolated from the core network	The link is in Configured state because there is no connectivity through the network core for the ICCP group that the link and its bundle are part of. Therefore, the link has been brought down to prevent any traffic being sent by the LACP partner device.
Incompatible with other links in the bundle (bandwidth out of range)	The link is in Configured state because its bandwidth is incompatible with other links configured to be in the same bundle. The bandwidth may be too high or too low.
LACP shutdown is configured for the bundle	The link is in Standby state because the bundle is configured with LACP shutdown.

Reason	Description
Incompatible with other links in the bundle (LACP vs non-LACP)	The link is in Configured state because its use of LACP is incompatible with other links configured in the same bundle. Some links might be running LACP while others are not.
Link is Attached and has not gone Collecting (reason unknown)	The link is in Negotiating state because the mLACP peer PoA has not indicated that the link has gone Collecting in the Mux machine. This could be because of an issue between the mLACP peer and its LACP partner or because this state has not been communicated to the local system.
Link is Collecting and has not gone Distributing (reason unknown)	The link is in Negotiating state because the mLACP peer PoA has not indicated that the link has gone Distributing in the Mux machine. This could be because of an issue between the mLACP peer and its LACP partner or because this state has not been communicated to the local system.
Link is being removed from the bundle	The link is being removed from the bundle and remains in Configured state while this happens.
Link is Defaulted; LACPDUs are not being received from the partner	The link is in Configured state because no LACPDUs are being received from the LACP partner device. Either the partner is not transmitting or the packets are getting lost.
Link is down	The link is in Configured state because it is operationally or administratively down.
Link is Expired; LACPDUs are not being received from the partner	The link is in Negotiating state because no LACPDUs have been received from the LACP Partner device in the Current-While period and the link is now marked as Expired in the Receive machine.
Link is in the process of being created	The link is in Configured state because the member configuration is still being processed.
Link is marked as Standby by mLACP peer	The link is in Standby state because this has been indicated by the mLACP peer PoA.
Link is Not Aggregatable (reason unknown)	The link is in Configured state because it is marked as an Individual link by the mLACP peer PoA.
Link is not operational as a result of mLACP negotiations	mLACP negotiations with the peer have led to this link being kept in Configured state. This is likely to indicate a misconfiguration between the two peer devices.

Reason	Description
Link is Standby; bundle has more links than are supported	The link is in Standby state because the number of links in Selected state has already reached the hard platform limit on the number of active links.
Link is Standby due to maximum-active links configuration	The link is in Standby state because the number of links in Selected state has already reached the configured maximum active links threshold.
Link is waiting for BFD session to start	The link is in BFD Running state because LACP is negotiated but the BFD session has not started from the remote device.
Loopback: Actor and Partner have the same System ID and Key	The link is in Configured state because a loopback condition has been detected on the link—two links configured to be members of the bundle are actually connected to each other.
Not enough links available to meet minimum-active threshold	The link is in Standby state because there are not enough selectable links (i.e. links which meet the criteria to be marked Selected within the bundle) to meet the minimum active links/bandwidth threshold.
Partner has marked the link as Not Aggregatable	The link is in Configured state because it is marked as an Individual link by the LACP partner device.
Partner has not advertised that it is Collecting	The link is in Negotiating state because the LACP partner device has not advertised that the link is in Collecting state in its LACPDUs.
Partner has not echoed the correct parameters for this link	The link is in Negotiating state because the LACP partner device has not correctly echoed the local system's port information in the LACPDUs it is sending.
Partner is not Synchronized (Waiting, not Selected, or out-of-date)	The link is in Negotiating state because the mLACP peer PoA has not indicated that its LACP partner device is Synchronized. This could be because the devices are genuinely not Synchronized or because this state has not been communicated to the local system.
Partner is not Synchronized (Waiting, Standby, or LAG ID mismatch)	The link is in Negotiating state because the LACP partner device has not indicated that it is Synchronized in the LACPDUs it is sending. On the partner device the link could still be waiting for the Wait-While timer to expire, it could be held in Standby state, or there could be a misconfiguration leading to a LAG ID mismatch between links configured to be within the same bundle.

Reason	Description
Partner System ID/Key do not match that of the Selected links	The link is in Configured state because the System ID or Operational Key specified by the LACP partner device does not match that seen on other Selected links within the same bundle. This probably indicates a misconfiguration.
Wait-while timer is running	The link is in Configured state because the Wait-While timer is still running and the new state has not yet been determined.

Related Commands

Command	Description
interface (bundle), on page 454	Specifies or creates a new bundle and enters interface configuration mode for that bundle.

show bundle brief

To display summary information about all configured bundles, use the **show bundle brief** command in EXEC configuration mode.

show bundle brief

Syntax Description

This command has no keywords or arguments.

Command Default

Information for all configured bundles is displayed.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
bundle	read

Examples

These examples shows the status of two bundles, BE16 and BE100, that are configured on the router. Both are Ethernet bundles and only bundle 16 is Up:

```
RP/0/0/CPU0:router# show bundle brief
Thu Mar  3 14:40:35.167 PST

Name    | IG       | State          | LACP | BFD |     Links     | Local b/w, |
        |          |                |      |     | act/stby/cfgd |    kbps    |
--------|----------|----------------|------|-----|---------------|------------|
BE16             - Up              On     Off         1 / 1 / 2      1000000
BE100            - Down            Off    Off         0 / 0 / 0            0
```

Table 31: show bundle brief Field Descriptions, on page 477 describes the fields shown in the display.

Table 31: show bundle brief Field Descriptions

Field	Description
Name	Abbreviated name of the bundle interface, with the following possible formats: • BE*x*—Ethernet bundle with ID number *x*. • BP*y*—POS bundle with ID number *y*.
IG	Interchassis group ID (if configured) of which the bundle is a member.
State	State of the bundle on the local device, with the following possible values: • Admin down—The bundle has been configured to be shut down. • Bundle shut—The bundle is holding all links in Standby state and will not support any traffic. • Down—The bundle is operationally down. It has no Active members on the local device. • • • Nak—The local and peer devices cannot resolve a configuration error. • Partner down—The partner system indicates that the bundle is unable to forward traffic at its end. • PE isolated—The bundle is isolated from the core. • Up—The bundle has Active members on this device.
LACP	Status of the Link Aggregation Control Protocol (LACP) on the bundle, with the following possible values: • On—LACP is in use on the bundle. • Off—LACP is not active.

Field	Description
BFD	When BFD is enabled, displays the state of BFD sessions on the bundle from the sessions running on bundle members that is communicated to interested protocols, with the following possible values: • Down—The configured minimim threshold for active links or bandwidth for BFD bundle members is not available so BFD sessions are down. • Off—BFD is not configured on bundle members. • Up—BFD sessions on bundle members are up because the minimum threshold for the number of active links or bandwidth is met.
Links act/stby/cfgd	Number of links on the bundle with a particular status in the format *x/y/z*, with the following values: • *x*—Number of links in Active state on the bundle for the local device (from 1 to the maximum number of links supported on the bundle). • *y*—Number of links in Standby state on the bundle for the local device (from 1 to the maximum number of links supported on the bundle). • *z*—Total number of links configured on the bundle for the local device (from 1 to the maximum number of links supported on the bundle).
Local b/w, kbps	Current bandwidth of the bundle on the local device (this effective bandwidth might be limited by configuration).

Related Commands

Command	Description
show bundle, on page 464	Displays information about configured bundles.

show bundle replication bundle-ether

To display the replication status of a link bundle interface, use the **show bundle replication bundle-ether** command in EXEC mode.

show bundle replication bundle-ether *bundle_id* **[all] [in-progress] [pending]**

Syntax Description

all	Shows replication status for all nodes.
in-progress	Shows only nodes with replication in progress.
pending	Shows only nodes pending replication.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
bundle	read

Examples

The following example shows how to

```
RP/0/0/CPU0:router# show bundle replication bundle-ether 1 all
```

show lacp bundle

To display detailed information about Link Aggregation Control Protocol (LACP) ports and their peers, enter the **show lacp bundle** command in EXEC mode.

show lacp bundle {**Bundle-Ether| bundle-POS**} *bundle-id*

Syntax Description

Bundle-Ether *bundle-id*	(Optional) Specifies the number of the Ethernet bundle whose information you want to display. Range is 1 through 65535.
Bundle-POS *bundle-id*	(Optional) Specifies the number of the POS bundle whose information you want to display. Range is 1 through 65535.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
bundle	read

Examples

The following example shows how to display LACP information for a specific Ethernet Bundle:

```
RP/0/0/CPU0:router# show lacp bundle Bundle-Ether 1

Flags: A - Device is in Active mode. P - Device is in Passive mode.
       S - Device sends PDUs at slow rate. F - Device sends PDUs at fast rate.
       D - Port is using default values for partner information
       E - Information about partner has expired
State: 0 - Port is Not Aggregatable. 1 - Port is Out Of Sync with peer.
       2 - Port is In Sync with peer. 3 - Port is Collecting.
       4 - Port is Collecting and Distributing.

Bundle-Ether1
                                Minimum active     Maximum active
  B/W (Kbps)   MAC address      Links  B/W (Kbps)  Links
  ----------   --------------   -----  ----------  -----
```

```
          0   0800.453a.651d       1      620000     32

Port           State  Flags  Port ID          Key     System-ID
------------   -----  -----  --------------   ------  -------------------------
Gi0/0/2/0      1      ASDE   0x8000, 0x0001   0x0001  0x8000, 08-00-45-3a-65-01
  PEER         0      PSD    0xffff, 0x0000   0x0000  0xffff, 00-00-00-00-00-00
```

Table 32: show lacp bundle Field Descriptions

Field	Description
Flags	Describes the possible flags that may apply to a device or port, under the “Flags” field.
State	Describes the possible flags that may apply the port state, under the “State” field.
Port	Port identifier, in the *rack/slot/module/port* notation.
State	Provides information about the state of the specified port. Possible flags are: • 0—Port is not aggregatable. • 1—Port is out of sync with peer. • 2—Port is in sync with peer. • 3—Port is collecting. • 4—Port is collecting and distributing.
Flags	Provides information about the state of the specified device or port. Possible flags are: • A—Device is in Active mode. • P—Device is in Passive mode. • S—Device requests peer to send PDUs at a slow rate. • F—Device requests peer to send PDUs at a fast rate. • D—Port is using default values for partner information. • E—Information about partner has expired.
Port ID	Port identifier, expressed in the format *N*x*nnnn*. *N* is the port priority, and *nnnn* is the port number assigned by the sending router.

Field	Description
Key	Two-byte number associated with the specified link and aggregator. Each port is assigned an operational key. The ability of one port to aggregate with another is summarized by this key. Ports which have the same key select the same bundled interface. The system ID, port ID and key combine to uniquely define a port within a LACP system.
System-ID	System identifier. The system ID is a LACP property of the system which is transmitted within each LACP packet together with the details of the link.

Related Commands

Command	Description
bundle id, on page 442	Adds a port to an aggregated interface or bundle.
show bundle, on page 464	Displays information about configured bundles.

show lacp counters

To display Link Aggregation Control Protocol (LACP) statistics, enter the **show lacp counters** command in EXEC mode.

show lacp counters {**Bundle-Ether| bundle-POS**} *bundle-id*

Syntax Description

Bundle-Ether *bundle-id*	Specifies the Ethernet bundle whose counters you want to display. Replace *bundle-id* with a bundle identifier. Range is from 1 through 65535.
Bundle-POS *bundle-id*	Specifies the POS bundle whose counters you want to display. Replace *bundle-id* with a bundle identifier. Range is from 1 through 65535.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
bundle	read

Examples

The following example shows how to display LACP counters on an Ethernet bundle:

```
RP/0/0/CPU0:router# show lacp counters bundle-ether 1

Bundle-Ether1
                    LACPDUs                 Marker
Port           Sent         Received    Received    Resp. Sent  Last Cleared
-------------  -----------------------  ----------------------  ------------
Gi0/0/2/0              12            0           0            0  never

Port           Excess                  Excess                  Pkt Errors
-------------  ----------              ----------              ----------
Gi0/0/2/0               0                       0                       0
```

Table 33: show lacp counters Field Descriptions

Field	Description
LACPDUs	Provides the following statistics for Link Aggregation Control Protocol data units (LACPDUs): • Port • Sent • Received • Last Cleared • Excess • Pkt Errors
Marker	Provides the following statistics for marker packets: • Received • Resp. Sent • Last Cleared • Excess • Pkt Errors **Note** The Marker Protocol is used by IEEE 802.3ad bundles to ensure that data no longer is transmitted on a link when a flow is redistributed away from that link.

Related Commands

Command	Description
clear lacp counters, on page 452	Clears LACP counters for all members of all bundles, all members of a specific bundle, or for a specific port.

show lacp io

To display the Link Aggregation Control Protocol (LACP) transmission information that used by the transmitting device for sending packets on an interface, use the **show lacp io** command in EXEC mode.

show lacp io {**Bundle-Ether| bundle-POS**} *bundle-id* {**GigabitEthernet| POS| TenGigE**} *interface-path-id*

Syntax Description

Bundle-Ether *bundle-id*	(Optional) Displays information for the Ethernet bundle interface with the specified *bundle-id*. The range is 1 through 65535.
Bundle-POS *bundle-id*	(Optional) Displays information for the POS bundle interface with the specified *bundle-id*. The range is 1 through 65535.
GigabitEthernet	(Optional) Displays information for the Gigabit Ethernet interface with the specified *interface-path-id*.
TenGigE	(Optional) Displays information for the Ten Gigabit Ethernet interface with the specified *interface-path-id*.
POS	(Optional) Displays information for the POS interface with the specified *interface-path-id*.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

The default takes no parameters and displays information for all actively transmitting interfaces.

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

This command displays information only for interfaces that are actively transmitting packets.

Task ID

Task ID	Operations
bundle	read

Examples

The following example shows how to display Link Aggregation Control Protocol (LACP) information for the Ethernet bundle interface with bundle ID 28.

```
RP/0/0/CPU0:router# show lacp io bundle-ether 28

Thu Jun 18 16:28:54.068 PST

Bundle-Ether28

Interface GigabitEthernet0/1/5/6
================================
Interface handle:       0x01180100
Interface media type:   Ethernet
Fast periodic interval: 1000ms
Source MAC address:     0015.63c0.b3b8
Actor system:   0x8000, 00-15-63-c0-b0-04
Actor key:      0x001c
Actor port:     0x8000, 0x0001
Actor state:     Act  (T/o)  Agg   Sync   Coll   Dist  (Def) (Exp)
Partner system: 0x8000, 00-15-63-58-b9-04
Partner key:    0x001c
Partner port:   0x0001, 0x0003
Partner state:   Act  (T/o)  Agg   Sync   Coll   Dist  (Def) (Exp)

Interface GigabitEthernet0/1/5/7
================================
Interface handle:       0x01180120
Interface media type:   Ethernet
Fast periodic interval: 1000ms
Source MAC address:     0015.63c0.b3b9
Actor system:   0x8000, 00-15-63-c0-b0-04
Actor key:      0x001c
Actor port:     0x8000, 0x0002
Actor state:     Act  (T/o)  Agg   Sync  (Coll) (Dist) (Def) (Exp)
Partner system: 0x8000, 00-15-63-58-b9-04
Partner key:    0x001c
Partner port:   0x0002, 0x0004
Partner state:   Act  (T/o)  Agg  (Sync) (Coll) (Dist) (Def) (Exp)
```

The following example shows how to display Link Aggregation Control Protocol (LACP) information for all actively transmitting interfaces:

```
RP/0/0/CPU0:router# show lacp io

Thu Jun 18 16:33:57.330 PST

Bundle-Ether28

Interface GigabitEthernet0/1/5/6
================================
Interface handle:       0x01180100
Interface media type:   Ethernet
Fast periodic interval: 1000ms
Source MAC address:     0015.63c0.b3b8
Actor system:   0x8000, 00-15-63-c0-b0-04
Actor key:      0x001c
Actor port:     0x8000, 0x0001
Actor state:     Act  (T/o)  Agg   Sync   Coll   Dist  (Def) (Exp)
```

```
Partner system: 0x8000, 00-15-63-58-b9-04
Partner key:    0x001c
Partner port:   0x0001, 0x0003
Partner state:   Act  (T/o)  Agg   Sync   Coll   Dist  (Def) (Exp)

Interface GigabitEthernet0/1/5/7
================================
Interface handle:       0x01180120
Interface media type:   Ethernet
Fast periodic interval: 1000ms
Source MAC address:     0015.63c0.b3b9
Actor system:   0x8000, 00-15-63-c0-b0-04
Actor key:      0x001c
Actor port:     0x8000, 0x0002
Actor state:     Act  (T/o)  Agg   Sync  (Coll) (Dist) (Def) (Exp)
Partner system: 0x8000, 00-15-63-58-b9-04
Partner key:    0x001c
Partner port:   0x0002, 0x0004
Partner state:   Act  (T/o)  Agg  (Sync) (Coll) (Dist) (Def) (Exp)


Bundle-POS24

Interface POS0/1/4/0
====================
Interface handle:       0x011804c0
Interface media type:   POS
Fast periodic interval: 1000ms
Actor system:   0x8000, 00-15-63-c0-b0-04
Actor key:      0x0018
Actor port:     0x8000, 0x0003
Actor state:     Act  (T/o)  Agg   Sync   Coll   Dist  (Def) (Exp)
Partner system: 0x8000, 00-15-63-58-b9-04
Partner key:    0x0018
Partner port:   0x8000, 0x0001
Partner state:   Act  (T/o)  Agg   Sync   Coll   Dist  (Def) (Exp)

Interface POS0/1/4/1
====================
Interface handle:       0x011804e0
Interface media type:   POS
Fast periodic interval: 1000ms
Actor system:   0x8000, 00-15-63-c0-b0-04
Actor key:      0x0018
Actor port:     0x8000, 0x0004
Actor state:     Act  (T/o)  Agg   Sync   Coll   Dist  (Def) (Exp)
Partner system: 0x8000, 00-15-63-58-b9-04
Partner key:    0x0018
Partner port:   0x8000, 0x0002
Partner state:   Act  (T/o)  Agg   Sync   Coll   Dist  (Def) (Exp)
```

Related Commands

Command	Description
show lacp packet-capture, on page 488	Displays the contents of LACP packets that are sent and received on an interface.
lacp period short, on page 459	Enables a short period time interval for the transmission and reception of LACP packets.
lacp packet-capture, on page 456	Captures LACP packets so that their information can be displayed.

show lacp packet-capture

To display the contents of Link Aggregation Control Protocol (LACP) packets that are sent and received on an interface, use the **show lacp packet-capture** command in EXEC mode.

show lacp packet-capture [decoded] [**in**| **out**] {**GigabitEthernet**| **POS**| **TenGigE**} *interface-path-id*

Syntax Description

decoded	(Optional) Displays packet information in decoded form for the specified interface.
in	(Optional) Displays packet information for ingress packets only.
out	(Optional) Displays packet information for egress packets only.
GigabitEthernet	Displays packet information for the Gigabit Ethernet interface specified by *interface-path-id*.
POS	Displays packet information for the POS interface specified by *interface-path-id*.
TenGigE	Displays packet information for the Ten Gigabit Ethernet interface specified by *interface-path-id*.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

The default displays both in and out information.

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelin

Note The **lacp packet-capture** command captures transmit and receive packets on a single interface. The contents of these packets can then be displayed by the **show lacp packet-capture** command. If the **lacp packet-capture** command is not issued, the **show lacp packet-capture** command does not display any information.

Task ID

Task ID	Operations
bundle	read

Examples

The following example shows how to display the contents of an LACP packet, in hexadecimal, for a Gigabit Ethernet interface:

Note In the following example, after you issue the **lacp packet-capture** command, you must wait for a reasonable amount of time for the system to capture packets that are sent and received on the interface before you issue the **show lacp packet-capture** command. Otherwise, there is no information to display.

```
RP/0/0/CPU0:router# lacp packet-capture gigabitethernet 0/1/0/0 100
RP/0/0/CPU0:router# show lacp packet-capture gigabitethernet 0/1/0/0

Wed Apr 29 16:27:40.996 GMT
OUT  Apr 29 17:05:50.123
========================
01 01 01 14 80 00 02 a7 4c 81 95 04 00 01 80 00 00 01 45 00
00 00 02 14 ff ff 00 00 00 00 00 00 00 00 ff ff 00 00 40 00
00 00 03 10 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00

OUT  Apr 29 17:35:50.124
========================
...
```

The following example shows how to display the LACP parameters, decoded from individual packets, transmitted and received on a Gigabit Ethernet interface:

Note In the following example, after you issue the **lacp packet-capture** command, you must wait for a reasonable amount of time for the system to capture packets that are sent and received on the interface before you issue the **show lacp packet-capture** command. Otherwise, there is no information to display.

```
RP/0/0/CPU0:router# lacp packet-capture gigabitethernet 0/1/0/0 100
RP/0/0/CPU0:router# show lacp packet-capture decoded gigabitethernet 0/1/0/0

Wed Apr 29 16:27:54.748 GMT
OUT  Apr 29 17:06:03.008
```

```
=========================
Subtype: 0x01 - LACP     Version: 1

TLV: 0x01 - Actor Information       Length:  20
System: Priority: 32768, ID: 02-a7-4c-81-95-04
Key: 0x0001, Port priority: 32768, Port ID:     1
State:  Act  (T/o)  Agg  (Sync) (Coll) (Dist)  Def  (Exp)

TLV: 0x02 - Partner Information     Length:  20
System: Priority: 65535, ID: 00-00-00-00-00-00
Key: 0x0000, Port priority: 65535, Port ID:     0
State: (Act) (T/o) (Agg) (Sync) (Coll) (Dist)  Def  (Exp)

TLV: 0x03 - Collector Information   Length:  16
Max delay: 65535

TLV: 0x00 - Terminator              Length:   0
```

Related Commands

Command	Description
show lacp io, on page 485	Displays the LACP transmission information that used by the transmitting device for sending packets on an interface.
lacp period short, on page 459	Enables a short period time interval for the transmission and reception of LACP packets.
lacp packet-capture, on page 456	Captures LACP packets so that their information can be displayed.

show lacp port

To display detailed information about Link Aggregation Control Protocol (LACP) ports, enter the **show lacp port** command in EXEC mode.

show lacp port [[**GigabitEthernet**| **POS**| **TenGigE**] *interface_instance*]

Syntax Description

GigabitEthernet	(Optional) Gigabit Ethernet interface. Use the *interface-path-id* argument to specify the Gigabit Ethernet interface whose LACP counters you want to display.
TenGigE	(Optional) Ten Gigabit Ethernet interface. Use the *interface-path-id* argument to specify the Ten Gigabit Ethernet interface whose LACP counters you want to display.
POS	(Optional) Packet-over-SONET/SDH (POS) interface. Use the *interface-path-id* argument to specify the POS interface whose LACP counters you want to display.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, if specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:

- *rack*: Chassis number of the rack.
- *slot*: Physical slot number of the line card.
- *module*: Module number. A physical layer interface module (PLIM) is always 0.
- *port*: Physical port number of the interface.

Task ID

Task ID	Operations
bundle	read

Examples

The following example shows how to display LACP port information for all link bundles on a router:

```
RP/0/0/CPU0:router# show lacp port

Flags: A - Device is in Active mode. P - Device is in Passive mode.
       S - Device sends PDUs at slow rate. F - Device sends PDUs at fast rate.
       D - Port is using default values for partner information
       E - Information about partner has expired
State: 0 - Port is Not Aggregatable. 1 - Port is Out Of Sync with peer.
       2 - Port is In Sync with peer. 3 - Port is Collecting.
       4 - Port is Collecting and Distributing.

Bundle-Ether1
                               Minimum active     Maximum active
  B/W (Kbps)   MAC address      Links  B/W (Kbps)  Links
  ----------   --------------   -----  ----------  -----
           0   0800.453a.651d       1      620000     32

  Port           State  Flags  Port ID          Key     System-ID
  ------------   -----  -----  --------------   ------  -------------------------
  Gi0/0/2/0      1      ASDE   0x8000, 0x0001   0x0001  0x8000, 08-00-45-3a-65-01
   PEER          0      PSD    0xffff, 0x0000   0x0000  0xffff, 00-00-00-00-00-00
```

Table 34: show lacp port Field Descriptions

Field	Description
Port	Identifies the LACP port whose information is displayed. The port number is expressed in the *rack/slot/module/port* notation.
State	Provides information about the state of the specified device or port. Possible flags are: • 0—Port is not aggregatable. • 1—Port is out of sync with peer. • 2—Port is in sync with peer. • 3—Port is collecting. • 4—Port is collecting and distributing.

Field	Description
Flags	Provides information about the state of the specified port. Possible flags are: • A—Device is in Active mode. • P—Device is in Passive mode. • S—Device requests peer to send PDUs at a slow rate. • F—Device requests peer to send PDUs at a fast rate. • D—Port is using default values for partner information. • E—Information about partner has expired.
Port ID	Port identifier, expressed in the following format: *Nxnnnn*. *N* is the port priority, and *nnnn* is the port number assigned by the sending router.
Key	Two-byte number associated with the specified link and aggregator. Each port is assigned an operational key. The ability of one port to aggregate with another is summarized by this key. Ports which have the same key select the same bundled interface. The system ID, port ID and key combine to uniquely define a port within a LACP system.
System-ID	System identifier. The System ID is an LACP property of the system which is transmitted within each LACP packet together with the details of the link.

Related Commands

Command	Description
bundle id, on page 442	Adds a port to an aggregated interface or bundle.
show bundle, on page 464	Displays information about configured bundles.

show lacp system-id

To display the local system ID used by the Link Aggregation Control Protocol (LACP), enter the **show lacp system-id** command in EXEC mode.

show lacp system-id

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelin

Note The System ID and details about the specific link are transmitted within each LACP packet.

Task ID

Task ID	Operations
bundle	read

Examples

The following example shows how to display the system ID used by the LACP:

```
RP/0/0/CPU0:router# show lacp system-id

Priority  MAC Address
--------  -----------------
  0x8000  08-00-45-3a-65-01
```

Table 35: show lacp system-id Field Descriptions

Field	Description
Priority	Priority for this system. A lower value is higher priority.

Field	Description
MAC Address	MAC address associated with the LACP system ID.

Related Commands

Command	Description
bundle id, on page 442	Adds a port to an aggregated interface or bundle.
show bundle, on page 464	Displays information about configured bundles.

Management Ethernet Interface Commands on the Cisco IOS XR Software

This module provides command line interface (CLI) commands for configuring Management Ethernet interfaces on the Cisco XR 12000 Series Router.

duplex (Management Ethernet)

To configure duplex mode operation on a Management Ethernet interface, use the **duplex** command in interface configuration mode. To return the interface to autonegotiated duplex mode, use the **no** form of the **duplex** command.

duplex {**full**| **half**}

no duplex

Syntax Description

full	Configures the Management Ethernet interface to operate in full duplex mode.
half	Configures the Management Ethernet interface to operate in half duplex mode.

Command Default

Autonegotiates duplex operation

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was first supported.

Usage Guidelines

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure the Management Ethernet interface to operate in full duplex mode:

```
RP/0/0/CPU0:router(config)# interface MgmtEth 0/0/CPU0/0
RP/0/0/CPU0:router(config-if)# duplex full
```

The following example shows how to configure the Management Ethernet interface to operate in half duplex mode:

```
RP/0/0/CPU0:router(config)# interface MgmtEth 0/0/CPU0/0
RP/0/0/CPU0:router(config-if)# duplex half
```

The following example shows how to return a Management Ethernet interface to autonegotiated duplex mode:

```
RP/0/0/CPU0:router(config)# interface MgmtEth 0/0/CPU0/0
RP/0/0/CPU0:router(config-if)# no duplex
```

Related Commands

Command	Description
interface MgmtEth, on page 500	Enters interface configuration mode for the Management Ethernet interface.

interface MgmtEth

To enter interface configuration mode for the Management Ethernet interface, use the **interface MgmtEth** command in global configuration mode. To delete a Management Ethernet interface configuration, use the **no** form of this command.

interface MgmtEth *interface-path-id*

no interface MgmtEth *interface-path-id*

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was first supported.

Usage Guidelines

Task ID

Task ID	Operations
interface	read, write

Examples

This example shows how to enter interface configuration mode for a Management Ethernet interface:

```
RP/0/0/CPU0:router(config)# interface MgmtEth 0/0/CPU0/0
RP/0/0/CPU0:router(config-if)#
```

Related Commands

Command	Description
duplex (Management Ethernet), on page 498	Configures duplex mode operation on a Management Ethernet interface.
mac-address (Management Ethernet), on page 502	Sets the MAC layer address of a Management Ethernet interface.
speed (Management Ethernet), on page 504	Configures the speed for a Management Ethernet interface.

mac-address (Management Ethernet)

To set the MAC layer address of a Management Ethernet interface, use the **mac-address** command in interface configuration mode. To return the interface to its default MAC address, use the **no** form of the **mac-address** command.

mac-address *value1.value2.value3*

no mac-address

Syntax Description

value1	High 2 bytes of the MAC address in hexadecimal. Range is from 0 to ffff.
value2	Middle 2 bytes of the MAC address in hexadecimal. Range is from 0 to ffff.
value3	Low 2 bytes of the MAC address in hexadecimal. Range is from 0 to ffff.

Command Default

The default MAC address is read from the hardware burned-in address (BIA).

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was first supported.

Usage Guidelines

The MAC address must be in the form of three 4-digit values (12 digits in dotted decimal notation).

Task ID

Task ID	Operations
interface	read, write

Examples

This example shows how to set the MAC address of the Management Ethernet interface located at 0/RP0/CPU0/0:

```
RP/0/0/CPU0:router(config)# interface MgmtEth 0/0/CPU0/0
RP/0/0/CPU0:router(config-if)# mac-address 0001.2468.ABCD
```

Related Commands

Command	Description
interface MgmtEth, on page 500	Enters interface configuration mode for the Management Ethernet interface.

speed (Management Ethernet)

To configure the speed for a Management Ethernet interface, enter the **speed** command in interface configuration mode. To return the system to autonegotiate speed, use the **no** form of the **speed** command.

speed {**10**| **100**| **1000**}

no speed

Syntax Description

10	Configures the interface to transmit at 10 Mbps.
100	Configures the interface to transmit at 100 Mbps.
1000	Configures the interface to transmit at 1000 Mbps (1 Gbps).

Command Default

Interface speed is autonegotiated.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was first supported.

Usage Guidelines

Note Keep in mind that both ends of a link must have the same interface speed. A manually configured interface speed overrides any autonegotiated speed, which can prevent a link from coming up if the configured interface speed at one end of a link is different from the interface speed on the other end.

Table 36: Relationship Between duplex and speed Commands, on page 504 describes the performance of the system for different combinations of the duplex and speed modes. The specified **duplex** command configured with the specified **speed** command produces the resulting system action.

Table 36: Relationship Between duplex and speed Commands

duplex Command	speed Command	Resulting System Action
no duplex	no speed	Autonegotiates both speed and duplex modes.
no duplex	speed 1000	Forces 1000 Mbps (1 Gbps) and full duplex.

duplex Command	speed Command	Resulting System Action
no duplex	speed 100	Autonegotiates for duplex mode and forces 100 Mbps.
no duplex	speed 10	Autonegotiates for duplex mode and forces 10 Mbps.
duplex full	no speed	Forces full duplex and autonegotiates for speed.
duplex full	speed 1000	Forces 1000 Mbps (1 Gbps) and full duplex.
duplex full	speed 100	Forces 100 Mbps and full duplex.
duplex full	speed 10	Forces 10 Mbps and full duplex.
duplex half	no speed	Forces half duplex and autonegotiates for speed (10 or 100 Mbps.)
duplex half	speed 100	Forces 100 Mbps and half duplex.
duplex half	speed 10	Forces 10 Mbps and half duplex.

Task ID

Task ID	Operations
interface	read, write

Examples

This example shows how to configure the Management Ethernet interface to transmit at one gigabit:

```
RP/0/0/CPU0:router(config)# interface MgmtEth 0/0/CPU0/0
RP/0/0/CPU0:router(config-if)# speed 1000
```

Related Commands

Command	Description
interface MgmtEth, on page 500	Enters interface configuration mode for the Management Ethernet interface.

Multilink Commands on the Cisco IOS XR Software

This module provides command line interface (CLI) commands for configuring multilink interfaces on the Cisco XR 12000 Series Router.

bundle

To create a multilink interface bundle, use the **bundle** command in the interface configuration mode. To remove a multilink interface bundle, use the **no** form of this command.

bundle *bundleID*

Syntax Description

bundleID	ID number of the multilink interface bundle. Range is from 1 through 1023.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

The **bundle** command is used in mgmtmultilink controller mode to dynamically create a multilink interface. This command is similar to the **channel-group** command on the T1 controller, which dynamically creates a serial interface.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to create a multilink interface with a bundle ID of 1:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# controller mgmtmultilink 0/1/0/0
RP/0/0/CPU0:router(config-mgmtmultilink)# bundle 1
RP/0/0/CPU0:router(config-mgmtmultilink)# commit
```

Related Commands

Command	Description
multilink, on page 514	Enters the config-if-multilink submode.
multilink fragment-size, on page 515	

Command	Description
multilink group, on page 517	Attaches a serial interface to a multilink interface bundle.
ppp multilink minimum-active links, on page 521	Sets the minimum number of active links required before the multilink interface line can be brought to the up state.

controller MgmtMultilink

To configure a controller for a generic multilink bundle and enter MgmtMultilink configuration mode, use the **controller MgmtMultilink** command in global configuration mode. To return to the default state, use the **no** form of this command.

controller MgmtMultilink *interface-path-id*

no controller MgmtMultilink *interface-path-id*

Syntax Description

interface-path-id	Virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*instance*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number.
  - *instance*: Number of the controller instance. The instance is always 0.
- If specifying a virtual interface, the number range varies, depending on interface type.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter the MgmtMultilink configuration mode :

```
RP/0/0/CPU0:router# config
RP/0/0/CPU0:router(config)# controller MgmtMultilink 0/1/0/0
RP/0/0/CPU0:router(config-mgmtmultilink)#
```

Related Commands

Command	Description
show controllers mgmtmultilink, on page 522	Displays information about the state and the number of bundles of a multilink controller.

interface multilink

To configure a multilink interface and enter multilink interface configuration mode, use the **interface multilink** command in global configuration mode. To delete the interface configuration, use the **no** form of this command. To return to the default state, use the **no** form of this command.

interface multilink *interface-path-id*[**.***subinterface*{**l2transport**| **point-to-point**}]

no interface multilink *interface-path-id*[**.***subinterface*{**l2transport**| **point-to-point**}]

Syntax Description

interface-path-id [**.** *subinterface*]	Physical interface or virtual interface followed by the optional subinterface path ID. Naming notation is *interface-path-id***.***subinterface*.The period in front of the subinterface value is required as part of the notation. For more information about the syntax for the router, use the question mark (**?**) online help function.
l2transport	Configures interface to function as one endpoint on a Layer 2 link.
point-to-point	Configures interface to function as one endpoint on a point-to-point link.

Command Default

No interfaces are configured.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

The *subinterface* argument and keywords **l2transport** and **po in t-to-point** are only applicable if frame relay encapsulation is enabled using the **encapsulation frame-relay** command.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enable frame relay encapsulation for a multilink bundle, and enter subinterface configuration mode.

```
RP/0/0/CPU0:routerRP/0/0/CPU0:router#
RP/0/0/CPU0:router# configure terminal
RP/0/0/CPU0:router(config)# interface multilink 0/3/0/0/1
RP/0/0/CPU0:router(config-if)# encapsulation frame-relay
RP/0/0/CPU0:router(config-if)# exit
RP/0/0/CPU0:router(config)# interface multilink 0/3/0/0/1.1 point-to-point
RP/0/0/CPU0:router(config-subif)# ipv4 address 10.86.10.48/24
```

The following example shows how to enter interface configuration mode for a multilink bundle with ppp encapsulation. ppp encapsulation is the default encapsulation type:

```
RP/0/0/CPU0:router# configure terminal
RP/0/0/CPU0:router(config)# interface multilink 0/3/0/0/1
RP/0/0/CPU0:router(config-if)#ipv4 address 10.86.10.48/24
```

Related Commands

Command	Description
show interfaces multilink, on page 525	Displays information about a multilink interface.

multilink

To enter the config-if-multilink submode, use the **multilink** command in the interface configuration mode.

multilink

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

For multilink interfaces, the **multilink** command provides access to the config-if-multilink submode to use the **multilink fragment-size** command.

Task ID

Task ID	Operations
hdlc	read, write

Examples

The following example shows how to enter the config-if-multilink submode:

```
RP/0/0/CPU0:router# config
RP/0/0/CPU0:router(config)# interface serial 0/1/0/1/1/1:0
RP/0/0/CPU0:router(config-if)# multilink
RP/0/0/CPU0:router(config-if-multilink)# group 1
RP/0/0/CPU0:router(config-if-multilink)# commit
```

Related Commands

Command	Description
multilink fragment-size, on page 515	
multilink group, on page 517	Attaches a serial interface to a multilink interface bundle.
ppp multilink minimum-active links, on page 521	Sets the minimum number of active links required before the multilink interface line can be brought to the up state.

multilink fragment-size

To set the Layer 2 fragmentation size and enable counting of fragmented packets, for a multilink interface which is controlled by the **mtu** command, use the **multilink fragment-size** command in interface configuration mode. To set the fragment size back to the default, no fragment size, use the **no** form of this command.

multilink fragment-size *size* **[fragment-counter]**

no multilink fragment-size

Syntax Description

size	Fragment size. The allowed values are determined by the hardware. In the current release, the allowed values are 128, 256 and 512. The value 64 also appears in the CLI help for this parameter. However, 64 is not allowed in this release and will cause configuration problems in the system if used.
fragment-counter	Enables counting of the fragmented packets.

Command Default

The default is no multilink fragment-size, which means no fragmentation at Layer 2.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.4.1	This command was introduced.
Release 4.0.0	The **fragment-counter** keyword was added.

Usage Guidelines

Multilink fragmentation is only supported for ppp encapsulation, not for frame-relay enacapsulation.

Task ID

Task ID	Operations
hdlc	read, write

Examples

The following example shows how to set the fragment size to 128:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface multilink 0/1/0/0/1
RP/0/0/CPU0:router(config-if)# multilink fragmentation-size 128
RP/0/0/CPU0:router(config-if)# commit
```

The following example shows how to set the fragment size to 128 and enable the fragmentation counters:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface multilink 0/1/0/0/1
RP/0/0/CPU0:router(config-if)# multilink fragmentation-size 128 fragment-counter
RP/0/0/CPU0:router(config-if)# commit
```

Related Commands

Command	Description
multilink group, on page 517	Attaches a serial interface to a multilink interface bundle.
multilink, on page 514	Enters the config-if-multilink submode.
ppp multilink minimum-active links, on page 521	Sets the minimum number of active links required before the multilink interface line can be brought to the up state.

multilink group

To attach a serial interface to a multilink interface bundle, use the **multilink group** command in interface configuration mode. To remove a serial interface from a multilink interface bundle, use the **no** form of this command.

multilink group *bundleID*

no multilink group *bundleID*

Syntax Description

bundleID	Bundle ID number of the multilink interface, in the format *rack/slot/bay/controllerID/bundleID*)

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
hdlc	read, write

Examples

The following examples show how to attach a serial interface to a multilink interface bundle:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface serial 0/1/0/1/1/1:0
RP/0/0/CPU0:router(config-if)# multilink group 1
RP/0/0/CPU0:router(config-if)# commit
```

or

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface serial 0/1/0/1/1/1:0
RP/0/0/CPU0:router(config-if)# multilink
RP/0/0/CPU0:router(config-if-multilink)# group 1
(config-if-multilink)# commit
```

Related Commands

Command	Description
multilink fragment-size, on page 515	
multilink, on page 514	Enters the config-if-multilink submode.
ppp multilink minimum-active links, on page 521	Sets the minimum number of active links required before the multilink interface line can be brought to the up state.

multilink interleave

To enable interleave on a multilink interface, use the **multilink interleave** command in interface configuration mode.

multilink interleave

Syntax Description

This command has no keywords or arguments.

Command Default

The default is no interleave.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

Link Fragmentation and Interleaving (LFI) is designed for MLPPP interfaces and is required when integrating voice and data on low-speed interfaces that run at less than 768 Kbps.

Link Fragmentation and Interleaving (LFI) provides stability for delay-sensitive traffic, such as voice or video, traveling on the same circuit as data. Voice is susceptible to increased latency and jitter when the network processes large packets on low-speed interfaces that run at less than 768 Kbps. LFI reduces delay and jitter by fragmenting large datagrams and interleaving them with low-delay traffic packets.

Task ID

Task ID	Operations
hdlc	read, write

Examples

The following examples show how to enable interleave on a multilink interface.

```
RP/0/0/CPU0:router# configuration
RP/0/0/CPU0:router#(config)# interface multilink 0/1/0/0/1
RP/0/0/CPU0:router#(config-if)# multilink interleave
RP/0/0/CPU0:router#(config-if)# commit
```

or

```
RP/0/0/CPU0:router# configuration
RP/0/0/CPU0:router#(config)# interface multilink 0/1/0/0/1
RP/0/0/CPU0:router#(config-if)# multilink
RP/0/0/CPU0:router#(config-if-multilink)# interleave
RP/0/0/CPU0:router#(config-if-multilink)# commit
```

Related Commands

Command	Description
multilink, on page 514	Enters the config-if-multilink submode.
multilink fragment-size, on page 515	

ppp multilink minimum-active links

To set the minimum number of active links required before the multilink interface line can be brought to the up state, use the **ppp multilink minimum-active links** command in global configuration mode.

ppp multilink minimum-active links *value*

Syntax Description

value	Number of active links. The range is 1 through 12.

Command Default

The default value is 1 active link.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

When multiple links are active and one link goes down, the whole bundle goes down.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to set the minimum number of active links to 6:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface Multilink 0/1/0/0/1
RP/0/0/CPU0:router(config-if)# ppp multilink minimum-active links 6
```

Related Commands

Command	Description
multilink fragment-size, on page 515	
multilink group, on page 517	Attaches a serial interface to a multilink interface bundle.
multilink, on page 514	Enters the config-if-multilink submode.

show controllers mgmtmultilink

To display information about the state and the number of bundles of a multilink controller, use the **show controller mgmtmultilink** command in EXEC mode.

show controllers mgmtmultilink *interface-path-id* [**all**| **brief**| **internal-state**| **tabular**]

Syntax Description

interface-path-id	Virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
all	Displays all multilink management information.
brief	Displays brief multilink management information.
internal-state	Displays internal multilink management state.
tabular	Displays multilink management information in tabular format.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*instance*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *instance*: Number of the controller instance. The instance is always 0.

