Interface and Hardware Component Command Reference for Cisco CRS Routers, IOS XR Release 6.4.x

First Published: 2018-03-23

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

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

CONTENTS

Preface

This command reference describes the Cisco IOS XR Interfaces commands.

The preface for the *Interface and Hardware Component Command Reference for Cisco CRS Routers* contains the following sections:

Changes to This Document

Table 1: Changes to This Document

Date	Summary
Nov 2017	Initial release of the cumulative command reference document that covers all updates from Release 4.3.0 onwards.
March 2018	Republished for Release 6.3.2.
March 2018	Republished for Release 6.4.1.
July 2018	Republished for Release 6.5.1.
December 2018	Republished for Release 6.6.1
January 2019	Republished for Release 6.5.2
May 2019	Republished for Release 6.6.25.
August 2019	Republished for Release 7.0.1.
December 2019	Republished for Release 6.6.3
January 2020	Republished for Release 7.1.1
August 2020	Republished for Release 7.1.2
November 2020	Republished for Release 7.1.3

Date	Summary
February 2021	Republished for Release 7.3.1
July 2021	Republished for Release 7.4.1
November 2021	Republished for Release 7.5.1

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

ATM Commands

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 3.9.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/RP0/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 3.9.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/RP0/CPU0:router(config-if)# atm ilmi-config disable
```

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

```
RP/0/RP0/CPU0:router# configure
```

```
RP/0/RP0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/RP0/CPU0:router(config-if)# no atm ilmi-config disable
```

Related Commands

Command	Description
show atm ilmi-status, on page 53	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 3.9.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/6/0/1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/RP0/CPU0:router(config-if)# no atm ilmi-keepalive
```

Related Commands

Command	Description
show atm ilmi-status, on page 53	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 3.9.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/6/0/1
RP/0/RP0/CPU0:router(config-if)# no atm ilmi-trap disable
```

Related Commands

Command	Description
show atm interface atm, on page 55	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 3.9.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/RP0/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/RP0/CPU0:router# configure
```

```
RP/0/RP0/CPU0:router(config)# interface atm 0/6/0/1
RP/0/RP0/CPU0:router(config-if)# no atm maxvpi-bits 12
```

Related Commands

Command	Description
show atm interface atm, on page 55	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 3.7.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/RP0/CPU0:router(config-if)# atm mcpt-timers 50 100 200
RP/0/RP0/CPU0:router(config-if)# l2transport
RP/0/RP0/CPU0:router(config-if-l2)# cell-packing 6 1
```

Related Commands

Command	Description
cell-packing, on page 14	Configures the maximum number of cells allowed per packet, and specifies a MCPT timer for cell packing.
show atm interface atm, on page 55	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 3.9.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/6/0/0
RP/0/RP0/CPU0:router(config-if)# no atm oam flush
```

Related Commands

Command	Description
show atm interface atm, on page 55	Displays ATM-specific information about an ATM interface.

Command	Description
show atm class-link, on page 50	Displays configuration information for the parameters on a VC class that is associated with a particular PVC.
show atm vc-class, on page 71	Displays information about all ATM VC classes on the router or for a specific ATM VC-class.

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 3.7.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the atm mcpt-timers, on page 10 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/6/0/0
```

```
RP/0/RP0/CPU0:router(config-if)# l2transport
RP/0/RP0/CPU0:router(config-if-l2)# cell-packing 6 3
```

Related Commands

Command	Description
atm mcpt-timers, on page 10	Defines the three MCPT timers under a main ATM interface.
show atm cell-packing, on page 48	Displays cell packing information for the Layer 2 attachment circuits (ACs) configured on your system.
show atm interface atm, on page 55	Displays ATM-specific information about an ATM interface.
show atm pvc, on page 60	Displays ATM PVC and traffic information for the entire router.
show atm pvp, on page 66	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 3.9.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)#vc-class atm classA
RP/0/RP0/CPU0:router(config-vc-class-atm)# shape cbr 40000
RP/0/RP0/CPU0:router(config-vc-class-atm)# encapsulation aal5snap
```

```
RP/0/RP0/CPU0:router(config-vc-class-atm)# oam-pvc manage 300
RP/0/RP0/CPU0:router(config-vc-class-atm)# commit
RP/0/RP0/CPU0:router(config-vc-class-atm)# exit
RP/0/RP0/CPU0:router(config)# interface atm 0/6/0/1
RP/0/RP0/CPU0:router(config-if)# class-int classA
RP/0/RP0/CPU0:router(config-if)#
```

Related Commands

Command	Description
show atm class-link, on page 50	Displays configuration information for the parameters on a VC class that is associated with a particular PVC.
show atm vc-class, on page 71	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 3.9.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# vc atm classA
RP/0/RP0/CPU0:router(config-vc-class-atm)# shape cbr 40000
```

```
RP/0/RP0/CPU0:router(config-vc-class-atm)# commit
RP/0/RP0/CPU0:router(config-vc-class-atm)# exit
RP/0/RP0/CPU0:router(config)# interface atm 0/6/0/1.1 point-to-point
RP/0/RP0/CPU0:router(config-if)# pvc 10/100
RP/0/RP0/CPU0:router(config-atm-vc)# class-vc classA
RP/0/RP0/CPU0:router(config-atm-vc)#
```

Related Commands

Command	Description
show atm class-link, on page 50	Displays configuration information for the parameters on a VC class that is associated with a particular PVC.
show atm vc-class, on page 71	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 3.7.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# vc atm classA
RP/0/RP0/CPU0:router(config-vc-class-atm)# encapsulation aal5snap
```

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/2/0/0.1 point-to-point
RP/0/RP0/CPU0:router(config-subif)# pvc 10/100
RP/0/RP0/CPU0:router(config-atm-vc)# encapsulation aal5mux
```

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# vc atm classA
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/6/0/1.10 l2transport
RP/0/RP0/CPU0:router(config-if)# pvc 30/300
RP/0/RP0/CPU0:router(config-atm-l2transport-pvc)# encapsulation aal0
```

Related Commands

Command	Description
show atm pvc, on page 60	Displays ATM PVC and traffic information for the entire router.
show atm vc-class, on page 71	Displays information about all ATM VC classes on the router or for a specific ATM VC-class.