• If specifying a virtual interface, the number range varies, depending on interface type.

Task ID

Task ID	Operations
interface	read

Examples

The following example shows how to display information for a management multilink controller:

```
RP/0/0/CPU0:router# show controllers mgmtmultilink 0/3/0/0 all

Controller MgmtMultilink0/3/0/0
  State is up
  Number of bundles: 2
    Bundle 1 - Multilink0/3/0/0/1 (0x06186240)
      Type:  Full Framed T1s
      Bandwidth: 3072 kbps
      Encapsulation: Frame Relay
      Fragment size: 0
      Number of members: 2
      Ancestor name: SONET0/3/0/0
      Member(s):
           Serial0/3/0/0/1/1:0  (0x0619b640)    Active
           Serial0/3/0/0/1/2:0  (0x06176980)    Active

    Bundle 2 - Multilink0/3/0/0/2 (0x06176840)
      Type:  Full Framed T1s
      Bandwidth: 3072 kbps
      Encapsulation: Frame Relay
      Fragment size: 0
      Number of members: 2
      Ancestor name: SONET0/3/0/0
      Member(s):
           Serial0/3/0/0/1/3:0  (0x0619b3c0)    Active
           Serial0/3/0/0/1/4:0  (0x0618b9c0)    Active

RP/0/0/CPU0:router# show controllers mgmtmultilink 0/3/0/0 brief

  MgmtMultilink0/3/0/0 is up

RP/0/0/CPU0:router# show controllers mgmtmultilink 0/3/0/0 tabular

  MgmtMultilink0/3/0/0 is up

RP/0/0/CPU0:router# show controllers mgmtmultilink 0/3/0/0 internal-state

Interface(layer)      admin_up if_state
--------------------- -------- --------
MgmtMultilink0/3/0/0  up       up

RP/0/0/CPU0:router# show controllers mgmtmultilink 0/2/0/0

Controller MgmtMultilink0/2/0/0
   State is up
   Number of bundles: 1
     Bundle 1 - Multilink0/2/0/0/1 (0x0802e400)
       Type:  Full Framed T1s
       Bandwidth: 1536 kbps
       Encapsulation: PPP
       Fragment size: 0
       Number of members: 1
       Ancestor name: SONET0/2/0/0
       Member(s):
            Serial0/2/0/0/1/1:0  (0x08023c00)    Active
```

Related Commands

Command	Description
show interfaces multilink, on page 525	Displays information about a multilink interface.

show interfaces multilink

To display information about a multilink interface, use the **show interfaces multilink** command in EXEC mode.

show interfaces multilink *interface-path-id*

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.
- If specifying a virtual interface, the number range varies, depending on interface type.

Task ID

Task ID	Operations
interface	read

Examples

The following example shows how to display information about a multilink interface:

```
RP/0/0/CPU0:router# show interfaces multilink 0/1/0/0/1
 Multilink0/1/0/0/1 is up, line protocol is up
   Interface state transitions: 1
   Hardware is Multilink network interface(s)
   Internet address is 10.1.1.1/24
   MTU 1504 bytes, BW 1536 Kbit
      reliability 255/255, txload 3/255, rxload 3/255
   Encapsulation PPP,  loopback not set, keepalive set (10 sec)
   LCP Open
   Open: IPCP
   Last input 00:00:00, output 00:00:00
   Last clearing of "show interface" counters 02:06:24
   5 minute input rate 19000 bits/sec, 5 packets/sec
   5 minute output rate 19000 bits/sec, 5 packets/sec
      48769 packets input, 12425740 bytes, 0 total input drops
      0 drops for unrecognized upper-level protocol
      Received 0 runts, 0 giants, 0 throttles, 0 parity
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      67905 packets output, 17400050 bytes, 0 total output drops
      0 output errors, 0 underruns, 0 applique, 0 resets
      0 output buffer failures, 0 output buffers swapped out
Fragmentation Statistics
   Input Fragmented packets 0            Input Fragmented bytes 0
   Output Fragmented packets 0           Output Fragmented bytes 0
   Input Unfragmented packets 0          Input Unfragmented bytes 0
   Output Unfragmented packets 0         Output Unfragmented bytes 0
   Input Reassembled packets 0           Input Reassembled bytes 0
```

Null Interface Commands

This module provides command line interface (CLI) commands for configuring null interfaces on the Cisco XR 12000 Series Router.

interface null 0

To enter null0 interface configuration mode, use the **interface null 0** command in global configuration mode.

interface null 0

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was first supported.

Usage Guidelines

When you issue the **interface null 0** command in global configuration mode, the CLI prompt changes to "config-null0," indicating that you have entered interface configuration mode for the null interface. In the following sample output, the question mark (**?**) online help function displays all the commands available under the interface configuration mode for the null interface:

```
RP/0/0/CPU0:router(config)# interface null 0
RP/0/0/CPU0:router(config-null0)#?

  commit    Commit the configuration changes to running
  describe  Describe a command without taking real actions
  do        Run an exec command
  exit      Exit from this submode
  no        Negate a command or set its defaults
  show      Show contents of configuration
```

Task ID

Task ID	Operations
interface	read, write

Examples

This example shows how to enter null0 interface configuration mode:

```
RP/0/0/CPU0:router(config)# interface null 0
RP/0/0/CPU0:router(config-null0)#
```

show controllers null interface

To display null interface counters, use the **show controllers null interface** command in EXEC mode.

show controllers null interface

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
interface	read
sysmgr	read

Examples

The following is sample output from the **show controllers null interface** command, which displays null interface counters:

```
RP/0/0/CPU0:router# show controllers null interface

Null interface:
name     : Null0
handle   : 0x00080010
rx_count : 0
tx_count : 0
drops    : 0
```

Table 37: show controllers null interface Field Descriptions

Field	Description
name	Interface whose controller information is displayed.

Field	Description
handle	Number that identifies the caps node that hosts the node whose controller information is displayed.
rx_count	Total number of packets currently received by the interface.
tx_count	Total number of packets currently transmitted by the interface.
drops	Total number of packets dropped by the interface.

Related Commands

Command	Description
show interfaces null0, on page 531	Displays null0 interfaces.

show interfaces null0

To display null0 interfaces, use the **show interfaces null0** command with optional keywords in EXEC mode.

show interfaces null0 [**accounting rates**| **brief**| **description**| **detail**] [**location** *node-id*]

Syntax Description

accounting	Shows interface accounting option.
rates	Shows interface accounting (input/output) rates.
brief	Shows interface information in condensed format.
description	Describes interface.
detail	Shows interface information in detail.
location *node-id*	Specifies a fully qualified interface location.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.6.0	This command variant was added to the existing **show interfaces** command.

Usage Guidelines

The **show interfaces null0** command displays statistics about null interfaces. When no keywords are specified, information for all null interfaces is displayed.

Task ID

Task ID	Operations
interface	read

Examples

The following example shows how to use the **show interfaces null0** command:

```
RP/0/0/CPU0:router# show interfaces null0

Null0 is up, line protocol is up
```

```
Interface state transitions: 0
Hardware is Null interface
Internet address is Unknown
MTU 1500 bytes, BW Unknown
   reliability 255/255, txload Unknown, rxload Unknown
Encapsulation Null,  loopback not set,
Last clearing of "show interface" counters never
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   0 packets input, 0 bytes, 0 total input drops
   0 drops for unrecognized upper-level protocol
   Received 0 broadcast packets, 0 multicast packets
   0 packets output, 0 bytes, 0 total output drops
   Output 0 broadcast packets, 0 multicast packets
```

Packet-over-SONET Interface Commands on the Cisco IOS XR Software

This module provides command line interface (CLI) commands for configuring Packet-over-SONET/SDH (POS) on the Cisco XR 12000 Series Router.

This module describes the Cisco IOS XR commands used to configure, monitor, and troubleshoot Packet-over-SONET/SDH (POS).

POS provides a method for efficiently carrying data packets in SONET or Synchronous Digital Hierarchy (SDH) frames. High-bandwidth capacity and efficient link utilization are characteristics that make POS largely preferred for building the core of data networks. POS uses PPP in High-Level Data Link Control (HDLC)-like framing for data encapsulation at Layer 2 (data link) of the Open System Interconnection (OSI) stack. This method provides efficient packet delineation and error control.

In addition to high-bandwidth efficiency, POS offers secure and reliable transmission for data. Reliable data transfer depends on timing integrity.

The real-time POS functionality is performed in hardware, according to the hardware configuration setup. Configured hardware events are detected by the framer application-specific integrated circuits (ASICs) and the control is passed to the software. The generic POS driver is responsible for providing a mechanism to configure the hardware on a per-interface basis, to handle interface state transitions, and to collect POS-related statistics.

crc (POS)

To set the length of the cyclic redundancy check (CRC) on a Packet-over-SONET/SDH (POS) interface, use the **crc** command in POS configuration mode. To return the CRC setting on a POS interface to the 32-bit default setting, use the **no** form of this command.

crc {**16**| **32**}

no crc [**16**| **32**]

Syntax Description

16	Sets 16-bit CRC mode.
32	Sets 32-bit CRC mode. The default is 32 bits.

Command Default

The default CRC mode is 32 bits.

Command Modes

POS configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

CRC is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data. The designators 16 and 32 indicate the length (in bits) of the frame check sequence (FCS). A CRC of 32 bits provides more powerful error detection, but adds overhead. Both the sender and receiver must use the same setting.

CRC-16, the most widely used error checking method throughout the United States and Europe, is used extensively with WANs. CRC-32 is specified by IEEE standard 802 and as an option by some point-to-point transmission standards. It is often used on Switched Multimegabit Data Service (SMDS) networks and LANs.

Task ID

Task ID	Operations
pos-dpt	read, write

Examples

In this example, the 32-bit CRC on POS interface 0/1/0/2 is enabled:

```
rack/slot/module(config)# interface POS 0/1/0/2
rack/slot/module(config-if)# POS
```

```
rack/slot/module(config-if-pos)# crc 32
```

Related Commands

Command	Description
transmit-delay, on page 547	Specifies a number of flag sequences to be inserted between the packets.

encapsulation (POS)

To set the Layer 2 encapsulation of an interface, use the **encapsulation** command in interface configuration mode. To restore the system to the default encapsulation, use the **no** form of this command.

encapsulation {**hdlc**| **ppp**| **frame-relay [ietf]** }

no encapsulation [**hdlc**| **ppp**| **frame-relay [ietf]**]

Syntax Description

hdlc	Enables Cisco High-Level Data Link Control (cHDLC) encapsulation on the interface. This is the default encapsulation type.
ppp	Enables Point-to-Point Protocol (PPP) encapsulation on the interface.
frame -relay	Enables Frame Relay encapsuation on the interface.
ietf	(Optional) Enables RFC1490/RFC2427 encapsulation.

Command Default

For Packet-over-SONET/SDH (POS) interfaces, the default encapsulation is HDLC.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.4.0	The **frame-relay** and **ietf** keywords were added.

Usage Guidelines

The task ID hdlc (r,w) is required for use of the keyword **hdlc**. The task ID ppp(r,w) is required for use of the keyword **ppp**. The task ID fr(r,w) is required for use of the keyword **frame-relay**.

Task ID

Task ID	Operations
hdlc OR ppp OR fr	read, write
interface	read, write

Examples

In this example, PPP encapsulation is set on POS interface 0/3/0/1:

```
RP/0/0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/0/CPU0:router(config-if)# encapsulation ppp
```

Related Commands

Command	Description
show interfaces pos, on page 544	Displays information about a POS interface.
show ppp interfaces , on page 578	Displays PPP state information for an interface.

interface pos

To enter interface or subinterface configuration mode for a POS interface or subinterface, use the **interface pos** command in global configuration mode. To delete a POS configuration, use the **no** form of this command.

interface pos *interface-path-id*[**.***subinterface* {**l2 transport**| **point-to-point**}]

no interface pos *interface-path-id*[**.***subinterface* {**l2 transport**| **point-to-point**}]

Syntax Description

interface-path-id [.*subinterface*]	Physical interface or virtual interface followed by the optional subinterface path ID. Naming notation is *interface-path-id.subinterface*. The period in front of the subinterface value is required as part of the notation. For more information about the syntax for the router, use the question mark (?) online help function.
l2transport	(Optional) Configures the interface to function as an attachment circuit (AC) on one endpoint of a Layer 2 link.
point-to-point	(Optional) Configures interface to function as one endpoint of a point-to-point link.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Subinterfaces of a POS interface can only be configured using the **l2transport** keyword, if Frame Relay encapsulation is configured on the POS interface, using the **encapsulation frame-relay** command. Interfaces configured to use HDLC or PPP encapsulation cannot be configured using the **l2transport** keyword.

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.

- *port*: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter interface configuration mode for a POS interface:

```
RP/0/0/CPU0:router(config)# interface pos 0/1/0/0
RP/0/0/CPU0:router(config-if)#
```

The following example shows how to create a subinterface on a POS interface in slot 1, subslot 1, port 2 and enter subinterface configuration mode:

```
RP/0/0/CPU0:router(config)# interface pos 0/1/1/2.1
RP/0/0/CPU0:router(config-subif)#
```

The following example shows how to configure frame-relay encapsulation on the main POS interface before being able to configure an AC subinterface:

```
RP/0/0/CPU0:router# interface pos 0/1/0/0
RP/0/0/CPU0:router(config-if)# encapsulation frame-relay
RP/0/0/CPU0:router(config-if)# commit
RP/0/0/CPU0:router(config-if)# exit
RP/0/0/CPU0:router(config)# interface pos 0/1/0/0.1 l2transport
RP/0/0/CPU0:router(config-subif)# commit
```

Related Commands

Command	Description
show interfaces pos, on page 544	Displays information about a POS interface.

keepalive (POS)

To set the keepalive timer for a specific interface, use the **keepalive** command in interface configuration mode. To reset the keepalive timer to the default of 10 seconds, use the **no** form of this command.

keepalive {*interval* [*retry*]| **disable**}

no keepalive

Syntax Description

interval	Number of seconds (from 1 to 30) between keepalive messages. The default is 10.
retry	(Optional) Number of keepalive messages (from 1 to 255) that can be sent to a peer without a response before transitioning the link to the down state. The default is 5 for interfaces with PPP encapsulation, and 3 for interfaces with HDLC encapsulation.
disable	Turns off the keepalive timer.

Command Default

The default interval is 10 seconds between keepalive messages. The default number of retry keepalive messages that can be sent without a response is 5 for interfaces with PPP encapsulation, and 3 for interfaces with HDLC encapsulation. However, when more than 5 (or 3) keepalive messages are sent to a peer without a response, the link transitions to the down state.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.9.0	The *retry* argument was added.

Usage Guidelines

cHDLC keepalives require that the **keepalive** command is configured the same way on both routers. The two connected routers have no way of negotiating the keepalive value, because there is no way for the routers to tell each other what their configured values are. The keepalive value configured on each router (local and partner) sets the rate at which the Cisco IOS XR software sends packets. It also sets the rate at which the local end expects to receive incoming packets.

To set the keepalive value to the default value, use the **keepalive** command without specifying a value for the *seconds* argument.

If three keepalives are sent to the peer and no response is received from the peer, then the link makes the transition to the down state.

Task ID

Task ID	Operations
hdlc	read, write
ppp	read,write

Examples

This example shows how to configure keepalives for 3 seconds on POS interface 0/7/0/1:

```
RP/0/0/CPU0:router(config)# interface POS 0/7/0/1
RP/0/0/CPU0:router(config-if)# keepalive 3
```

pos

To access the POS configuration submode, use the **pos** command in interface configuration mode.

pos

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

When you issue the **pos** command in interface configuration mode for a POS interface, the CLI prompt changes to "config-if-pos," indicating that you have entered POS configuration submode. In the following sample output, the question mark (**?**) online help function displays all the commands available under POS configuration submode:

```
RP/0/0/CPU0:router(config)# interface POS 0/1/0/2
RP/0/0/CPU0:router(config-if)# POS
RP/0/0/CPU0:router(config-if-pos)# ?

  commit          Commit the configuration changes to running
  crc             Set the CRC on a POS interface
  describe        Describe a command without taking real actions
  do              Run an exec command
  exit            Exit from this submode
  no              Negate a command or set its defaults
  show            Show contents of configuration
  transmit-delay  Set POS transmit delay on an interface
```

Task ID

Task ID	Operations
pos-dpt	read, write

Examples

The following example shows how to access the POS configuration submode from the POS configuration mode:

```
RP/0/0/CPU0:router(config)# interface POS 0/1/0/2
RP/0/0/CPU0:router(config-if)# POS
RP/0/0/CPU0:router(config-if-pos)#
```

Related Commands

Command	Description
crc (POS), on page 534	Sets the length of the CRC on a Packet-over-SONET/SDH (POS) interface.
transmit-delay, on page 547	Specifies a number of flag sequences to be inserted between the packets.

show interfaces pos

To display information about a POS interface, use the **show interfaces pos** command in EXEC mode.

show interfaces pos *interface-path-id* [**accounting [rates]| brief| description| detail**] [**location** *node-id*]

Syntax Description

interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
accounting	(Optional) Displays accounting information for all POS interfaces on the router, for a specific POS interface instance, or for all POS interfaces on a specific node.
rates	(Optional) Displays interface accounting rates for all POS interfaces on the router, for a specific POS interface instance, or for all POS interfaces on a specific node.
brief	(Optional) Displays brief output for all POS interfaces on the router, for a specific POS interface instance, or for all POS interfaces on a specific node.
description	Displays descriptive output for all POS interfaces on the router, for a specific POS interface instance, or for all POS interfaces on a specific node.
detail	(Optional) Displays detailed output for all POS interfaces on the router, for a specific POS interface instance, or for all POS interfaces on a specific node.
location *node-id*	(Optional) Displays detailed POS information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

Enter the **show interfaces pos** command without including any of the optional keywords or arguments to display detailed information about all POS interfaces configured on the router.

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.
- If specifying a virtual interface, the number range varies, depending on interface type.

Task ID

Task ID	Operations
interface	read

Examples

The following example shows how to display summarized information for a POS interface on a specific node:

```
RP/0/0/CPU0:router# show interfaces pos summary location 0/1/CPU0

Interface Type          Total    UP       Down     Admin Down
--------------          -----    --       ----     ----------
ALL TYPES               4        1        1        2
--------------
IFT_POS                 4        1        1        2
```

Table 38: show interfaces pos summary Field Descriptions

Field	Description
Intf Type	Type of interface described in the display.
Total	Total number of configured interfaces of the specified type.
Up	Number of interfaces of the specified type that are in the “Up” state.
Down	Number of interfaces of the specified type that are in the “Down” state.
Admin Down	Number of interfaces of the specified type that are in the “Admin Down” state.

The following example shows how to display brief information for a specific POS interface:

```
RP/0/0/CPU0:router# show interfaces pos 0/2/0/0 brief

              Intf        Intf         LineP              Encap  MTU       BW
```

```
              Name         State         State                Type (byte)    (Kbps)
--------------------------------------------------------------------------------
          PO0/2/0/0    admin-down    admin-down               HDLC  4474    2488320
```

Table 39: show interfaces pos Field Descriptions

Field	Description
Intf Name	Interface identifier, in the *type***rack*/*slot*/*module*/*port* notation.
Intf State	Indicates whether the interface is in the admin-up or admin down state.
LineP State	Line protocol state.
Encap Type	Encapsulation type for the specified interface. Can be HDLC or PPP.
MTU (byte)	Maximum transmission unit (MTU) value configured for the specified interface, in bytes.
BW (Kbps)	Bandwidth of the interface, in kbps.

Related Commands

Command	Description
show controllers pos, on page 705	Displays information on the POS controllers.
show controllers sonet, on page 711	Displays information about the operational status of SONET layers.

transmit-delay

To specify a number of flag sequences to be inserted between the packets, use the **transmit-delay** command in POS configuration mode. To restore the default, use the **no** form of this command.

transmit-delay *microseconds*

no transmit-delay *microseconds*

Syntax Description

microseconds	Number of microseconds of minimum delay after sending a packet. Range is from 0 to 1023. Default is 0 (disabled).

Command Default

microseconds = 0 (disabled)

Command Modes

POS configuration

Command History

Releases	Modifications
Release 3.2	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
pos-dpt	read, write

Examples

In the following example, a delay of 2 microseconds is specified on POS interface 0/1/0/2:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface POS 0/1/0/2
RP/0/0/CPU0:router(config-if)# pos
RP/0/0/CPU0:router(config-if-pos)# transmit-delay 2
```

In the following example, the transmit delay on POS interface 0/1/0/2 is disabled:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface POS 0/1/0/2
RP/0/0/CPU0:router(config-if)# pos
RP/0/0/CPU0:router(config-if-pos)# no transmit-delay
```

Related Commands

Command	Description
show interfaces	

PPP Commands onthe Cisco IOS XR Software

This module provides command line interface (CLI) commands for configuring Point-to-Point Protocol (PPP) on the Cisco XR 12000 Series Router.

Point-to-Point Protocol (PPP) is an encapsulation scheme that can be used on Packet-over-SONET (POS), serial, and multilink interfaces. PPP is a standard protocol used to send data over synchronous serial links. PPP also provides a Link Control Protocol (LCP) for negotiating properties of the link. LCP uses echo requests and responses to monitor the continuing availability of the link.

PPP provides the following Network Control Protocols (NCPs) for negotiating properties of data protocols that will run on the link:

- Cisco Discovery Protocol Control Protocol (CDPCP) to negotiate CDP properties
- IP Control Protocol (IPCP) to negotiate IP properties
- IP Version 6 Control Protocol (IPv6CP) to negotiate IPv6 properties
- Multiprotocol Label Switching Control Protocol (MPLSCP) to negotiate MPLS properties
- Open System Interconnection Control Protocol (OSICP) to negotiate OSI properties

- ppp timeout authentication, page 575
- ppp timeout retry, page 577
- show ppp interfaces , page 578

encapsulation ppp

To enable encapsulation for communication with routers or bridges using the Point-to-Point Protocol (PPP), use the **encapsulation ppp** command in interface configuration mode. To disable PPP encapsulation, use the **no** form of this command.

encapsulation ppp

no encapsulation ppp

Syntax Description

This command has no keywords or arguments.

Command Default

PPP encapsulation is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **encapsulation ppp** command to enable PPP encapsulation on an interface.

Task ID

Task ID	Operations
ppp	read, write
interface	read, write

Examples

The following example shows how to set up PPP encapsulation on interface POS 0/1/0/1:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface POS 0/1/0/1
RP/0/0/CPU0:router(config-if)# encapsulation ppp
```

The following example shows how to set up PPP encapsulation on a serial interface:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router# interface serial 0/0/1/2/4:3
RP/0/0/CPU0:router# encapsulation ppp
```

Related Commands

Command	Description
show ppp interfaces , on page 578	Displays PPP state information for an interface.

ppp authentication

To enable Challenge Handshake Authentication Protocol (CHAP), MS-CHAP, or Password Authentication Protocol (PAP), and to specify the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface, use the **ppp authentication** command an appropriate configuration mode. To disable PPP authentication, use the **no** form of this command.

ppp authentication *protocol* [*protocol* [*protocol*]] {*list-name*| **default**}

no ppp authentication

Syntax Description

protocol	Name of the authentication protocol used for PPP authentication. See Table 40: PPP Authentication Protocols for Negotiation, on page 554 for the appropriate keyword. You may select one, two, or all three protocols, in any order.
list-name	(Optional) Used with authentication, authorization, and accounting (AAA). Name of a list of methods of authentication to use. If no list name is specified, the system uses the default. The list is created with the **aaa authentication ppp** command.
default	(Optional) Specifies the name of the list of methods created with the **aaa authentication ppp** command.

Command Default

PPP authentication is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.2	This command was corrected to include the possibility of specifying three protocols simultaneously.

Usage Guidelines

When you enable CHAP or PAP authentication (or both), the local router requires the remote device to prove its identity before allowing data traffic to flow. PAP authentication requires the remote device to send a name and a password, which is checked against a matching entry in the local username database or in the remote security server database. CHAP authentication sends a challenge message to the remote device. The remote device encrypts the challenge value with a shared secret and returns the encrypted value and its name to the local router in a response message. The local router attempts to match the remote device's name with an associated secret stored in the local username or remote security server database; it uses the stored secret to encrypt the original challenge and verify that the encrypted values match.

You can enable CHAP, MS-CHAP, or PAP in any order. If you enable all three methods, the first method specified is requested during link negotiation. If the peer suggests using the second method, or refuses the first method, the second method is tried. Some remote devices support only one method. Base the order in which you specify methods on the remote device's ability to correctly negotiate the appropriate method, and on the level of data line security you require. PAP usernames and passwords are sent as clear text strings, which can be intercepted and reused.

Note If you use a *list-name* value that was not configured with the **aaa authentication ppp** command, then authentication does not complete successfully and the line does not come up.

Table 40: PPP Authentication Protocols for Negotiation, on page 554 lists the protocols used to negotiate PPP authentication.

Table 40: PPP Authentication Protocols for Negotiation

Protocol	Description
chap	Enables CHAP on an interface.
ms-chap	Enables Microsoft's version of CHAP (MS-CHAP) on an interface.
pap	Enables PAP on an interface.

Enabling or disabling PPP authentication does not affect the ability of the local router to authenticate itself to the remote device.

MS-CHAP is the Microsoft version of CHAP. Like the standard version of CHAP, MS-CHAP is used for PPP authentication. In this case, authentication occurs between a personal computer using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server.

Enabling or disabling PPP authentication does not affect the local router authenticating itself to the remote device.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

In this example, CHAP is enabled on POS 0/4/0/1 and uses the authentication list MIS-access:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface POS 0/4/0/1
RP/0/0/CPU0:router(config-if)# encapsulation ppp
RP/0/0/CPU0:router(config-if)# ppp authentication chap MIS-access
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
encapsulation	Sets the encapsulation method used by the interface.
username	Configures a new user with a username, establishes a password, and grants permissions for the user.

ppp chap password

To enable a router calling a collection of routers to configure a common Challenge Handshake Authentication Protocol (CHAP) secret password, use the **ppp chap password** command in interface configuration mode. To disable the password, use the **no** form of this command.

ppp chap password [**clear**| **encrypted**] *password*

no ppp chap password [**clear**| **encrypted**] *password*

Syntax Description

clear	(Optional) Specifies the cleartext encryption parameter for the password.
encrypted	(Optional) Indicates that the password is already encrypted.
password	Cleartext or already-encrypted password.

Command Default

The password is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

The **ppp chap password** command is sent in CHAP responses and is used by the peer to authenticate the local router. This does not affect local authentication of the peer. This command is useful for routers that do not support this command (such as routers running older Cisco IOS XR images).

The CHAP secret password is used by the routers in response to challenges from an unknown peer.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

In this example, a password (xxxx) is entered as a cleartext password:

```
RP/0/0/CPU0:router(config-if)# ppp chap password xxxx
```

When the password is displayed (as shown in the following example, using the **show running-config** command), the password xxxx appears as 030752180500:

```
RP/0/0/CPU0:router(config)# show running-config interface POS 1/0/1/0

interface POS0/1/4/2

description Connected to P1 POS 0/1/4/3
ipv4 address 10.12.32.2 255.255.255.0
encapsulation ppp
ppp authentication chap pap
ppp chap password encrypted 030752180500
```

On subsequent logins, entering any of the three following commands would have the same effect of making xxxx the password for remote CHAP authentication:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface POS 1/0/1/0
RP/0/0/CPU0:router(config-if)# ppp chap password xxxx
RP/0/0/CPU0:router(config-if)# ppp chap password clear xxxx
RP/0/0/CPU0:router(config-if)# ppp chap password encrypted 1514190900
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces running PPP.
ppp authentication , on page 553	Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.
ppp chap refuse, on page 558	Refuses CHAP authentication from peers requesting it.
ppp max-bad-auth , on page 560	Configures a PPP interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.

ppp chap refuse

To refuse Challenge Handshake Authentication Protocol (CHAP) authentication from peers requesting it, use the **ppp chap refuse** command in interface configuration mode. To allow CHAP authentication, use the **no** form of this command.

ppp chap refuse

no ppp chap refuse

Syntax Description

This command has no keywords or arguments.

Command Default

CHAP authentication is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

The **ppp chap refuse** command specifies that CHAP authentication is disabled for all calls, meaning that all attempts by the peer to force the user to authenticate using CHAP are refused.

If outbound Password Authentication Protocol (PAP) has been configured (using the **ppp authentication** command), PAP is suggested as the authentication method in the refusal packet.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

The following example shows how to specify POS interface 0/3/0/1 and disable CHAP authentication from occurring if a peer calls in requesting CHAP authentication. The method of encapsulation on the interface is PPP.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/0/CPU0:router(config-if)# encapsulation ppp
RP/0/0/CPU0:router(config-if)# ppp chap refuse
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces running PPP.
ppp authentication , on page 553	Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.
ppp max-bad-auth , on page 560	Configures a PPP interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries.
ppp pap sent-username password, on page 573	Enables remote PAP support for an interface, and includes the **sent-username** and **password** commands in the PAP authentication request packet to the peer.

ppp max-bad-auth

To configure a PPP interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries, use the **ppp max-bad-auth** command in the appropriate configuration mode. To reset to the default of immediate reset, use the **no** form of this command.

ppp max-bad-auth *retries*

no ppp max-bad-auth

Syntax Description

retries	Number of retries after which the interface is to reset itself. Range is from 0 to 10. Default is 0 retries.

Command Default

retries: 0

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

The **ppp max-bad-auth** command applies to any interface on which PPP encapsulation is enabled.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

In this example, POS interface 0/3/0/1 is set to allow two additional retries after an initial authentication failure (for a total of three failed authentication attempts):

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/0/CPU0:router(config-if)# encapsulation ppp
RP/0/0/CPU0:router(config-if)# ppp authentication chap
RP/0/0/CPU0:router(config-if)# ppp max-bad-auth 3
```

ppp max-configure

To specify the maximum number of configure requests to attempt (without response) before stopping the requests, use the **ppp max-configure** command in an appropriate configuration mode. To disable the maximum number of configure requests and return to the default, use the **no** form of this command.

ppp max-configure *retries*

no ppp max-configure

Syntax Description

retries	Maximum number of retries. Range is 4 through 20. Default is 10.

Command Default

retries: 10

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **ppp max-configure** command to specify how many times an attempt is made to establish a Link Control Protocol (LCP) session between two peers for a particular interface. If a configure request message receives a reply before the maximum number of configure requests are sent, further configure requests are abandoned.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

This example shows a limit of four configure requests:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/0/CPU0:router(config-if)# encapsulation ppp
RP/0/0/CPU0:router(config-if)# ppp max-configure 4
```

Related Commands

Command	Description
ppp max-failure , on page 563	Configures the maximum number of consecutive CONFNAKs to permit before terminating a negotiation.

ppp max-failure

To configure the maximum number of consecutive Configure Negative Acknowledgments (CONFNAKs) to permit before terminating a negotiation, use the **ppp max-failure** command in an appropriate configuration mode. To disable the maximum number of CONFNAKs and return to the default, use the **no** form of this command.

ppp max-failure *retries*

no ppp max-failure

Syntax Description

retries	Maximum number of CONFNAKs to permit before terminating a negotiation. Range is from 2 to 10. Default is 5.

Command Default

retries: 5

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

The **ppp max-failure** command specifies that no more than three CONFNAKs are permitted before terminating the negotiation:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/0/CPU0:router(config-if)# encapsulation ppp
RP/0/0/CPU0:router(config-if)# ppp max-failure 3
```

Related Commands

Command	Description
ppp max-configure , on page 561	Specifies the maximum number of configure requests to attempt (without response) before stopping the requests.

ppp max-terminate

To configure the maximum number of terminate requests (TermReqs) to send without reply before closing down the Link Control Protocol (LCP) or Network Control Protocol (NCP), use the **ppp max-terminate** command in interface configuration mode. To disable the maximum number of TermReqs and return to the default, use the **no** form of this command.

ppp max-terminate *number*

no ppp max-terminate

Syntax Description

number	Maximum number of TermReqs to send without reply before closing down the LCP or NCP. Range is from 2 to 10. Default is 2.

Command Default

number: 2

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ppp	read, write

Examples

In the following example, a maximum of five TermReqs are specified to be sent before terminating and closing LCP or NCP:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/0/CPU0:router(config-if)# encapsulation ppp
RP/0/0/CPU0:router(config-if)# ppp max-terminate 5
```

Related Commands

Command	Description
ppp max-configure , on page 561	Specifies the maximum number of configure requests to attempt (without response) before stopping the requests.
ppp max-failure , on page 563	Configures the maximum number of consecutive CONFNAKs to permit before terminating a negotiation.

ppp ms-chap password

To configure a common Microsoft Challenge Handshake Authentication (MS-CHAP) secret password, use the **ppp ms-chap password** command in interface configuration mode. To disable the password, use the **no** form of this command.

ppp ms-chap password [**clear**| **encrypted**] *password*

no ppp ms-chap password [**clear**| **encrypted**] *password*

Syntax Description

clear	(Optional) Specifies the cleartext encryption parameter for the password.
encrypted	(Optional) Indicates that the password is already encrypted.
password	Cleartext or already-encrypted password.

Command Default

The password is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

The **ppp ms-chap password** command is sent in CHAP responses and is used by the peer to authenticate the local router. This does not affect local authentication of the peer. The **ppp ms-chap password** command is useful for routers that do not support this command (such as routers running older software images).

The MS-CHAP secret password is used by the routers in response to challenges from an unknown peer.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to enter a password (xxxx) as a cleartext password:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/0/CPU0:router(config-if)# encapsulation ppp
```

```
RP/0/0/CPU0:router(config-if)# ppp ms-chap password clear xxxx
```

ppp ms-chap refuse

To refuse Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) authentication from peers requesting it, use the **ppp ms-chap refuse** command in interface configuration mode. To allow MS-CHAP authentication, use the **no** form of this command.

ppp ms-chap refuse

no ppp ms-chap refuse

Syntax Description

This command has no keywords or arguments.

Command Default

MS-CHAP authentication is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

The **ppp ms-chap refuse** command specifies that MS-CHAP authentication is disabled for all calls, meaning that all attempts by the peer to force the user to authenticate using MS-CHAP are refused.

If outbound Password Authentication Protocol (PAP) has been configured (using the **ppp authentication** command), PAP is suggested as the authentication method in the refusal packet.

Task ID

Task ID	Operations
ppp	read, write

Examples

This example shows how to specify POS interface 0/3/0/1 and disable MS-CHAP authentication from occurring if a peer calls in requesting MS-CHAP authentication. The method of encapsulation on the interface is PPP.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/0/CPU0:router(config-if)# encapsulation ppp
RP/0/0/CPU0:router(config-if)# ppp ms-chap refuse
```

Related Commands

Command	Description
ppp authentication , on page 553	Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.

ppp pap refuse

To refuse Password Authentication Protocol (PAP) authentication from peers requesting it, use the **ppp pap refuse** command in interface configuration mode. To allow PAP authentication, use the **no** form of this command.

ppp pap refuse

no ppp pap refuse

Syntax Description

This command has no keywords or arguments.

Command Default

PAP authentication is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

The **ppp pap refuse** command specifies that PAP authentication is disabled for all calls, meaning that all attempts by the peer to force the user to authenticate using PAP are refused.

If outbound Challenge Handshake Authentication Protocol (CHAP) has been configured (using the **ppp authentication** command), CHAP is suggested as the authentication method in the refusal packet.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

The following example shows how to specify POS 0/3/0/1 using PPP encapsulation on the interface. This example shows PAP authentication being specified as disabled if a peer calls in requesting PAP authentication.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/0/CPU0:router(config-if)# encapsulation ppp
RP/0/0/CPU0:router(config-if)# ppp pap refuse
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces running PPP.
ppp authentication , on page 553	Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.
ppp max-bad-auth , on page 560	Configures a PPP interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries.
ppp pap sent-username password, on page 573	Enables remote PAP support for an interface, and includes the **sent-username** and **password** commands in the PAP authentication request packet to the peer.

ppp pap sent-username password

To enable remote Password Authentication Protocol (PAP) support for an interface, and to use the values specified for username and password in the PAP authentication request, use the **ppp pap sent-username password** command in interface configuration mode. To disable remote PAP support, use the **no** form of this command.

ppp pap sent-username *username* **password** [**clear**| **encrypted**] *password*

no ppp pap sent-username *username* **password** [**clear**| **encrypted**] *password*

Syntax Description

username	Username sent in the PAP authentication request.
clear	(Optional) Specifies the cleartext encryption parameter for the password.
encrypted	(Optional) Indicates that the password is already encrypted.
password	Cleartext or already-encrypted password.

Command Default

Remote PAP support is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **ppp pap sent-username password** command to enable remote PAP support (for example, to respond to the peer's request to authenticate with PAP) and to specify the parameters to be used when sending the PAP authentication request.

You must configure the **ppp pap sent-username password** command for each interface.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

In the following example, a password is entered as a cleartext password, xxxx:

```
RP/0/0/CPU0:router(config-if)# ppp pap sent-username xxxx password notified
```

When the password is displayed (as shown in the following example, using the **show running-config** command), the password notified appears as 05080F1C2243:

```
RP/0/0/CPU0:router(config-if)# show running-config

interface POS0/1/0/0
description Connected to P1 POS 0/1/4/2
 ipv4 address 10.12.32.2 255.255.255.0
 encapsulation ppp
 ppp pap sent-username P2 password encrypted 05080F1C2243
```

On subsequent logins, entering any of the three following commands would have the same effect of making xxxx the password for remote PAP authentication:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface POS 0/1/0/0
RP/0/0/CPU0:router(config-if)# ppp pap sent-username xxxx password notified
RP/0/0/CPU0:router(config-if)# ppp pap sent-username xxxx password clear notified
RP/0/0/CPU0:router(config-if)# ppp pap sent-username xxxx encrypted 1514190900
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces running PPP.
ppp authentication , on page 553	Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.
ppp multilink multiclass	Refuses PAP authentication from peers requesting it
ppp timeout authentication, on page 575	Sets PPP authentication timeout parameters.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.

ppp timeout authentication

To set PPP authentication timeout parameters, use the **ppp timeout authentication** command in interface configuration mode. To reset the default value, use the **no** form of this command.

ppp timeout authentication *seconds*

no ppp timeout authentication

Syntax Description

seconds	Maximum time, in seconds, to wait for a response to an authentication packet. Range is from 3 to 30 seconds. Default is 10 seconds.

Command Default

seconds: 10

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

The default authentication time is 10 seconds, which should allow time for a remote router to authenticate and authorize the connection and provide a response. However, it is also possible that it will take much less time than 10 seconds. In such cases, use the **ppp timeout authentication** command to lower the timeout period to improve connection times in the event that an authentication response is lost.

Note The timeout affects connection times only if packets are lost.

Note Although lowering the authentication timeout is beneficial if packets are lost, sending authentication requests faster than the peer can handle them results in churn and a slower connection time.

Task ID

Task ID	Operations
ppp	read, write

Examples

In the following example, PPP timeout authentication is set to 20 seconds:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/0/CPU0:router(config-if)# encapsulation ppp
RP/0/0/CPU0:router(config-if)# ppp timeout authentication 20
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces running PPP.
ppp authentication , on page 553	Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.

ppp timeout retry

To set PPP timeout retry parameters, use the **ppp timeout retry** command in interface configuration mode. To reset the time value, use the **no** form of this command.

ppp timeout retry *seconds*

no ppp timeout retry

Syntax Description

seconds	Maximum time, in seconds, to wait for a response during PPP negotiation. Range is from 1 to 10 seconds. Default is 3 seconds.

Command Default

seconds: 3

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

The **ppp timeout retry** command is useful for setting a maximum amount of time PPP should wait for a response to any control packet it sends.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows the retry timer being set to 8 seconds:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/0/CPU0:router(config-if)# encapsulation ppp
RP/0/0/CPU0:router(config-if)# ppp timeout retry 8
```

show ppp interfaces

To display PPP state information for an interface, use the **show ppp interfaces** command in EXEC mode.

show ppp interfaces [**brief**| **detail**] {**all**| *type interface-path-id*| **location** *node-id*}

Syntax Description

brief	(Optional) Displays brief output for all interfaces on the router, for a specific POS interface instance, or for all interfaces on a specific node.
detail	(Optional) Displays detailed output for all interfaces on the router, for a specific interface instance, or for all interfaces on a specific node.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
all	(Optional) Displays detailed PPP information for all nodes.
location *node-id*	(Optional) Displays detailed PPP information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command introduced.

Usage Guidelines

There are seven possible PPP states applicable for either the Link Control Protocol (LCP) or the Network Control Protocol (NCP).

The command output displays a summary of the interface as it is in the PPP Interface Descriptor Block (IDB). The output includes the following information (where applicable):

- Interface state
- Line protocol state
- Link Control Protocol (LCP) state
- Network Control Protocol (NCP) state
- Multilink PPP state
- Multilink PPP configuration
- Keepalive configuration
- Authentication configuration
- Negotiated MRUs
- Negotiated IP addresses

This command can display information for a single interface, all interfaces on a specified node, or all interfaces on the router.

Task ID

Task ID	Operations
ppp	read

Examples

This example shows how to display PPP state information for a POS interface:

```
RP/0/0/CPU0:router# show ppp interface POS 0/2/0/3

    POS0/2/0/3 is up, line protocol is up
      LCP: Open
         Keepalives enabled (10 sec)
         Local MRU: 4470 bytes
         Peer  MRU: 4470 bytes
      Authentication
         Of Us:    CHAP (Completed as 'test-user')
         Of Peer:  PAP (Completed as 'peer-user')
      CDPCP: Listen
      IPCP: Open
         Local IPv4 address: 55.0.0.1
         Peer IPv4 address:  55.0.0.2
         Peer DNS Primary:   55.0.0.254
         Peer DNS Secondary: 155.0.0.254
      IPV6CP: Open
         Local IPv6 address: fe80::3531:35ff:fe55:5747/128
         Peer IPv6 address:  fe80::3531:35ff:fe55:4213/128
      MPLSCP: Stopped
```

This example shows how to display PPP state information for a POS interface that is running as a Layer 2 attachment circuit:

```
RP/0/0/CPU0:# show ppp interface POS0/2/0/2

    POS0/2/0/2 is up, line protocol is up
```

```
      LCP: Open
         Running as L2 AC
```

This example shows how to display PPP state information for a multilink interface:

```
RP/0/0/CPU0:router:# show ppp interface Multilink 0/3/0/0/100

    Multilink0/3/0/0/100 is up, line protocol is down
      LCP: Open
         SSO-State: Standby-Up
         Keepalives disabled
      IPCP: Open
         SSO-State: Standby-Up
         Local IPv4 address: 100.0.0.1
         Peer IPv4 address:  100.0.0.2
      IPV6CP: Open
         Local IPv6 address: fe80::3531:35ff:fe55:4600/128
         Peer IPv6 address:  fe80::3531:35ff:fe55:3215/128
      Multilink
         Local MRRU: 1500 bytes
         Peer MRRU:  1500 bytes
         Local Endpoint Discriminator: 1234567812345678
         Peer Endpoint Discriminator:  1111222233334444
         MCMP classes: Local 4, Remote 2
         Member links: 2 active, 6 inactive (min-active 2)
           - Serial0/3/1/3/1  ACTIVE
           - Serial0/3/1/3/2  ACTIVE
           - Serial0/3/1/3/3  INACTIVE : LCP not negotiated
           - Serial0/3/1/3/4  INACTIVE : Mismatching peer endpoint
           - Serial0/3/1/3/5  INACTIVE : Mismatching peer auth name
           - Serial0/3/1/3/6  INACTIVE : MRRU option rejected by Peer
           - Serial0/3/1/3/7  INACTIVE : Mismatching local MCMP classes
           - Serial0/3/1/3/8  INACTIVE : MCMP option rejected by peer
```

This example shows how to display PPP state information for a serial interface:

```
RP/0/0/CPU0:router# show ppp interface Serial 0/3/1/3/1

    Serial0/3/1/3/1 is down, line protocol is down
      LCP: Open
         SSO-State: Standby-Up
         Keepalives enabled (10 sec)
         Local MRU: 1500 bytes
         Peer MRU:  1500 bytes
         Local Bundle MRRU: 1500 bytes
         Peer Bundle MRRU:  1500 bytes
         Local Endpoint Discriminator: 1234567812345678
         Peer Endpoint Discriminator:  1111222233334444
         Local MCMP Classes:  Not negotiated
         Remote MCMP Classes: Not negotiated
      Authentication
         Of Us:    CHAP (Completed as 'test-user')
         Of Peer:  PAP (Completed as 'peer-user')
      Multilink
         Multilink group id: 100
         Member status: ACTIVE
```

Table 41: show ppp interfaces Field Descriptions

Field	Description
Ack-Rcvd	Configuration acknowledgemt was received; waiting for peer to send configuration request.
Ack-Sent	Configuration acknowledgemt was sent; waiting for peer to respond to configuration request.

Field	Description
Authentication	Type of user authentication configured on the local equipment and on the peer equipment. Possible PPP authentication protocols are Challenge Handshake Authentication Protocol (CHAP), MS-CHAP, and Password Authentication Protocol (PAP).
Closed	Lower layer is up, but this layer is not required.
Closing	Shutting down due to local change.
Initial	Connection is idle.
IPCP	IP Control Protocol (IPCP) state. The seven possible states that may be displayed are as follows: • Initial—Lower layer is unavailable (Down), and no Open has occurred. The Restart timer is not running in the Initial state. • Starting—An administrative Open has been initiated, but the lower layer is still unavailable (Down). The Restart timer is not running in the Starting state. When the lower layer becomes available (Up), a Configure-Request is sent. • Closed— IPCP is not currently trying to negotiate. • Stopped—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. • Closing—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. Upon reception of a Terminate-Ack, the Closed state is entered. Upon the expiration of the Restart timer, a new Terminate-Request is transmitted, and the Restart timer is restarted. After the Restart timer has expired Max-Terminate times, the Closed state is entered. • Stopping—A Terminate-Request has been sent and the Restart timer is running, but a IPCP-Ack has not yet been received. Req-Sent. • ACKsent—IPCP has received a request and has replied to it. • ACKrcvd—IPCP has received a reply to a request it sent. • Open—IPCP is functioning properly.

Field	Description
Keepalive	Keepalive setting and interval in seconds for echo request packets.
LCP	Indicates the current state of LCP. The state of the LCP will report the following states: • Initial—Lower layer is unavailable (Down), and no Open has occurred. The Restart timer is not running in the Initial state. • Starting—An administrative Open has been initiated, but the lower layer is still unavailable (Down). The Restart timer is not running in the Starting state. When the lower layer becomes available (Up), a Configure-Request is sent. • Closed— LCP is not currently trying to negotiate. • Stopped—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. • Closing—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. Upon reception of a Terminate-Ack, the Closed state is entered. Upon the expiration of the Restart timer, a new Terminate-Request is transmitted, and the Restart timer is restarted. After the Restart timer has expired Max-Terminate times, the Closed state is entered. • Stopping—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. Req-Sent. • ACKsent—LCP has received a request and has replied to it. • ACKrcvd—LCP has received a reply to a request it sent. • Open—LCP is functioning properly
Local IPv4 address	IPv4 address for the local interface.
Local MRU	Maximum receive unit. The maximum size of the information transported, in bytes, in the PPP packet received by the local equipment.

Field	Description
Open	Connection open.
OSICP	Open System Interconnection Control Protocol (OSICP) state. The possible states that may be displayed are as follows: • Initial—Lower layer is unavailable (Down), and no Open has occurred. The Restart timer is not running in the Initial state. • Starting—An administrative Open has been initiated, but the lower layer is still unavailable (Down). The Restart timer is not running in the Starting state. When the lower layer becomes available (Up), a Configure-Request is sent. • Closed— OSICP is not currently trying to negotiate. • Stopped—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. • Closing—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. Upon reception of a Terminate-Ack, the Closed state is entered. Upon the expiration of the Restart timer, a new Terminate-Request is transmitted, and the Restart timer is restarted. After the Restart timer has expired Max-Terminate times, the Closed state is entered. • Stopping—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. Req-Sent. • ACKsent—OSICP has received a request and has replied to it. • ACKrcvd—OSICP has received a reply to a request it sent. • Open—OSICP is functioning properly.
Peer IPv4 address	IPv4 address for the peer equipment.
Peer MRU	Maximum receive unit. The maximum size of the information transported, in bytes, in the PPP packet received by the peer equipment.

Field	Description
Req-Sent	Configuration request was sent; waiting for peer to respond.
Starting	This layer is required, but lower layer is down.
Stopped	Listening for a configuration request.
Stopping	Shutting down as a result of interactions with peer.

Serial Interface Commands on the Cisco IOS XR Software

This module provides CLI commands for configuring serial interfaces on the Cisco XR 12000 Series Router.

clear iphc ipv4

To clear all Real Time Protocol (RTP) and Transport Control Protocol (TCP) statistics for IP header compression (IPHC) packets sent and received on an interface, use the **clear iphc ipv4** command in EXEC mode.

clear iphc ipv4 {**interface** {**serial| multilink**} *interface-path-id*| **location** *node-id*}

Syntax Description

interface	Specifies the interface to be configured, by type and the *interface-path-id* argument.
serial	Specifies a serial network interface.
multilink	Specifies a multilink network interface.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location	Specifies the interface to be configured by its *node-id*.
node-id	Fully qualified path of the node in the *rack/slot/module notation*.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

Note The **clear counters** command also clears the IPHC statistics for all the interfaces.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to clear RTP and TCP statistics on an interface:

```
RP/0/0/CPU0:router# clear iphc ipv4 interface Serial 0/1/0/1/26:0
Thu Jan  8 20:30:38.155 UTC
```

The following example shows how to clear RTP and TCP statistics on a node:

```
RP/0/0/CPU0:router# clear iphc ipv4 location 0/3/CPU0
Mon Oct 12 22:47:51.430 DST
```

crc (serial)

To set the length of the cyclic redundancy check (CRC) on a serial interface, use the **crc** command in serial configuration mode. To return the CRC setting on a serial interface to the default setting, use the **no** form of this command.

crc {**16**| **32**}

no crc {**16**| **32**}

Syntax Description

16	Sets 16-bit CRC mode.
32	Sets 32-bit CRC mode.

Command Default

The default is 16 bits for serial interfaces.

Command Modes

Serial configuration

Command History

Release 3.3.0	This command was introduced.

Usage Guidelines

CRC is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data. The designators 16 and 32 indicate the length (in bits) of the frame check sequence (FCS). A CRC of 32 bits provides more powerful error detection, but adds overhead. Both the sender and receiver must use the same setting.

CRC-16, the most widely used error checking method throughout the United States and Europe, is used extensively with WANs. CRC-32 is specified by IEEE standard 802 and as an option by some point-to-point transmission standards. It is often used on Switched Multimegabit Data Service (SMDS) networks and LANs.

Task ID

Task ID	Operations
hdlc	read, write

Examples

In the following example, the 32-bit CRC on serial interface 0/3/0/0/0:10 is enabled:

```
RP/0/0/CPU0:router(config)# interface serial 0/3/0/0/0:10
RP/0/0/CPU0:router(config-if)# serial
RP/0/0/CPU0:router(config-if-serial)# crc 32
```

Related Commands

Command	Description
show interfaces, on page 423	Displays statistics for all interfaces configured on the router or for a specific node.

description (IPHC profile)

To add a description to an IPHC profile, use the **description** command in IPHC profile configuration mode. To remove a description for an IPHC profile, use the **no** form of this command.

description *description*

no description

Syntax Description

description	Description to be added to the IPHC profile.

Command Default

By default, no description is attached to an IPHC profile.

Command Modes

IPHC profile configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ip-services	read, write

Examples

In the following example, a description is attached to the IPHC profile test:

```
RP/0/0/CPU0:router(config)# config
RP/0/0/CPU0:router(config)# iphc profile test type iphc
RP/0/0/CPU0:router(config-iphc-profile)# description testprofile
RP/0/0/CPU0:router(config-iphc-profile)# commit
```

encapsulation (serial)

To set the Layer 2 encapsulation of an interface, use the **encapsulation** command in interface configuration mode. To restore the system to the default encapsulation, use the **no** form of this command.

encapsulation {**hdlc**| **ppp**| **frame-relay**| **mfr**}

no encapsulation

Syntax Description

hdlc	Enables Cisco High-Level Data Link Control (HDLC) encapsulation on the interface. This is the default encapsulation type.
ppp	Enables PPP encapsulation on the interface.
frame -relay	Enables Frame Relay encapsulation on the interface.
mfr	Enables multilink Frame Relay encapsulation on the interface.

Command Default

For serial interfaces, the default encapsulation is HDLC.

Command Modes

Interface configuration

Command History

Release 3.2	This command was first supported.
Release 3.4.0	Frame Relay encapsulation was supported on serial interfaces.
Release 3.6.0	Multilink Frame Relay encapsulation was supported on serial interfaces.

Usage Guidelines

Task ID

Task ID	Operations
hdlc	read, write
interface	read, write

Examples

The following example shows how to enable PPP encapsulation on serial interface 0/3/0/1:

```
RP/0/0/CPU0:router(config)# interface serial 0/3/0/1
```

```
RP/0/0/CPU0:router(config-if)# encapsulation ppp
```

Related Commands

Command	Description
show interfaces, on page 423	Displays statistics for all interfaces configured on the router or for a specific node.
show ppp interfaces , on page 578	Displays PPP state information for an interface.

feedback disable

To disable the IP header compression (IPHC) context status feedback messages on an interface, use the **feedback disable** command in IPHC profile configuration mode. To re-enable feedback messages after they are disabled, use the **no** form of this command.

feedback disable

no feedback disable

Syntax Description

This command has no keywords or arguments.

Command Default

Feedback messages are enabled by default.

Command Modes

IPHC profile configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

Note Feedback disable can be configured only within an IPHC profile.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to disable the IP header compression (IPHC) context status feedback messages within an IPHC profile:

```
RP/0/0/CPU0:router(config)# config
RP/0/0/CPU0:router(config)# iphc profile Profile_1 type iphc
RP/0/0/CPU0:router(config-iphc-profile)# feedback disable
```

fragment end-to-end

To enable fragmentation of Frame Relay frames on an interface and enter Frame Relay virtual circuit fragment configuration mode, use the **fragment end-to-end** command in serial Frame Relay PVC configuration mode. To disable Frame Relay fragmentation, use the **no** form of this command.

fragment end-to-end *fragment-size* **[fragment-counter]**

no fragment end-to-end

Syntax Description

fragment-size	Number of payload bytes from the original Frame Relay frame that go into each fragment. This number excludes the Frame Relay header of the original frame. All the fragments of a Frame Relay frame, except the last, have a payload size equal to fragment-size; the last fragment has a payload less than or equal to fragment-size. Valid values are from 64 to 512 bytes, depending on your hardware.
fragment-counter	(Optional) Enables fragmentation counters.

Command Default

Command Modes

Command History

Release 3.5.0	This command was introduced.
Release 4.0.0	• The supported fragment size range was changed to 64 to 512 bytes. • The **fragment-counter** keyword was added.

Usage Guidelines

The Cisco 8-Port Channelized T1/E1 SPA supports fragment sizes of 128, 256, and 512 bytes.

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows how to enter serial Frame Relay virtual circuit configuration mode, set the fragmentation size of Frame Relay frames on subinterface 0/6/2/4.1 to 512 bytes and enable fragmentation counters:

```
RP/0/0/CPU0:router(config)# interface serial 0/6/2/4.1 point-to-point
```

```
RP/0/0/CPU0:router(config-subif)# pvc 100
RP/0/0/CPU0:router(config-fr-vc)# fragment end-to-end 512 fragment-counter
```

Related Commands

Command	Description
interface serial, on page 599	Configures a serial interface and enters interface or subinterface configuration mode.
pvc (serial), on page 615	Creates a Frame Relay PVC under a serial subinterface and enters Frame Relay virtual circuit configuration mode.
fragment-counter, on page 597	Enables fragmentation counters for a Frame Relay subinterface and PVC.

fragment-counter

To enable fragmentation counters for a Frame Relay subinterface and PVC, use the **fragment-counter** command in Frame Relay virtual circuit fragment configuration mode. To disable collection of fragmentation counters, use the **no** form of this command.

fragment-counter

no fragment-counter

Syntax Description

This command has no keywords or arguments.

Command Default

Fragmentation counters are disabled.

Command Modes

Frame Relay virtual circuit fragment configuration

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows how to enter serial Frame Relay PVC configuration mode, set the fragmentation size of Frame Relay frames on subinterface 0/6/2/4.1 to 512 bytes and enable the fragmentation counter:

```
RP/0/0/CPU0:router(config)# interface serial 0/6/2/4.1 l2transport
RP/0/0/CPU0:router(config-subif)# pvc 100
RP/0/0/CPU0:router(config-fr-vc)# fragment end-to-end 512
RP/0/0/CPU0:router(config-fr-vc-frag)# fragment-counter
```

Related Commands

Command	Description
interface serial, on page 599	Configures a serial interface and enters interface or subinterface configuration mode.
pvc (serial), on page 615	Creates a Frame Relay PVC under a serial subinterface and enters Frame Relay virtual circuit configuration mode.

Command	Description
fragment end-to-end, on page 595	
show frame-relay pvc, on page 391	Displays statistics about Frame Relay PVCs.

interface serial

To configure a serial interface and enter interface or subinterface configuration mode, use the **interface serial** command in global configuration mode. To delete a serial configuration, use the **no** form of this command.

interface serial *interface-path-id* [. *subinterface*] {**point-to-point| l2transport**}

no interface serial *interface-path-id* [. *subinterface*] {**point-to-point| l2transport**}

Syntax Description

interface-path-id[.*subinterface*]	Physical interface or virtual interface followed by the optional subinterface path ID. Naming notation is *interface-path-id.subinterface*. The period in front of the subinterface value is required as part of the notation. For more information about the syntax for the router, use the question mark (?) online help function.
point-to-point	Interface functions as one endpoint of a point-to-point link.
l2transport	Interface functions as one endpoint on an Layer 2 link.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release 3.3.0	This command was introduced.
Release 3.5.0	The **l2transport** keyword was added to support Layer 2 configuration on serial interfaces.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

Note A slash between values is required as part of the notation.

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*—Chassis number of the rack.
  - *slot*—Physical slot number of the line card.
  - *module*—Module number. A physical layer interface module (PLIM) is always 0.

- *port*—Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.
- The naming notation for T1 interfaces on a channelized SPA is *rack*/*slot*/*module*/*port*/*channel-num*:*channel-group-number*, as shown in the following example:

```
interface serial 0/0/1/2/4:3
```

- If a subinterface is configured under the serial interface, then the router includes the subinterface number at the end of the serial interface address. In this case, the naming notation is *rack*/*slot*/*module*/*port*[/*channel-num*:*channel-group-number*].*subinterface*, as shown in the following example:

```
interface serial 0/0/1/2.1
```

- The naming notation syntax for serial interfaces is as follows:
  - *rack*—Chassis number of the rack.
  - *slot*—Physical slot number of the modular services card or line card.
  - *module*—Module number. Shared port adapters (SPAs) are referenced by their subslot number.
  - *port*—Physical port number of the controller.
  - *channel-num*:—T1 channel number. T1 channels range from 0 to 23.
  - *channel-group-number*:—Time slot number. T1 time slots range from 1 to 24. The *channel-group-number* is preceded by a colon and not a slash.
  - *subinterface*—Subinterface number.

- Use the question mark (?) online help function following the **serial** keyword to view a list of all valid interface choices.

Serial interfaces on channelized T3 can be deleted using the **no channel-group** command in T1 configuration mode. If there are nondefault serial parameters defined, you need to use the **no interface serial** command first to revert to the default configuration, and then delete the serial interface using the **no channel-group** command.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter interface configuration mode for a serial interface in slot 6, subslot 2, port 4, T1 channel number 10 and channel group 8:

```
RP/0/0/CPU0:router(config)# interface serial 0/6/2/4/10:8
RP/0/0/CPU0:router(config-if)#
```

The following example shows how to create a subinterface on a serial interface in slot 6, subslot 2, port 3 and enter subinterface configuration mode:

```
RP/0/0/CPU0:router(config)# interface serial 0/6/2/3.1
RP/0/0/CPU0:router(config-if)#
```

The following example shows how to reference the serial interface on channel group 3 of T1 channel group 4 on port 2 of a SPA in subslot 1 and enter subinterface configuration mode:

```
RP/0/0/CPU0:router(config)# interface serial 0/0/1/2/4:3
RP/0/0/CPU0:router(config-if)#
```

Related Commands

Command	Description
channel-group, on page 764	Configures a DS0 channel group and enters channel group configuration mode.
show interfaces, on page 423	Displays statistics for all interfaces configured on the router or for a specific node.

invert

To invert the data stream on a serial interface, use the **invert** command in serial configuration mode. To disable data inversion, use the **no** form of this command.

invert

no invert

Syntax Description

This command has no keywords or arguments.

Command Default

Data is not inverted.

Command Modes

Serial configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

To verify that data inversion is configured on the interface, use the **show interfaces serial** command.

Task ID

Task ID	Operations
hdlc	read, write

Examples

In the following example, data inversion is enabled on serial interface 0/3/0/0/0:10:

```
RP/0/0/CPU0:router(config)# interface serial 0/3/0/0/0:10
RP/0/0/CPU0:router(config-if)# serial
RP/0/0/CPU0:router(config-if-serial)# invert
```

Related Commands

Command	Description
show interfaces, on page 423	Displays statistics for all interfaces configured on the router or for a specific node.

iphc non-tcp connections

To set the maximum number of non-TCP connections that may be configured for IP header compression (IPHC) on a line card, use the **iphc tcp connections** command in configuration mode. To remove this setting, use the **no** form of this command.

iphc non-tcp connections *max-number* **location** *node-id*

no iphc non-tcp connections *max-number* **location** *node-id*

Syntax Description

max-number	Maximum number of non-TCP connections that may be configured for IPHC. The range is 1 to 20000.
location	Location, specified by *node-id*, on which to set the maximum number of connections for IPHC.
node-id	Fully qualified path of the node in the format *rack/slot/port*.

Command Default

No default behavior or values

Command Modes

Configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to set the maximum number of non-TCP connections that may be configured for IP header compression (IPHC) on a line card:

```
RP/0/0/CPU0:router# config
RP/0/0/CPU0:router(config)# iphc non-tcp connections 20000 location 0/1/cpu0
```

iphc profile

To create an IP header compression (IPHC) profile and enter the IPHC profile configuration mode, use the **iphc profile** command in configuration mode. To remove the profile, use the **no** form of this command.

iphc profile *profile-name* **type** {**ietf**| **iphc**}

no iphc profile *profile-name* [**type** {**ietf**| **iphc**}]

Syntax Description

profile-name	Text name for the IPHC profile. The maximum number of characters is 50.
type	Specifies the type of compression format.
ietf	Specifies Internet Engineering Task Force (IETF) standard format. Uses RFC2507 and RFC2508 compression schemes.
iphc	Specifies Internet Protocol Header Compression (IPHC) format.Provides options similar to IETF.

Command Default

No default behavior or values

Command Modes

Configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

After you create a profile and enter the IPHC profile configuration mode, you can configure IPHC features in the profile and attach the profile to multiple interfaces. The maximum number of profiles allowed on a router is 250.

A profile cannot be deleted if it is attached to any interfaces. You must remove the profile from all interfaces first. Then, delete the profile using the **no** form of this command.

On-the-fly modifications to IPHC profiles are not supported.

A profile name cannot exceed 50 characters. If you attempt to create a profile name that exceeds 50 characters, you receive the following error message:

```
iphc profile test1test1test1test1test1test1test1test1test1test1test11 type iphc
!!% 'iphc_profilemgr' detected the 'warning' condition
'Name is longer than allowed character length of 50'
!
```

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to create the IPHC profile Profile_1

```
RP/0/0/CPU0:router(config)# config
RP/0/0/CPU0:router(config)# iphc profile Profile_1 type iphc
RP/0/0/CPU0:router(config-iphc-profile)#
```

iphc tcp connections

To set the maximum number of TCP connections that may be configured for IP header compression (IPHC) on a line card, use the **iphc tcp connections** command in configuration mode. To remove this setting, use the **no** form of this command.

iphc tcp connections *max-number* **location** *node-id*

no iphc tcp connections *max-number* **location** *node-id*

Syntax Description

max-number	Maximum number of TCP connections that may be configured for IPHC. The range is 1 to 2000.
location	Location of the card, specified by *node-id*.
node-id	Fully qualified path of the node in the format *rack/slot/port*.

Command Default

No default behavior or values

Command Modes

Configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to set the maximum number of TCP connections that may be configured for IP header compression (IPHC) on a line card:

```
RP/0/0/CPU0:router(config)# config
RP/0/0/CPU0:router(config)# iphc tcp connections 2000 location 0/1/cpu0
```

ipv4 iphc profile

To attach an IP header compression (IPHC) profile to an interface, use the **ipv4 iphc profile** command in interface configuration mode. To remove the profile from the interface, use the **no** form of this command.

ipv4 iphc profile *profile-name* [**mode service-policy**]

no ipv4 iphc profile [*profile-name* [**mode service-policy**]]

Syntax Description

profile-name	Text name of the configured IPHC profile to attach to this interface.
mode service-policy	(Optional) Specifies that the IPHC profile applies to a QoS service policy.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

If the profile name is not recognized the system returns the following error message:

```
!!% 'iphc_ma' detected the 'warning' condition 'Profile doesn't exist'
```

If the encapsulation on the interface is not supported, the system returns the following error message:

```
!!% 'iphc_ma' detected the 'warning' condition 'IPHC capability: Encap type not supported'
```

Task ID

Task ID	Operations
ip-services	read, write
ipv4	read, write

Examples

The following example shows how to attach an IP header compression (IPHC) profile to an interface.

```
RP/0/0/CPU0:router(config)# config
RP/0/0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/0/CPU0:router(config-if)# ipv4 iphc profile Profile_1
```

The following example shows how to attach an IPHC profile that applies to a QoS service policy to an interface:

```
RP/0/0/CPU0:router(config)# config
RP/0/0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/0/CPU0:router(config-if)# ipv4 iphc profile Profile_1 mode service-policy
```

keepalive (serial)

To set the keepalive timer for a specific serial interface, use the **keepalive** command in interface configuration mode. To reset the keepalive timer to the default of 10 seconds, use the **no** form of this command.

keepalive {*interval* [*retry*]| **disable**}

no keepalive

Syntax Description

interval	Number of seconds (from 1 to 30) between keepalive messages. The default is 10.
disable	Turns off the keepalive timer.
retry	(Optional) Number of keepalive messages (from 1 to 255) that can be sent to a peer without a response before transitioning the link to down state. The default is 5.

Command Default

The default interval is 10 seconds between keepalive messages. The default retry is 5 keepalive messages that can be sent without a response. However, when more than 5 keepalive messages are sent to a peer without a response, the link transitions to the down state.

Command Modes

Interface configuration

Command History

Release 3.2	This command introduced.

Usage Guidelines

HDLC keepalives require that the **keepalive** command is configured the same way on both ends of a single connection. The two connected routers have no way of negotiating the keepalive value because there is no way for one router to tell the other about its configured values. The keepalive value configured on each router (local or partner) sets the rate at which the Cisco IOS XR software sends packets. It also sets the rate at which the local end expects to receive incoming packets.

To set the keepalive value to the default value, use the **keepalive** command without specifying a value for the *interval* argument.

By default, if more than five keepalive messages are sent to a peer and no response is received from the peer, then the link transitions to the down state.

Task ID

Task ID	Operations
hdlc	read, write

Examples

The following example shows how to configure keepalives for 3 seconds on serial interface 0/7/0/1:

```
RP/0/0/CPU0:router(config)# interface serial 0/7/0/1
RP/0/0/CPU0:router(config-if)# keepalive 3
```

Related Commands

Command	Description
show interfaces, on page 423	Displays statistics for all interfaces configured on the router or for a specific node.

max-header

To define the maximum size header that can be compressed, use the **max-header** command in IPHC profile configuration mode. To return to the default maximum size, use the **no** form of this command.

max-header *number-of-bytes*

no max-header [*number-of-bytes*]

Syntax Description

number-of-bytes	Maximum size, in bytes, of a header that can be compressed.The range is from 20 to 40. The default is 40.

Command Default

Number-of-bytes; 40.

Command Modes

IPHC profile configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

Note The maximum header size can be configured only within an IPHC profile.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to define the maximum size header that can be compressed.

```
RP/0/0/CPU0:router(config)# config
RP/0/0/CPU0:router(config)# iphc profile Profile_1 type iphc
RP/0/0/CPU0:router(config-iphc-profile)# max-header 20
```

non-tcp compression

To enable non-TCP compression in an IP header compression (IPHC) profile, use the **non-tcp compression** command in IPHC profile configuration mode. To disable non-TCP compression in the profile, use the **no** form of this command.

non-tcp compression

no non-tcp

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

IPHC profile configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelin

Note NON-TCP compression can be enabled only within an IPHC profile. Non-TCP compression does not work unless it is enabled under a profile.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to enable NON-TCP compression within an IP header compression (IPHC) profile:

```
RP/0/0/CPU0:router(config)# config
RP/0/0/CPU0:router(config)# iphc profile Profile_1 type iphc
RP/0/0/CPU0:router(config-iphc-profile)# non-tcp compression
```

non-tcp context absolute

To configure the maximum number of non-TCP contexts that are allowed for IPHC under a profile, use the **non-tcp context absolute** command in IPHC profile configuration mode. To remove the non-TCP context from the profile, use the **no** form of this command.

non-tcp context absolute *number-of-contexts*

no non-tcp context [**absolute** [*number-of-contexts*]]

Syntax Description

number-of-contexts	Numeric value that specifies the maximum number of non-TCP contexts allowed for IPHC under this profile. The range is from 0 to 6000.

Command Default

If the number of contexts is not specified, and only non-TCP compression is enabled, the default number of contexts is 16.

Command Modes

IPHC profile configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

The maximum allowed number of non-tcp contexts on a Line Card, across all IPHC profiles and interfaces, is 6000.

Note Non-TCP context can be set only within an IPHC profile.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to enable non-TCP compression within an IP header compression (IPHC) profile:

```
RP/0/0/CPU0:router(config)# config
RP/0/0/CPU0:router(config)# iphc profile Profile_1 type iphc
```

```
RP/0/0/CPU0:router(config-iphc-profile)# non-tcp context absolute 255
```

pvc (serial)

To create a Frame Relay permanent virtual circuit (PVC) under a serial subinterface and enter Frame Relay virtual circuit configuration mode, use the **pvc** command in subinterface configuration mode. To remove a PVC from a subinterface, use the **no** form of this command.

pvc *dlci*

no pvc *dlci*

Syntax Description

dlci	DLCI number used to identify the PVC. Range is from 16 to 1007.

Command Default

No PVC is defined.

Command Modes

Subinterface configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

The **pvc** command creates a PVC and attaches it to the specified DLCI.

The Cisco IOS XR software dynamically creates rate queues as necessary to satisfy the requests of the PVC commands.

When you issue the **pvc** command in global configuration mode, the CLI prompt changes to "config-fr-vc," indicating that you have entered the Frame Relay virtual circuit configuration submode.

In the following sample output, the question mark (**?**) online help function displays all the commands available under the Frame Relay virtual circuit configuration submode for the serial subinterface:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface serial 0/3/2/0.1
RP/0/0/CPU0:router(config-subif)# pvc 20
RP/0/0/CPU0:router(config-fr-vc)# ?

  commit    Commit the configuration changes to running
  describe  Describe a command without taking real actions
  do        Run an exec command
  exit      Exit from this submode
  no        Negate a command or set its defaults
  show            Show contents of configuration
```

Task ID

Task ID	Operations
fr	read, write

Examples

The following example shows how to create a Frame Relay PVC on a serial subinterface, and enter Frame Relay virtual circuit configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface serial 0/6/0/1.1 point-to-point
RP/0/0/CPU0:router(config-if)# pvc 16
RP/0/0/CPU0:router(config-fr-vc)#
```

refresh max-period

To configure the maximum number of compressed IP header packets exchanged on a link before IPHC context is refreshed, use the **refresh max-period** command in IPHC profile configuration mode. To return to the default context refresh settings, use the **no** form of this command.

refresh max-period {*max-number*| **infinite**}

no refresh max-period [*max-number*| **infinite**]

Syntax Description

max- number	Maximum number of compressed IP header packets allowed between full headers or before the context is refreshed. Range is from 0 to 65535.
infinite	Allows an unlimited number of packets to be exchanged before context refresh.

Command Default

max-number: 256

Command Modes

IPHC profile configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

To enable the configured context refresh settings for RTP packets, the **refresh rtp** command must be used.

Note The maximum period between context refreshes can be set only within an IPHC profile.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to configure the maximum number of compressed IP header packets that are exchanged on a link before the context is refreshed, in an IPHC profile.

```
RP/0/0/CPU0:router(config)# config
RP/0/0/CPU0:router(config)# iphc profile Profile_1 type iphc
```

```
RP/0/0/CPU0:router(config-iphc-profile)# refresh max-period 50
```

refresh rtp

To enable the configured context refresh settings for RTP packets, use the **refresh rtp** command in IPHC profile configuration mode. To disable context refresh settings for RTP packets, use the **no** form of this command.

refresh rtp

no refresh rtp

Syntax Description

This command has no keywords or arguments.

Command Default

By default, refresh RTP is disabled and only the first packet in the flow is sent as a 'full-header' packet.

Command Modes

IPHC profile configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to enable the configured refresh settings for RTP packets:

```
RP/0/0/CPU0:router(config)# config
RP/0/0/CPU0:router(config)# iphc profile Profile_1 type iphc
RP/0/0/CPU0:router(config-iphc-profile)# refresh rtp
```

rtp

To enable Real Time Protocol (RTP) compression and decompression on the interface, use the **rtp** command in IPHC profile configuration mode. To remove RTP from the interface, use the **no** form of this command.

rtp

no rtp

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

IPHC profile configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

Note RTP can be enabled only within an IPHC profile.

```
You must enable RTP before attaching a profile to an interface. If you do not enable RTP
first, the router will display the following message: '!!% 'iphc_capability' detected the
'warning' condition 'IPHC Capability: RTP Compression NOT enabled in the profile'!
```

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to

```
RP/0/0/CPU0:router(config)# config
RP/0/0/CPU0:router(config)# iphc profile Profile_1 type iphc
RP/0/0/CPU0:router(config-iphc-profile)# rtp
```

scramble

To enable payload scrambling (encryption) on a serial interface, use the **scramble** command in interface configuration mode. To disable scrambling, use the **no** form of this command.

scramble

no scramble

Syntax Description

This command has no keywords or arguments.

Command Default

Scrambling is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

Scrambling is used to assist clock recovery on the receiving end. Scrambling is designed to randomize the pattern of 1s and 0s carried in the physical layer frame. Randomizing the digital bits can prevent continuous, nonvariable bit patterns—in other words, long strings of all 1s or all 0s. Several physical layer protocols rely on transitions between 1s and 0s to maintain clocking.

Scrambling can prevent some bit patterns from being mistakenly interpreted as alarms by switches placed between the Data Service Units (DSUs).

The local interface configuration must match the remote interface configuration. For example, if you enable scrambling on the local port, you must also do the same on the remote port.

To verify that scrambling is configured on the interface, use the **show interfaces serial** command.

Task ID

Task ID	Operations
hdlc	read, write

Task ID

Examples

In the following example, scrambling is enabled on serial interface 0/3/0/0/0:10:

```
RP/0/0/CPU0:router(config)# interface serial 0/3/0/0/0:10
RP/0/0/CPU0:router(config-if)# serial
```

```
RP/0/0/CPU0:router(config-if-serial)# scramble
```

Related Commands

Command	Description
show controllers t3, on page 837	Displays information about the T3 links and hardware and software drivers for the T3 controller.

serial

To configure the serial parameters and enter serial configuration mode, use the **serial** command in interface configuration mode. To return to the default state of the serial interface, use the **no** form of this command.

serial

no serial

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

Serial interfaces are automatically created for unchannelized ports; for channelized ports, serial interfaces are created when you add T1/E1 channel groups.

Task ID

Task ID	Operations
hdlc	read, write

Examples

The following example shows how to enter serial configuration mode:

```
RP/0/0/CPU0:router(config-if)# serial
RP/0/0/CPU0:router(config-if-serial)#
```

show iphc idb

To display status information for an IP header compression (IPHC) interface description block (IDB), use the **show iphc idb** command in EXEC mode.

show iphc idb {**detail**| **interface** *type interface-path-id* **[detail]**| **location** *node-id* **[detail]**}

Syntax Description

detail	Includes statistics information and internal data.
interface	Specifies the interface for which IPHC information is to be displayed.
type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location	Specifies the node location for which IPHC information is to be displayed.
node-id	Specifies the fully qualified path of a node. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

The default (no parameters) displays information for all interfaces configured for IPHC.

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ip-services	read

Examples

The following examples show how to display status information for an IP header compression (IPHC) interface description block (IDB).

```
RP/0/0/CPU0:router# show iphc idb interface Serial 0/1/0/1/26:0

Thu Jan  8 20:25:41.079 UTC
EA Status Codes:                  Neg Status Code:
  CFG_AS: Cfg Apply Succeed         NEG_I: Negotiation Init
  CFG_AF: Cfg Apply Failed          NEG_P: Negotiation Progress
  NEG_AS: Neg Apply Succeed         NEG_D: Negotiation Done
  NEG_AF: Neg Apply Failed          NEG_F: Negotiation Failed

Interface_Name:   Serial0/1/0/1/26:0   Ifhandle  : 0x02008e00
EA Status     : NEG_AS                 Neg Status: NEG_D
MQC Mode      : F                      Prof_Name : iphcfmt


RP/0/0/CPU0:router# show iphc idb interface Serial 0/1/0/1/26:0  detail

Thu Jan  8 20:25:44.731 UTC
EA Status Codes:                  Neg Status Code:
  CFG_AS: Cfg Apply Succeed         NEG_I: Negotiation Init
  CFG_AF: Cfg Apply Failed          NEG_P: Negotiation Progress
  NEG_AS: Neg Apply Succeed         NEG_D: Negotiation Done
  NEG_AF: Neg Apply Failed          NEG_F: Negotiation Failed

Interface_Name: Serial0/1/0/1/26:0   Ifhandle  : 0x02008e00
EA Status     : NEG_AS               Neg Status: NEG_D
MQC Mode      : F                    Prof_Name : iphcfmt

              Tcp    Non-Tcp       Max         Max         Max   RTP
            Space      Space    Header      Period        Time
-------------------------------------------------------------------------
 Cfg_Option     1         60        40         256           5     T
 Neg_Option     1         50        40         256           5     T
```

show iphc ipv4 rtp

To display IPv4 statistics for Real Time Protocol (RTP) and User Datatgram Protocol (UDP) packets sent and received on an interface, use the **show iphc ipv4 rtp** command in EXEC mode.

show iphc ipv4 rtp interface *type interface-path-id* [**location** *node-id*]

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location	(Optional) Specifies the location of the interface
node-id	(Optional) Node-id entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release 3.9.0	This command was introduced.

Usage Guidelin

Caution These Cisco support commands are normally reserved for use by Cisco Technical Support personnel only. If used incorrectly. there is some risk that they may cause performance or other issues that impact products, and we highly recommend that you contact Cisco Technical Support before using any of these commands.

Task ID

Task ID	Operations
ip-services	read
cisco-support	read

Examples

The following example shows how to display IPv4, Real Time Protocol (RTP), User Datatgram Protocol (UDP), and Non-Transmission Control Protocol (non-TCP) statistics about IP header compression (IPHC) packets sent and received on an interface:

```
RP/0/0/CPU0:router# show iphc ipv4 rtp interface Serial 0/1/0/1/26:0

Thu Jan  8 20:28:47.569 UTC
RTP/UDP/IP header compression statistics:
  Interface Serial0/1/0/1/26:0
    Rcvd:    100 total, 93 compressed, 7 full header
             0 dropped, 0 status msgs
    Sent:    0 total, 0 compressed, 0 fullheader, 0 status msgs
             0 bytes saved, 0 bytes sent
             1.00 efficiency improvement factor
```

show iphc ipv4 tcp

To display IPv4 Transport Control Protocol (TCP) statistics about IP header compression (IPHC) packets sent and received on an interface, use the **show iphc ipv4 tcp** command in EXEC mode.

show iphc ipv4 tcp interface *type interface-path-id [* **location** *node-id]*

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location	(Optional) Specifies the location of the interface
node-id	(Optional) Node-id entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release 3.9.0	This command was introduced.

Usage Guidelin

Caution These Cisco support commands are normally reserved for use by Cisco Technical Support personnel only. If used incorrectly. there is some risk that they may cause performance or other issues that impact products, and we highly recommend that you contact Cisco Technical Support before using any of these commands.

Task ID

Task ID	Operations
ip-services	read
cisco-support	read

Examples

The following example shows how to display IPv4, Transport Control Protocol (TCP) statistics about IP header compression (IPHC) packets sent and received on an interface:

```
RP/0/0/CPU0:router# show iphc ipv4 tcp interface Serial 0/1/0/1/26:0

Thu Jan  8 20:28:54.407 UTC
TCP/IP header compression statistics:
  Interface Serial0/1/0/1/26:0
    Rcvd:    100 total, 93 compressed, 7 full header
             0 dropped, 0 status msgs
    Sent:    0 status msgs
```

show iphc platform trace

show iphc platform trace [**error**| **internal [error]**] **[flow]** [**unique**| **wrapping**] **[hexdump]** [**last** *number-of-entries*] **[reverse] [stats] [tailf] [verbose]** [**file** *file-name* **original location** *node-id*| **location** {*node-id*| **all**| **mgmt-nodes**}]

Syntax Description

events	(Optional) Displays event platform trace information.
error	(Optional) Displays errors found in the trace.
internal	(Optional) Displays internal trace information.
flow	(Optional) Displays trace information for the flow.
unique	(Optional) Displays trace information for unique entries with counts.
wrapping	Optional) Displays wrapping entries.
hexdump	(Optional) Displays trace information in hexadecimal format.
last *number_of_entries*	(Optional) Displays trace information for the last specified number of entries. The range is 1 to 4294967295.
reverse	(Optional) Displays trace information in reverse order (latest traces first).
stats	(Optional) Displays statistics information for the trace.
tailf	(Optional) Displays new traces as they are added.
verbose	(Optional) Displays internal debugging information.
file *file_name*	(Optional) Displays trace information for the specified file.
original	(Optional) Specifies the original location of file.
location *node_id*	(Optional) Displays trace information for the specified card location.
all	(Optional) Displays trace information for all nodes.
mgmt-nodes	(Optional) Displays trace information for all management nodes.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

The keywords **hexdump**, **last**, **reverse**, **stats**, **tailf**, and **verbose** may be entered in any order.

Use of the keywords **file** and **location** allows any number of desired files or locations to be entered. For more information, use the question mark (**?**) online help function.

Caution These Cisco support commands are normally reserved for use by Cisco Technical Support personnel only. If used incorrectly. there is some risk that they may cause performance or other issues that impact products, and we highly recommend that you contact Cisco Technical Support before using any of these commands.

Task ID

Task ID	Operations
ip-services	read
cisco-support	read

Examples

The following example shows how to display platform trace information for a specified location:

```
RP/0/0/CPU0:router# show iphc platform trace location 0/3/CPU0

Thu Aug 13 14:41:13.983 UTC
5 wrapping entries (8192 possible, 0 filtered, 5 total)
Aug  6 12:27:16.840 iphc_ea/internal 0/3/CPU0 t1  Platform IPHC - Calling LC Platform init
Aug  6 12:27:17.183 iphc_ea/internal 0/3/CPU0 t1  Registering with hfa
Aug  6 12:27:19.481 iphc_ea/internal 0/3/CPU0 t1  Registering with uIDB Manager
Aug  6 12:27:19.841 iphc_ea/internal 0/3/CPU0 t1  Registering with fm
Aug  6 12:27:21.733 iphc_ea/internal 0/3/CPU0 t1  fsram_virtual_addr = 0x46000000
```

show iphc profile

To display the configuration information of an IP header compression (IPHC) profile, use the **show iphc profile** command in EXEC mode.

show iphc profile {*profile-name*| **all**} **[detail]**

Syntax Description

profile-name	Text name of the IPHC profile for which to display information.
all	Displays information for all profiles on the router.
detail	(Optional) Displays the interfaces to which the profile is attached.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
ip-services	read

Examples

The following examples show how to display information about an IPHC profile:

```
RP/0/0/CPU0:router# show iphc profile ietf-test1
Tue Aug 10 06:53:19.711 PDT
IPHC Profile: ietf-test1
Type: IETF
 Compressing : TCP  NON-TCP (RTP)
 Context     : TCP fixed at 1 NON-TCP fixed at 10
 Refresh     : NON-TCP every 60 seconds or 100 packets
 Feedback    : ON
 Max_Header  : 40
 Refresh RTP : OFF


RP/0/0/CPU0:router# show iphc profile Profile_1 detail
Thu Jan  8 20:22:24.276 UTC
```

```
IPHC Profile: Profile_1
Type: IPHC
 Compressing : TCP  NON-TCP (RTP)
 Context     : TCP fixed at 1 NON-TCP fixed at 60
 Refresh     : NON-TCP every 5 seconds or 256 packets
 Feedback    : ON
 Max_Header  : 40

*** No of Intf 1 ****
 Serial0_4_3_1_1:0


RP/0/0/CPU0:router# show iphc profile all
Thu Mar 12 11:05:35.987 UTC
IPHC Profiles : 3
IPHC Profile: p1
Type: IETF
 Compressing : TCP  NON-TCP (RTP)
 Context     : TCP fixed at 1 NON-TCP fixed at 16
 Refresh     : NON-TCP every 5 seconds or 256 packets
 Feedback    : ON
 Max_Header  : 40

IPHC Profile: p2
Type: IETF
 Compressing : TCP  NON-TCP (RTP)
 Context     : TCP fixed at 1 NON-TCP fixed at 16
 Refresh     : NON-TCP every 5 seconds or 256 packets
 Feedback    : ON
 Max_Header  : 40

IPHC Profile: test
Type: IETF
 Compressing : TCP  NON-TCP (RTP)
 Context     : TCP fixed at 1 NON-TCP fixed at 16
 Refresh     : NON-TCP every 5 seconds or 256 packets
 Feedback    : ON
 Max_Header  : 40


RP/0/0/CPU0:router# show iphc profile all detail
Thu Mar 12 11:06:26.902 UTC
IPHC Profiles : 3
IPHC Profile: p1
Type: IETF
 Compressing : TCP  NON-TCP (RTP)
 Context     : TCP fixed at 1 NON-TCP fixed at 16
 Refresh     : NON-TCP every 5 seconds or 256 packets
 Feedback    : ON
 Max_Header  : 40

 *** No of Intf 1 ****
 Serial0_4_3_1_1:0

IPHC Profile: p2
Type: IETF
 Compressing : TCP  NON-TCP (RTP)
 Context     : TCP fixed at 1 NON-TCP fixed at 16
 Refresh     : NON-TCP every 5 seconds or 256 packets
 Feedback    : ON
 Max_Header  : 40

 *** No of Intf 2 ****
 Serial0_4_3_1_2:0
 Serial0_4_3_1_8:0

IPHC Profile: test
Type: IETF
 Compressing : TCP  NON-TCP (RTP)
 Context     : TCP fixed at 1 NON-TCP fixed at 16
 Refresh     : NON-TCP every 5 seconds or 256 packets
 Feedback    : ON
 Max_Header  : 40
```

```
*** No of Intf 0 ****
```

show iphc trace all

To display trace results for all IP header compression (IPHC) configurations on the router, use the **show iphc trace all** command in EXEC mode.

show iphc trace all [**unique**| **wrapping**] **[hexdump]** [**last** *number-of-entries*] **[reverse] [stats] [tailf] [verbose]** [**file** *file-name* **original location** *node-id*| **location** {*node-id*| **all**| **mgmt-nodes**}]

Syntax Description

unique	(Optional) Displays trace information for unique entries with counts.
wrapping	Optional) Displays wrapping entries.
hexdump	(Optional) Displays trace information in hexadecimal format.
last *number_of_entries*	(Optional) Displays trace information for the last specified number of entries. The range is from 1 to 4294967295.
reverse	(Optional) Displays trace information in reverse order (latest traces first).
stats	(Optional) Displays statistics information for the trace.
tailf	(Optional) Displays new traces as they are added.
verbose	(Optional) Displays internal debugging information.
file *file_name*	(Optional) Displays trace information for the specified file.
original	(Optional) Specifies the original location of file.
location *node_id*	(Optional) Displays trace information for the specified card location.
all	(Optional) Displays trace information for all nodes.
mgmt-nodes	(Optional) Displays trace information for all management nodes.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release 3.9.0	This command was introduced.

Usage Guidelines

The keywords **hexdump**, **last**, **reverse**, **stats**, **tailf**, and **verbose** may be entered in any order. The keywords **unique** or **wrapping** may only be entered as the first keyword in the command. The keywords **file** or **location** may only be entered as the last keyword in the command.

Use of the keywords **file** and **location** allows any number of desired files or locations to be entered. For more information, use the question mark (**?**) online help function.

Caution These Cisco support commands are normally reserved for use by Cisco Technical Support personnel only. If used incorrectly. there is some risk that they may cause performance or other issues that impact products, and we highly recommend that you contact Cisco Technical Support before using any of these commands.

Task ID

Task ID	Operations
ip-services	read
cisco-support	read

Examples

The following example shows how to display IPHC trace information:

```
RP/0/0/CPU0:router# show iphc trace all

Wed Jul 22 21:48:07.339 DST
20 wrapping entries (3072 possible, 0 filtered, 20 total)
Jul 22 03:31:39.770 iphc/profilemgr/int 0/5/CPU0 t1  : Event Mgr Create Successl
Jul 22 03:31:39.799 iphc/profilemgr/int 0/5/CPU0 t1  : Sysmgr Init Successful
Jul 22 03:31:39.894 iphc/profilemgr/int 0/5/CPU0 t1  : Ens Init Successful
Jul 22 03:31:39.910 iphc/profilemgr/int 0/5/CPU0 t1  : Sysdb Init Successful
Jul 22 03:31:39.911 iphc/profilemgr/int 0/5/CPU0 t1  : Stats thread Init Succesl
Jul 22 03:31:39.942 iphc/profilemgr/int 0/5/CPU0 t1  : Cfg thread Init Successfl
Jul 22 03:31:39.951 iphc/profilemgr/int 0/5/CPU0 t1  : Registered verifier call7
Jul 22 03:31:39.952 iphc/profilemgr/eve 0/5/CPU0 t1  : Scanning Profile: *** Pr*
Jul 22 03:31:39.952 iphc/profilemgr/eve 0/5/CPU0 t1  : Scanning Option (format))
Jul 22 03:31:39.952 iphc/profilemgr/eve 0/5/CPU0 t1  : Scanning Option (tcp_com)
Jul 22 03:31:39.952 iphc/profilemgr/eve 0/5/CPU0 t1  : Scanning Option (tcp_con)
Jul 22 03:31:39.952 iphc/profilemgr/eve 0/5/CPU0 t1  : Scanning Option (non_tcp)
Jul 22 03:31:39.952 iphc/profilemgr/eve 0/5/CPU0 t1  : Scanning Option (rtp) in)
Jul 22 03:31:39.952 iphc/profilemgr/eve 0/5/CPU0 t1  : Scanning Option (max-per)
Jul 22 03:31:39.952 iphc/profilemgr/eve 0/5/CPU0 t1  : Scanning Option (non_tcp)
Jul 22 03:31:39.952 iphc/profilemgr/eve 0/5/CPU0 t1  : +++++ Profile Verificati+
Jul 22 03:31:39.952 iphc/profilemgr/eve 0/5/CPU0 t1  : Verify Profile (Profile_n
Jul 22 03:31:39.959 iphc/profilemgr/eve 0/5/CPU0 t1  : +++++ Profile Verificati+
Jul 22 03:31:39.981 iphc/profilemgr/int 0/5/CPU0 t1  : Registered applier calle7
Jul 22 03:31:39.999 iphc/profilemgr/eve 0/5/CPU0 t1  : Registered Profile (Profy
```

show tech-support iphc

show tech-support iphc [**file**| **interface** *type interface-path-id* [**location** *node-id*| **rack** *rack_name*]| **location** *node-id*| **rack** *rack_name*] **file location** *file_name* **[background]** [**compressed**| **uncompressed**]

Syntax Description

background	(Optional) Runs this command in the background.
compressed	(Optional) Compresses the output.
uncompressed	(Optional) Does not compress the output.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
basic-services	read
cisco-support	read
ipv4	read

Examples

The following example shows how to collect and display IP header compression (IPHC) data:

```
RP/0/0/CPU0:router# show tech-support iphc

Mon Oct 12 20:30:58.660 DST
++ Show tech start time: 2009-Oct-12.203059.DST ++
Mon Oct 12 20:31:05 DST 2009 Waiting for gathering to complete
......
Mon Oct 12 20:31:46 DST 2009 Compressing show tech output
Show tech output available at 0/5/CPU0 : disk0:/showtech/showtech-iphc-2009-Octz
++ Show tech end time: 2009-Oct-12.203148.DST ++
```

tcp compression

To enable TCP compression in an IP header compression (IPHC) profile, use the **tcp compression** command in IPHC profile configuration mode. To disable TCP compression in the profile, use the **no** form of this command.

tcp compression

no tcp

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

IPHC profile configuration

Command History

Release 3.9.0	This command was introduced.

Usage Guidelines

Where the IPHC profile used by a router is configured using this command, the router will negotiate TCP compression with its peer router and decompress any compressed TCP packets sent by its peer. TCP packets transmitted to the peer are transmitted uncompressed.

Note TCP compression can be enabled only within an IPHC profile. TCP compression does not work unless it is enabled under a profile.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to enable TCP compression within an IP header compression (IPHC) profile:

```
RP/0/0/CPU0:router(config)# config
RP/0/0/CPU0:router(config)# iphc profile Profile_1 type iphc
RP/0/0/CPU0:router(config-iphc-profile)# tcp compression
RP/0/0/CPU0:router(config-iphc-profile)#
```

tcp context absolute

To configure the maximum number of TCP contexts that are allowed for IPHC under a profile, use the **tcp context absolute** command in IPHC profile configuration mode. To remove the TCP context from the profile, use the **no** form of this command.

tcp context absolute *number-of-contexts*

no tcp context [absolute] [*number-of-contexts*]

Syntax Description

number-of-contexts	Numeric value that specifies the maximum number of TCP contexts allowed for IPHC under this profile. The range is from 0 to 255.

Command Default

If *number-of-contexts* is not specified, and only TCP compression is enabled, the default *number-of-contexts* is 1.

Command Modes

IPHC profile configuration

Command History

Release 3.9.0	This command was introduced.

Usage Guidelines

The maximum allowed number of tcp contexts on a Line Card, across all IPHC profiles and interfaces, is 255.

Note TCP context can be set only within an IPHC profile.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to enable TCP compression within an IP header compression (IPHC) profile:

```
RP/0/0/CPU0:router(config)# config
RP/0/0/CPU0:router(config)# iphc profile Profile_1 type iphc
RP/0/0/CPU0:router(config-iphc-profile)# tcp context absolute 255
```

transmit-delay (serial)

transmit-delay *microseconds*

no transmit-delay *microseconds*

Command Default

Command Modes

Command History

Release 3.2	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
hdlc	read, write

Examples

In the following example, a delay of 2 microseconds is specified on serial interface 0/3/0/0/0:0:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface serial 0/3/0/0/0:0
RP/0/0/CPU0:router(config-if)# serial
RP/0/0/CPU0:router(config-if-serial)# transmit-delay 2
```

In the following example, the transmit delay on serial interface 0/3/0/0/0:0 is disabled:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface serial 0/3/0/0/0:0
RP/0/0/CPU0:router(config-if)# serial
RP/0/0/CPU0:router(config-if-serial)# no transmit-delay
```

Related Commands

Command	Description
show interfaces, on page 423	Displays statistics for all interfaces configured on the router or for a specific node.

SONET Controller Commands on the Cisco IOS XR Software

This module provides command line interface (CLI) commands for configuring SONET operation, using Layer 1 SONET transport technology, on the Cisco XR 12000 Series Router.

The configuration of the SONET controller includes SONET Automatic Protection Switch (APS), which is a feature offering recovery from fiber (external) or equipment (interface and internal) failures at the SONET line layer. You must configure a SONET controller before you can configure a Packet-over-SONET/SDH (POS) interface or a Spatial Reuse Protocol (SRP) interface.

All SONET-related configurations of a SONET-based physical port are grouped under the SONET controller configuration submode. The SONET path-related configuration commands are grouped under the SONET path submode.

ais-shut (SONET)

To enable automatic insertion of a line alarm indication signal (LAIS) in the sent SONET signal whenever the SONET port enters the administrative shutdown state, use the **ais-shut** command in SONET/SDH configuration mode. To disable automatic insertion of a LAIS, use the **no** form of this command.

ais-shut

no ais-shut

Syntax Description

This command has no keywords or arguments.

Command Default

This command is disabled by default; no AIS is sent.

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

When the line is placed in administrative shutdown state, use the **ais-shut** command to send a signal to downstream equipment that indicates that there is a problem with the line.

The **ais-shut** command is ignored if automatic protection switching (APS) is running for the corresponding port, because the setting must be enabled for proper APS operation.

For SONET ports that do not have hardware support for LAIS insertion, the **ais-shut** command is disabled.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

In the following example, the alarm indication is forced on the SONET OC-3 controller:

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/0/CPU0:router(config-sonet)# ais-shut
```

Related Commands

Command	Description
show controllers sonet, on page 711	Displays information about the operational status of SONET layers.

ais-shut (SONET path)

To enable automatic insertion of path alarm indication signal (PAIS) in the sent SONET signal whenever the SONET path enters the administratively down state, use the **ais-shut** command in SONET/SDH path configuration mode. To disable automatic insertion of PAIS in the SONET signal, use the **no** form of this command.

ais-shut

no ais-shut

Syntax Description

This command has no keywords or arguments.

Command Default

This command is disabled by default; no AIS is sent.

Command Modes

SONET/SDH path configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **ais-shut** command to enable automatic insertion of PAIS in the appropriate sent SONET path overhead whenever the corresponding SONET path enters the administratively down state.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows the alarm indication being enabled on all paths:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/0/CPU0:router(config-sonet)# path
RP/0/0/CPU0:router(config-sonet-path)# ais-shut
```

Related Commands

Command	Description
show controllers sonet, on page 711	Displays information about the operational status of SONET layers.

aps group

To manually switch an automatic protection switching (APS) channel, use the **aps group** command in EXEC configuration mode.

aps group *number* {**force**| **manual**} {**0**| **1**} {**disable**| **enable**}

Syntax Description

number	Number of the APS group. Range is from 1 to 255.
force	Sends a forced APS request at the local end of a SONET link with the assigned channel number.
manual	Sends a manual APS request at the local end of a SONET link with the assigned channel number, which is implemented when no other higher-priority user-initiated or automatic requests are in effect.
0	Specifies that the protect channel should be switched.
1	Specifies that the working channel should be switched.
disable	Stops sending the SONET K1/K2 bit pattern that informs the remote end to switch ports.
enable	Starts sending a SONET K1/K2 bit pattern to inform the remote end to switch ports.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

In a multirouter APS topology, a manual or force request is supported only on the protect router.

Specify **0** or **1** to identify on which channel the traffic should be stopped and switched to the other channel. Therefore, **force 0** or **manual 0** moves traffic from the protect to the working channel, and **force 1** or **manual 1** moves traffic from the working to the protect channel.

Use the **force** keyword to manually switch the traffic to a protect channel. For example, if you need to change the fiber connection, you can manually force the working channel to switch to the protect interface.

A forced switch can be used to override an automatic (Signal Failed Signal Degraded) or a manual switch request. A lockout request (using the **lockout** command) overrides a force request.

Note If a request of equal or higher priority is in effect, you cannot use the **force** keyword to initiate a forced APS request at the local end of the SONET link.

Use the **manual** keyword to manually switch the circuit to a protect channel. For example, you can use this feature when you need to perform maintenance on the working channel. If a protection switch is already up, you can also use the **manual** keyword to revert the communication link to the working channel before the wait to restore (WTR) time period has expired. The WTR time period is set by the **revert** command. Use the **no** form of this command to cancel the switch.

A manual switch request can be used to control which channel carries the traffic when no other higher-priority user-initiated or automatic requests are in effect.

The manual request has the lowest priority among all user-initiated or automatic requests. Any other such requests override a manual request.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following examples show how to use the **aps group** command in EXEC mode to force or manually switch traffic, and enable and disable sending of the K1/K2 bit pattern to signal the switchover to the remote end:

```
RP/0/0/CPU0:router# aps group 1 force 1 enable
RP/0/0/CPU0:router# aps group 1 force 1 disable

RP/0/0/CPU0:router# aps group 1 manual 1 enable
RP/0/0/CPU0:router# aps group 1 manual 1 disable

RP/0/0/CPU0:router# aps group 1 force 0 enable
RP/0/0/CPU0:router# aps group 1 force 0 disable

RP/0/0/CPU0:router# aps group 1 manual 0 enable
RP/0/0/CPU0:router# aps group 1 manual 0 disable
```

Related Commands

Command	Description
aps group (global), on page 649	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
lockout, on page 674	Overrides a manual or forced APS request at the local end of the SONET link and block the protect channel from receiving traffic.
revert, on page 694	Enables automatic switchover from the protect interface to the working interface after the working interface becomes available.

Command	Description
signalling, on page 722	Configures the K1K2 overhead byte signaling protocol used for APS.
show aps, on page 698	Displays the operational status for all configured SONET APS groups.

aps group (global)

To add an automatic protection switching (APS) group and enter APS group configuration mode, use the **aps group** command in global configuration mode. To remove a group, use the **no** form of this command.

aps group *number*

no aps group *number*

Syntax Description

number	Number of the group. Range is from 1 to 255.

Command Default

No APS groups are defined.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

An APS group contains one protect (P) SONET port and one working (W) SONET port. The working and protect ports can reside on the same logical channel (LC), on different LCs in the same router, or on different routers. One APS group must be configured for each protect port and its corresponding working ports.

Use the **aps group (global)** command to enter APS group configuration mode and configure APS connections with other SONET equipment.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to use the **aps group** command in global configuration mode to configure APS group 1 and enter APS group configuration mode:

```
RP/0/0/CPU0:router(config)# aps group 1
RP/0/0/CPU0:router(config-aps)#
```

Related Commands

Command	Description
aps group, on page 646	Manually switches an APS channel.
authenticate (PGP), on page 653	Configures the authentication string for the PGP message exchange between the protect and working routers.
channel local, on page 656	Assigns local SONET physical ports as SONET APS channels in the current APS group.
channel remote, on page 658	Assigns a port and interface that is physically located in a remote router as a SONET working or protect APS channel.
lockout, on page 674	Overrides a manual or forced APS request at the local end of the SONET link and block the protect channel from receiving traffic.
revert, on page 694	Enables automatic switchover from the protect interface to the working interface after the working interface becomes available.
signalling, on page 722	Configures the K1K2 overhead byte signaling protocol used for APS.
timers (APS), on page 725	Changes the time between hello packets and the time before the protect interface process declares a working interface router to be down.
unidirectional, on page 734	Configures a protect interface for unidirectional mode.
show aps, on page 698	Displays the operational status for all configured SONET APS groups.

au

To specify the administrative unit (AU) group number and enter the AU controller configuration mode, use the **au** command in SONET controller configuration mode.

au *number*

Syntax Description

number	Administrative unit group number in the range from 1 to 48.

Command Default

The default is 1.

Command Modes

SONET controller configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

The **au** command enables you to begin configuring the interface in the AU controller configuration mode, where you can configure tributary unit groups (TUGs), virtual containers (VCs), and DS3s, such as shown in the following path example:

STM-1 -> AU-4 -> TUG-3 -> VC-3 -> DS-3

One AU-4 path is equivalent to three AU-3 paths. An administrative unit type 4 (AU-4) consists of three STM-1s or one STM-3. An administrative unit type 3 (AU-3) consists of one STM-1.

Note Use the **au** command to configure one of the AUGs available for your card. The **au** command is not used to configure the *type* of AU path that you are configuring, such as AU-3 or AU-4, but rather is used to identify one AU group number in the supported range for the card and AU type that you are configuring. For example, the 1-Port Channelized OC-48/STM-16 SPA supports 16 AU-4 groups. Therefore, you can specify a number between 1 and 16 for the **au** command to configure SDH AU-4 on that card. The 1-Port Channelized OC-3/STM-1 SPA supports 1 AUG for AU-4, so you would specify **au 1**.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to specify AU 1.

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/0/CPU0:router(config-sonet)# au 1
RP/0/0/CPU0:router(config-auPath)#
```

Related Commands

Command	Description
tug3, on page 731	Specifies the tributary unit group (TUG) number and enters the TUG3 controller configuration mode.

authenticate (PGP)

To configure the authentication string for the Protect Group Protocol (PGP) message exchange between the protect and working routers, use the **authenticate** command in APS group configuration mode. To revert to the default authentication string, use the **no** form of this command.

authenticate *string*

no authenticate *string*

Syntax Description

string	Authentication string that the router uses to authenticate PGP message exchange between protect or working routers. The maximum length of the string is eight alphanumeric characters. Spaces are not accepted.

Command Default

The default authentication string is “cisco.”

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **authenticate** command to configure the authentication string for the PGP message exchange between the protect and working routers. Use the **no** form of this command to revert to the default authentication string.

The **authenticate** command applies only in multirouter automatic protection switching (APS) group configurations.

In multirouter APS topologies, the protect and working routers communicate with each other through the User Datagram Protocol (UDP)-based Pretty Good Privacy protocol. Each Pretty Good Privacy packet contains an authentication string used for packet validation. The authentication string on all routers involved in the same APS group operation must match for proper APS operation.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example enables authentication for APS group 1 in abctown:

```
RP/0/0/CPU0:router(config)# aps group 1
```

```
RP/0/0/CPU0:router(config-aps)# authenticate abctown
```

Related Commands

Command	Description
aps group (global), on page 649	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
channel local, on page 656	Assigns local SONET physical ports as SONET APS channels in the current APS group.
channel remote, on page 658	Assigns a port and interface that is physically located in a remote router as a SONET working or protect APS channel.
show aps, on page 698	Displays the operational status for all configured SONET APS groups.

b3-ber-prdi

To enable sending of a path-level remote defect indication (PRDI) when the bit error rate (BER) bit interleaved parity (BIP) B3 threshold is exceeded, use the **b3-ber-prdi** command in SONET/SDH path configuration mode. To disable sending a PRDI, use the **no** form of this command.

b3-ber-prdi

no b3-ber-prdi

Syntax Description

This command has no keywords or arguments.

Command Default

This command is disabled by default; a PRDI is not sent.

Command Modes

SONET/SDH path configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows a PRDI enabled on all paths:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/0/CPU0:router(config-sonet)# path
RP/0/0/CPU0:router(config-sonet-path)# b3-ber-prdi
```

Related Commands

Command	Description
path (SONET), on page 688	Enters SONET/SDH path configuration mode.
show controllers sonet, on page 711	Displays information about the operational status of SONET layers.

channel local

To assign local SONET physical ports as SONET automatic protection switching (APS) channels in the current APS group, use the **channel local** command in APS group configuration mode. To return to the default setting, use the **no** form of this command.

channel {**0**| **1**} **local [preconfigure] sonet** *interface-path-id*

no channel {**0**| **1**} **local [preconfigure] sonet** *interface-path-id*

Syntax Description

{**0** | **1**}	Assigns a protect or working channel type. **0** is protect, **1** is working.
preconfigure	(Optional) Specifies a SONET preconfiguration. This keyword is used only when a modular services or line card is not physically installed in a slot.
sonet	Specifies a SONET interface type.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show controllers sonet** command to see a list of all controllers currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

A SONET APS local channel is not assigned.

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

Use the **channel local** command to designate SONET physical ports as SONET APS channels in the current APS group. Use the **channel remote** command to assign channels that are physically located in a different router.

Preconfigured interfaces are supported.

If the protect channel is local, it must be assigned using a **channel** command *before* any of the working channels are assigned. The reason is that having only a working channel assigned is a valid configuration for a working router in a multirouter APS topology and further attempts to configure a local protect channel are rejected.

The interface type must be a SONET controller.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to configure SONET 0/2/0/2 as a local protect channel:

```
RP/0/0/CPU0:router(config)# aps group 1
RP/0/0/CPU0:router(config-aps)# channel 0 local SONET 0/2/0/2
```

Related Commands

Command	Description
aps group (global), on page 649	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
channel remote, on page 658	Assigns a port and interface that is physically located in a remote router as a SONET working or protect APS channel.
show aps, on page 698	Displays the operational status for all configured SONET APS groups.

channel remote

To assign a port and interface that is physically located in a remote router as a SONET working or protect automatic protection switching (APS) channel, use the **channel remote** command in APS group configuration mode. To return to the default setting, use the **no** form of this command.

channel {**0**| **1**} **remote** *ip-address*

no channel {**0**| **1**} **remote** *ip-address*

Syntax Description

{**0** | **1**}	Assigns a protect or working channel type. **0** is protect, **1** is working.
ip-address	Remote router IP address in A.B.C.D format.

Command Default

A SONET APS remote channel is not assigned.

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **channel remote** command to assign working or protect channels that are physically located in a different router.

Use the **channel local** command to assign channels in the local router.

Note The **channel remote** command should not be used in single-router APS topologies.

The *IP address* of the remote router is required only if a working channel configured as the protect router contacts all working routers.

Specifying a remote protect channel is optional. If you do not specify a remote protect channel, the default value of 0.0.0.0 is used. The protect router is always the one that contacts the working router. The working router replies to the protect router using the source address extracted from the incoming messages as the destination address. If an address other than 0.0.0.0 (the default value) is specified, the working router always uses that address when sending messages to the protect router.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

In the following examples, a remote channel with IP address 192.168.1.1 is assigned as the working channel:

```
RP/0/0/CPU0:router(config)# aps group 1
RP/0/0/CPU0:router(config-aps)# channel 1 remote 192.168.1.1
```

Related Commands

Command	Description
aps group (global), on page 649	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
channel local, on page 656	Assigns local SONET physical ports as SONET APS channels in the current APS group.
show aps, on page 698	Displays the operational status for all configured SONET APS groups.

clear counters sonet

To clear SONET counters for a specific SONET controller, use the **clear counters sonet** command in EXEC mode.

clear counters sonet *interface-path-id*

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show controllers sonet** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.
- If specifying a virtual interface, the number range varies, depending on interface type.

Use the **clear counters sonet** command to clear SONET counters for a specific SONET controller.

Task ID

Task ID	Operations
sonet-sdh	read, write

Task ID	Operations
basic-services	read, write

Examples

The following example shows the SONET counters being cleared on the SONET interface:

```
RP/0/0/CPU0:router# clear counters sonet 0/1/0/0
```

Related Commands

Command	Description
show controllers sonet, on page 711	Displays information about the operational status of SONET layers.

clock source (SONET)

To set the clock source of the sent signal on SONET ports, use the **clock source** command in SONET/SDH configuration mode. To cancel a clock source setting, use the **no** form of this command.

clock source {**internal**| **line**}

no clock source {**internal**| **line**}

Syntax Description

internal	Specifies that the controller will clock its sent data from its internal clock.
line	Specifies that the controller will clock its sent data from a clock recovered from the receive data stream of the line. This is the default value.

Command Default

The clock source for the controller is **line**.

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **clock source** command to configure which reference clock is used by the sender.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

In the following example, the SONET controller is configured to clock its sent data from its internal clock:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/0/CPU0:router(config-sonet)# clock source internal
```

Related Commands

Command	Description
show controllers sonet, on page 711	Displays information about the operational status of SONET layers.

controller (SONET)

To enter SONET/SDH configuration mode so that you can configure a specific SONET controller, use the **controller (SONET)** command in global configuration mode. To return to the default state, use the **no** form of this command.

controller [preconfigure] sonet *interface-path-id*

no controller [preconfigure] sonet *interface-path-id*

Syntax Description

preconfigure	(Optional) Specifies a SONET preconfiguration. Use the **preconfigure** keyword only when a modular services card in not physically installed in a slot.
sonet	Enters the SONET configuration mode or configures the SONET port controller specified by *interface-path-id*.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

Use the **path (SONET)** command to enter SONET/SDH path configuration mode to specify other SONET options for a SONET path.

Task ID

Task ID	Operations
interface	read, write

Task ID

Examples

The following example shows how to enter SONET/SDH configuration mode for the SONET controller in slot number 2:

```
RP/0/0/CPU0:router(config)# controller SONET 0/2/0/1
RP/0/0/CPU0:router(config-sonet)#
```

The following example shows how to configure the SONET controller path (0/2/0/1) to send a path-level remote defect indication (PRDI) when the bit error rate (BER) bit interleaved parity (BIP) B3 threshold is exceeded. :

```
RP/0/0/CPU0:router(config)# controller SONET 0/2/0/1 path b3-ber-prdi
RP/0/0/CPU0:router(config-sonet)#
```

Related Commands

Command	Description
path (SONET), on page 688	Enters SONET/SDH path configuration mode.
show controllers sonet, on page 711	Displays information about the operational status of SONET layers.

delay clear

To configure the amount of time before a Synchronous Transport Signal (STS) path delay trigger alarm is cleared, use the **delay clear** command in STS path configuration mode. To return the command to its default setting, use the **no** form of this command.

delay clear *value*

no delay clear *value*

Syntax Description

value	Value, in milliseconds, before an STS path delay trigger alarm is cleared. The range is from 0 to 180000. The default is 10 seconds.

Command Default

The default is 10 seconds.

Command Modes

STS path configuration

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to specify that STS path delay trigger alarms should be cleared after 7000 milliseconds:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/3
RP/0/0/CPU0:router(config-sonet)# sts 1
RP/0/0/CPU0:router(config-stsPath)# delay clear 7000
```

Related Commands

Command	Description
delay trigger, on page 666	Configures a time value for the STS path delay trigger.

delay trigger

To configure a time value for the Synchronous Transport Signal (STS) path delay trigger, use the **delay trigger** command in STS path configuration mode. To return the command to its default setting, use the **no** form of this command.

delay trigger *value*

no delay trigger *value*

Syntax Description

value	Value, in milliseconds, for the STS path delay trigger. The range is from 0 through 60000. The default is 0 seconds, which means that there is no delay.

Command Default

The default is 0 seconds, which means that there is no delay.

Command Modes

STS path configuration

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

If the timer for the STS path delay trigger expires, an alarm is declared.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to set the STS path delay trigger to 6000 milliseconds:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/3
RP/0/0/CPU0:router(config-sonet)# sts 1
RP/0/0/CPU0:router(config-stsPath)# delay trigger 6000
```

Related Commands

Command	Description
delay clear, on page 665	Configures the amount of time before a STS path delay trigger alarm is cleared.

down-when-looped

To configure a SONET controller to inform the system that it is down when loopback is detected, use the **down-when-looped** command in SONET/SDH configuration mode.

down-when-looped

Syntax Description

This command has no keywords or arguments.

Command Default

The default is disabled.

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

This command does not have a **no** form.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to configure a SONET controller to inform the system that the associated line is down if a loopback is detected:

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/0/CPU0:router(config-sonet)# down-when-looped

down-when-looped is a traffic-affecting operation
```

Related Commands

Command	Description
loopback (SONET), on page 676	Configures the SONET controller for loopback mode.

force

To initiate a forced automatic protection switching (APS) request at the local end of the SONET link, use the **force** command in EXEC configuration mode.

Note Effective with Cisco IOS XR Release 3.8.0, this command is replaced by the **aps group force** command. See the aps group, on page 646 command for more information.

force {**0**| **1**}

Syntax Description

0 | **1**	initiate a forced automatic protection switching (APS) request at the local end of the SONET link Assigned channel number. **0** = protect, **1** = working.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.8.0	This command was replaced by the **aps group** command.

Usage Guidelin

Note If a request of equal or higher priority is in effect, you cannot use the **force** command to initiate a forced APS request at the local end of the SONET link.

Use the **force** command to manually switch the traffic to a protect channel. For example, if you need to change the fiber connection, you can manually force the working channel to switch to the protect interface.

The **0** or **1** keyword (by default 1) identifies on which channel the traffic should be stopped and moved on the protect channel. The **force 1 command** moves traffic from the working channel to the protect channel; the **force 0 command** moves traffic from the protect channel back to the working channel.

A forced switch can be used to override an automatic (Signal Failed Signal Degraded) or a manual switch request. A lockout request (via the **lockout** command) overrides a force request.

In a multirouter APS topology, a force request is allowed only on the protect router.

This command remains in effect until it is unconfigured by using the **no** form of the command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to move traffic from the working channel back to the protect channel:

```
RP/0/0/CPU0:router(config)# aps group 1
RP/0/0/CPU0:router(config-aps)# force 1
```

Related Commands

Command	Description
lockout, on page 674	Overrides a manual or forced APS request at the local end of the SONET link and block the protect channel from receiving traffic.
manual, on page 678	Initiates a manual APS request at the local end of the SONET link.

framing (SONET)

To specify the framing used on the SONET controller, use the **framing** command in SONET/SDH configuration mode. To disable framing on the SONET controller, use the **no** form of this command.

framing {**sdh**| **sonet**}

no framing {**sdh**| **sonet**}

Syntax Description

sdh	Selects Synchronous Digital Hierarchy (SDH) framing. This framing mode is typically used in Europe.
sonet	Selects SONET framing. This is the default.

Command Default

The default framing on SONET controllers is **sonet**.

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **framing** command to select either SONET or SDH framing on the selected physical port, if supported. For physical ports that do not support either of these two options, the **framing** command is disabled.

Use the **no** form of this command to disable SONET or SDH framing on the SONET controller.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

In the following example, the SONET controller is configured for SDH framing:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/0/CPU0:router(config-sonet)# framing sdh
```

In the following example, the SONET controller is configured for SONET framing:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
```

```
RP/0/0/CPU0:router(config-sonet)# framing sonet
```

Related Commands

Command	Description
show controllers sonet, on page 711	Displays information about the operational status of SONET layers.

line delay clear

To configure the amount of time before a SONET/SDH line delay trigger alarm is cleared, use the **line delay clear** command in SONET controller configuration mode. To return the command to its default setting, use the **no** form of this command.

line delay clear *value*

no line delay clear

Syntax Description

value	Value, in milliseconds, before a SONET/SDH line delay trigger alarm is cleared. The range is 1000 to 180000. The default is 10.

Command Default

The default is 10.

Command Modes

SONET controller configuration

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

If the timer for the SONET/SDH line delay clear expires, an alarm is cleared.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to specify that SONET/SDH line delay trigger alarms should be cleared after 4000 milliseconds:

```
RP/0/0/CPU0:router(config)# controller SONET 0/0/0/2
RP/0/0/CPU0:router(config-sonet)# line delay clear 4000
```

Related Commands

Command	Description
line delay trigger, on page 673	Configures a time value for the SONET/SDH line delay trigger.

line delay trigger

To configure a time value for the SONET/SDH line delay trigger, use the **line delay trigger** command in SONET controller configuration mode. To return the command to its default setting, use the **no** form of this command.

line delay trigger *value*

no line delay trigger

Syntax Description

value	Value, in milliseconds, for the SONET/SDH line delay trigger. The range is 0 to 60000.

Command Default

The default is 0, which means that there is no delay.

Command Modes

SONET controller configuration

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

If the timer for the SONET/SDH line delay trigger expires, an alarm is raised.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to set the SONET/SDH line delay trigger to 3000 milliseconds:

```
RP/0/0/CPU0:router(config)# controller SONET 0/0/0/2
RP/0/0/CPU0:router(config-sonet)# line delay trigger 3000
```

Related Commands

Command	Description
line delay clear, on page 672	Configures the amount of time before a SONET/SDH line delay trigger alarm is cleared.

lockout

To override a manual or forced APS request at the local end of the SONET link and block the protect channel from receiving traffic, use the **lockout** command in APS group configuration mode. To remove the lockout, use the **no** form of this command.

lockout [0]

no lockout [0]

Syntax Description

[**0**]	(Optional) Specifies blocking of the protect channel from a manual or forced APS request. This is the default.

Command Default

The default is 0.

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

A lockout switch request can be used to override a force, an automatic (Signal Failed or Signal Degraded), or a manual switch request. No other request can override a lockout request; it has the highest possible priority.

In a multirouter APS topology, a **lockout** request is allowed only on the protect router.

This command remains in effect until it is unconfigured by using the **no** form of the command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to lock out or prevent the channel from switching to a protect router in the event that the working channel becomes unavailable:

```
RP/0/0/CPU0:router(config)# aps group 1
RP/0/0/CPU0:router(config-aps)# lockout 0
```

Related Commands

Command	Description
aps group (global), on page 649	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
aps group, on page 646	Manually switches an APS channel.

loopback (SONET)

To configure the SONET controller for loopback mode, use the **loopback** command in SONET/SDH configuration mode. To remove the loopback SONET command from the configuration file, use the **no** form of this command.

loopback {**internal**| **line**}

no loopback {**internal**| **line**}

Syntax Description

internal	Specifies that all the packets be looped back from the source.
line	Specifies that the incoming network packets be looped back to the SONET network.

Command Default

This command is disabled by default.

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

The SONET and Synchronous Digital Hierarchy (SDH) transport layers support two loopback operation modes for diagnostic purposes: internal and line. In the terminal (internal) loopback, the sent signal is looped back to the receiver. In the facility (line) loopback, the signal received from the far end is looped back and sent on the line. The two loopback modes cannot be active at the same time. In normal operation mode, neither of the two loopback modes is enabled.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

In the following example, all packets are looped back to the SONET controller:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/0/CPU0:router(config-sonet)# loopback internal
```

Related Commands

Command	Description
show controllers sonet, on page 711	Displays information about the operational status of SONET layers.

manual

To initiate a manual automatic protection switching (APS) request at the local end of the SONET link, use the **manual** command in APS group configuration mode. To cancel the switch, use the **no** form of this command.

Note Effective with Cisco IOS XR Release 3.8.0, this command is replaced by the **aps group manual** command. See the aps group, on page 646 command for more information.

manual *channel-number* {**0**| **1**}

no manual *channel-number* {**0**| **1**}

Syntax Description

channel-number	The assigned channel number: **0** = protect, **1**= working.

Command Default

No circuit is switched.

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.8.0	This command was replaced by the **aps group** command.

Usage Guidelines

Use the **manual** command to manually switch the circuit to a protect channel. For example, you can use this feature when you need to perform maintenance on the working channel. If a protection switch is already up, you can also use the **manual** command to revert the communication link to the working channel before the wait to restore (WTR) time period has expired. The WTR time period is set by the **revert** command. Use the **no** form of this command to cancel the switch.

A manual switch request can be used to control which channel carries the traffic when no other higher-priority user-initiated or automatic requests are in effect.

The **0** or **1** keyword identifies the channel from which the traffic should be moved on the protect channel:

- **The manual 1 command** moves traffic on to the protect channel.
- **The manual 0** command moves traffic on to the working channel.

The manual request has the lowest priority among all user-initiated or automatic requests. Any other such requests override a manual request.

In a multirouter APS topology a **manual** request is allowed only on the protect router.

This command remains in effect until it is unconfigured by using the **no** form of the command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to move traffic on to the protect router:

```
RP/0/0/CPU0:router(config)# aps group 1
RP/0/0/CPU0:router(config-aps)# manual 1
```

Related Commands

Command	Description
force, on page 668	Initiates a forced APS request at the local end of the SONET link.
lockout, on page 674	Overrides a manual or forced APS request at the local end of the SONET link and block the protect channel from receiving traffic.

mode (SONET)

To set the mode of an STS path, AU path, T3 controller, or TUG3 controller, use the **mode** command in the applicable controller configuration mode. To disable the mode, use the **no** form of this command.

STS Controller Configuration Mode

mode {**t3**| **vt15-t1**| **pos**}

no mode {**t3**| **vt15-t1**| **pos**}

AU Controller Configuration Mode

mode {**e3**| **t3**| **tug 3**}

no mode {**e3**| **t3**| **tug 3**}

T3 Controller Configuration Mode

mode {**e1**| **serial**| **t1**}

no mode {**e1**| **serial**| **t1**}

TUG3 Controller Configuration Mode

mode {**c12**| **c12-e1**| **e3**| **serial**| **t3**}

no mode {**c12**| **c12-e1**| **e3**| **serial**| **t3**}

Syntax Description

t3	Specifies the mode of the port to be channelized as an AU3 or a TUG3 path carrying T3.
vt15-t1	Specifies the mode of the port to be channelized VT15-T1.
pos	Specifies the mode of the port to be channelized POS.
tug3	Specifies the mode of the port to be channelized TUG3.
e1	Specifies the mode of the port to be channelized E1.
serial	Specifies the mode of the port to be clear channel serial.
t1	Specifies the mode of the port to be channelized T1.
c12	Specifies the mode of the port to be channelized as a TUG3 path carrying TU-12.
c12-e1	Specifies the mode of the port to be channelized be TUG3 path carrying c12 to E1.
e3	Specifies the mode of the port to be channelized as an AU3 or a TUG3 path carrying E3.

Command Default

No default behavior or values

Command Modes

STS controller configuration

AU controller configuration

T3 controller configuration

TUG3 controller configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

For channelized SPAs, you must use the **mode** command before you can configure any channelized controllers.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to set the mode of a T3 controller to channelized T1:

```
RP/0/0/CPU0:router(config)# controller t3 0/1/0/0/1
RP/0/0/CPU0:router(config-t3)# mode t1
```

Related Commands

Command	Description
width, on page 736	Sets the number of paths in a stream.

overhead (SONET)

To set the SONET overhead bytes in the frame header to a specific standards requirement, or to ensure interoperability with equipment from another vendor, use the **overhead** command in SONET/SDH configuration mode. To remove the setting of the SONET overhead bytes from the configuration file and restore the default condition, use the **no** form of this command.

overhead {**j0**| **s1s0**} *byte-value*

no overhead {**j0**| **s1s0**} *byte-value*

Syntax Description

j0	Sets the J0/C1 byte value in the SONET section overhead. For interoperability with Synchronous Digital Hierarchy (SDH) equipment in Japan, use the value 0x1. Default is 0xcc.
s1s0	Sets the SS bits value of the H1 byte in the SONET line overhead. Use the following values to tell the SONET transmission equipment the S1and S0 bit: • For SONET mode, use **0** (this is the default). • For SDH mode, use **2**. Range is from 0 to 3. Default is 0. Values 1 and 3 are undefined.
byte-value	Byte value to which the **j1** or **s1s0** keyword should be set. Range is from 0 to 255.

Command Default

byte-value: 0x01 (j0)

byte-value: 0 (sls0)

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **overhead** command to set the SONET overhead bytes in the frame header to a specific standards requirement.

Use the **no** form of this command to remove the setting of the SONET overhead bytes from the configuration file and restore the default condition.

For the **j0** keyword, the value that you use for the trace byte depends on the type of equipment being used. For the **s1s0** keyword, the value that you use depends on whether you are using the SONET or SDH mode. For SONET mode, use the value 0 (the default). For SDH mode, use the value 2.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to set the SS bits value of the H1 byte in the SONET line overhead to 2 for SDH:

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/1
RP/0/0/CPU0:router(config-sonet)# overhead sls0 2
```

The following example shows how to set the SS bits value of the H1 byte in the SONET line overhead to 0 for SONET:

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/1
RP/0/0/CPU0:router(config-sonet)# overhead sls0 0
```

overhead (SONET path)

To set the SONET path overhead bytes in the frame header to a specific standards requirement or to ensure interoperability with equipment from another vendor, use the **overhead** command in SONET/SDH path configuration mode. To remove the setting of the SONET path overhead bytes from the configuration file and restore the system to its default condition, use the **no** form of this command.

overhead {**c2** *byte-value*| **expected-trace** *LINEascii-text*| **j1** *ascii-value*}

no overhead {**c2** *byte-value*| **expected-trace** *LINEascii-text*| **j1** *ascii-value*}

Syntax Description

c2 *byte-value*	Specifies Synchronous Transport Signal (STS) synchronous payload envelope (SPE) content (C2) byte. The transmitted **c2** value is automatically set to 0xCF for unscrambled payload and 0x16 for scrambled payload. If c2 is configured to a user-specified value, the user-specified value is always applied regardless of scrambling. Replace the *byte-value* argument with the byte value to which the **c2** keyword should be set. Range is from 0 to 255. Default value is 0.
j1 *ascii-value*	Configures the SONET path trace (j1) buffer. Replace the *ascii-value* argument with a text string that describes the SONET path trace buffer. Default is a 64-byte path trace ASCII message, which includes default information such as router name, (Layer 2 —POS) interface name, and IP address, if applicable.
expected-trace *LINE ascii-text*	Configures the SONET/SDH path trace. The trace monitoring feature allows a node to perform trace monitoring by using the SONET/SDH capabilities. Replace the *LINE* with the expected trace message Replace the *ascii-text* argument with a text string that describes the SONET path trace buffer. Default is a 64-byte path trace ASCII message, which includes default information such as router name, (Layer 2 —POS) interface name, and IP address, if applicable. the LINE is the expected trace message which should match else ptim mismatch would be reported

Command Default

byte-value: 0xCF

byte-value: 0

Command Modes

SONET/SDH path configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

The SONET standards permit or require user access for configuration of some bytes or bits in the SONET path overhead. Use the **overhead** command to set the SONET path overhead bytes in the frame header to a specific standards requirement. Use the **no** form of this command to remove the setting of the SONET path overhead bytes from the configuration file and restore the system to its default condition.

Use the **c2** keyword to configure the desired C2 byte value in the SONET path overhead.

Use the **j1** keyword to configure a user-defined path trace message in the j1 bytes of the SONET path overhead. For the **j1** keyword, use the default message or insert your own message that has a maximum of 62 characters. If no user-defined message is configured, a default message is automatically generated, containing the router name, the controller name, its IP address, and the values of the sent and received K1 and K2 bytes in the SONET line overhead.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to set the STS SPE C2 byte in the SONET path frame header:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/0/CPU0:router(config-sonet)# path
RP/0/0/CPU0:router(config-sonet-path)# overhead c2 0x13
```

Related Commands

Command	Description
scrambling disable (SONET path), on page 696	Disables payload scrambling on a SONET path.

path delay clear

To configure the amount of time before a SONET/SDH path delay trigger alarm is cleared, use the **path delay clear** command in SONET controller configuration mode. To return the command to its default setting, use the **no** form of this command.

path delay clear *value*

no path delay clear

Syntax Description

value	Value, in milliseconds, before a SONET/SDH path delay trigger alarm is cleared. The range is 1000 to 180000. The default is 10 seconds.

Command Default

The default is 10 seconds.

Command Modes

SONET controller configuration

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to specify that SONET/SDH path delay trigger alarms should be cleared after 7000 milliseconds:

```
RP/0/0/CPU0:router(config)# controller SONET 0/0/0/1
RP/0/0/CPU0:router(config-sonet)# path delay clear 7000
```

Related Commands

Command	Description
path delay trigger, on page 687	Configures a time value for the SONET/SDH path delay trigger.

path delay trigger

To configure a time value for the SONET/SDH path delay trigger, use the **path delay trigger** command in SONET controller configuration mode. To return the command to its default setting, use the **no** form of this command.

path delay trigger *value*

no path delay trigger

Syntax Description

value	Value, in milliseconds, for the SONET/SDH path delay trigger. The range is 0 to 60000.

Command Default

The default is 0, which means that there is no delay.

Command Modes

SONET controller configuration

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

If the timer for the SONET/SDH path delay trigger expires, an alarm is declared.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to set the SONET/SDH path delay trigger to 6000 milliseconds:

```
RP/0/0/CPU0:router(config)# controller SONET 0/0/0/1
RP/0/0/CPU0:router(config-sonet)# path delay trigger 6000
```

Related Commands

Command	Description
path delay clear, on page 686	Configures the amount of time before a SONET/SDH path delay trigger alarm is cleared.

path (SONET)

To enter SONET/SDH path configuration mode, use the **path** command in SONET controller configuration mode.

path

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

SONET controller configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to access SONET path submode from SONET controller configuration mode:

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/0/CPU0:router(config-sonet)# path
```

Related Commands

Command	Description
ais-shut (SONET path), on page 645	Enables automatic insertion of PAIS in the sent SONET signal whenever the SONET path enters the administratively down state.
b3-ber-prdi, on page 655	Enables sending of a PRDI when the BER bit interleaved parity (BIP) B3 threshold is exceeded.
delay clear, on page 665	Configures the amount of time before a STS path delay trigger alarm is cleared.

Command	Description
delay trigger, on page 666	Configures a time value for the STS path delay trigger.
overhead (SONET path), on page 684	Sets the SONET path overhead bytes in the frame header to a specific standards requirement or to ensure interoperability with equipment from another vendor.
report (SONET path), on page 692	Configures whether or not selected SONET alarms are logged to the console for a SONET path controller.
scrambling disable (SONET path), on page 696	Disables payload scrambling on a SONET path.
threshold (SONET path), on page 729	Sets the bit error rate (BER) threshold values of the specified alarms for a SONET path.
uneq-shut (SONET path), on page 733	Enables automatic insertion of P-UNEQ code (0x00) in the sent SONET path overhead C2 byte.

report (SONET)

To permit selected SONET alarms to be logged to the console for a SONET controller, use the **report** command in SONET/SDH configuration mode. To disable logging of select SONET alarms, use the **no** form of this command.

report [**b1-tca**| **b2-tca**| **lais**| **lrdi**| **sd-ber**| **sf-ber**| **slof**| **slos**]

no report [**b1-tca**| **b2-tca**| **lais**| **lrdi**| **sd-ber**| **sf-ber**| **slof**| **slos**]

Syntax Description

b1-tca	(Optional) Reports bit 1 (B1) bit error rate (BER) threshold crossing alert (TCA) errors.
b2-tca	(Optional) Reports bit 2 (B2) BER TCA errors.
lais	(Optional) Reports line alarm indication signal (LAIS) errors.
lrdi	(Optional) Reports line remote defect indication errors.
sd-ber	(Optional) Reports signal degradation BER errors.
sf-ber	(Optional) Reports signal failure BER errors.
slof	(Optional) Reports section loss of frame (SLOF) errors.
slos	(Optional) Reports section loss of signal (SLOS) errors.

Command Default

Alarms from the following keywords are reported by default:

- b1-tca
- b2-tca
- sf-ber
- slof
- slos

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Reporting an alarm means that the alarm can be logged to the console, but it is no guarantee that it is logged. SONET alarm hierarchy rules dictate that only the most severe alarm of an alarm group is reported. Whether an alarm is reported or not, you can check the current state of masked alarm, a problem indication that is a candidate for an alarm, by displaying the "Masked Alarms" line in the **show controllers sonet** command output.

For B1, the bit interleaved parity (BIP) error report is calculated by comparing the BIP-8 code with the BIP-8 code that is extracted from the B1 byte of the following frame. Differences indicate that section-level bit errors have occurred.

For B2, the BIP error report is calculated by comparing the BIP-8/24 code with the BIP-8 code that is extracted from the B2 byte of the following frame. Differences indicate that line-level bit errors have occurred.

Path AIS is sent by line terminating equipment to alert the downstream path terminating equipment (PTE) that it has detected a defect on its incoming line signal.

Path loss of pointer (LOP) is reported as a result of an invalid pointer (H1, H2) or an excess number of new data flag enabled indications.

SLOF is detected when an error-framing defect on the incoming SONET signal persists for 3 microseconds.

SLOS is detected when an all-zeros pattern on the incoming SONET signal is observed. This defect might also be reported if the received signal level drops below the specified threshold.

To determine the alarms that are reported on the controller, use the **show controllers sonet** command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to enable the reporting of line AIS alarms on the path controller:

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/1
RP/0/0/CPU0:router(config-sonet)# report lais
```

Related Commands

Command	Description
show controllers sonet, on page 711	Displays information about the operational status of SONET layers.

report (SONET path)

To configure whether or not selected SONET alarms are logged to the console for a SONET path controller, use the **report** command in SONET/SDH path configuration mode. To disable or re-enable the logging of select SONET alarms, use the **no** form of this command.

report [**b3-tca**| **pais**| **plop**| **pplm**| **prdi**| **ptim**]

no report [**b3-tca**| **pais**| **plop**| **pplm**| **prdi**| **ptim**]

Syntax Description

b3-tca	(Optional) Reports bit 3 (B3) bit error rate (BER) threshold crossing alert (TCA) errors.
pais	(Optional) Reports path alarm indication signal (PAIS) errors.
plop	(Optional) Reports path loss of pointer (PLOP) errors.
pplm	(Optional) Reports path payload mismatch (PPLM) defect errors.
prdi	(Optional) Reports path remote defect indication (PRDI) errors.
ptim	(Optional) Reports path trace identity mismatch (PTIM) defect errors.

Command Default

Alarms from the following keywords are reported:

- b3-tca
- plop

Command Modes

SONET/SDH path configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Reporting an alarm means that the alarm can be logged to the console, but it is no guarantee that it is logged. SONET alarm hierarchy rules dictate that only the most severe alarm of an alarm group is reported. Whether an alarm is reported or not, you can view the current state of a masked alarm, a problem indication that is a candidate for an alarm, by inspecting the “Masked Alarms” line displayed in the **show controllers sonet** command output.

For B3, the bit interleaved parity (BIP) error report is calculated by comparing the BIP-8 code with the BIP-8 code that is extracted from the B3 byte of the following frame. Differences indicate that path-level bit errors have occurred.

Path AIS is sent by line-terminating equipment to alert the downstream path-terminating equipment (PTE) that it has detected a defect on its incoming line signal.

Path LOP is reported as a result of an invalid pointer (H1, H2) or an excess number of new data flag enabled indications.

To determine the alarms that are reported on the controller, use the **show controllers sonet** command.

All report commands accept the default option. The default reporting values are determined based upon the SONET standards specifications and are clearly identified in the corresponding command's help string.

Note The reporting of B3 BER TCA errors and path LOP errors is enabled by default.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

In the following example, reporting of path PAIS alarms is enabled:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/0/CPU0:router(config-sonet)# path
RP/0/0/CPU0:router(config-sonet-path)# report pais
```

Related Commands

Command	Description
show controllers sonet, on page 711	Displays information about the operational status of SONET layers.

revert

To enable automatic switchover from the protect interface to the working interface after the working interface becomes available, use the **revert** command in APS configuration mode. To disable automatic switchover, use the **no** form of this command.

revert *minutes*

no revert *minutes*

Syntax Description

minutes	Number of minutes until the circuit is switched back to the working interface after the working interface is available.

Command Default

minutes: 0

Automatic switchover is disabled.

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **revert** command to enable and disable revertive APS operation mode, if needed. The revertive APS operation mode of the routers should be matched with the APS operation mode of the connected SONET equipment. Use the **no** form of this command to disable automatic switchover.

The revertive APS operation mode is the recommended operation mode because it offers better traffic protection during various possible software failures and upgrade or downgrade scenarios.

The *minutes* argument indicates how many minutes will elapse until automatic protection switching (APS) decides to switch traffic back from protect to working after the condition that caused an automatic (Signal Failed or Signal Degrade) switch to protect disappears. A value of 0 (default) disables APS revertive mode.

In a multirouter APS topology, the **revert** command is allowed only on the protect router.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to enable APS to revert to the protect or working channel after 5 minutes have elapsed:

```
RP/0/0/CPU0:router(config)# aps group 1
RP/0/0/CPU0:router(config-aps)# revert 5
```

Related Commands

Command	Description
aps group (global), on page 649	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
show aps, on page 698	Displays the operational status for all configured SONET APS groups.

scrambling disable (SONET path)

To disable payload scrambling on a SONET path, use the **scrambling disable** command in SONET/SDH path configuration mode. To enable payload scrambling after it has been disabled, use the **no** form of this command.

scrambling disable

no scrambling disable

Syntax Description

This command has no keywords or arguments.

Command Default

The default is enable (SONET payload scrambling is on).

Command Modes

SONET/SDH path configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

SONET payload scrambling applies a self-synchronous scrambler (x43+1) to the synchronous payload envelope (SPE) of the controller to ensure sufficient bit transition density. Both ends of the connection must be configured using SONET path scrambling.

If the hardware payload scrambling support is not user-configurable, or is not supported, the **scrambling disable** command may be rejected.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

In the following example, scrambling is disabled for the path:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/0/CPU0:router(config-sonet)# path
RP/0/0/CPU0:router(config-sonet-path)# scrambling disable
```

Related Commands

Command	Description
show controllers sonet, on page 711	Displays information about the operational status of SONET layers.

show aps

To display the operational status for all configured SONET automatic protection switching (APS) groups, use the **show aps** command in EXEC mode.

show aps

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **show aps** command to display operational status for all configured SONET APS groups.

Displaying the SONET APS operational data is considered of lower priority than the APS operation itself. Because the information is collected from several sources scattered across the various nodes involved, there is a small probability that some states will change while the command is being run.

The command should be reissued for confirmation before decisions are made based on the results displayed.

Task ID

Task ID	Operations
sonet-sdh	read

Examples

The following is sample output from the **show aps** command:

```
RP/0/0/CPU0:router# show aps

APS Group 1:
Protect ch 0 (SONET3_0):Enabled
    SONET framing, SONET signalling, bidirectional, revertive (300 sec)
    Rx K1:0x21 (Reverse Request - Working)
       K2:0x15 (bridging Working, 1+1, bidirectional)
    Tx K1:0x81 (Manual Switch - Working)
       K2:0x15 (bridging Working, 1+1, bidirectional)
  Working ch 1 (SONET2_0):Disabled
    Rx K1:0x00 (No Request - Null)
       K2:0x00 (bridging Null, 1+1, non-aps)
    Tx K1:0x00 (No Request - Null)
       K2:0x00 (bridging Null, 1+1, non-aps)
```

```
APS Group 3:
PGP:protocol version: native 2 adopted 2
  PGP:Authentication "cisco", hello timeout 1 sec, hold timeout 3 sec
Protect ch 0 (SONET3_1):Disabled
    SONET framing, SONET signalling, bidirectional, non-revertive
    Rx K1:0x00 (No Request - Null)
       K2:0x05 (bridging Null, 1+1, bidirectional)
    Tx K1:0x00 (No Request - Null)
       K2:0x05 (bridging Null, 1+1, bidirectional)
  Working ch 1 (192.168.1.1):Enabled
APS Group 49:
  Protect ch 0 (SONET0_2_0_0):Disabled
    SONET framing, SONET signalling, unidirectional, non-revertive
    Rx K1:0x00 (No Request - Null)
       K2:0x00 (bridging Null, 1+1, non-aps)
    Tx K1:0x00 (No Request - Null)
       K2:0x04 (bridging Null, 1+1, unidirectional)
  Working ch 1 (SONET0_2_0_1):Enabled
    SONET framing, unidirectional
    Rx K1:0x00 (No Request - Null)
       K2:0x00 (bridging Null, 1+1, non-aps)
    Tx K1:0x00 (No Request - Null)
       K2:0x00 (bridging Null, 1+1, non-aps)
APS Group 6:
PGP:protocol version: native 2 adopted 2
PGP:Authentication "cisco", hello timeout 1 sec, hold timeout 3 sec
  Protect ch 0 (192.168.3.2 - auto):Disabled
  Working ch 1 (SONET6_0):Enabled
    Rx K1:0x00 (No Request - Null)
       K2:0x00 (bridging Null, 1+1, non-aps)
    Tx K1:0x00 (No Request - Null)
       K2:0x00 (bridging Null, 1+1, non-aps)
```

Table 42: show aps Field Descriptions

Field	Description
APS Group	Assigned number of the APS group. Range is from 1 through 255.
Protect ch	Number and address of the protect channel interface.
Working ch	Number and address of the working channel interface.

Related Commands

Command	Description
show aps agents, on page 700	Displays the status of the APS WP distributed communication subsystem.
show aps group, on page 702	Displays information about the APS groups.

show aps agents

To display the status of the automatic protection switching (APS) working to protect (WP) distributed communication subsystem, use the **show aps agents** command in EXEC mode.

show aps agents

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **show aps agents** command to display the status of the APS WP distributed communication subsystem.

The WP communication is critical for the APS functionality. The **show aps agents** command is typically used as a debugging aid for unexpected or unusual APS operation.

Displaying the APS operational data is considered of lower priority than the APS operation itself. Because the information is collected from several sources scattered across the various nodes involved, there is a small probability that some states will change while the command is being run.

The command should be reissued for confirmation before decisions are made based on the results displayed.

Task ID

Task ID	Operations
sonet-sdh	read

Examples

The following is sample output from the **show aps agents** command:

```
RP/0/0/CPU0:router# show aps agents

SONET APS Manager working-Protect (WP) connections:
Remote peer (192.168.3.2 - auto) is up:
  Group 6   [P.Ch0] 192.168.3.2 === Manager --- SONET6_0 (node6) --- [W.Ch1]
Remote peer (10.1.1.1) is up:
  Group 3   [W.Ch1] 192.168.1.1 === Manager --- SONET3_1 (node3) --- [P.Ch0]
Local agent (node2) is up:
  Group 1   [W.Ch1] --- SONET2_0 --- SONET3_0 (node3) --- [P.Ch0]
Local agent (node3) is up:
  Group 1   [P.Ch0] --- SONET3_0 --- SONET2_0 (node2) --- [W.Ch1]
```

```
  Group 3   [P.Ch0] --- SONET3_1 --- Manager === 192.168.1.1 [W.Ch1]
  Group 5   [P.Ch0] --- SONET3_2 --- SONET3_3 (node3) --- [W.Ch1]
  Group 5   [W.Ch1] --- SONET3_3 --- SONET3_2 (node3) --- [P.Ch0]
Local agent (node6) is up:
  Group 6   [W.Ch1] --- SONET6_0 --- Manager === 192.168.3.2 [P.Ch0]
```

Table 43: show aps agents Field Descriptions

Field	Description
Remote peer	IP address of the remote Protect Group Protocol (PGP) peer for the working router in an APS group. An IP address of 0.0.0.0 indicates a dynamically discovered PGP peer not yet contacted, shown on working routers only. (The protect router contacts the working router.)
Local agent	Node name of the local agent, such as (node2).
Group	The interface location or IP address of the SONET APS group. Internal WP communication channel segments are represented as "---" if the segment is operational or "-/-" if the connection is broken. PGP segments are represented as "===" if operational or "==" if broken.

Related Commands

Command	Description
show aps, on page 698	Displays the operational status for all configured SONET APS groups.

show aps group

To display information about the automatic protection switching (APS) groups, use the **show aps group** command in EXEC mode.

show aps group [*number*]

Syntax Description

number	(Optional) The assigned group number.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

The **show aps group** command displays information about APS groups, and is useful if multiple APS groups are configured.

Displaying the APS operational data is considered of lower priority than the APS operation itself. Because the information is collected from several sources scattered across the various nodes involved, there is a small probability that some states will change while the command is being run.

The command should be reissued for confirmation before decisions are made based on the results displayed.

Task ID

Task ID	Operations
sonet-sdh	read

Examples

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

```
RP/0/0/CPU0:router# show aps group 3

APS Group 3:
  PGP:Authentication "cisco", hello timeout 1 sec, hold timeout 3 sec
  Protect ch 0 (SONET3_1):Admin Down, Disabled
    SONET framing, SONET signalling, bidirectional, non-revertive
    Rx K1:0x00 (No Request - Null)
       K2:0x05 (bridging Null, 1+1, bidirectional)
    Tx K1:0x00 (No Request - Null)
       K2:0x05 (bridging Null, 1+1, bidirectional)
```

```
Working ch 1 (192.168.1.1):Admin Down, Enabled
```

Table 44: show aps group Field Descriptions

Field	Description
APS Group	Group number assigned to the displayed APS group. For each channel in the group, the following information is displayed: • Authentication string • Hello timer value • Hold timer value • Role of the channel (working or protect) • Channel number • Name of the assigned physical port • Channel status (Enabled, Disabled, Admin Down, Signal Fail, Signal Degraded, or Not Contacted) • Group-related information (for protect channels only) that includes: ◦ Framing of the SONET port ◦ Kilobytes signaling protocol ◦ Unidirectional or bidirectional APS mode ◦ APS revert time, in seconds (in revertive operation mode only)
Rx	Received error signaling bytes and their APS decoded information.
Tx	Sent error signaling bytes and their APS decoded information.
Working ch	IP address of the corresponding Protect Group Protocol (PGP) peer.

The information displayed for the channels local to the routers is identical to the channel information displayed for single-router APS groups.

Related Commands

Command	Description
show aps, on page 698	Displays the operational status for all configured SONET APS groups.
show aps agents, on page 700	Displays the status of the APS WP distributed communication subsystem.

show controllers pos

To display information on the Packet-over-SONET/SDH (POS) controllers, use the **show controllers pos** command in EXEC mode.

show controllers pos *interface-path-id* [**all**| **framer** {**internal**| **register**| **statistics**}| **internal**] [**begin line**| **exclude line**| **file filename**| **include line**]

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
all	(Optional) Displays information for all POS interface controllers.
framer	(Optional) Displays all POS framer information.
internal	(Optional) Displays all POS internal information.
register	(Optional) Displays the POS framer registers.
statistics	(Optional) Displays the POS framer cumulative counters.
begin line	(Optional) Displays information beginning with the line that includes the regular expression given by the *line* argument.
exclude line	(Optional) Displays information excluding all lines that contain regular expressions that match the *line* argument.
file *filename*	(Optional) Saves the configuration to the designated file. For more information on which standard filenames are recognized, use the question mark (?) online help function.
include *line*	(Optional) Displays only those lines that contain the regular expression given by the *line* argument.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.
- If specifying a virtual interface, the number range varies, depending on interface type.

The information displayed is generally useful for diagnostic tasks performed by technical support personnel only.

Task ID

Task ID	Operations
interface	read

Examples

The following is sample output from the **show controllers pos** command:

```
RP/0/0/CPU0:router# show controllers POS 0/3/0/2

Port Number         : 2
Interface           : POS0/3/0/2
Ifhandle            : 0x1380120
CRC                 : 32
MTU                 : 4474
Port Bandwidth Kbps : 2488320
Admin state         : Up
Driver Link state   : Up


Bundle member       : No
Bundle MTU          : 4474
Bundle Adminstate   : Up
```

The following is sample output from the **show controllers pos all** command:

```
RP/0/0/CPU0:router# show controllers POS 0/3/0/2 all

Port Number         : 2
Interface           : POS0/3/0/2
Ifhandle            : 0x1380120
CRC                 : 32
MTU                 : 4474
Port Bandwidth Kbps : 2488320
Admin state         : Up
Driver Link state   : Up


Bundle member       : No
Bundle MTU          : 4474
```

```
Bundle Adminstate   : Up


POS Driver Internal Cooked Stats Values for port 2
==================================================
Rx Statistics                   Tx Statistics
-------------                   -------------
Total Bytes:    1200            Total Bytes:    0
Good Bytes:     1200            Good Bytes:     0
Good Packets:   25              Good Packets:   0
Aborts:         0               Aborts:         0
FCS Errors:     0               Min-len errors: 0
Runts:          0               Max-len errors: 0
FIFO Overflows: 0               FIFO Underruns: 0
Giants:         0
Drops:          0


Sky4402 asic #2 registers:


0x000 general_cntrl               0x00
0x002 sys_intf_cntrl_1            0x06
0x003 sys_intf_cntrl_2            0x00
0x004 JTAG3                       0x10
0x005 JTAG2                       0x10
0x006 JTAG1                       0x10
0x007 JTAG0                       0x2f
0x010 active_led                  0x01
0x011 gpio_port_mode              0x01
0x012 gpio_port_fault             0x00
0x013 gpio_port_data              0x58
0x015 gpio_port_cntrl             0x3f
0x017 gpio_port_transition        0x00
0x019 gpio_port_intr_mask         0xff
0x01b gpio_port_intr              0x3f
0x01c master_intr_status          0x00
0x01d master_mask                 0x00
0x020 interrupt_4                 0x04
0x021 interrupt_3                 0x00
0x022 interrupt_2                 0x00
0x023 interrupt_1                 0x00
0x024 status_4                    0x04
0x025 status_3                    0x00
0x026 status_2                    0x0c
0x027 status_1                    0x80
0x028 mask_4                      0x07
0x029 mask_3                      0x03
0x02a mask_2                      0x1c
0x02b mask_1                      0x8f
0x02d link_state_cntrl            0x80
0x041 diag                        0x00
0x042 stcks                       0x03
0x043 short_frame_cntrl           0x00
0x0c0 ror_ram_c2                  0x16
0x0c1 ror_ram_g1                  0x00
0x0c2 ror_ram_f2                  0x00
0x0c3 ror_ram_h4                  0x00
0x0c4 ror_ram_z3                  0x00
0x0c5 ror_ram_z4                  0x00
0x0c6 ror_ram_z5                  0x00
0x0c7 ror_ram_db_c2               0x16
0x0c8 ror_ram_db_g1               0x00
0x142 tor_ram_c2                  0x16
0x143 tor_ram_g1                  0x00
0x144 tor_ram_f2                  0x00
0x145 tor_ram_h4                  0x00
0x146 tor_ram_z3                  0x00
0x147 tor_ram_z4                  0x00
0x148 tor_ram_z5                  0x00
0x170 tor_ram_s1                  0x00
0x171 tor_ram_e2                  0x00
```

```
0x172 tor_ram_e1                  0x00
0x173 tor_ram_f1                  0x00
0x174 tor_ram_k1                  0x00
0x175 tor_ram_k2                  0x00
0x177 tor_ram_z2                  0x00
0x180 rsp_cntrl_1                 0x00
0x181 rsp_cntrl_2                 0x02
0x184 rtop_f1_ovrhd               0x00
0x185 rtop_k1_ovrhd               0x00
0x186 rtop_k2_ovrhd               0x00
0x187 rtop_s1_ovrhd               0x00
0x188 rtop_e1_ovrhd               0x00
0x189 rtop_e2_ovrhd               0x00
0x18a rtop_deb_s1_ovrhd           0x00
0x18c rtop_b1_mismatch_cnt_u      0x00
0x18d rtop_b1_mismatch_cnt_l      0x00
0x190 rtop_b2_mismatch_cnt_u      0x00
0x191 rtop_b2_mismatch_cnt_l      0x00
0x194 rtop_rei_l_cnt_u            0x00
0x195 rtop_rei_l_cnt_l            0x00
0x198 rtop_ber_thresh_u           0x00
0x199 rtop_ber_thresh_l           0x00
0x19a rtop_ber_leak_u             0x00
0x19b rtop_ber_leak_l             0x00
0x19c rtop_ber_delay_u            0x00
0x19d rtop_ber_delay_l            0x00
0x1c0 rpop_signal_lbl_c2          0x16
0x1c2 rpop_valid_ptr_u            0x02
0x1c3 rpop_valid_ptr_l            0x0a
0x1c4 rpop_b3_mismatch_cnt_u      0x00
0x1c5 rpop_b3_mismatch_cnt_l      0x00
0x1c8 rpop_rei_p_cnt_u            0x00
0x1c9 rpop_rei_p_cnt_l            0x00
0x1cc rpop_ber_thresh_u           0x00
0x1cd rpop_ber_thresh_l           0x00
0x1ce rpop_ber_leak_u             0x00
0x1cf rpop_ber_leak_l             0x00
0x1d0 rpop_ber_delay_u            0x00
0x1d1 rpop_ber_delay_l            0x00
0x200 rpp_cntrl_1                 0x11
0x201 rpp_cntrl_2                 0x03
0x202 rpp_cntrl_3                 0x3e
0x203 rpp_cntrl_4                 0x00
0x204 rpp_cntrl_5                 0x00
0x208 rpp_max_pkt_len_u           0x08
0x209 rpp_max_pkt_len_l           0xbd
0x20a rpp_min_pkt_len             0x04
0x244 tpp_inter_pkt_u             0x00
0x245 tpp_inter_pkt_l             0x00
0x246 tpp_idle_cell_hdr           0x00
0x247 tpp_idle_cell_filldata      0x00
0x248 tpp_cntrl                   0x04
0x280 tpog_cntrl                  0x20
0x2c0 ttog_cntrl                  0x00
0x2c2 ttog_ovrhd_src_1            0x00
0x2c3 ttog_ovrhd_src_2            0x00
0x2c9 ttog_ovrhd_fill             0x00
```

Table 45: show controllers pos Field Descriptions

Field	Description
Cisco POS ASIC Register Dump (Receive)	Header for display of the contents of the receive ASIC1 register log.
asic mode	Address in hex of the ASIC mode flag.

Field	Description
error source	Address in hex of the error source flag.
error mask	Address in hex of the error mask flag.
error detail 1	Address in hex of the error detail 1 flag.
error detail 2	Address in hex of the error detail 2 flag.
rx offset	Address in hex of the receive offset.
Channel Modes	Location in hex of the channel mode flag.
Port 0:	Port 0 (the first port) statistics display.
Port 1:	Port 1 (the second port) statistics display.
Port 2:	Port 2 (the third port) statistics display.
Port 3:	Port 3 (the fourth port) statistics display.
Runt Threshold	Limit in packets set for runts on the specified port.
Tx Delay	Transmit delay that has been set for the specified port.
Cisco POS ASIC Register Dump (Transmit)	Header for display of the contents of the transmit ASIC register log.
POS Driver Internal Cooked Stats Values for port 0	Statistics relating to the specified POS port (POS port 0).
Rx Statistics	Receive statistics for the indicated POS port.
Total Bytes	Total number of bytes, including data and MAC encapsulation, received by the system.
Good Bytes	Number of bytes received without errors.
Good Packets	Number of packets received without errors.
Aborts	Number of receive bytes that have been aborted
FCS Errors	Number of FCS2 errors that have been received.
Runts	Number of received packets that are discarded because they are smaller than the minimum packet size of the medium.
FIFO Overflows	Number of received packets that exceeded the FIFO stack limit.

Field	Description
Giants	Number of received packets that are discarded because they exceed the maximum packet size of the medium.
Drops	Number of received packets that have been dropped from the system.
Tx Statistics	Transmit statistics for the indicated POS port.
Total Bytes	Total number of bytes, including data and MAC encapsulation, sent by the system.
Good Bytes	Number of bytes sent without errors.
Good Packets	Number of packets sent without errors.
Aborts	Number of sent bytes that have been aborted.
Min-len errors	Minimum queue length violations.
Max-len errors	Maximum queue length violations.
FIFO Underruns	First-in, first-out, a buffering scheme where the first byte of data entering the buffer is the first byte retrieved by the CPU. FIFO underruns reports the number of times that the transmitter has been running faster than the router can handle.

[1] [2]

1 1. application-specific integrated circuit
2 2. frame check sequence

show controllers sonet

To display information about the operational status of SONET layers, use the **show controllers sonet** command in EXEC mode.

show controllers sonet *interface-path-id* {**all**| **framers**| **internal-state**}

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
all	Displays all information.
framers	Displays framer information.
internal-state	Displays internal SONET state.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.
- If specifying a virtual interface, the number range varies, depending on interface type.

Use the **show controllers sonet** command to display information about the operational status of SONET layers on a particular SONET port.

If the manageability PIE is not installed, you can use the **show controllers sonet** command to display the counters for the current 15 minutes only without history data. However, the SONET MIB is still available but is limited to the current bucket of data. History data is still available only when the manageability PIE is loaded. The **show controllers sonet** command is available at any time to display current data, and history data is stored in the line card rather in the history bucket.

Task ID

Task ID	Operations
interface	read

Examples

The following is sample output from the **show controllers sonet** command:

```
RP/0/0/CPU0:router# show controllers sonet 0/1/2/1

Port SONET0/1/2/1:

Status: Up

Loopback: None

SECTION
  LOF = 0          LOS    = 0                            BIP(B1) = 0
LINE
  AIS = 0          RDI    = 1          FEBE = 0          BIP(B2) = 0
PATH
  AIS = 0          RDI    = 0          FEBE = 0          BIP(B3) = 0
  LOP = 0          NEWPTR = 0          PSE  = 0          NSE     = 0
  PLM = 0          TIM    = 0

Line delays trigger:      0 ms clear:  10000 ms
Path delays trigger:      0 ms clear:  10000 ms
Last clearing of "show controllers SONET" counters never

Detected Alarms: None
Asserted Alarms: None
Mask for Detected->Asserted: None
Detected Alerts: None
Reported Alerts: None
Mask for Detected->Reported: None
Alarm reporting enabled for: SLOS SLOF SF_BER PLOP
Alert reporting enabled for: B1-TCA B2-TCA B3-TCA

Framing: SONET
SPE Scrambling: Enabled
C2 State: Stable   C2_rx = 0x16 (22)   C2_tx = 0x16 (22) / Scrambling Derived
S1S0(tx): 0x0  S1S0(rx): 0x0 / Framing Derived

PATH TRACE BUFFER : STABLE
  Remote hostname : P1_CRS-8
  Remote interface: POS0/1/4/0
  Remote IP addr  : 0.0.0.0

APS
No APS Group Configured
  Protect  Channel 0   DISABLED
  Rx(K1/K2) : 0x00/0x00
  Tx(K1/K2) : 0x00/0x00
  Remote Rx(K1/K2): 01/0   Remote Tx(K1/K2): 01/0
```

```
BER thresholds:  SF = 10e-3  SD = 10e-6
TCA thresholds:  B1 = 10e-6  B2 = 10e-6  B3 = 10e-6

  Optics type: OC48 SR/STM16 I-16
  Clock source: internal (actual) internal (configured)
  Rx S1: 0xf  Tx S1: 0x50

Optical Power Monitoring (accuracy: +/- 1dB)
  Rx power = 0.3162 mW, -5.0 dBm
  Tx power = 0.2883 mW, -5.4 dBm
  Tx laser current bias = 17.2 mA
```

Table 46: show controllers sonet Field Descriptions

Field	Description
Port	Slot number of the POS interface.
Status	Displays whether the link associated with the specified port is up or down.
Loopback	Loopback identifier, if applicable.
LOF	Section loss of frame is detected when a severely error-framing (SEF) defect on the incoming SONET signal persists for 3 milliseconds.
LOS	Section loss of signal is detected when an all-zeros pattern on the incoming SONET signal lasts 19(+-3) microseconds or longer. This defect might also be reported if the received signal level drops below the specified threshold.
BIP	Bit interleaved parity error reported. • For B1, the bit interleaved parity error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B1 byte of the following frame. Differences indicate that section-level bit errors have occurred. • For B2, the bit interleaved parity error report is calculated by comparing the BIP-8/24 code with the BIP-8 code extracted from the B2 byte of the following frame. Differences indicate that line-level bit errors have occurred. • For B3, the bit interleaved parity error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B3 byte of the following frame. Differences indicate that path-level bit errors have occurred.

Field	Description
AIS	Alarm indication signal. • Line alarm indication signal is sent by the STE1 to alert the downstream LTE2 that a LOS or LOF defect has been detected on the incoming SONET section. • Path alarm indication signal is sent by the LTE to alert the downstream PTE3 that it has detected a defect on its incoming line signal.
RDI	Remote defect indication. • Line remote defect indication is reported by the downstream LTE when it detects LOF4, LOS5, or AIS6. • Path remote defect indication is reported by the downstream PTE when it detects a defect on the incoming signal.
FEBE	Far-end block errors. • Line far-end block error (accumulated from the M0 or M1 byte) is reported when the downstream LTE detects BIP7 (B2) errors. • Path far-end block error (accumulated from the G1 byte) is reported when the downstream PTE detects BIP (B3) errors.
LOP	Path loss of pointer is reported as a result of an invalid pointer (H1, H2) or an excess number of NDF8 enabled indications.
NEWPTR	Inexact count of the number of times the SONET framer has validated a new SONET pointer value (H1, H2).
PSE	Inexact count of the number of times the SONET framer has detected a positive stuff event in the received pointer (H1, H2).
NSE	Inexact count of the number of times the SONET framer has detected a negative stuff event in the received pointer (H1, H2).
PLM	Payload label mismatch. A different payload-specific functionality than the provisioned functionality is reported. For example, 02 to E0, or FD to FE.

Field	Description
TIM	Trace identifier mismatch. Reported TIM defects that occur primarily as a result of provisioning errors; for example, incorrect cross-connections in the network.
Line delays trigger	Line triggers delayed and cleared, in milliseconds.
Path delays trigger	Path triggers delayed and cleared, in milliseconds.
Last clearing of "show controllers SONET" counters	When the counters associated with the **show controllers sonet** command were last cleared.
Detected/Asserted Alarms	Any alarms detected by the controller are displayed here. Alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver is getting AIS. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms.
Mask for Detected -> Asserted	Masked alarms for the asserted alarm. For example, when SLOS is asserted, all low-level alarms are masked and are listed in this section of the output.
Detected Alerts	List of alerts that are detected.
Reported Alerts	List of reported alerts, such as B1-TCA B2-TCA B3-TCA, sent to the application layer.
Mask for Detected -> Reported	List of masked alerts for asserted alarms that are reported.
Alarm reporting enabled for	Types of alarms that generate an alarm message.
Alert reporting enabled for	Types of alarms that generate an alert message.
Framing	Type of framing enabled on the controller.
SPE Scrambling	Status of synchronous payload envelope (SPE) scrambling: Enabled, Disabled.
C2 State	Value extracted from the SONET path signal label byte (C2).

Field	Description
S1S0(tx)	Two S bits received in the last H1 byte.
PATH TRACE BUFFER	SONET path trace buffer is used to communicate information regarding the remote hostname, interface name/number, and IP address. This use of the J1 (path trace) byte is proprietary to Cisco.
Remote hostname	Name of the remote host.
Remote interface	Interface of the remote host.
Remote IP addr	IP address of the remote host.
APS	Configuration status of the APS feature
APS Group	Indicates whether or not an APS group is configured.
Protect Channel 0	Indicates whether or not channel 0 is protected.
Rx(K1/K2)/Tx(K1/K2)	Contents of the received and transmitted K1 and K2 bytes at the local end in an APS configuration.
Remote Rx(K1/K2)/Tx(K1/K2)	Contents of the received and transmitted K1 and K2 bytes at the remote end in an APS configuration.
BER thresholds	List of the bit error rate (BER) thresholds you configured with the **threshold** (SONET) command.
TCA thresholds	List of threshold crossing alarms (TCA) you configured with the **threshold** (SONET) command.
Optics type	Type of small form-factor pluggable (SFP) used in the associated port.
Tx laser current bias	Measured laser bias current, in milliamps (mA). The valid range is 0 through 131 mA.
Clock source	Actual and configured clock source.
Optical Power Monitoring	Power status of the SONET controller.
Tx laser current bias	Current information, in milliamps (mA), in the transmit direction.

[3] [4] [5] [6] [7] [8] [9] [10] [11]

The following is sample output from the **show controllers sonet** command with the **framers** option:

```
RP/0/0/CPU0:router# show controllers sonet 0/1/2/1 framers

Common Regs
 reg[0]                Master Reset and Identity 0x01
 reg[1]                              Master Cfg 0000
 reg[3]                  Master Clock Monitors 0x37
 reg[100]                   Master Intr Status 1 0000
 reg[101]                Master Intr Status Ch 0-7 0000
 reg[102]               Master Intr Status Ch 8-15 0000
 reg[1000]                  Master Clock Source Cfg 0000
 reg[1001]               Master DCC Interface Cfg 1 0x0f
 reg[1002]               Master DCC Interface Cfg 2 0000
 reg[1004]                       APS Cfg and Status 0000
 reg[1005]                  APS FIFO Cfg and Status 0x0f
 reg[1006]                        APS Intr Status 1 0000
 reg[1007]                        APS Intr Status 2 0000
 reg[1008]                           APS Reset Ctrl 0000
 reg[1010]                      TUL3 Interface Cfg 0x80
 reg[1011]                TUL3 Intr Status/Enable 1 0000
 reg[1012]                TUL3 Intr Status/Enable 2 0000
 reg[1013]                TUL3 ATM Level 3 FIFO Cfg 0x03
 reg[1014]            TUL3 ATM Level 3 Signal Label 0x01
 reg[1015]     TUL3 POS Level 3 FIFO Low Water Mark 0x15
 reg[1016]    TUL3 POS Level 3 FIFO High Water Mark 0x17
 reg[1017]            TUL3 POS Level 3 Signal Label 0000
 reg[1018]                                TUL3 burst 0x0f
--More--
```

The following is sample output from the **show controllers sonet** command with the **internal-state** keyword:

```
RP/0/0/CPU0:router# show controllers sonet 0/1/2/1 internal-state

Interface(layer)      admin_up if_state
--------------------- -------- --------

SONET0/1/2/1          up       up
(SONET Section)       up       up
(SONET Line)          up       up
(SONET Path)          up       up
 SonetPath0/1/2/1     up       up
  POS0/1/2/1          up       up
```

Table 47: show controllers sonet Field Descriptions

Field	Description
Interface (layer)	Slot number of the POS interface.

[3] 1. section terminating equipment
[4] 2. line terminating equipment
[5] 3. path terminating equipment
[6] 4. loss of frame
[7] 5. loss of synchronization
[8] 6. alarm indication signal
[9] 7. bit interleaved parity
[10] 8. new data flag
[11]

Field	Description
admin_up	Whether the interface and its associated layers are in the admin-up state.
if_state	Whether the interface and its associated layers are in the up or down state.

show sonet-local trace frr

To display the alarms associated with Fast Re-Route (FRR) for all nodes or for a specific node, use the **show sonet-local trace frr** command in EXEC mode.

show sonet-local trace frr location *node-id*

Syntax Description

location *node-id*	Full path location of the node. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

Displays the FRR alarms for all nodes on the router.

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
cisco-support	read

Examples

The following example shows how to display the FRR alarms for a specific node:

```
RP/0/0/CPU0:router# show sonet-local trace frr location 0/1/0/0
```

The following example shows how to display the FRR alarms for all nodes on the router:

```
RP/0/0/CPU0:router# show sonet-local trace frr
```

Related Commands

Command	Description
show controllers sonet, on page 711	Displays information about the operational status of SONET layers.

shutdown (SONET)

To disable SONET controller processing, use the **shutdown** command in SONET/SDH configuration mode. To bring back up a SONET controller and enable SONET controller processing, use the **no form of this** command.

shutdown

no shutdown

Syntax Description

This command has no keywords or arguments.

Command Default

The SONET controller is up, and SONET controller processing is enabled.

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **shutdown** command to shut down a SONET controller and disable SONET controller processing. Use the **no shutdown** command to bring back up a SONET controller and enable SONET controller processing.

The SONET controller must be brought up for the proper operation of the Layer 2 interface. The Layer 2 interface has a separate **shutdown** command available, which does not operate on the SONET controller's administrative state.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to bring down the SONET controller and disable SONET controller processing:

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/2
RP/0/0/CPU0:router(config-sonet)# shutdown
```

Related Commands

Command	Description
show controllers sonet, on page 711	Displays information about the operational status of SONET layers.

signalling

To configure the K1K2 overhead byte signaling protocol used for automatic protection switching (APS), use the **signalling** command in APS group configuration mode. To reset APS signaling to the default, use the **no** form of this command.

signalling {**sonet**| **sdh**}

no signalling {**sonet**| **sdh**}

Syntax Description

sonet	Sets signaling to SONET.
sdh	Sets signaling to Synchronous Digital Hierarchy (SDH).

Command Default

SONET signaling is set by default.

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

By default, APS uses the signaling mode matching the framing mode. The **signalling** command may be required, depending upon the transport equipment capabilities, only on “transition” links interconnecting SONET and SDH networks.

In a multirouter APS topology, the **signalling** command is allowed only on the protect router.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to reset the signaling protocol from the default SONET value to SDH:

```
RP/0/0/CPU0:router(config)# aps group 1

RP/0/0/CPU0:router(config-aps)# signalling sdh
```

The following example sets the signaling to SONET:

```
RP/0/0/CPU0:router(config)# aps group 1
RP/0/0/CPU0:router(config-aps)# signalling sonet
```

Related Commands

Command	Description
aps group (global), on page 649	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
show aps group, on page 702	Displays information about the APS groups.

sts

To specify the Synchronous Transport Signal (STS) path and enter the STS controller configuration mode, use the **sts** command in SONET controller configuration mode.

sts *number*

Syntax Description

number	STS path number. The range varies by the type of line card.

Command Default

No default behavior or values

Command Modes

SONET controller configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to specify STS 1:

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/0/CPU0:router(config-sonet)# sts 1
RP/0/0/CPU0:router(config-stsPath)#
```

Related Commands

Command	Description
au, on page 651	Specifies the administrative unit (AU) group number and enters the AU controller configuration mode.

timers (APS)

To change the time between hello packets and the time before the protect interface process declares a working interface router to be down, use the **timers** command in APS group configuration mode. To return to the default timers, use the **no** form of this command.

timers *hello-seconds hold-seconds*

no timers

Syntax Description

hello-seconds	Number of seconds to wait before sending a hello packet (hello timer). Range is from 1 through 255 seconds. Default is 1 second.
hold-seconds	Number of seconds to wait to receive a response from a hello packet before the interface is declared down (hold timer). Range is from 1 through 255 seconds. Default is 3 seconds.

Command Default

hello-seconds: 1

hold-seconds: 3

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **timers** command to change the time between hello packets and the time before the protect interface process declares a working interface router to be down.

The hello time, in seconds, represents the interval between the periodic message exchange between the Protect Group Protocol (PGP) peers. The hold time, in seconds, represents the interval starting with the first failed periodic message after which, if no successful exchange takes place, the PGP link is declared dead.

If many multirouter APS groups are configured and the CPU load or the User Datagram Protocol (UDP) traffic associated with the PGP communication is considered too high, then the hello interval should be increased.

Increasing the hold time is suggested if the PGP link is flapping. The possible causes include high route processor (RP) CPU load, high traffic, or high error rates on the links between the working and the protect routers.

We recommend that you have a hold time at least three times longer than the hello time (allowing three or more consecutive failed periodic message exchange failures).

The **timers** command is typically used only on the protect router. After the PGP connection is established, the working router learns about the timer settings from the protect router and automatically adjusts accordingly, regardless of its own timer configuration.

The **timers** command is meaningful only in multirouter automatic protection switching (APS) topologies and is ignored otherwise.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to configure APS group 3 with the hello timer at *2* seconds and the hold timer at 6 seconds:

```
RP/0/0/CPU0:router(config)# aps group 3
RP/0/0/CPU0:router(config-aps)# timers 2 6
```

Related Commands

Command	Description
aps group (global), on page 649	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
show aps group, on page 702	Displays information about the APS groups.

threshold (SONET)

To set the bit error rate (BER) threshold values of the specified alarms for a SONET controller, use the **threshold** command in SONET/SDH configuration mode. To remove the setting of the threshold from the configuration file and restore the default condition, use the **no** form of this command.

threshold {**b1-tca**| **b2-tca**| **sd-ber**| **sf-ber**} *bit-error-rate*

no threshold {**b1-tca**| **b2-tca**| **sd-ber**| **sf-ber**} *bit-error-rate*

Syntax Description

b1-tca	Sets the B1 BER threshold crossing alarm (TCA). Range is from 3 through 9. Default is 10e-6.
b2-tca	Sets the B2 BER threshold crossing alarm (TCA). Range is from 3 through 9. Default is 10e-6.
sd-ber	Sets the signal degrade BER threshold. Range is from 3 through 9. Default is 10e-6.
sf-ber	Sets the signal failure BER threshold. Range is from 3 through 9. Default is 10e-3.
bit-error-rate	BER from 3 to 9 (10 to the minus *x*).

Command Default

b1-tca: 10e-6

b2-tca: 10e-6

sd-ber: 10e-6

sf-ber: 10e-3

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

For B1, the bit interleaved parity (BIP) error report is calculated by comparing the BIP-8 code with the BIP-8 code that is extracted from the B1 byte of the following frame. Differences indicate that section-level bit errors have occurred.

For B2, the BIP error report is calculated by comparing the BIP-8/24 code with the BIP-8 code that is extracted from the B2 byte of the following frame. Differences indicate that line-level bit errors have occurred.

Signal failure BER and signal degrade BER are sourced from B2 BIP-8 error counts (as is B2-TCA). The **b1-tca** and **b2-tca** keywords print only a log message to the console (if reports for them are enabled).

To determine the BER thresholds configured on the controller, use the **show controllers sonet** command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to configure thresholds on the SONET controller:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/0/CPU0:router(config-sonet)# threshold sd-ber 8
RP/0/0/CPU0:router(config-sonet)# threshold sf-ber 4
RP/0/0/CPU0:router(config-sonet)# threshold b1-tca 4
```

Related Commands

Command	Description
report (SONET), on page 690	Permits selected SONET alarms to be logged to the console for a SONET controller.
show controllers sonet, on page 711	Displays information about the operational status of SONET layers.

threshold (SONET path)

To set the bit error rate (BER) threshold values of the specified alarms for a SONET path, use the **threshold** command in SONET/SDH path configuration mode. To remove the setting of the SONET path threshold from the configuration file and restore the default condition, use the **no** form of this command.

threshold b3-tca *bit-error-rate*

no threshold b3-tca *bit-error-rate*

Syntax Description

b3-tca	Sets the B3 BER threshold crossing alarm (TCA). Default is 6.
bit-error-rate	BER from 3 to 9 (10 to the minus *x*).

Command Default

b3-tca: 6

Command Modes

SONET/SDH path configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

For B3, the bit interleaved parity (BIP) error report is calculated by comparing the BIP-8 code with the BIP-8 code that is extracted from the B3 byte of the following frame. Differences indicate that path-level bit errors have occurred.

In addition to BIP errors detected at the local end in the receive direction, B3 error counts detected in the G1 byte (P-REI or P-FEBE) by the far-end SONET equipment are returned.

The **b3-tca** keyword prints only a log message to the console (if reports for them are enabled).

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

In the following example, the BER is set to 4:

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/1
RP/0/0/CPU0:router(config-sonet)# path
RP/0/0/CPU0:router(config-sonet-path)# threshold b3-tca 4
```

Related Commands

Command	Description
report (SONET), on page 690	Permits selected SONET alarms to be logged to the console for a SONET controller.
show controllers sonet, on page 711	Displays information about the operational status of SONET layers.

tug3

To specify the tributary unit group (TUG) number and enter the TUG3 controller configuration mode, use the **tug3** command in SONET controller configuration mode.

tug3 *number*

Syntax Description

number	The tributary unit group (TUG) number. The ranges are: • AU4—The only value is 1. • AU3—The range is 1 to 3.

Command Default

The default is 1.

Command Modes

SONET controller configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

The **tug3** command enables you to begin configuring the interface in the TUG3 controller configuration mode, where you can configure virtual containers (VCs) and DS3s:

STM1 -> AU4 -> TUG3 -> VC-3 -> DS3

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to specify tug3 1.

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/0/CPU0:router(config-sonet)# au 1
RP/0/0/CPU0:router(config-auPath)# tug3 1
RP/0/0/CPU0:router(config-tug3Path)#
```

Related Commands

Command	Description
au, on page 651	Specifies the administrative unit (AU) group number and enters the AU controller configuration mode.

uneq-shut (SONET path)

To enable automatic insertion of P-UNEQ code (0x00) in the sent SONET path overhead C2 byte, use the **uneq-shut** command in SONET/SDH path configuration mode. To disable this feature, use the **no** form of this command.

uneq-shut

no uneq-shut

Syntax Description

This command has no keywords or arguments.

Command Default

Automatic insertion is enabled.

Command Modes

SONET/SDH path configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **uneq-shut** command to disable automatic insertion of P-UNEQ code in the sent SONET path overhead C2 byte whenever the SONET path enters the administratively down state.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

In the following example, automatic insertion of P-UNEQ code is disabled in the sent SONET path overhead C2 byte:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/0/CPU0:router(config-sonet)# path
RP/0/0/CPU0:router(config-sonet-path)# uneq-shut
```

unidirectional

To configure a protect interface for unidirectional mode, use the **unidirectional** command in APS group configuration mode. To restore the default setting, bidirectional mode, use the **no** form of this command.

unidirectional

no unidirectional

Syntax Description

This command has no keywords or arguments.

Command Default

Bidirectional mode is the default mode for the protect interface.

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **unidirectional** command to configure a protect interface for unidirectional mode. Use the **no** form of this command to restore the default setting.

The unidirectional or bidirectional automatic protection switching (APS) operation mode of the routers should be matched with the APS operation mode of the connected SONET equipment.

Note We recommend using bidirectional APS mode when it is supported by the interconnecting SONET equipment. When the protect interface is configured as unidirectional, the working and protect interfaces must cooperate to switch the transmit and receive SONET channel in a bidirectional fashion. Cooperation occurs automatically when the SONET network equipment is in bidirectional mode.

In a multirouter APS topology, the **unidirectional** command is allowed only on the protect router.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to configure an APS group for unidirectional mode:

```
RP/0/0/CPU0:router(config)# aps group 1
```

```
RP/0/0/CPU0:router(config-aps)# unidirectional
```

Related Commands

Command	Description
aps group (global), on page 649	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
show aps, on page 698	Displays the operational status for all configured SONET APS groups.

width

To set the number of paths in a stream, use the **width** command in the STS or AU controller configuration mode.

width *number*

Syntax Description

number	Number of STS streams that are concatenated. The possible values are: • 1—Indicating one STS stream • 3—Indicating three STS streams (STS-3c) • 12—Indicating concatenation of 12 STS streams (STS-12c) • 48—Indicating concatenation of 48 STS streams (STS-48c) Widths 3, 12, and 48 are configured on STS paths at natural boundaries, which coincide with the following path numbers: • 1, 4, 7, 10, and so on, for STS-3c • 1, 13, 25, and 37 for STS-12c • 1 for STS-48c

Command Default

The default is 1.

Command Modes

SONET controller configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to specify a width of 3:

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/0/CPU0:router(config-sonet)# sts 1
RP/0/0/CPU0:router(config-stsPath)# width 3
```

Related Commands

Command	Description
mode (SONET), on page 680	Sets the mode of an STS path, AU path, T3 controller, or TUG3 controller.

T3, E3, T1, E1 Controller Commands on the Cisco IOS XR Software

This module provides command line interface (CLI) commands for configuring T3/E3 and T1/E1 controllers on the Cisco XR 12000 Series Router.

bert e1

To start or stop a configured bit error rate test (BERT) on an E1 controller or channel group, use the **bert e1** command in EXEC mode. To return to the default state, use the **no** form of this command.

bert e1 *interface-path-id* [**channel-group** *channel-group-number*] **[error]** {**start**| **stop**}

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
channel-group *channel-group-number*	(Optional) Channel group number. When an E1 data line is configured, channel group numbers can be values from 0 to 30. **Note** For any of the DS0 time slots within the time slot range provided for the channel group, use time slot -1 as the channel number.
error	(Optional) Injects errors into the running BERT stream.
start	Starts the BERT on the E1 controller or channel.
stop	Stops the BERT on the E1 controller or channel.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.6.0	The **error** keyword was added.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.

- *module*: Module number. A physical layer interface module (PLIM) is always 0.
- *port*: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

Note Before you can start a BERT on an E1 controller or channel group, you must configure a BERT pattern using the **bert pattern** command. If desired, you can also adjust the default setting (1 minute) of the BERT interval using the **bert interval** command. Both of these commands are available in E1 configuration mode and channel group configuration mode.

To view the BERT results, use the **show controllers e1** command in EXEC mode. The BERT results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BERT
- Total bit errors
- Total bits received

BERT is data intrusive. Regular data cannot flow on a line while the test is in progress. The line is put in an alarm state when a BERT is in progress and restored to a normal state after a BERT has been terminated.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to start and stop a BERT on an E1 controller:

```
RP/0/0/CPU0:router# bert e1 0/3/0/0 start
RP/0/0/CPU0:router# bert e1 0/3/0/0 stop
```

The following example shows how to inject errors into the BERT stream on an E1 controller:

```
RP/0/0/CPU0:router# bert e1 0/3/0/0 error
```

Related Commands

Command	Description
bert interval, on page 748	Specifies the duration of a bit error rate test (BERT) pattern on a T3/E3 or T1/E1 line.
bert pattern, on page 750	Enables a BERT pattern on a T3/E3 or T1/E1 line or an individual channel group.

Command	Description
show controllers e1, on page 822	Displays information about the E1 links and hardware and software drivers for the E1 controller.

bert e3

To start or stop a configured bit error rate test (BERT) on an E3 controller or channel group, use the **bert e3** command in EXEC mode. To return to the default state, use the **no** form of this command.

bert e3 *interface-path-id* **[error]** {**start**| **stop**}

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
error	(Optional) Injects errors into the running BERT stream.
start	Starts the BERT on the E3 controller or channel.
stop	Stops the BERT on the E3 controller or channel.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.
- If specifying a virtual interface, the number range varies, depending on interface type.

Note Before you can start a BERT on an E3 controller, you must configure a BERT pattern using the **bert pattern** command. If desired, you can also adjust the default setting (1 minute) of the BERT interval using the **bert interval** command. Both of these commands are available in E3 configuration mode.

To view the BERT results, use the **show controllers e3** command in EXEC mode. The BERT results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BERT
- Total bit errors
- Total bits received

BERT is data intrusive. Regular data cannot flow on a line while the test is in progress. The line is put in an alarm state when a BERT is in progress and restored to a normal state after a BERT has been terminated.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to start and stop a BERT on an E3 controller:

```
RP/0/0/CPU0:router# bert e3 0/3/0/0/0 start
RP/0/0/CPU0:router# bert e3 0/3/0/0/0 stop
```

The following example shows how to inject errors into the BERT stream on an E3 controller:

```
RP/0/0/CPU0:router# bert e3 0/3/0/0 error
```

Related Commands

Command	Description
bert interval, on page 748	Specifies the duration of a bit error rate test (BERT) pattern on a T3/E3 or T1/E1 line.
bert pattern, on page 750	Enables a BERT pattern on a T3/E3 or T1/E1 line or an individual channel group.
show controllers e3, on page 826	Displays information about the E3 links and hardware and software drivers for the E3 controller.

bert error

To insert errors into a BERT stream on a T3/E3 or T1/E1 line, use the **bert error** command in T3 or T1 configuration mode. To disable a BERT pattern, use the **no** form of this command.

bert error [*number*]

no bert error [*number*]

Syntax Description

number	Specifies the number of BERT errors to introduce into the bit stream. The range is from 1 to 255. The default is 1.

Command Default

The default is 1.

Command Modes

T3 configuration

E3 configuration

T1 configuration

E1 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

Use the **bert error** command with the **bert pattern** command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to insert 10 errors into the BERT bit stream on the T3 controller in slot 0, subslot 3:

```
RP/0/0/CPU0:router(config)# controller t3 0/0/3/1/10
RP/0/0/CPU0:router(config-t3e3)# bert error 10
```

Related Commands

Command	Description
bert interval, on page 748	Specifies the duration of a bit error rate test (BERT) pattern on a T3/E3 or T1/E1 line.
bert pattern, on page 750	Enables a BERT pattern on a T3/E3 or T1/E1 line or an individual channel group.
show controllers e1, on page 822	Displays information about the E1 links and hardware and software drivers for the E1 controller.
show controllers e3, on page 826	Displays information about the E3 links and hardware and software drivers for the E3 controller.
show controllers t1, on page 830	Displays information about the T1 links and hardware and software drivers for the T1 controller.
show controllers t3, on page 837	Displays information about the T3 links and hardware and software drivers for the T3 controller.

bert interval

To specify the duration of a bit error rate test (BERT) pattern on a T3/E3 or T1/E1 line, use the **bert interval** command in the appropriate configuration mode. To revert to the default interval, use the **no** form of this command.

bert interval *time*

no bert interval *time*

Syntax Description

time	Duration (in minutes) of the BERT. The interval can be a value from 1 to 14400. The default is 1 minute.

Command Default

A BERT runs for 1 minute.

Command Modes

T3 configuration

E3 configuration

T1 configuration

E1 configuration

Channel group configuration for T1 and E1

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

Use the **bert interval** command with the **bert pattern** command. If the **bert interval** command is not used, then the BERT runs for a default of 1 minute.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to limit the BERT to 10 minutes on the T3 controller in slot 0, subslot 3:

```
RP/0/0/CPU0:router(config)# controller t3 0/0/3/1/10
RP/0/0/CPU0:router(config-t3e3)# bert interval 10
```

Related Commands

Command	Description
bert error, on page 746	Insert errors into a BERT stream on a T3/E3 or T1/E1 line.
bert pattern, on page 750	Enables a BERT pattern on a T3/E3 or T1/E1 line or an individual channel group.
show controllers e1, on page 822	Displays information about the E1 links and hardware and software drivers for the E1 controller.
show controllers e3, on page 826	Displays information about the E3 links and hardware and software drivers for the E3 controller.
show controllers t1, on page 830	Displays information about the T1 links and hardware and software drivers for the T1 controller.
show controllers t3, on page 837	Displays information about the T3 links and hardware and software drivers for the T3 controller.

bert pattern

To enable a bit error rate test (BERT) pattern on a T3/E3 or T1/E1 line or an individual channel group, use the **bert pattern** command in T3, E3, T1, E1, or channel group configuration mode. To disable a BERT pattern, use the **no** form of this command.

bert pattern {**0s**| **1in8**| **1s**| **2^11**| **2^15**| **2^20**| **2^20-QRSS**| **2^23**| **2^9**| **3in24**| **55Daly**| **55Octet**| **alt-0-1**| **ds0-1**| **ds0-2**| **ds0-3**| **ds0-4**}

no bert pattern {**0s**| **1in8**| **1s**| **2^11**| **2^15**| **2^20**| **2^20-QRSS**| **2^23**| **2^9**| **3in24**| **55Daly**| **55Octet**| **alt-0-1**| **ds0-1**| **ds0-2**| **ds0-3**| **ds0-4**}

Syntax Description

0s	Invokes a repeating pattern of zeros (...000...).
1in8	(T1 and E1 only) Invokes a repeating pattern of one (1) bit in eight (8).
1s	Invokes a repeating pattern of ones (...111...).
2^11	(Channel group only) Invokes a pseudorandom O.151 test pattern that is 32,768 bits in length.
2^15	Invokes a pseudorandom O.151 test pattern that is 32,768 bits in length.
2^20	Invokes a pseudorandom O.153 test pattern that is 1,048,575 bits in length.
2^20-QRSS	Invokes a pseudorandom quasi-random signal sequence (QRSS) 0.151 test pattern that is 1,048,575 bits in length.
2^23	Invokes a pseudorandom O.151 test pattern that is 8,388,607 bits in length.
2^9	(Channel group only) Invokes a pseudorandom 0.153 test pattern of 511 bits in length.
3in24	(T1 and E1 only) Invokes a repeating pattern in which three (3) bits in twenty-four (24) are set to one (1) and the others are set to zero (0).
55Daly	(T1 and E1 only) Invokes a repeating pattern of fifty-five (55) 8-bit octets of data. This pattern introduces rapid transitions from long sequences of low-density octets to high-density octets, high-density octets to low-density octets, and rapid 1010 bit transitions.
55Octet	(T1 and E1 only) Invokes a repeating pattern of fifty-five (55) 8-bit octets of data. This pattern has fifteen (15) consecutive zeros.
alt-0-1	Invokes a repeating pattern of alternating zeros and ones (...01010...).
ds0-1	(Channel group only) Invokes a repeating sequence of 100x FFh, followed by 100x 00h. This combination of minimum and maximum densities causes stressing of the signal recovery circuitry.

ds0-2	(Channel group only) Invokes a repeating sequence of 100x 7Eh, followed by 100x 00h. This combination provides minimum ones density stressing as well as Layer 2 flag bytes.
ds0-3	(Channel group only) Invokes a repeating sequence of 200x 4Ch. This combination represents the typical SDD traffic patterns.
ds0-4	(Channel group only) Invokes a repeating sequence of 200x 40h. This combination represents the typical DEC VT traffic.

Command Default

BERT pattern test is disabled

Command Modes

T3 configuration

E3 configuration

T1 configuration

E1 configuration

Channel group configuration for T1 and E1

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.6.0	The **1in8**, **2^11**, **2^9**, **3in24**, **55Daly**, **55Octet**, **ds0-1**, **ds0-2**, **ds0-3**, and **ds0-4** keywords were added.
Release 3.7.0	The **none** keyword was removed.

Usage Guidelines

BERT is supported on each of the T3/E3 or T1/E1 links. It is done only over an unframed T3/E3 or T1/E1 signal and is run on only one port at a time. It is also supported on an individual channel group.

To begin a BERT, commit the configuration and use the **bert t1**, **bert e1**, **bert t3**, or **bert e3** command in EXEC mode.

To view the BERT results, use the **show controllers t1** or **show controllers t3** command in EXEC mode. The BERT results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BERT
- Total bit errors

- Total bits received

BERT is data intrusive. Regular data cannot flow on a line while the test is in progress. The line is put in an alarm state when a BERT is in progress and restored to a normal state after a BERT has been terminated.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to enable the running of a BERT pattern of all zeros on the T3 controller in slot 0, subslot 3:

```
RP/0/0/CPU0:router(config)# controller t3 0/0/3/1/10
RP/0/0/CPU0:router(config-t3e3)# bert pattern 0s
```

Related Commands

Command	Description
bert error, on page 746	Insert errors into a BERT stream on a T3/E3 or T1/E1 line.
bert interval, on page 748	Specifies the duration of a bit error rate test (BERT) pattern on a T3/E3 or T1/E1 line.
show controllers e1, on page 822	Displays information about the E1 links and hardware and software drivers for the E1 controller.
show controllers e3, on page 826	Displays information about the E3 links and hardware and software drivers for the E3 controller.
show controllers t1, on page 830	Displays information about the T1 links and hardware and software drivers for the T1 controller.
show controllers t3, on page 837	Displays information about the T3 links and hardware and software drivers for the T3 controller.

bert t1

To start or stop a configured bit error rate test (BERT) on a T1 controller or channel group, use the **bert t1** command in EXEC mode.

bert t1 *interface-path-id* [**channel-group** *channel-group-number*] **[error]** {**start**| **stop**}

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
channel-group *channel-group-number*	**Note** (Optional) Channel group number. When a T1 data line is configured, channel group numbers can be values from 0 to 23.
error	(Optional) Injects errors into the running BERT stream.
start	Starts the BERT on the T1 controller or channel.
stop	Stops the BERT on the T1 controller or channel.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.6.0	The **error** keyword was added.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.

- *port*: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

Note Before you can start a BERT on a T1 controller or channel group, you must configure a BERT pattern using the **bert pattern** command. If desired, you can also adjust the default setting (1 minute) of the BERT interval using the **bert interval** command. Both of these commands are available in T1 configuration mode and channel group configuration mode.

To view the BERT results, use the **show controllers t1** command in EXEC mode. The BERT results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BERT
- Total bit errors
- Total bits received

BERT is data intrusive. Regular data cannot flow on a line while the test is in progress. The line is put in an alarm state when a BERT is in progress and restored to a normal state after a BERT has been terminated.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to start and stop a BERT on a T1 controller:

```
RP/0/0/CPU0:router# bert t1 0/3/0/0/0 start
RP/0/0/CPU0:router# bert t1 0/3/0/0/0 stop
```

The following example shows how to inject errors into the BERT stream on an T1 controller:

```
RP/0/0/CPU0:router# bert t1 0/3/0/0 error
```

Related Commands

Command	Description
bert interval, on page 748	Specifies the duration of a bit error rate test (BERT) pattern on a T3/E3 or T1/E1 line.
bert pattern, on page 750	Enables a BERT pattern on a T3/E3 or T1/E1 line or an individual channel group.

Command	Description
show controllers t1, on page 830	Displays information about the T1 links and hardware and software drivers for the T1 controller.

bert t3

To start or stop a configured bit error rate test (BERT) on a T3 controller or channel group, use the **bert t3** command in EXEC mode.

bert t3 *interface-path-id* **[error]** {**start**| **stop**}

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
error	(Optional) Injects errors into the running BERT stream.
start	Starts the BERT on the T3 controller or channel.
stop	Stops the BERT on the T3 controller or channel.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.
- If specifying a virtual interface, the number range varies, depending on interface type.

Note Before you can start a BERT on a T3 controller, you must configure a BERT pattern using the **bert pattern** command. If desired, you can also adjust the default setting (1 minute) of the BERT interval using the **bert interval** command. Both of these commands are available in T3 configuration mode.

To view the BERT results, use the **show controllers t3** command in EXEC mode. The BERT results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BERT
- Total bit errors
- Total bits received

BERT is data intrusive. Regular data cannot flow on a line while the test is in progress. The line is put in an alarm state when a BERT is in progress and restored to a normal state after a BERT has been terminated.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to start and stop a BERT on a T3 controller:

```
RP/0/0/CPU0:router# bert t3 0/3/0/0 start
RP/0/0/CPU0:router# bert t3 0/3/0/0 stop
```

The following example shows how to inject errors into the BERT stream on a T3 controller:

```
RP/0/0/CPU0:router# bert t3 0/3/0/0 error
```

Related Commands

Command	Description
bert interval, on page 748	Specifies the duration of a bit error rate test (BERT) pattern on a T3/E3 or T1/E1 line.
bert pattern, on page 750	Enables a BERT pattern on a T3/E3 or T1/E1 line or an individual channel group.
show controllers t3, on page 837	Displays information about the T3 links and hardware and software drivers for the T3 controller.

cablelength

To specify the distance of the cable from the routers to the network equipment, use the **cablelength** command in T3 or E3 configuration mode. To restore the default cable length, use the **no** form of this command.

cablelength *feet*

no cablelength

Syntax Description

feet	Number of feet in the range from 0 to 450. The default is 224 feet.

Command Default

The default is 224 feet.

Command Modes

T3 configuration

E3 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

You can specify a cable length from 0 to 450 feet; however, the hardware recognizes only two ranges: 0 to 49 and 50 to 450. For example, entering 35 feet uses the 0 to 49 range. If you later change the cable length to 40 feet, there is no change because 40 is still within the 0 to 49 range. However, if you change the cable length to 50, the 50 to 450 range is used. The actual number you enter is stored in the configuration file.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to set the cable length for the router to 300 feet:

```
RP/0/0/CPU0:router(config)# controller t3 0/6/0/0
RP/0/0/CPU0:router(config-t3)# cablelength 300
```

Related Commands

Command	Description
cablelength long, on page 760	Increase the pulse of a signal at the receiver and to decrease the pulse from the transmitter using pulse equalization and line build-out for a T1 cable.
cablelength short, on page 762	Sets a cable length of 655 feet or shorter for a DS1 link.

cablelength long

To increase the pulse of a signal at the receiver and to decrease the pulse from the transmitter using pulse equalization and line build-out for a T1 cable, use the **cablelength long** command in T1 configuration mode. To return the pulse equalization and line build-out values to their default settings, use the **no** form of this command.

cablelength long *db-gain-value db-loss-value*

no cablelength long *db-gain-value db-loss-value*

Syntax Description

db-gain-value	Number of decibels (dB) by which the receiver signal is increased. Use one of the following values: • gain26 • gain36 The default is gain26.
db-loss-value	Number of decibels by which the transmit signal is decreased. Use one of the following values: • 0db • -7.5db • -15db • -22.5db The default is 0db.

Command Default

db-gain-value: gain26

db-loss-value: 0db

Command Modes

T1 configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

Use the **cablelength long** command to configure DS1 links (meaning, to build CSU/DSU links) when the cable length is longer than 655 feet.

A pulse equalizer regenerates a signal that has been attenuated and filtered by a cable loss. Pulse equalization does not produce a simple gain, but it filters the signal to compensate for complex cable loss. A gain26 receiver gain compensates for a long cable length equivalent to 26 dB of loss, whereas a gain36 compensates for 36 dB of loss.

The lengthening or *building out* of a line is used to control far-end crosstalk. Line build-out attenuates the stronger signal from the customer installation transmitter so that the transmitting and receiving signals have similar amplitudes. A signal difference of less than 7.5 dB is ideal. Line build-out does not produce simple flat loss (also known as resistive flat loss). Instead, it simulates a cable loss of 7.5 dB, 15 dB, or 22.5 dB so that the resulting signal is handled properly by the receiving equalizer at the other end.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to increase the receiver gain by 36 decibels and decrease the transmitting pulse by 15 decibels:

```
RP/0/0/CPU0:router(config)#controller t1 0/4/2/0/1
RP/0/0/CPU0:router(config-t1)#cablelength long gain36 -15db
```

Related Commands

Command	Description
cablelength, on page 758	Specifies the distance of the cable from the routers to the network equipment.
cablelength short, on page 762	Sets a cable length of 655 feet or shorter for a DS1 link.

cablelength short

To set a cable length of 655 feet or shorter for a DS1 link, use the **cablelength short** command in T1 configuration mode. To delete the cablelength short value, use the **no** form of this command.

cablelength short *length*

no cablelength short *length*

Syntax Description

length	Specifies a cable length. Use one of the following values: • 133ft—Specifies a cable length from 0 to 133 feet. • 266ft—Specifies a cable length from 134 to 266 feet. • 399ft—Specifies a cable length from 267 to 399 feet. • 533ft—Specifies a cable length from 400 to 533 feet. • 655ft—Specifies a cable length from 534 to 655 feet. The default is 533 feet.

Command Default

The default cable length is 533 feet.

Command Modes

T1 configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

Use the **cablelength short** command to configure DSX-1 links when the cable length is 655 feet or less. This command is supported on T1 controllers only.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to set the cable length for the DS1 link to 655 feet:

```
RP/0/0/CPU0:router(config)# controller t1 0/4/2/0/1
```

```
RP/0/0/CPU0:router(config-t3)# cablelength short 655ft
```

Related Commands

Command	Description
cablelength, on page 758	Specifies the distance of the cable from the routers to the network equipment.
cablelength long, on page 760	Increase the pulse of a signal at the receiver and to decrease the pulse from the transmitter using pulse equalization and line build-out for a T1 cable.

channel-group

To configure a DS0 channel group and enter channel group configuration mode, use the **channel-group** command in T1 or E1 configuration mode. To unassign a channel group, use the **no** form of this command.

channel-group *channel-group-number*

no channel-group *channel-group-number*

Syntax Description

channel-group-number	**Note**	Channel group number. When a T1 controller is configured, channel group numbers can be values from 0 to 23.

Command Default

No default behavior or values

Command Modes

T1 configuration

E1 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

The **channel-group** command is available only on channelized SPAs.

Use the **channel-group** command in configurations in which the router must communicate with a T1 or an E1 fractional data line. The channel group number may be arbitrarily assigned and must be unique for the controller. An associated serial interface is created with each defined channel group.

Before the channel group configuration is valid, you must define the associated DS0 time slots using the **timeslots** command.

Use the **no channel group** command to delete a channel group.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to enter channel group configuration mode for channel group number 5 and change the speed of the underlying DS0s in the channel group to 56 kbps:

```
RP/0/0/CPU0:router(config)# controller t1 0/6/0/0/10
RP/0/0/CPU0:router(config-t1)# channel-group 5
```

```
RP/0/0/CPU0:router(config-t1-channel_group)# speed 56
```

The following example shows how to associate DS0 time slots 1, 6, 8, 9, and 10 to channel group 5:

```
RP/0/0/CPU0:router(config)# controller t1 0/6/0/0/10
RP/0/0/CPU0:router(config-t1)# channel-group 5
RP/0/0/CPU0:router(config-t1-channel_group)# timeslots 1:6:8-10
```

Related Commands

Command	Description
bert pattern, on page 750	Enables a BERT pattern on a T3/E3 or T1/E1 line or an individual channel group.
framing (E1), on page 800	Selects the frame type for an E1 data line.
framing (T1), on page 804	Selects the frame type for a T1 data line.
mode, on page 818	Sets the mode of the T3/E3 or T1/E1 controller.
speed (DS0), on page 850	Specifies the speed of the underlying DS0s in a channel group.
timeslots, on page 852	Associates one or more DS0 time slots to a channel group and create an associated serial subinterface.

clear controller t1

To clear T1 controller data, use the **clear controller t1** command in EXEC configuration mode.

clear controller t1 *interface-path-id*

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show controllers** command to see a list of all controllers currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

When specifying a channelized T1 controller, use the following guidelines for the *interface-path-id*:

- The naming notation is *rack*/*slot*/*module*/*port*/*T3Num*/*T1num*.
- The slash between values is required as part of the notation.
- The following list describes the components of the notation:
  - *rack*—Chassis number of the rack.
  - *slot*—Physical slot number of the line card.
  - *module*—Module number or subslot (for a SPA). A physical layer interface module (PLIM) is always 0.
  - *port*—Physical port number of the interface.
  - *T3num*—T3 controller number.
  - *T1num*—T1 controller number.
- If specifying a virtual interface, the number range varies, depending on interface type.

- When specifying a virtual tributary group, the naming notation is *rack*/*slot*/*module*/*port*/*vtg*/*vt*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*—Chassis number of the rack.
  - *slot*—Physical slot number of the line card.
  - *module*—Module number or subslot (for a SPA). A physical layer interface module (PLIM) is always 0.
  - *port*—Physical port number of the interface.
  - *vtg*—Virtual tributary group.
  - *vt*—Virtual tributary instance.

To view the status of the controllers, use the **show controllers t1** command.

Task ID

Task ID	Operations
dwdm	read, write
interface	read, write
sonet-sdh	read, write

Examples

The following example shows how to clear controller data for the channelized T1 controller 1 that is located in chassis 0, for a SIP installed in slot 1 with a SPA in subslot 0, and port 0 with T3 controller 1, and channelized T1 controller 1:

```
RP/0/0/CPU0:router# clear controller t1 0/1/0/0/1/1
```

Related Commands

Command	Description
controller t1, on page 778	
show controllers t1, on page 830	Displays information about the T1 links and hardware and software drivers for the T1 controller.

clear controller t3

To clear T3 controller data, use the **clear controller t3** command in EXEC configuration mode.

clear controller t3 *interface-path-id*

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show controllers** command to see a list of all controllers currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- When specifying a T3 controller, the naming notation is *rack*/*slot*/*module*/*port*/*T3num*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*—Chassis number of the rack.
  - *slot*—Physical slot number of the line card or SIP.
  - *module*—Module number or subslot (for a SPA). A physical layer interface module (PLIM) is always 0.
  - *port*—Physical port number of the interface.
  - *T3num*—T3 controller number.

To view the status of the controllers, use the **show controllers t3** command.

Task ID

Task ID	Operations
dwdm	read, write

Task ID	Operations
interface	read, write
sonet-sdh	read, write

Examples

The following example shows how to clear controller data for T3 controller 1 that is located in chassis 0, for a SIP installed in slot 6 with a SPA in subslot 2, and port 0 with T3 controller 1:

```
RP/0/0/CPU0:router(config)# controller t3 0/6/2/0/1
```

Related Commands

Command	Description
controller t3, on page 780	Configures a T3 controller and enters T3 configuration mode.
show controllers t3, on page 837	Displays information about the T3 links and hardware and software drivers for the T3 controller.

clock source (T1/E1)

To set clocking for individual T1 or E1 links, use the **clock source** command in T1 or E1 configuration mode. To return to the default, use the **no** form of this command.

clock source {**internal**| **line**}

no clock source

Syntax Description

internal	Specifies that the clock is generated from the internal clock of the T1 or E1 controller. The default is internal. **Note** When configuring clocking on a serial link, you need to configure one end to be **internal** and the other end to be **line**. If you configure **internal** clocking on both ends of a connection, framing slips occur. If you configure **line** clocking on both ends of a connection, the line does not come up.
line	Specifies that the clock on this controller derives its clocking from the external source to which the controller is connected, which is generally the telephone company central office (CO).

Command Default

The default clock source is internal.

Command Modes

T1 configuration

E1 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to set the clocking on the T1 controller in slot 6, subslot 0 to internal:

```
RP/0/0/CPU0:router(config)# controller t1 0/6/0/0/1/1
RP/0/0/CPU0:router(config-t1e1)# clock source internal
```

Related Commands

Command	Description
controller e1, on page 774	Configures an E1 controller and enters E1 configuration mode.
controller t1, on page 778	

clock source (T3/E3)

To set clocking for individual T3 or E3 links, use the **clock source** command in T3 or E3 configuration mode. To return to the default, use the **no** form of this command.

clock source {**internal**| **line**}

no clock source

Syntax Description

internal	Specifies that the clock is generated from the internal clock of the T3 or E3 controller. The default is internal. **Note** When configuring clocking on a serial link, you need to configure one end to be **internal** and the other end to be **line**. If you configure **internal** clocking on both ends of a connection, framing slips occur. If you configure **line** clocking on both ends of a connection, the line does not come up.
line	Specifies that the clock on this controller derives its clocking from the external source to which the controller is connected, which is generally the telephone company central office (CO).

Command Default

The default clock source is internal.

Command Modes

T3 configuration

E3 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

If you do not specify the **clock source** command, the default clock source is used.

Configure the **clock source line** command if your telephone company or the remote data service unit provides the master clock of the T3 or E3 connection.

Configure the **clock source internal** command if your router provides the master clock of the T3 or E3 connection.

Note For a back-to-back connection between two T3 or E3 network modules, one controller must be configured for internal clocking while the other controller must be configured for line clocking.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to set the clocking to line on the T3 controller 1 that is located in chassis 0, on a SIP installed in slot 6 with a SPA in subslot 0, on port 0 with T3 controller 1:

```
RP/0/0/CPU0:router(config)# controller t3 0/6/0/0/1
RP/0/0/CPU0:router(config-t3)# clock source line
```

Related Commands

Command	Description
controller e3, on page 776	Configures an E3 controller and enters E3 configuration mode.
controller t3, on page 780	Configures a T3 controller and enters T3 configuration mode.

controller e1

To configure an E1 controller and enter E1 configuration mode, use the **controller e1** command in global configuration mode. To return to the default state, use the **no** form of this command.

controller e1 *interface-path-id*

no controller e1 *interface-path-id*

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show controllers** command to see a list of all controllers currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.
- If specifying a virtual interface, the number range varies, depending on interface type.

The **controller e1** command is used in configurations in which the router is intended to communicate with an E1 fractional data line. The **controller e1** command is available only on channelized interfaces.

Use the **mode** command in T3 configuration mode to specify the mode for the port. The default mode for 2-Port and 4-Port Channelized T3 SPAs is T1.

Note If you do not use the **mode** command to define the port to be E1, you cannot configure the E1 controller.

To view the status of the controllers, use the **show controllers e1** command.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter E1 configuration mode for a controller:

```
RP/0/0/CPU0:router(config)# controller e1 0/1/0/0
RP/0/0/CPU0:router(config-e1)#
```

Related Commands

Command	Description
mode, on page 818	Sets the mode of the T3/E3 or T1/E1 controller.
show controllers e1, on page 822	Displays information about the E1 links and hardware and software drivers for the E1 controller.

controller e3

To configure an E3 controller and enter E3 configuration mode, use the **controller e3** command in global configuration mode. To return to the default state, use the **no** form of this command.

controller e3 *interface-path-id*

no controller e3 *interface-path-id*

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show controllers** command to see a list of all controllers currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.
- If specifying a virtual interface, the number range varies, depending on interface type.

The **controller e3** command applies only to the 2-Port and 4-Port Clear Channel T3/E3 SPAs. Use the **card type** command to define the controller type to be E3.

To view the status of the controllers, use the **show controllers e3** command.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter E3 configuration mode for a controller in slot 6, on the SPA in subslot 2, on E3 controller 0:

```
RP/0/0/CPU0:router(config)# controller e3 0/6/2/0
RP/0/0/CPU0:router(config-e3)#
```

Related Commands

Command	Description
hw-module subslot cardtype, on page 808	Sets the ports on a SPA in T3, E3, T1, or E1 mode.
show controllers e3, on page 826	Displays information about the E3 links and hardware and software drivers for the E3 controller.

controller t1

To configure a T1 controller and enter T1 configuration mode, use the **controller t1** command in global configuration mode. To return to the default state, use the **no** form of this command.

controller t1 *interface-path-id*

no controller t1 *interface-path-id*

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show controllers** command to see a list of all controllers currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

When specifying a channelized T1 controller, use the following guidelines for the *interface-path-id*:

- The naming notation is *rack*/*slot*/*module*/*port*/*T3Num*/*T1num*.
- The slash between values is required as part of the notation.
- The following list describes the components of the notation:
  - *rack*—Chassis number of the rack.
  - *slot*—Physical slot number of the line card.
  - *module*—Module number or subslot (for a SPA). A physical layer interface module (PLIM) is always 0.
  - *port*—Physical port number of the interface.
  - *T3num*—T3 controller number.
  - *T1num*—T1 controller number.
- If specifying a virtual interface, the number range varies, depending on interface type.

- When specifying a virtual tributary group, the naming notation is *rack*/*slot*/*module*/*port*/*vtg*/*vt*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*—Chassis number of the rack.
  - *slot*—Physical slot number of the line card.
  - *module*—Module number or subslot (for a SPA). A physical layer interface module (PLIM) is always 0.
  - *port*—Physical port number of the interface.
  - *vtg*—Virtual tributary group.
  - *vt*—Virtual tributary instance.

The **controller t1** command is used in configurations in which the router is intended to communicate with a T1 fractional data line. The **controller t1** command is available only on channelized SPAs.

Use the **mode** command in T3 configuration mode to specify the mode for each T3 port. The default mode for 2-Port and 4-Port Channelized T3 SPAs is T1.

To view the status of the controllers, use the **show controllers t1** command.

If the T1 framing type is super frame (SF), you should consider disabling yellow alarm detection as the yellow alarm can be incorrectly detected with SF framing.

Serial interface may flap and eventually, go down if yellow alarm detection is not disabled on its T1 controller configured with SF framing.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter T1 configuration mode for a controller:

```
RP/0/0/CPU0:router(config)# controller t1 0/1/0/0/1
RP/0/0/CPU0:router(config-t1)#
```

Related Commands

Command	Description
mode, on page 818	Sets the mode of the T3/E3 or T1/E1 controller.
show controllers t1, on page 830	Displays information about the T1 links and hardware and software drivers for the T1 controller.

controller t3

To configure a T3 controller and enter T3 configuration mode, use the **controller t3** command in global configuration mode. To return to the default state, use the **no** form of this command.

controller t3 *interface-path-id*

no controller t3 *interface-path-id*

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show controllers** command to see a list of all controllers currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- When specifying a T3 controller, the naming notation is *rack*/*slot*/*module*/*port*/*T3num*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*—Chassis number of the rack.
  - *slot*—Physical slot number of the line card or SIP.
  - *module*—Module number or subslot (for a SPA). A physical layer interface module (PLIM) is always 0.
  - *port*—Physical port number of the interface.
  - *T3num*—T3 controller number.
- If specifying a virtual interface, the number range varies, depending on interface type.

For the 2-Port and 4-Port Clear Channel T3/E3 SPAs, use the **card type** command to define the controller type to be T3.

To view the status of the controllers, use the **show controllers t3** command.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter T3 configuration mode for T3 controller 1 that is located in chassis 0, for a SIP installed in slot 6 with a SPA in subslot 2, and port 0 with T3 controller 1:

```
RP/0/0/CPU0:router(config)# controller t3 0/6/2/0/1
RP/0/0/CPU0:router(config-t3)#
```

Related Commands

Command	Description
hw-module subslot cardtype, on page 808	Sets the ports on a SPA in T3, E3, T1, or E1 mode.
show controllers t3, on page 837	Displays information about the T3 links and hardware and software drivers for the T3 controller.

delay clear (T1/E1)

To configure the amount of time before a T1 or E1 path delay trigger alarm is cleared, use the **delay clear** command in T1 or E1 configuration mode. To return the command to its default setting, use the **no** form of this command.

delay clear *value*

no delay clear *value*

Syntax Description

value	Value, in milliseconds, before a T1 path delay trigger alarm is cleared. The range is from 0 through 180000. The default is 10 seconds.

Command Default

The default is 10 seconds.

Command Modes

T1 configuration

E1 configuration

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to specify that T1 path delay trigger alarms should be cleared after 9000 seconds:

```
RP/0/0/CPU0:router(config)# controller t1 0/4/2/0/1
RP/0/0/CPU0:router(config-t1)#delay clear 9000
```

Related Commands

Command	Description
delay trigger (T1/E1), on page 784	Configures a time value for the T1 or E1 path delay trigger.

delay clear (T3/E3)

To configure the amount of time before a T3 or E3 path delay trigger alarm is cleared, use the **delay clear** command in T3 or E3 configuration mode. To return the command to its default setting, use the **no** form of this command.

delay clear *value*

no delay clear *value*

Syntax Description

value	Value, in milliseconds, before a T3 or E3 path delay trigger alarm is cleared. The range is from 0 through 180000. The default is 10 seconds.

Command Default

The default is 10 seconds.

Command Modes

T3 configuration

E3 configuration

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to specify that T3 path delay trigger alarms should be cleared after 9000 seconds:

```
RP/0/0/CPU0:router(config)# controller t3 0/4/2/0/1
RP/0/0/CPU0:router(config-t3)# delay clear 9000
```

Related Commands

Command	Description
delay trigger (T3/E3), on page 785	Configures a time value for the T3 or E3 path delay trigger.

delay trigger (T1/E1)

To configure a time value for the T1 or E1 path delay trigger, use the **delay trigger** command in T1 or E1 configuration mode. To return the command to its default setting, use the **no** form of this command.

delay trigger *value*

no delay trigger

Syntax Description

value	Sets the T1 path delay trigger value, in milliseconds. The range is from 0 through 60000. The default is 2.5 seconds.

Command Default

The default is 2.5 seconds.

Command Modes

T1 configuration

E1 configuration

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

If the timer for the T1 or E1 path delay trigger expires, an alarm is declared.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to set the T1 path delay trigger to 8000 milliseconds:

```
RP/0/0/CPU0:router(config)# controller t1 0/4/2/0/1/1
RP/0/0/CPU0:router(config-t1)# delay trigger 8000
```

Related Commands

Command	Description
delay clear (T1/E1), on page 782	Configures the amount of time before a T1 or E1 path delay trigger alarm is cleared.

delay trigger (T3/E3)

To configure a time value for the T3 or E3 path delay trigger, use the **delay trigger** command in T3 or E3 configuration mode. To return the command to its default setting, use the **no** form of this command.

delay trigger *value*

no delay trigger

Syntax Description

value	Sets the T3 or E3 path delay trigger value, in milliseconds. The range is from 0 through 60000. The default is 2.5 seconds.

Command Default

The default is 2.5 seconds.

Command Modes

T3 configuration

E3 configuration

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

If the timer for the T3 or E3 path delay trigger expires, an alarm is declared.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to set the T3 path delay trigger to 8000 milliseconds:

```
RP/0/0/CPU0:router(config)# controller t3 0/4/2/0/1
RP/0/0/CPU0:router(config-t3)# delay trigger 8000
```

Related Commands

Command	Description
delay clear (T3/E3), on page 783	Configures the amount of time before a T3 or E3 path delay trigger alarm is cleared.

description (T1/E1)

To configure a description for a T1 or E1 controller, use the **description** command in T1 or E1 configuration mode. To delete a T1 or E1 controller description, use the **no** form of this command.

description *text*

no description [*text*]

Syntax Description

text	A text string comprised of alphanumeric characters.

Command Default

No description is configured.

Command Modes

T1 configuration

E1 configuration

Command History

Release	Modification
Release 3.7.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
sonet-sdh	read, write
interface	read, write

Examples

The following example shows how to configure a description for a T1 controller:

```
RP/0/0/CPU0:router(config)# controller t1 0/6/2/0
RP/0/0/CPU0:router(config-t1)# description This is a sample description for T1 controller
0/6/2/0
```

Related Commands

Command	Description
show controllers e1, on page 822	Displays information about the E1 links and hardware and software drivers for the E1 controller.

Command	Description
show controllers t1, on page 830	Displays information about the T1 links and hardware and software drivers for the T1 controller.

description (T3/E3)

To configure a description for a T3 or E3 controller, use the **description** command in T3 or E3 configuration mode. To delete a T3 or E3 controller description, use the **no** form of this command.

description *text*

no description [*text*]

Syntax Description

text	A text string comprised of alphanumeric characters.

Command Default

No description is configured.

Command Modes

T3 configuration

E3 configuration

Command History

Release	Modification
Release 3.7.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
sonet-sdh	read, write
interface	read, write

Examples

The following example shows how to configure a description for a T3 controller:

```
RP/0/0/CPU0:router(config)# controller t3 0/6/2/0
RP/0/0/CPU0:router(config-t3)# description This is a sample description for T3 controller
0/6/2/0
```

Related Commands

Command	Description
show controllers e3, on page 826	Displays information about the E3 links and hardware and software drivers for the E3 controller.

Command	Description
show controllers t3, on page 837	Displays information about the T3 links and hardware and software drivers for the T3 controller.

down-when-looped (T1/E1)

To configure a T1 or E1 controller to inform the system that it is down when loopback is detected, use the **down-when-looped** command in T1 or E1 configuration mode.

down-when-looped

Syntax Description

This command has no keywords or arguments.

Command Default

By default, a T1 or E1 controller does not inform the system that it is down when loopback is detected.

Command Modes

T1 configuration

E1 configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

This command does not have a **no** form.

Task ID

Task ID	Operations
sonet-sdh	read, write
interface	read, write

Examples

The following example shows how to configure a T1 controller to inform the system that the associated line is down if a loopback is detected:

```
RP/0/0/CPU0:router(config)# controller t1 0/4/2/0/1
RP/0/0/CPU0:router(config-t1)# down-when-looped

down-when-looped is a traffic-affecting operation if any loopback is present
```

Related Commands

Command	Description
loopback (T1/E1), on page 812	Loops individual T1 or E1 channels on the channelized T3 controller.

down-when-looped (T3/E3)

To configure a T3 or E3 controller to inform the system that it is down when loopback is detected, use the **down-when-looped** command in T3 or E3 configuration mode.

down-when-looped

Syntax Description

This command has no keywords or arguments.

Command Default

By default, a T3 or E3 controller does not inform the system that it is down when loopback is detected.

Command Modes

T3 configuration

E3 configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

This command does not have a **no** form.

Task ID

Task ID	Operations
sonet-sdh	read, write
interface	read, write

Examples

The following example shows how to configure a T3 controller to inform the system that the associated line is down if a loopback is detected:

```
RP/0/0/CPU0:router(config)# controller t3 0/4/2/0
RP/0/0/CPU0:router(config-t3)# down-when-looped

down-when-looped is a traffic-affecting operation if any loopback is present
```

Related Commands

Command	Description
loopback (T3/E3), on page 814	Loops the entire T3 or E3 line on the T3 controller or E3 controller.

dsu bandwidth

To specify the maximum allowable bandwidth used by a T3 or an E3 controller, use the **dsu bandwidth** command in T3 or E3 configuration mode. To return to the default state, use the **no** form of this command.

dsu bandwidth kbps

no dsu bandwidth

Syntax Description

kbps	Maximum bandwidth, in kilobits per second (kbps). Range is from 75 to 44210. The default is 44210.

Command Default

The default bandwidth is 44210.

Command Modes

T3 configuration

E3 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

The local interface configuration must match the remote interface configuration. For example, if you reduce the maximum bandwidth to 16,000 on the local port, you must also do the same on the remote port.

The **dsu bandwidth** command reduces the bandwidth by padding the E3 and T3 frame.

To verify the data service unit (DSU) bandwidth configured on the interface, use the **show controllers t3** or **show controllers e3** command in EXEC mode.

When G.751 framing is used on E3 links, DSU bandwidth can be used to select a payload subrate from 34,010 kbps down to 22 kbps. Before framing bypass can be used, a DSU bandwidth of 34,010 kbps must be configured.

Although software allows the user to configure a continuous range of bandwidths in subrate modes, vendors support bandwidths only in quantums (for example, in a ADC Kentrox T3 link, bandwidth must be in multiples of 500 kbps). Therefore, the software sets the user-configured bandwidth to the closest vendor-supported bandwidth. Use the **show controllers t3** or **show controllers e3** command to display the actual bandwidth that is configured.

The following table shows DSU modes and vendor-supported bandwidths.

Table 48: DSU Modes and Vendor-supported Bandwidths

Mode	Bandwidth (in kbps)	Bandwidth Multiples (in kbps)
Digital Link or Cisco	358–34010 for E3300–44210 for T3	358 300.746
ADC Kentrox T3/E3 IDSU	1000–34010 for E31500–44210 for T3	500 500
Larscom Access T45	3100–44210 kbps	3158
Adtran T3SU 300	75–44210 kbps	75.186
Verilink HDM 2182	1500–44210 kbps	1579

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to set the maximum allowable DSU bandwidth to 16,000 kbps on a SIP in slot 6, on the SPA in subslot 2, for port 0, and T3 controller 1:

```
RP/0/0/CPU0:router(config)# controller t3 0/6/2/0/1
RP/0/0/CPU0:router(config-t3)# dsu bandwidth 16000
```

Related Commands

Command	Description
show controllers e3, on page 826	Displays information about the E3 links and hardware and software drivers for the E3 controller.
show controllers t3, on page 837	Displays information about the T3 links and hardware and software drivers for the T3 controller.

dsu mode

To specify the interoperability mode used by a T3 or an E3 controller, use the **dsu mode** command in T3 or E3 configuration mode. To return to the default state, use the **no** form of this command.

dsu mode mode

no dsu mode

Syntax Description

mode	DSU mode. Valid values are as follows: • (T3 only) **adtran** • cisco • digital-link • kentrox • (T3 only) **larscom** • (T3 only) **verilink** The default is cisco.

Command Default

The default is cisco.

Command Modes

T3 configuration

E3 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

Refer to Table 48: DSU Modes and Vendor-supported Bandwidths, on page 793 for more information regarding the modes.

The local interface configuration must match the remote interface configuration. For example, if you define the data service unit (DSU) interoperability mode as **digital-link** on the local port, you must also do the same on the remote port.

You must know what type of DSU is connected to the remote port to determine if it interoperates with a T3 or an E3 controller. The **dsu mode** command enables and improves interoperability with other DSUs.

To verify the DSU mode configured on the interface, use the **show controllers t3** command in EXEC mode.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to set the DSU mode to **digital-link** for T3 controller 1 located in chassis 0, on a SIP in slot 6 and SPA in subslot 2, and port 0 with T3 controller 1:

```
RP/0/0/CPU0:router(config)# controller t3 0/6/2/0/1
RP/0/0/CPU0:router(config-t3)# dsu mode digital-link
```

Related Commands

Command	Description
show controllers e3, on page 826	Displays information about the E3 links and hardware and software drivers for the E3 controller.
show controllers t3, on page 837	Displays information about the T3 links and hardware and software drivers for the T3 controller.

dsu remote

To control the bandwidth usage with the remote port, use the **dsu remote** command in T3 or E3 configuration mode. To return to the default state, use the **no** form of this command.

dsu remote {**disable**| **fullrate**}

no dsu remote

Syntax Description

disable	Denies incoming remote requests to reset the bandwidth to the full rate.
fullrate	Requests that the remote port set its bandwidth to full rate.

Command Default

Remote accept is the default.

Command Modes

T3 configuration

E3 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

To verify the DSU remote settings configured on the interface, use the **show controllers t3** or **show controllers e3** command in EXEC mode.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to specify that the connected remote port set its bandwidth to full rate:

```
RP/0/0/CPU0:router(config)# controller t3 0/6/2/0
RP/0/0/CPU0:router(config-t3)# dsu remote fullrate
```

Related Commands

Command	Description
show controllers e3, on page 826	Displays information about the E3 links and hardware and software drivers for the E3 controller.
show controllers t3, on page 837	Displays information about the T3 links and hardware and software drivers for the T3 controller.

fdl

To enable or disable the transmission of performance reports through Facility Data Link (FDL) for a T1 channel on the channelized T3 interface, use the **fdl** command in T1 configuration mode. To return to the default state of performance reporting, use the **no** form of this command.

fdl {**ansi**| **att**} {**enable**| **disable**}

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

Syntax Description

ansi	Specifies the transmission of ANSI T1.403 once-per-second performance reports.
att	Specifies the transmission of AT&T TR54016 once-per-second performance reports.
enable	Enables transmission of the specified performance reports.
disable	Disables transmission of the specified performance reports. The default is disable.

Command Default

The transmission of ANSI T1.403 and AT&T TR54016 performance reports through FDL are disabled.

Command Modes

T1 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

The **fdl** command applies only to T1 lines and can be used only if the T1 framing type is Extended Super Frame (ESF).

To display the performance report information, use the **show controllers t1** command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to enable ANSI T1.403 performance reports for T1 channel 10:

```
RP/0/0/CPU0:router(config)# controller t1 0/6/0/1/10
RP/0/0/CPU0:router(config-t1e1)# fdl ansi enable
```

Related Commands

Command	Description
show controllers t1, on page 830	Displays information about the T1 links and hardware and software drivers for the T1 controller.

framing (E1)

To select the frame type for an E1 data line, use the **framing** command in E1 configuration mode. To disable E1 framing, use the **no** form of this command.

framing {**crc4**| **no-crc4**| **unframed**}

no framing {**crc4**| **no-crc4**| **unframed**}

Syntax Description

crc4	Specifies framing with CRC-4 error-monitoring capabilities. The default is crc4.
no-crc4	Specifies framing without CRC-4 error-monitoring capabilities.
unframed	Specifies unframed E1.

Command Default

The default is **crc4**.

Command Modes

E1 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

Use the **framing** command in configurations in which the router or access server is intended to communicate with E1 fractional data lines. The service provider determines the framing type required for your E1 circuit.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to select E1 framing without CRC-4 error-monitoring capabilities:

```
RP/0/0/CPU0:router(config)# controller e1 0/6/0/0/10
RP/0/0/CPU0:router(config-t1e1)# framing no-crc4
```

Related Commands

Command	Description
show controllers e1, on page 822	Displays information about the E1 links and hardware and software drivers for the E1 controller.

framing (E3)

To select the frame type for E3 data lines, use the **framing** command in E3 configuration mode. To disable E3 framing, use the **no** form of this command.

framing {**g751**| **g832**}

no framing {**g751**| **g832**}

Syntax Description

g751	Specifies that G.751 framing is used as the E3 framing type. The default is G.751.
g832	Specifies that G.832 framing is used as the E3 framing type.

Command Default

The default is G.751.

Command Modes

E3 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

If you do not use the **framing** command, the default is used by the E3 controllers to automatically determine the framing type received from the far-end equipment. You can also set the framing for each T1/E1 channel by using the **framing** command in T1 or E1 configuration mode.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to select G751 as the E3 frame type:

```
RP/0/0/CPU0:router(config)# controller e3 0/6/0/0
RP/0/0/CPU0:router(config-e3)# framing g751
```

Related Commands

Command	Description
show controllers e3, on page 826	Displays information about the E3 links and hardware and software drivers for the E3 controller.

framing (T1)

To select the frame type for a T1 data line, use the **framing** command in T1 configuration mode. To disable T1 framing, use the **no** form of this command.

framing {**esf**| **sf**}

no framing {**esf**| **sf**}

Syntax Description

esf	Specifies extended super frame as the T1 frame type. The default is **esf**.
sf	Specifies super frame as the T1 frame type.

Command Default

The default is **esf**.

Command Modes

T1 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

Use the **framing** command in configurations in which the router or access server is intended to communicate with T1 fractional data lines. The service provider determines the framing type required for your T1 /E1 circuit.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to select super frame as the T1 frame type:

```
RP/0/0/CPU0:router(config)# controller t1 0/6/0/0/10
RP/0/0/CPU0:router(config-t1)# framing sf
```

Related Commands

Command	Description
show controllers t1, on page 830	Displays information about the T1 links and hardware and software drivers for the T1 controller.

framing (T3)

To select the frame type for T3 data lines, use the **framing** command in T3 configuration mode. To disable T3 framing, use the **no** form of this command.

framing {**auto-detect** | **c-bit**| **m23**}

no framing {**auto-detect** | **c-bit**| **m23**}

Syntax Description

auto-detect	Specifies that application identification channel signal framing is used as the T3 framing type.
c-bit	Specifies that C-bit framing is used as the T3 framing type. The default is **c-bit**.
m23	Specifies that M23 framing is used as the T3 framing type.

Command Default

The default is **c-bit**.

Command Modes

T3 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

If you do not use the **framing** command, the default is used by the T3 controllers to automatically determine the framing type received from the far-end equipment. You can also set the framing for each T1 or E1 channel by using the **framing** command in T1 or E1 configuration mode.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to select M23 as the T3 frame type:

```
RP/0/0/CPU0:router(config)# controller t3 0/6/0/0/1
RP/0/0/CPU0:router(config-t3)# framing m23
```

Related Commands

Command	Description
show controllers t3, on page 837	Displays information about the T3 links and hardware and software drivers for the T3 controller.

hw-module subslot cardtype

To set the ports on a SPA in T3, E3, T1, or E1 mode, use the **hw-module subslot cardtype** command in global configuration mode. To deselect the card type, use the **no** form of this command.

hw-module subslot subslot-id cardtype {**e1**| **e3**| **t1**| **t3**}

no hw-module subslot subslot-id cardtype {**e1**| **e3**| **t1**| **t3**}

Syntax Description

subslot-id	Subslot to be power cycled. The *subslot-id* argument is entered in the *rack/slot/subslot* notation.
e1	E1 fractional data line.
t1	T1 fractional data line. The default for the 8-Port Channelized T1/E1 SPA is T1.

Command Default

The default for the 2-Port and 4-Port Clear Channel T3/E3 SPAs is T3.

The default for the 8-Port Channelized T1/E1 SPA is T1.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.6.0	The **t1** and **e1** keywords were added.

Usage Guidelines

The **hw-module subslot cardtype** command applies only to the following SPAs:

- 2-Port and 4-Port Clear Channel T3/E3 SPAs
- 8-Port Channelized T1/E1 SPA

By default, the 2-Port and 4-Port Clear Channel T3/E3 SPAs boot in T3 mode , while the 8-Port Channelized T1/E1 SPA boots in T1 mode. Use the **hw-module subslot cardtype** command to change the setting to E3 for the 2-Port and 4-Port Clear Channel T3/E3 SPAs and to E1 for the 8-Port Channelized T1/E1 SPA.

If there are nondefault configurations on the card interfaces, you must delete them before you can change the card type. Use the **no controller** { **e1** | **e3** | **t1** | **t3**}and **no interface serial** commands to delete any T3, E3, T1, E1, or serial configurations.

Task ID

Task ID	Operations
root-lr	read, write

Examples

The following example shows how to configure all ports of a 2-Port or 4-Port Clear Channel T3/E3 SPA located in slot 5, subslot 2 to E3 mode:

```
RP/0/0/CPU0:router(config)# hw-module subslot 0/5/2 cardtype e3
```

The following example shows how to configure all ports of an 8-Port Channelized T1/E1 SPA located in slot 2, subslot 1to E1 mode:

```
RP/0/0/CPU0:router(config)# hw-module subslot 0/2/1 cardtype e1
```

Related Commands

Command	Description
controller e1, on page 774	Configures an E1 controller and enters E1 configuration mode.
controller e3, on page 776	Configures an E3 controller and enters E3 configuration mode.
controller t1, on page 778	
controller t3, on page 780	Configures a T3 controller and enters T3 configuration mode.
interface serial, on page 599	Configures a serial interface and enters interface or subinterface configuration mode.

linecode

To select the line-code type for T1 or E1 lines, use the **linecode** command in T1 or E1 configuration mode. To return the line to the default line-code type, use the **no** form of this command.

linecode {**ami**| **b8zs**| **hdb3**}

no linecode {**ami**| **b8zs**| **hdb3**}

Syntax Description

ami	Specifies alternate mark inversion (AMI) as the line-code type. This value is the default for E1 lines.
b8zs	(T1 only) Specifies B8ZS as the line-code type. This value is the default for T1 lines.
hdb3	(E1 only) Specifies high-density bipolar 3 (HDB3) as the line-code type.

Command Default

T1 lines: the default is B8ZS.

E1 lines: the default is AMI.

Command Modes

T1 configuration

E1 configuration

Command History

Release 3.6.0	This command was introduced.

Usage Guidelines

Use this command in configurations where the router must communicate with T1 or E1 fractional data lines. The T1 or E1 service provider determines which line-code type is required for your T1 or E1 circuit.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to select AMI as the T1 line-code type:

```
RP/0/0/CPU0:router(config)# controller t1 0/6/0/0/1/1
RP/0/0/CPU0:router(config-t1)# linecode ami
```

The following example shows how to select HDB3 as the E1 line-code type:

```
RP/0/0/CPU0:router(config)# controller e1 0/4/1/1
RP/0/0/CPU0:router(config-e1)# linecode hdb3
```

Related Commands

Command	Description
show controllers e1, on page 822	Displays information about the E1 links and hardware and software drivers for the E1 controller.
show controllers t1, on page 830	Displays information about the T1 links and hardware and software drivers for the T1 controller.

loopback (T1/E1)

To loop individual T1 or E1 channels on the channelized T3 controller, use the **loopback** command in T1 or E1 configuration mode. To remove the loop, use the **no** form of this command.

loopback {**local**| **network** {**line**| **payload**}| **remote** {**line** {**fdl** {**ansi**| **bellcore**}| **inband**}| **payload fdl ansi**}}

no loopback {**local**| **network** {**line**| **payload**}| **remote** {**line** {**fdl** {**ansi**| **bellcore**}| **inband**}| **payload fdl ansi**}}

Syntax Description

local	Loops the router output data back toward the router at the T1 framer and sends an alarm indication signal (AIS) signal out toward the network.
network {**line** | **payload**}	T1 loopback with encapsulation HDLC: Loops the data back toward the network before the T1 framer and automatically sets a local loopback at the High-Level Data Link Control (HDLC) controllers (line), or loops the payload data back toward the network at the T1 framer and automatically sets a local loopback at the HDLC controllers (payload). T1 loopback with encapsulation PPP: Loops the data back toward the network before the T1 framer and automatically sets a local loopback at the PPP serial interface (line), or loops the payload data back toward the network at the T1 framer and automatically sets a local loopback at the PPP serial interface (payload).
remote line fdl	(T1 only) Sends a repeating, 16-bit Extended Superframe (ESF) data link code word (00001110 11111111 for FDL ANSI and 00010010 11111111 for FDL Bellcore) to the remote end, requesting that it enter into a network line loopback.
remote line inband	(T1 only) Sends a repeating, 5-bit inband pattern (00001) to the remote end requesting that it enter into a network line loopback.
remote payload fdl	(T1 only) Sends a repeating, 16-bit ESF data link code word (00010100 11111111) to the remote end, requesting that it enter into a network payload loopback. Enables the remote payload FDL ANSI bit loopback on the T1 channel.
ansi	(T1 only) Enables the remote line Facility Data Link (FDL) ANSI bit loopback on the T1 channel, based on the ANSI T1.403 specification.
bellcore	(T1 only) Enables the remote SmartJack loopback on the T1 channel, based on the TR-TSY-000312 specification.

Command Default

No loops are configured.

Command Modes

T1 configuration

E1 configuration

Command History

Release 3.3.0	This command was introduced.

Usage Guidelines

Use the **loopback** command for troubleshooting purposes. To verify that a loopback is configured on the interface, use the **show controllers t1** or **show controllers e1** command in EXEC mode.

For E1 lines, only the **local** and **network** options are valid. For T1 lines, all listed options are valid.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to configure the T1 for a local loopback:

```
RP/0/0/CPU0:router(config)# controller t1 0/6/0/0/10
RP/0/0/CPU0:router(config-t1)# loopback local
```

Related Commands

Command	Description
framing (E1), on page 800	Selects the frame type for an E1 data line.
framing (T1), on page 804	Selects the frame type for a T1 data line.
show controllers e1, on page 822	Displays information about the E1 links and hardware and software drivers for the E1 controller.
show controllers t1, on page 830	Displays information about the T1 links and hardware and software drivers for the T1 controller.

loopback (T3/E3)

To loop the entire T3 or E3 line (all 28 T1 channels or all 21 E1 channels) on the T3 controller or E3 controller, use the **loopback** command in T3 or E3 configuration mode. To remove the loop, use the **no** form of this command.

loopback {**local**| {**network**| **remote** {**line**| **payload**}}}

no loopback

Syntax Description

local	Loops the data back toward the router and sends an alarm indication signal (AIS) out toward the network.
network {**line** | **payload**}	Sets the loopback toward the network before going through the framer (**line**) or after going through the framer (**payload**).
remote {**line** | **payload**}	Sends a far-end alarm control (FEAC) request to the remote end requesting that it enter into a network line loopback. FEAC requests (and therefore remote loopbacks) are possible only when the T3 is configured for C-bit framing. The M23 format does not support remote loopbacks.

Command Default

No loops are configured on the T3 line.

Command Modes

T3 configuration

E3 configuration

Command History

Release 3.3.0	This command was introduced.

Usage Guidelines

Use the **loopback** command for troubleshooting purposes. To verify that a loopback is configured on the interface, use the **show controllers t3** or **show controllers e3** command in EXEC mode. Note that remote loopback is valid only in C-bit parity mode.

You can also loopback each T1 or E1 channel by using the **loopback** command in T1 or E1 configuration mode.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to configure the T3 for a local loopback:

```
RP/0/0/CPU0:router(config)# controller t3 0/3/0/0
RP/0/0/CPU0:router(config-t3)# loopback local
```

Related Commands

Command	Description
framing (E1), on page 800	Selects the frame type for an E1 data line.
framing (T1), on page 804	Selects the frame type for a T1 data line.
loopback (T1/E1), on page 812	Loops individual T1 or E1 channels on the channelized T3 controller.
show controllers e3, on page 826	Displays information about the E3 links and hardware and software drivers for the E3 controller.
show controllers t3, on page 837	Displays information about the T3 links and hardware and software drivers for the T3 controller.

mdl

To configure the Maintenance Data Link (MDL) message defined in the ANSI T1.107a-1990 specification, use the **mdl** command in T3 configuration mode. To remove the message, use the **no** form of this command.

{**mdl string** {**eic**| **fi**| **fic**| **gen-number**| **lic**| **port-number**| **unit**} *string*| **transmit** {**idle-signal**| **path**| **test-signal**} {**disable**| **enable**}}

{**no mdl string** {**eic**| **fi**| **fic**| **gen-number**| **lic**| **port-number**| **unit**} *string*| **transmit** {**idle-signal**| **path**| **test-signal**} {**disable**| **enable**}}

Syntax Description

string eic *string*	Specifies the Equipment Identification Code; can be up to 10 characters.
string fi *string*	Specifies the Facility Identification Code sent in the MDL Path message; can be up to 38 characters.
string fic *string*	Specifies the Frame Identification Code; can be up to 10 characters.
string gen-number *string*	Specifies the Generator number string sent in the MDL Test Signal message; can be up to 38 characters.
string lic *string*	Specifies the Location Identification Code; can be up to 11 characters.
string port-number *string*	Specifies the Port number string sent in the MDL Idle Signal message; can be up to 10 characters.
string unit *string*	Specifies the Unit Identification Code; can be up to 6 characters.
transmit idle-signal	Specifies the transmission of the MDL Idle Signal message.
transmit path	Specifies the transmission of the MDL Path message.
transmit test-signal	Specifies the transmission of the MDL Test Signal message.
disable | **enable**	Disables or enables transmission of the specified message.

Command Default

No MDL message is configured.

Command Modes

T3 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

Use the **show controllers t3** command to display MDL information (received strings). MDL information is displayed only when framing is set to C-bit.

Note MDL is supported only when the DS3 framing is C-bit parity.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows the **mdl** commands on a T3 controller in slot 1, subslot 2, port 0:

```
RP/0/0/CPU0:router(config)# controller t3 0/1/2/0
RP/0/0/CPU0:router(config-t3)# clock source line
RP/0/0/CPU0:router(config-t3)# mdl string eic ID
RP/0/0/CPU0:router(config-t3)# mdl string fic Building B
RP/0/0/CPU0:router(config-t3)# mdl string unit ABC
RP/0/0/CPU0:router(config-t3)# mdl string fi Facility Z
RP/0/0/CPU0:router(config-t3)# mdl string port-number Port 7
RP/0/0/CPU0:router(config-t3)# mdl transmit path enable
RP/0/0/CPU0:router(config-t3)# mdl transmit idle-signal enable
```

Related Commands

Command	Description
show controllers t3, on page 837	Displays information about the T3 links and hardware and software drivers for the T3 controller.

mode

To set the mode of the T3/E3 or T1/E1 controller, use the **mode** command in T3, E3, T1, or E1 configuration mode. To disable the controller mode, use the **no** form of this command.

mode {**atm**| **e1**| **serial**| **t1**}

no mode {**atm**| **e1**| **serial**| **t1**}

Syntax Description

atm	Specifies the mode of the port to be a clear channel transporting ATM.
e1	(T3 and E3 only) Specifies the mode of the port to be channelized E1.
serial	(T3 and E3 only) Specifies the mode of the port to be clear channel serial. The default for the 2-Port and 4-Port Clear Channel T3/E3 SPAs is serial.
t1	(T3 and E3 only) Specifies the mode of the port to be channelized T1.

Command Default

The default for the 2-Port and 4-Port Clear Channel T3/E3 SPAs is serial.

There is no default for the 2-Port and 4-Port Channelized T3 SPAs.

Command Modes

T3 configuration

E3 configuration

T1 configuration

E1 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

You can change the mode of a controller only when there are no subinterfaces defined for the controller. For example, if you previously defined channelized T1 subinterfaces on a T3 interface and now you want to change this to E1 subinterfaces or a clear channel interface, you must first clear the subinterfaces. To do this, use the **no controller t1** command for all defined T1/E1 subinterfaces. If you have defined serial parameters, you also need to use the **no interface serial** command.

For channelized SPAs, you must use the **mode** command before you can configure any channelized controllers.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to change the mode of a T3 port to channelized T1:

```
RP/0/0/CPU0:router(config)# controller t3 0/6/0/0
RP/0/0/CPU0:router(config-t3)# mode t1
```

Related Commands

Command	Description
show controllers e1, on page 822	Displays information about the E1 links and hardware and software drivers for the E1 controller.
show controllers e3, on page 826	Displays information about the E3 links and hardware and software drivers for the E3 controller.
show controllers t1, on page 830	Displays information about the T1 links and hardware and software drivers for the T1 controller.
show controllers t3, on page 837	Displays information about the T3 links and hardware and software drivers for the T3 controller.

national bits (E1)

To specify the national reserved bits for an E1 port, use the **national bits** command in E1 configuration mode. To revert to the default national bits, use the **no** form of this command.

national bits *bits*

no national bits *bits*

Syntax Description

bits	Bit pattern. Values can be from 0 to 31. The default is 0.

Command Default

The default is 0, which corresponds to 0x1f.

Command Modes

E1 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to specify the national bits for the E1 controller:

```
RP/0/0/CPU0:router(config)# controller e1 0/6/0/0/10
RP/0/0/CPU0:router(config-t1e1)# national bits 3
```

Related Commands

Command	Description
show controllers e1, on page 822	Displays information about the E1 links and hardware and software drivers for the E1 controller.

national bits (E3)

To enable or disable the national reserved bit pattern on an E3 port, use the **national bits** command in E3 configuration mode. To revert to the default value, use the **no** form of this command.

national bits {**disable**| **enable**}

no national bits {**disable**| **enable**}

Syntax Description

disable	Disables national reserved bits for an E3 port.
enable	Enables national reserved bits for an E3 port. The default is **enable**.

Command Default

The default is **enable**.

Command Modes

E3 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to enable the national bits for an E3 controller:

```
RP/0/0/CPU0:router(config)# controller e3 0/6/2/0
RP/0/0/CPU0:router(config-e3)# national bits enable
```

Related Commands

Command	Description
show controllers e3, on page 826	Displays information about the E3 links and hardware and software drivers for the E3 controller.

show controllers e1

To display information about the E1 links and hardware and software drivers for the E1 controller, use the **show controllers e1** command in EXEC mode.

show controllers e1 *interface-path-id* [**all**| **bert**| **brief**| **internal-state**| **tabular**]

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
all	Displays all information for the controllers.
bert	Displays internal E1 bit error rate test results.
brief	Displays summary information for the E1 controller.
internal-state	Displays internal E1 state information.
tabular	Displays E1 controller information in tabular format.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.

• If specifying a virtual interface, the number range varies, depending on interface type.

Task ID

Task ID	Operations
interface	read

Examples

The following example shows sample output from the **show controllers e1** command for a single E1 channel:

```
RP/0/0/CPU0:router# show controllers e1 0/1/0/0

  E1 0/1/0/0 is down
  timeslots:
  Receiver has no alarms.
  Framing is E1 CRC, Clock Source is internal
  Data in current interval (0 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs, 0 Stuffed Secs
     0 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
```

Table 49: show controllers e1 Field Descriptions

Field	Description
E1 0/1/0/0 is down	E1 channel is not operating. The channel state can be up, down, or administratively down. Loopback conditions are shown by (Locally Looped) or (Remotely Looped).
timeslots	DS0 time slots assigned to the E1 channel.
Receiver has no alarms	Any alarms detected by the E1 controller are displayed here. Possible alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver is getting AIS. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms.
Framing	Framing type on the channelized controller.
Clock Source	Clock source controller. Values are internal and line.

Field	Description
Line Code Violations	Line Code Violations (LCVs) is a count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) that occur over the accumulation period. An EXZ increments the LCV by one regardless of the length of the zero string.
P-bit Coding Violation	For all DS3 applications, a P-bit coding violation (PCV) error event is a P-bit parity error event. A P-bit parity error event is the occurrence of a received P-bit code on the DS3 M-frame that is not identical to the corresponding locally calculated code.
Slip Secs	Controlled slip second (CSS) is a 1-second interval that contains one or more controlled slips.
Fr Loss Secs	Frame loss seconds (SELS) is the number of seconds for which an out-of-frame error is detected.
Line Err Secs	Line errored seconds (LES) is a second in which one or more line code violation errors are detected.
Degraded Mins	Degraded minute (DM) is a minute in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3. For more information, see RFC 1406, *Definitions of Managed Objects for DS1 and E1 Interface Types*.
Errored Secs	Errored seconds (ES) is a second with one or more path coding violations, one or more out-of-frame defects, or one or more controlled slip events or a detected AIS defect.
Bursty Err Secs	Bursty errored seconds (BES) is a second with fewer than 320 and more than one path coding violation error events, no severely errored frame defects, and no detected incoming AIS defects. Controlled slips are not included in this parameter.
Severely Err Secs	Severely errored seconds (SES) is a second with 320 or more path code violation errors events, one or more out-of-frame defects, or a detected AIS defect.
Unavailable Secs	Number of seconds during which the interface was not available in this interval, referred to as UAS.

Field	Description
Stuffed Secs	Stuffed seconds (SS) is a second in which one more bit stuffings take place. This happens when the Pulse Density Enforcer detects a potential violation in the output stream and inserts a 1 to prevent it. Such bit stuffings corrupt user data and indicate that the network is configured incorrectly. This counter can be used to help diagnose this situation.
Near-end path failures	Path failure (PFC)
Far-end path failures	(PFCFE)
SEF/AIS Secs	(SAS)

Related Commands

Command	Description
controller e1, on page 774	Configures an E1 controller and enters E1 configuration mode.

show controllers e3

To display information about the E3 links and hardware and software drivers for the E3 controller, use the **show controllers e3** command in EXEC mode.

show controllers e3 *interface-path-id* [**all**| **bert**| **brief**| **internal-state**| **tabular**]

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
all	Displays all information for the controllers.
bert	Displays internal E3 bit error rate test results.
brief	Displays summary information for the E3 controller.
internal-state	Displays internal E3 state information.
tabular	Displays E3 controller information in tabular format.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

Task ID

Task ID	Operations
interface	read

Examples

The following example shows sample output from the **show controllers e3** command for a single E3 port:

```
RP/0/0/CPU0:router# show controllers e3 0/2/0/0

  E3 0/2/0/0 is down
  Transmitter is sending RAI.
  Receiver has loss of frame.
  Framing is G.751, Line Code is B3ZS, Clock Source is Internal
  Subrate is enabled. Mode: Cisco(default), Bandwidth: 34010 kbps
  Remote accept is enabled
  Remote fullrate has no request outstanding
  Data in current interval (360 seconds elapsed):
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     360 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
```

The following example shows sample output from the **show controllers e3** command using the **tabular** keyword, for a single E3 port:

```
RP/0/0/CPU0:router# show controllers e3 0/2/0/0 tabular

  E3 0/2/0/0 is down
  Transmitter is sending RAI.
  Receiver has loss of frame.
  Framing is G.751, Line Code is B3ZS, Clock Source is Internal
  Subrate is enabled. Mode: Cisco(default), Bandwidth: 34010 kbps
  Remote accept is enabled
  Remote fullrate has no request outstanding
  INTERVAL      LCV   PCV   CCV   PES  PSES  SEFS   UAS   LES   CES  CSES
  07:49-07:56    0     0     0     0     0     0     380   0     0     0
  Data in current interval (380 seconds elapsed):
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     380 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
```

Table 50: show controllers e3 Field Descriptions

Field	Description
Transmitter is sending RAI	Any alarms detected by the controller are displayed here. Possible alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver is getting AIS. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms.
Framing	Framing type on the controller. Values are G.751 and G.832.
Line Code	Line coding format on the controller.
Clock Source	Clock source on the channelized controller. Values are internal and line.
Data in current interval (seconds elapsed)	Shows the current accumulation period, which rolls into the 24-hour accumulation every 15 minutes. The accumulation period is from 1 to 900 seconds. The oldest 15-minute period falls off the back of the 24-hour accumulation buffer.
Line Code Violations	Line Code Violations (LCVs) is a count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) that occur over the accumulation period. An EXZ increments the LCV by one regardless of the length of the zero string.
P-bit Coding Violation	For all DS3 applications, a P-bit coding violation (PCV) error event is a P-bit parity error event. A P-bit parity error event is the occurrence of a received P-bit code on the DS3 M-frame that is not identical to the corresponding locally calculated code.
C-bit Coding Violation	For C-bit parity and SYNTRAN DS3 applications, the C-bit coding violation (CCV) is the count of coding violations reported by the C-bits. For C-bit parity, it is the count of CP-bit parity errors that occur during the accumulation interval. For SYNTRAN, it is a count of CRC-9 errors that occur during the accumulation interval.

Field	Description
P-bit Err Secs	P-bit errored seconds (PES) is a second with one or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge does not increment when unavailable seconds are counted.
P-bit Severely Err Secs	P-bit severely errored seconds (PSES) is a second with 44 or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge does not increment when unavailable seconds are counted.
Severely Err Framing Secs	Severely errored framing seconds (SEFS) is a second with one or more out-of-frame defects or a detected incoming AIS.
Unavailable Secs	The number of unavailable seconds (UAS) is calculated by counting the number of seconds for which the interface is unavailable. For more information, see RFC 1407, *DS3 MIB Variables*.
Line Errored Secs	Line errored seconds (LES) is a second in which one or more code violations or one or more LOS defects occurred.
C-bit Errored Secs	C-bit errored seconds (CES) is a second with one or more C-bit code violations (CCV), one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.
C-bit Severely Errored Secs	C-bit severely errored seconds (CSES) is a second with 44 or more CCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.
Total Data (last 24 hours)	Shows the last 15-minute accumulation period.

Related Commands

Command	Description
controller e3, on page 776	Configures an E3 controller and enters E3 configuration mode.

show controllers t1

To display information about the T1 links and hardware and software drivers for the T1 controller, use the **show controllers t1** command in EXEC mode.

show controllers t1 *interface-path-id* [**all**| **bert**| **brief**| **internal-state**| **remote** {**performance brief**| **tabular**}| **tabular**]

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
all	Displays all information for the controllers.
bert	Displays internal T1 bit error rate test results.
brief	Displays summary information for the T1 controller.
internal-state	Displays internal T1 state information.
remote {**performance brief** | **tabular**}	Displays remote performance information in a brief summary or table format.
tabular	Displays T1 controller information in table format.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

When specifying a channelized T1 controller, use the following guidelines for the *interface-path-id*:

- The naming notation is *rack*/*slot*/*module*/*port*/*T3Num*/*T1num*.
- The slash between values is required as part of the notation.
- The following list describes the components of the notation:

- *rack*—Chassis number of the rack.
- *slot*—Physical slot number of the line card.
- *module*—Module number or subslot (for a SPA). A physical layer interface module (PLIM) is always 0.
- *port*—Physical port number of the interface.
- *T3num*—T3 controller number.
- *T1num*—T1 controller number.

- If specifying a virtual interface, the number range varies, depending on interface type.
- When specifying a virtual tributary group, the naming notation is *rack*/*slot*/*module*/*port*/*vtg*/*vt*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*—Chassis number of the rack.
  - *slot*—Physical slot number of the line card.
  - *module*—Module number or subslot (for a SPA). A physical layer interface module (PLIM) is always 0.
  - *port*—Physical port number of the interface.
  - *vtg*—Virtual tributary group.
  - *vt*—Virtual tributary instance.

Task ID

Task ID	Operations
interface	read

Examples

The following example shows sample output from the **show controllers t1** command with the **brief** keyword for a single T1 channel:

```
RP/0/0/CPU0:router# show controllers t1 0/4/2/0/1 brief

T1 0/4/2/0/1 is up
  mode: ATM
  timeslots: 1-24
  FDL per AT&T 54016 spec.
  Receiver has no alarms.
  Framing is ESF, Line Code is B8ZS, Clock Source is internal
  Alarm Soaking Interval:
                 Alarm Declaring= 2500 msec
                 Alarm clearing = 10000 msec

  Bert Test on controller port : T1 0/4/2/0/1
  BERT test result (not running)
     Test Pattern : Not Configured, Status : not running, Sync Detected : 0
     Interval : 1 minute(s), Time Remain : 0 (ms)
     Bit Errors (since BERT started): 0 bits,
     Bits Received (since BERT started): 0 Kbits
```

```
Bit Errors (since last sync): 0 bits
Bits Received (since last sync): 0 Kbits
```

Table 51: show controllers t1 brief Field Descriptions

Field	Description
T1 0/4/2/0/1 is up	T1 channel is operating. The channel state can be up, down, or administratively down. Loopback conditions are shown by (Locally Looped) or (Remotely Looped).
mode	Mode of the T1 controller, which can be ATM.
timeslots	DS0 time slots assigned to the T1 channel.
FDL per *spec-name* spec.	Performance monitoring is through Facility Data Link based on ANSI T1.403 specification or AT&T standard specification number 54016.
Receiver has no alarms.	Any alarms detected by the T1 controller are displayed here. Possible alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver is getting AIS. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms.
Framing	Framing type on the channelized controller. Values are ESF and SF.
Line Code	Line coding format on the channelized controller. Values are AMI or B8ZS.
Clock Source	Clock source on the T1 channel. Values are internal and line.
Alarm Soaking Interval	Values of the following alarm soaking intervals: • Alarm declarings: amount of time, in milliseconds, after which an alarm is declared. • Alarm clearing: amount of time, in milliseconds, after which an alarm is cleared.

Field	Description
Bert Test on controller port	Indicates controller port on which BERT test can be run.
BERT test result	Indicates the current state of the test. Can be one of the following: • running— BER test is still in progress. • done—BER test is complete. • not running—BER test is not running on the controller.
Test Pattern	Indicates the test pattern you selected for the test.
Status	Indicates the current synchronization state (sync).
Sync Detected	Indicates the number of times synchronization has been detected during this test.
Interval	Indicates the length of the test.
Time Remain	Indicates the time remaining for the test to run. **Note** If you terminate a BER test, you receive a message similar to the following: Time Remain : 2 minute(s) (unable to complete) "(Unable to complete)" signifies that you interrupted the test.
Bit Errors (since BERT started)	Bit errors that have been detected since the test started.
Bits Received (since BERT started)	Total number of test bits that have been received since the test started.
Bit Errors (since last sync)	Bit errors that have been detected since the synchronization started.
Bits Received (since last sync)	Total number of test bits that have been received since the synchronization started.

The following example shows sample output from the **show controllers t1** command for a single T1 channel:

```
RP/0/0/CPU0:router# show controllers t1 0/4/2/0/1

T1 0/4/2/0/1 is up
  mode: ATM
  timeslots: 1-24
  FDL per AT&T 54016 spec.
  Receiver has no alarms.
```

```
  Framing is ESF, Line Code is B8ZS, Clock Source is internal
  Data in current interval (38 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs, 0 Stuffed Secs
     0 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
  Data in Interval 1:
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs, 0 Stuffed Secs
     0 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
  Data in Interval 2:
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs, 0 Stuffed Secs
     0 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
.
.
.
```

The following example shows sample output from the **show controllers t1** command with the **tabular** keyword for a single T1 channel:

```
RP/0/0/CPU0:router# show controllers t1 0/4/2/0/1 tabular

T1 0/4/2/0/1 is up
  mode: ATM
  timeslots: 1-24
  FDL per AT&T 54016 spec.
  Receiver has no alarms.
  Framing is ESF, Line Code is B8ZS, Clock Source is internal
  INTERVAL      LCV   PCV   CSS  SEFS   LES    DM    ES   BES   SES   UAS    SSS
  08:30-08:35    0     0     0     0     0     0     0     0     0     0     0
  08:15-08:30    0     0     0     0     0     0     0     0     0     0     0
  08:00-08:15    0     0     0     0     0     0     0     0     0     0     0
  07:45-08:00    0     0     0     0     0     0     0     0     0     0     0
  07:30-07:45    0     0     0     0     0     0     0     0     0     0     0
  07:15-07:30    0     0     0     0     0     0     0     0     0     0     0
  07:00-07:15    0     0     0     0     0     0     0     0     0     0     0
  06:45-07:00    0     0     0     0     0     0     0     0     0     0     0
  06:30-06:45    0     0     0     0     0     0     0     0     0     0     0
  06:15-06:30    0     0     0     0     0     0     0     0     0     0     0
  06:00-06:15    0     0     0     0     0     0     0     0     0     0     0
  05:45-06:00    0     0     0     0     0     0     0     0     0     0     0
  05:30-05:45    0     0     0     0     0     0     0     0     0     0     0
  05:15-05:30    0     0     0     0     0     0     0     0     0     0     0
.
.
.
```

Table 52: show controllers t1 and show controllers t1 tabular Field Descriptions

Field	Description
T1 0/4/2/0/1 is up	T1 channel is operating. The channel state can be up, down, or administratively down. Loopback conditions are shown by (Locally Looped) or (Remotely Looped).
mode	Mode of the T1 controller, which can be ATM.
timeslots	DS0 time slots assigned to the T1 channel.

Field	Description
FDL per *spec-name* spec.	Performance monitoring is through Facility Data Link based on ANSI T1.403 specification or AT&T standard specification number 54016.
Receiver has no alarms.	Any alarms detected by the T1 controller are displayed here. Possible alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver is getting AIS. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms.
Framing	Framing type on the channelized controller. Values are ESF and SF.
Line Code	Line coding format on the channelized controller. Values are AMI or B8ZS.
Clock Source	Clock source on the T1 channel. Values are internal and line.
Data in current interval (seconds elapsed)	Shows the current accumulation period, which rolls into the 24-hour accumulation every 15 minutes. The accumulation period is from 1 to 900 seconds. The oldest 15-minute period falls off the back of the 24-hour accumulation buffer.
Line Code Violations	Line Code Violations (LCVs) is a count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) that occur over the accumulation period. An EXZ increments the LCV by one regardless of the length of the zero string.
Slip Secs	Controlled slip second (CSS) is a 1-second interval that contains one or more controlled slips.
Fr Loss Secs	Frame loss seconds (SELS) is the number of seconds for which an out-of-frame error is detected.
Line Err Secs	Line errored seconds (LES) is a second in which one or more line code violation errors are detected.

Field	Description
Degraded Mins	Degraded minute (DM) is a minute in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3. For more information, see RFC 1406, *Definitions of Managed Objects for DS1 and E1 Interface Types*.
Errored Secs	Errored seconds (ES) is a second with one or more path coding violations, one or more out-of-frame defects, or one or more controlled slip events or a detected AIS defect.
Bursty Err Secs	Bursty errored seconds (BES) is a second with fewer than 320 and more than one path coding violation error events, no severely errored frame defects, and no detected incoming AIS defects. Controlled slips are not included in this parameter.
Severely Err Secs	Severely errored seconds (SES) is a second with 320 or more path code violation errors events, one or more out-of-frame defects, or a detected AIS defect.
Unavailable Secs	Number of seconds during which the interface was not available in this interval, referred to as UAS.
Stuffed Secs	Stuffed seconds (SSS) is a second in which one more bit stuffings take place. This happens when the Pulse Density Enforcer detects a potential violation in the output stream and inserts a 1 to prevent it. Such bit stuffings corrupt user data and indicate that the network is configured incorrectly. This counter can be used to help diagnose this situation.
Near-end path failures	Total number of near-end path failures.
Far-end path failures	Total number of far-end path failures.
SEF/AIS Secs	Total number or Severely Errored Framing (SEF) and Alarm Indication Signal (AIS) errors.

Related Commands

Command	Description
controller t1, on page 778	

show controllers t3

To display information about the T3 links and hardware and software drivers for the T3 controller, use the **show controllers t3** command in EXEC mode.

show controllers t3 *interface-path-id* [**all**| **bert**| **brief**| **internal-state**| **tabular**]

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
all	Displays all information for the controllers.
bert	Displays internal T3 bit error rate test results.
brief	Displays summary information for the controller.
internal-state	Displays internal T3 state information.
tabular	Displays T3 controller information in tabular format.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.5.0	The command output was updated to display new fields.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- When specifying a T3 controller, the naming notation is *rack*/*slot*/*module*/*port*/*T3num*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*—Chassis number of the rack.
  - *slot*—Physical slot number of the line card or SIP.

- *module*—Module number or subslot (for a SPA). A physical layer interface module (PLIM) is always 0.
- *port*—Physical port number of the interface.
- *T3num*—T3 controller number.

- If specifying a virtual interface, the number range varies, depending on interface type.

Task ID

Task ID	Operations
interface	read

Examples

The following example shows sample output from the **show controllers t3** command using the **brief** keyword for a single T3 port:

```
RP/0/0/CPU0:router# show controllers t3 0/4/2/0/1 brief

T3 0/4/2/0 is up
  No alarms detected.
  mode: serial
  MDL transmission is disabled
    EIC: , LIC: , FIC: , UNIT:
     Path FI:
     Idle Signal PORT_NO:
     Test Signal GEN_NO:
  FEAC code received: No code is being received
  Framing is C-BIT Parity, Line Code is B3ZS, Clock Source is Internal
  Alarm Soaking Interval:
                 Alarm Declaring= 2500 msec
                 Alarm clearing = 10000 msec
  BERT test result (not running)
     Test Pattern : Not Configured, Status : not running, Sync Detected : 0
     Interval : 1 minute(s), Time Remain : 0 (ms)
     Bit Errors (since BERT started): 0 bits,
     Bits Received (since BERT started): 0 Kbits
     Bit Errors (since last sync): 0 bits
     Bits Received (since last sync): 0 Kbits
```

Table 53: show controllers t3 brief Field Descriptions

Field	Description
T3 0/4/2/0/1 is up	T3 channel is operating. The channel state can be up, down, or administratively down. Loopback conditions are shown by (Locally Looped) or (Remotely Looped).

Field	Description
No alarms detected	Any alarms detected by the controller are displayed here. Possible alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver is getting AIS. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms.
mode	Mode of the T3 controller, which can be ATM, serial, or T1serial or T1 .
MDL transmission	Status of the Maintenance Data Link (either enabled or disabled) and the values of the MDL message fields.
EIC	Equipment Identification Code.
LIC	Location Identification Code.
FIC	Frame Identification Code.
UNIT	Unit Identification Code.
Path FI	Path facility identifier.
Idle Signal PORT_NO	Identifies the port that initiates the idle signal message.
Test Signal GEN_NO	Generator number to send in test signal messages.

Field	Description
FEAC code received	Whether or not a far-end alarm code request is being received. Possible values are as follows: • DS3 Eqpt. Failure (SA) • DS3 LOS/HBER • DS3 Out-of-Frame • DS3 AIS Received • DS3 IDLE Received • DS3 Eqpt. Failure (NSA) • Common Eqpt. Failure (NSA) • Multiple DS1 LOS/HBER • DS1 Eqpt. Failure • Single DS1 LOS/HBER • DS1 Eqpt. Failure (NSA) • No code is being received
Framing	Framing type on the channelized controller. Values are auto-detect, M23, and C-Bit.
Line Code	Line coding format on the channelized controller. Values are AMI and B8ZS.
Clock Source	Clock source on the channelized controller. Values are internal and line.
Alarm Soaking Interval	Values of the following alarm soaking intervals: • Alarm declarings: amount of time, in milliseconds, after which an alarm is declared. • Alarm clearing: amount of time, in milliseconds, after which an alarm is cleared.
BERT test result	Indicates the current state of the test. Can be one of the following: • running—BER test is still in progress. • done—BER test is complete. • not running—BER test is not running on the controller.
Test Pattern	Indicates the test pattern you selected for the test.

Field	Description
Status	Indicates the current synchronization state (sync).
Sync Detected	Indicates the number of times synchronization has been detected during this test.
Interval	Indicates the length of the test.
Time Remain	Indicates the time remaining for the test to run. **Note** If you terminate a BER test, you receive a message similar to the following: Time Remain : 2 minute(s) (unable to complete) "(Unable to complete)" signifies that you interrupted the test.
Bit Errors (since BERT started)	Bit errors that have been detected since the test started.
Bits Received (since BERT started)	Total number of test bits that have been received since the test started.
Bit Errors (since last sync)	Bit errors that have been detected since the synchronization started.
Bits Received (since last sync)	Total number of test bits that have been received since the synchronization started.

The following example shows sample output from the **show controllers t3** command using the **tabular** keyword, for a single T3 port:

```
RP/0/0/CPU0:router# show controllers 0/4/2/0/1 tabular

T3 0/4/2/0/1 is up
  INTERVAL      LCV    PCV    CCV    PES   PSES   SEFS   UAS   LES   CES  CSES
  09:00-09:02    0      0      0      0      0      0      0     0     0     0
  08:45-09:00    0      0      0      0      0      0      0     0     0     0
  08:30-08:45    0      0      0      0      0      0      0     0     0     0
  08:15-08:30    0      0      0      0      0      0      0     0     0     0
  08:00-08:15    0      0      0      0      0      0      0     0     0     0
  07:45-08:00    0      0      0      0      0      0      0     0     0     0
  07:30-07:45    0      0      0      0      0      0      0     0     0     0
.
.
.
```

The following example shows sample output from the **show controllers t3** command for a single T3 port:

```
RP/0/0/CPU0:router# show controllers t3 0/4/2/0/1

  T3 0/4/2/0/1 is up
  No alarms detected.
  mode: serial
  MDL transmission is disabled
    EIC: , LIC: , FIC: , UNIT:
     Path FI:
```

```
    Idle Signal PORT_NO:
    Test Signal GEN_NO:
  FEAC code received: No code is being received
  Framing is C-BIT Parity, Line Code is B3ZS, Clock Source is Internal
  Data in current interval (695 seconds elapsed):
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     0 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
  Data in Interval 1:
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     0 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
  Data in Interval 2:
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     0 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
  Data in Interval 3:
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     0 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
.
.
.
```

Table 54: show controllers t3 and show controllers t3 tabular Field Descriptions

Field	Description
T3 0/4/2/0/1 is up	T3 channel is operating. The channel state can be up, down, or administratively down. Loopback conditions are shown by (Locally Looped) or (Remotely Looped).
No alarms detected	Any alarms detected by the controller are displayed here. Possible alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver is getting AIS. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms.
mode	Mode of the T3 controller, which can be ATM, serial, T1, or E1 serial or T1 ATM or serial .

Field	Description
MDL transmission	Status of the Maintenance Data Link (either enabled or disabled) and the values of the MDL message fields.
EIC	Equipment Identification code.
LIC	Location Identification code.
FIC	Frame Identification code.
UNIT	Unit Identification code.
Path FI	Path facility identifier.
Idle Signal PORT_NO	Identifies the port that initiates the idle signal message.
Test Signal GEN_NO	Generator number to send in test signal messages.
FEAC code received	Whether or not a far-end alarm code request is being received. Possible values are as follows: • DS3 Eqpt. Failure (SA) • DS3 LOS/HBER • DS3 Out-of-Frame • DS3 AIS Received • DS3 IDLE Received • DS3 Eqpt. Failure (NSA) • Common Eqpt. Failure (NSA) • Multiple DS1 LOS/HBER • DS1 Eqpt. Failure • Single DS1 LOS/HBER • DS1 Eqpt. Failure (NSA) • No code is being received
Framing	Framing type on the channelized controller. Values are M23 and C-Bit.
Line Code	Line coding format on the channelized controller. Values are AMI and B8ZS.
Clock Source	Clock source on the channelized controller. Values are internal and line.

Field	Description
Data in current interval (seconds elapsed)	Shows the current accumulation period, which rolls into the 24-hour accumulation every 15 minutes. The accumulation period is from 1 to 900 seconds. The oldest 15-minute period falls off the back of the 24-hour accumulation buffer.
Line Code Violations	Line Code Violations (LCVs) is a count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) that occur over the accumulation period. An EXZ increments the LCV by one regardless of the length of the zero string.
P-bit Coding Violation	For all DS3 applications, a P-bit coding violation (PCV) error event is a P-bit parity error event. A P-bit parity error event is the occurrence of a received P-bit code on the DS3 M-frame that is not identical to the corresponding locally calculated code.
C-bit Coding Violation	For C-bit parity and SYNTRAN DS3 applications, the C-bit coding violation (CCV) is the count of coding violations reported by the C-bits. For C-bit parity, it is the count of CP-bit parity errors that occur during the accumulation interval. For SYNTRAN, it is a count of CRC-9 errors that occur during the accumulation interval.
P-bit Err Secs	P-bit errored seconds (PES) is a second with one or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge does not increment when unavailable seconds are counted.
P-bit Severely Err Secs	P-bit severely errored seconds (PSES) is a second with 44 or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge does not increment when unavailable seconds are counted.
Severely Err Framing Secs	Severely errored framing seconds (SEFS) is a second with one or more out-of-frame defects or a detected incoming AIS.
Unavailable Secs	The number of unavailable seconds (UAS) is calculated by counting the number of seconds for which the interface is unavailable. For more information, see RFC 1407, *DS3 MIB Variables*.
Line Errored Secs	Line errored seconds (LES) is a second in which one or more code violations or one or more LOS defects occurred.

Field	Description
C-bit Errored Secs	C-bit errored seconds (CES) is a second with one or more C-bit code violations (CCV), one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.
C-bit Severely Errored Secs	C-bit severely errored seconds (CSES) is a second with 44 or more CCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.

Related Commands

Command	Description
controller t3, on page 780	Configures a T3 controller and enters T3 configuration mode.

shutdown (T1/E1)

To disable the T1 or E1 controller, use the **shutdown** command in T1 or E1 configuration mode. To restart a disabled T1 or E1 controller, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

T1 configuration

E1 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

Shutting down the T1 or E1 controller disables all functions on the interface and sends an AIS alarm to the network. The **shutdown** command marks the interface as unavailable. To check if the controller is disabled, use the **show controllers t1** or **show controllers e1** command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to bring up a controller that was previously shut down:

```
RP/0/0/CPU0:router(config)# controller t1 0/6/0/0/10
RP/0/0/CPU0:router(config-t1e1)# no shutdown
```

Related Commands

Command	Description
show controllers e1, on page 822	Displays information about the E1 links and hardware and software drivers for the E1 controller.

Command	Description
show controllers t1, on page 830	Displays information about the T1 links and hardware and software drivers for the T1 controller.

shutdown (T3/E3)

To disable a T3 or E3 controller, use the **shutdown** command in T3 or E3 configuration mode. To restart a disabled T3 or E3 controller, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

T3 configuration

E3 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

Shutting down the T3 or E3 controller disables all functions on the interface and sends an AIS alarm to the network. The **shutdown** command marks the interface as unavailable. To check if the controller is disabled, use the **show controllers t3** or **show controllers e3** command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to bring up a controller that was previously shut down:

```
RP/0/0/CPU0:router(config)# controller t3 0/6/0/0
RP/0/0/CPU0:router(config-t3)# no shutdown
```

Related Commands

Command	Description
show controllers e3, on page 826	Displays information about the E3 links and hardware and software drivers for the E3 controller.

Command	Description
show controllers t3, on page 837	Displays information about the T3 links and hardware and software drivers for the T3 controller.

speed (DS0)

To specify the speed of the underlying DS0s in a channel group, use the **speed** command in channel group configuration mode. To revert to the default speed, use the **no** form of this command.

speed *kbps*

no speed *kbps*

Syntax Description

kbps	Speed of the underlying DS0s in kilobits per second (kbps). Valid values are 56 and 64. The default is 64 kbps.

Command Default

The default speed is 64 kbps.

Command Modes

Channel group configuration for T1

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

Before the channel group configuration is valid, you must define the associated DS0 time slots using the **timeslots** command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to define the speed for the underlying DS0 to be 56 kbps:

```
RP/0/0/CPU0:router(config)# controller t1 0/6/0/0/10
RP/0/0/CPU0:router(config-t1e1)# channel-group 5
RP/0/0/CPU0:router(config-t1e1-channel_group)# speed 56
```

Related Commands

Command	Description
timeslots, on page 852	Associates one or more DS0 time slots to a channel group and create an associated serial subinterface.

Command	Description
channel-group, on page 764	Configures a DS0 channel group and enters channel group configuration mode.

timeslots

To associate one or more DS0 time slots to a channel group and create an associated serial subinterface, use the **timeslots** command in channel group configuration mode. To unassign the DS0 time slots and delete the associated serial interface, use the **no** form of this command.

timeslots *range*

no timeslots

Syntax Description

range

Command Default

No default behavior or values

Command Modes

Channel group configuration for T1 and E1

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

The time slot range must match the DS0 time slots assigned to the channel group. The service provider defines the DS0 time slots that compose a channel group.

Before the channel group configuration is valid, you must define the associated DS0 time slots using the **timeslots** command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to associate DS0 time slots 1, 6, 8, 9 and 10 to channel group 5:

```
RP/0/0/CPU0:router(config)# controller t1 0/6/0/0/10
RP/0/0/CPU0:router(config-t1e1)# channel-group 5
RP/0/0/CPU0:router(config-t1e1-channel_group)# timeslots 1:6:8-10
```

Related Commands

Command	Description
framing (E1), on page 800	Selects the frame type for an E1 data line.
framing (T1), on page 804	Selects the frame type for a T1 data line.
speed (DS0), on page 850	Specifies the speed of the underlying DS0s in a channel group.
channel-group, on page 764	Configures a DS0 channel group and enters channel group configuration mode.

yellow

To enable detection and generation of T1 yellow alarms, use the **yellow** command in T1 configuration mode. To disable detection and generation of T1 yellow alarms, use the **no** form of this command.

yellow {**detection**| **generation**} {**disable**| **enable**}

no yellow {**detection**| **generation**} {**disable**| **enable**}

Syntax Description

detection	Detects yellow alarms.
generation	Generates yellow alarms.
disable	Disables detection or generation of T1 yellow alarms.
enable	Enables detection or generation of T1 yellow alarms. The default is enable.

Command Default

Yellow alarms are detected and generated on the T1 channel.

Command Modes

T1 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

If the T1 framing type is super frame (SF), you should consider disabling yellow alarm detection as the yellow alarm can be incorrectly detected with SF framing.

Serial interface may flap and eventually, go down if yellow alarm detection is not disabled on its T1 controller configured with SF framing.

The default state of the **yellow** command is enabled. If you disable yellow alarm detection and want to reenable it, you can use the **no** form of the command. Alternatively, you can use the **enable** keyword.

The **yellow** command is only applicable to T1 lines.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to disable yellow alarm generation:

```
RP/0/0/CPU0:router(config)# controller t1 0/6/0/0/10
RP/0/0/CPU0:router(config-t1e1)# yellow generation disable
```

yellow

802.1Q VLAN Subinterface Commandsonthe Cisco IOS XR Software

This module provides command line interface (CLI) commands for configuring 802.1Q VLANs on the Cisco XR 12000 Series Router.

dot1q native vlan

To assign the native VLAN ID of a physical interface trunking 802.1Q VLAN traffic, use the **dot1q native vlan** command in interface configuration mode. To remove the VLAN ID assignment, use the **no** form of this command.

dot1q native vlan *vlan-id*

no dot1q native vlan *vlan-id*

Syntax Description

vlan-id	Trunk interface ID. Range is from 1 to 4094 inclusive (0 and 4095 are reserved).

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was first supported.

Usage Guidelines

The **dot1q native vlan** command defines the default, or native VLAN, associated with a 802.1Q trunk interface. The native VLAN of a trunk interface is the VLAN to which all untagged VLAN packets are logically assigned.

Note The native VLAN cannot be configured on a subinterface of the trunk interface. The native VLAN must be configured with the same value at both ends of the link, or traffic can be lost or sent to the wrong VLAN.

Task ID

Task ID	Operations
vlan	read, write

Examples

The following example shows how to configure the native VLAN of a TenGigE0/2/0/4 trunk interface as 1. Packets received on this interface that are untagged, or that have an 802.1Q tag with VLAN ID 1, are received on the main interface. Packets sent from the main interface are transmitted without an 802.1Q tag.

```
RP/0/0/CPU0:router(config)# interface TenGigE 0/2/0/4
```

```
RP/0/0/CPU0:router(config-if)# dot1q native vlan 1
```

Related Commands

Command	Description
dot1q vlan, on page 860	Assigns a VLAN ID to a subinterface (or modifies the VLAN ID that is currently assigned to a subinterface).

dot1q vlan

To assign a VLAN ID to a subinterface (or to modify the VLAN ID that is currently assigned to a subinterface), use the **dot1q vlan** command in subinterface configuration mode. To remove the VLAN ID assigned to a subinterface, use the **no** form of this command.

dot1q vlan *vlan-id* [*vlan-id2*| **any**]

no dot1q vlan *vlan-id*

Syntax Description

vlan-id	ID of the subinterface. Range is from 1 to 4094 (0 and 4095 are reserved).
vlan-id2	(Optional) Identifies the host VLAN of a Q-in-Q VLAN pair. Replace *vlan-id2* with a number that specifies the host VLAN. Range is from 1 to 4094.
any	(Optional) Identifies the host VLAN of a Q-in any VLAN pair.

Command Default

No default behavior or values

Command Modes

Subinterface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

The VLAN ID specifies where 802.1Q tagged packets are sent and received on a specified subinterface. An 802.1Q VLAN subinterface must have a configured VLAN ID to send and receive traffic; without a VLAN ID, the subinterface remains in the down state. All VLAN IDs must be unique among all subinterfaces configured on the same physical interface. To change a VLAN ID, the new VLAN must not already be in use on the same physical interface. To exchange VLAN IDs, you must remove the configuration information and reconfigure the ID for each device.

Note The subinterface does not pass traffic without an assigned VLAN ID.

Task ID

Task ID	Operations
vlan	read, write

Examples

This example shows how to configure the VLAN ID and IP address on a subinterface:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface TenGigE 0/2/0/4.1
RP/0/0/CPU0:router(config-subif)# dot1q vlan 10
RP/0/0/CPU0:router(config-subif)# ipv4 addr 10.0.0.1/24
```

This example shows how to configure the VLAN IDs for both VLANS in a single Q-in-Q attachment circuit (AC). In this case, incoming traffic must match both of the VLAN IDs before it is accepted by the subinterface:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface TenGigE 0/2/0/4.1
RP/0/0/CPU0:router(config-subif)# dot1q vlan 10 20
```

This example shows how to configure the VLAN IDs for a Q-in-any AC. In this case, all incoming traffic must have two VLAN tags, where the outer VLAN ID matches the configured value, while the inner VLAN ID can be any value.

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface TenGigE 0/2/0/4.1 l2transport
RP/0/0/CPU0:router(config-subif)# dot1q vlan 10 any
```

Related Commands

Command	Description
dot1q native vlan, on page 858	Assigns the native VLAN ID of a physical interface trunking 802.1Q VLAN traffic.
show interfaces, on page 423	Displays statistics for all interfaces configured on the router or for a specific node.
show vlan interface, on page 864	Displays summarized information about VLAN subinterfaces.
show vlan tags, on page 866	Displays VLAN tagging allocation information.

interface (VLAN)

To create a VLAN subinterface, use the **interface** command in global configuration mode. To delete a subinterface, use the **no** form of this command.

interface *type interface-path-id.subinterface* **[l2transport]**

no interface *type interface-path-id.subinterface* **[l2transport]**

Syntax Description

type	Type of Ethernet interface on which you want to create a VLAN. Enter **GigabitEthernet**, **TenGigE**, **FastEthernet**, or **Bundle-Ether**.
interface-path-id.subinterface	Physical interface or virtual interface followed by the subinterface path ID. Naming notation is *interface-path-id.subinterface*. The period in front of the subinterface value is required as part of the notation. For more information about the syntax for the router, use the question mark (?) online help function.
l2transport	Enables Layer 2 transport port mode on the specified VLAN interface and enters Layer 2 transport configuration mode. The l2transport keyword creates the Vlan interface in L2 mode so that it can be used for L2VPNs and local switching.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.

- If specifying an Ethernet bundle interface, the range is from 1 through 65535.

For the *subinterface* argument, the range is from 0 through 4095.

To configure a large number of subinterfaces, we recommend entering all configuration data before you commit the **interface** command.

To change an interface from Layer 2 to Layer 3 mode and back, you must delete the interface first and then re-configure it in the appropriate mode.

Note A subinterface does not pass traffic without an assigned VLAN ID.

Task ID

Task ID	Operations
vlan	read, write

Examples

This example shows how to configure a VLAN subinterface on a 10-Gigabit Ethernet interface:

```
RP/0/0/CPU0:router(config)# interface TenGigE 0/0/0/1.2
RP/0/0/CPU0:router(config-subif)# dot1q vlan 1
RP/0/0/CPU0:router(config-subif)# ipv4 address 50.0.0.1/24
```

This example shows how to create a VLAN subinterface with Layer 2 transport port mode enabled, and enter Layer 2 transport configuration mode under that VLAN:

```
RP/0/0/CPU0:router(config)# interface GigabitEthernet 0/4/0/1.1
RP/0/0/CPU0:router(config-if-l2)#
```

Related Commands

Command	Description
dot1q native vlan, on page 858	Assigns the native VLAN ID of a physical interface trunking 802.1Q VLAN traffic.
dot1q vlan, on page 860	Assigns a VLAN ID to a subinterface (or modifies the VLAN ID that is currently assigned to a subinterface).

show vlan interface

To display summarized information about VLAN subinterfaces, use the **show vlan interface** command in EXEC mode.

show vlan interface [*type interface-path-id.subinterface*| **location** *instance*]

Syntax Description

type	(Optional) Type of Ethernet interface whose VLAN information you want to display. Enter **GigabitEthernet**, **TenGigE**, **FastEthernet**, or **Bundle-Ether**.
interface-path-id .subinterface	Physical interface or virtual interface followed by the subinterface path ID. Naming notation is *interface-path-id.subinterface*. The period in front of the subinterface value is required as part of the notation. For more information about the syntax for the router, use the question mark (?) online help function.
location *instance*	(Optional) Displays VLAN subinterfaces on a particular port. The *instance* argument is entered in the *rack*/*slot*/*module*/*port* notation.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.
- If specifying an Ethernet bundle interface, the range is from 1 through 65535.

For the *subinterface* argument, the range is from 0 through 4095.

Enter the **show vlan interface** command without including any of the optional parameters to display summarized information about all VLANs configured on the router.

Task ID

Task ID	Operations
vlan	read

Table 55: show vlan interface Field Descriptions

Field	Description
interface	VLAN subinterface.
encapsulation	Encapsulation of the VLAN subinterface. Currently, this is always 802.1Q.
Outer VLAN	VLAN ID currently assigned to the subinterface. Range is from 1 to 4094 (or blank if no VLAN ID has been assigned).
2nd VLAN	VLAN ID currently assigned to the second subinterface in a pair. Range is from 1 to 4094 (or blank if no VLAN ID has been assigned). For Q-in-any VLANS, this field shows “Any.”
Service	Service currently assigned to the VLAN. Possible services are L2 and L3.
MTU	Maximum transmission unit (MTU) value configured for the specified VLAN, in bytes.
LineP state	Displays the line protocol state of the VLAN interface. Possible states: up, down, admin-down. The line protocol state reflects whether a VLAN ID is configured or not.

Related Commands

Command	Description
show interfaces, on page 423	Displays statistics for all interfaces configured on the router or for a specific node.
show vlan trunks, on page 868	Displays information about VLAN trunks.

show vlan tags

To display VLAN tagging allocation information, use the **show vlan tags** command in EXEC mode.

show vlan tags [*type interface-path-id*| **location** *node-id*]

Syntax Description

type	Displays VLAN tagging information for a specific bundle type. **Note** Use the **show interfaces** command with the **Bundle-Ether**, **FastEthernet**, **GigabitEthernet** or **TenGigE** keyword to see a list of all Ethernet bundles currently configured on the router.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location *node-id*	Displays VLAN tagging information for a specific node. The *node-id* argument is entered in the *rack*/*slot*/*module* notation.

Command Default

Enter the command without any of the optional keywords or arguments to display tagging allocation information for all VLANS configured on the router.

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.
- If specifying an Ethernet bundle interface, the range is from 1 through 65535.

Task ID

Task ID	Operations
vlan	read

Examples

The following example shows how to display VLAN tagging allocation information for a router:

```
RP/0/0/CPU0:router(config-subif)# show vlan tagsl2protocol cdp drop

Interface           Outer  2nd   Service  MTU    LineP
                    VLAN   VLAN                  State
Gi0/1/5/0.1           10          L3        1518  up
Gi0/1/5/0.2           20          L3        1518  up
Gi0/1/5/0.3           30          L3        1518  up
```

Table 56: show vlan tags Field Descriptions

Field	Description
Outer Vlan	The first (outermost) 802.1Q VLAN ID. This field is empty if no VLAN ID is configured. An asterisk (*) indicate the native VLAN.
2nd Vlan	The second 802.1Q VLAN ID. This field reports “any” for a Q-in-Any service. If no VLAN ID is configured, then this field is empty.
Service	Service currently assigned to the subinterface. Can be Layer 2 (L2) or Layer 3 (L3).
MTU	Maximum transmission unit (MTU) value configured for the specified VLAN, in bytes.
LineP state	Displays the state of the VLAN interface. Possible states: up, down, admin-down.

Related Commands

Command	Description
dot1q vlan, on page 860	Assigns a VLAN ID to a subinterface (or modifies the VLAN ID that is currently assigned to a subinterface).
show vlan interface, on page 864	Displays summarized information about VLAN subinterfaces.
show vlan trunks, on page 868	Displays information about VLAN trunks.

show vlan trunks

To display information about VLAN trunks, use the **show vlan trunks** command in EXEC mode.

show vlan trunks [brief] [**location** *node-id*] [*type interface-path-id*] **[summary]**

Syntax Description

type	(Optional) Type of Ethernet interface whose VLAN trunk information you want to display. Possible Ethernet types are **GigabitEthernet**, **TenGigE** , **FastEthernet**, or **Bundle-Ether**.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
brief	(Optional) Displays a short summary output.
summary	(Optional) Displays a summarize output. **Note** The **summary** option can be specified only if the trunk interface is not specified.
location *node-id*	(Optional) Displays VLAN trunk information for a specific node. The *node-id* is expressed in the *rack/slot/module* notation. **Note** For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.

- *slot*: Physical slot number of the line card.
- *module*: Module number. A physical layer interface module (PLIM) is always 0.
- *port*: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

The **show vlan trunks** command provides summary information about VLAN trunk interfaces. It is used to determine the number of configured subinterfaces and verify the state of the subinterfaces.

Task ID

Task ID	Operations
vlan	read

Examples

The following is sample output from the **show vlan trunks** command:

```
RP/0/0/CPU0:router# show vlan trunks

GigabitEthernet0/4/0/0 is up
  Outer VLAN tag format is Dot1Q (0x8100)
  L3 Encapsulations: Ether, 802.1Q
    Sub-interfaces: 2
      2 are up
      Single tag sub-interfaces: 2
    No native VLAN Id
  L2 Encapsulations: 802.1Q
    VLAN ACs: 1
      1 are up
      Single tag ACs: 1
```

Table 57: show vlan trunks summary Field Descriptions

Field	Description
Outer VLAN tag format	The first (outermost) 802.1Q VLAN Id. • This field is empty if no VLAN ID is configured. • An asterisk (*) indicates that a native VLAN is configured.

Field	Description
L3 Encapsulations	VLAN encapsulations currently used for terminated Layer 3traffic. Possible Layer 3 encapsulations are as follows: • Nat – A Native VLAN is configured. • Q – One or more sub-interfaces are configured with either 0 or 1 802.1Q VLAN tags. • 2Q – One or more sub-interfaces have been configured with two 802.1Q VLAN tags.
Sub-interfaces	The number of subinterfaces configured on the main Ethernet interface, and the current state of those subinterfaces. Possible states are up, down, and admin-down. **Note** The number of Down and Admin-down subinterfaces is only reported only if that number is greater than 0.
Single tag sub-interfaces:	Number of sub-interfaces configured with a single 802.1Q tag. **Note** The number of sub-interfaces is displayed only if that number is greater than 0.
No native VLAN Id	Indicate that a native VLAN ID is not configured on this interface.
L2 Encapsulations:	VLAN encapsulations currently used for terminated L2 traffic. Possible Layer 2 encapsulations are as follows: • Q – One or more single 802.1Q tag ACs are configured. • 2Q – One or more double 802.1Q tag ACs have been configured. • Qany – One or more double 802.1Q tag ACs have been configured that have a wildcard “any” innertag.
VLAN ACs	Number of ACs currently configured under the specified interface.
Single tag ACs	**Note** The number of sub-interfaces sub-interfaces configured with a single 802.1Q tag is displayed only if that number is greater than 0.

Related Commands

Command	Description
show interfaces, on page 423	Displays statistics for all interfaces configured on the router or for a specific node.
interface (VLAN), on page 862	Creates a VLAN subinterface.

INDEX

D

E

F

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Y