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 3.7.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router(config)# interface atm 0/2/0/0
RP/0/RP0/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/RP0/CPU0:router(config)# interface atm 0/2/0/0.1 point-to-point
RP/0/RP0/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/RP0/CPU0:router(config)#interface atm 0/2/0/0.1 l2transport
RP/0/RP0/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/RP0/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 31 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/6/0/1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/2/0/0.1 point-to-point
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/2/0/0.1 l2transport
RP/0/RP0/CPU0:router(config-if)#
```

Related Commands

Command	Description
show atm interface atm, on page 55	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 3.7.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/2/0/0
RP/0/RP0/CPU0:router(config-if)# l2transport
RP/0/RP0/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/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface ATM 0/2/0/0
RP/0/RP0/CPU0:router(config-if)# l2transport
RP/0/RP0/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 31 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 3.9.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/2/0/0.1 point-to-point
RP/0/RP0/CPU0:router(config-subif)# pvc 50/100
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# vc atm classA
RP/0/RP0/CPU0:router(config-vc-class-atm)# oam ais-rdi 30 10
```

Related Commands

Command	Description
show atm class-link, on page 50	Displays configuration information for the parameters on a VC class that is associated with a particular PVC.
show atm pvc, on page 60	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 3.9.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/2/0/0.1 point-to-point
RP/0/RP0/CPU0:router(config-subif)# pvc 10/100
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/2/0/0.1 point-to-point
RP/0/RP0/CPU0:router(config-subif)# pvc 10/100
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# vc atm classA
RP/0/RP0/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/RP0/CPU0:router# configure
```

```
RP/0/RP0/CPU0:router(config)# vc atm classA
RP/0/RP0/CPU0:router(config-vc-class-atm)# no oam-pvc manage
```

Related Commands

Command	Description
show atm class-link, on page 50	Displays configuration information for the parameters on a VC class that is associated with a particular PVC.
show atm pvc, on page 60	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 3.9.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/2/0/0.1 point-to-point
RP/0/RP0/CPU0:router(config-subif)# pvc 10/100
RP/0/RP0/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/RP0/CPU0:router# configure
```

```
RP/0/RP0/CPU0:router(config)# vc atm classA
RP/0/RP0/CPU0:router(config-vc-class-atm)# oam retry 10 20 10
```

Related Commands

Command	Description
show atm class-link, on page 50	Displays configuration information for the parameters on a VC class that is associated with a particular PVC.
show atm pvc, on page 60	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 3.9.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router# ping atm interface atm 0/2/0/0.10 10/100
```

Related Commands

Command	Description
show atm interface atm, on page 55	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 3.9.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/2/0/0.1 point-to-point
RP/0/RP0/CPU0:router(config-if)# pvc 10/100
RP/0/RP0/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/RP0/CPU0:router# configure
```

```
RP/0/RP0/CPU0:router(config-if)# interface atm 0/2/0/0.1 point-to-point
RP/0/RP0/CPU0:router(config-subif)# pvc 20/200
RP/0/RP0/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/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config-if)# interface atm 0/2/0/0.1 l2transport
RP/0/RP0/CPU0:router(config-subif)# pvc 20/200
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/6/0/1
RP/0/RP0/CPU0:router(config-if)# pvc 5/100 ilmi
```

```
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config-if)# interface atm 0/2/0/0.1 point-to-point
RP/0/RP0/CPU0:router(config-subif)# pvc 20/200
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config-if)# interface atm 0/2/0/0.1 l2transport
RP/0/RP0/CPU0:router(config-subif)# pvc 20/200
RP/0/RP0/CPU0:router(config-atm-l2transport-pvc)#
```

Related Commands

Command	Description
show atm class-link, on page 50	Displays configuration information for the parameters on a VC class that is associated with a particular PVC.
show atm pvc, on page 60	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 3.7.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config-if)# interface atm 0/2/0/0.1 l2transport
RP/0/RP0/CPU0:router(config-subif)# pvp 20
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config-if)# interface atm 0/2/0/0.1 l2transport
RP/0/RP0/CPU0:router(config-subif)# pvp 20
RP/0/RP0/CPU0:router(config-atm-l2transport-pvp)#
```

Related Commands

Command	Description
show atm pvp, on page 66	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)

Command History

Release	Modification
Release 3.7.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router#config
RP/0/RP0/CPU0:router(config)# interface atm 0/6/0/0.2 point-to-point
RP/0/RP0/CPU0:router(config-subif)# pvc 20/200
RP/0/RP0/CPU0:router(config-atm-vc)# shape ubr 150000
```

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

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# vc-class atm class1
RP/0/RP0/CPU0:router(config-vc-class-atm)# shape vbr-nrt 100000 100000 8000
RP/0/RP0/CPU0:router(config-vc-class-atm)# exit
RP/0/RP0/CPU0:router(config)# exit
Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:y
RP/0/RP0/CPU0:router#
```

Related Commands

Command	Description
show atm pvc, on page 60	Displays ATM PVC and traffic information for the entire router.
show atm pvp, on page 66	Displays ATM PVP and traffic information for the entire router, or a specific VPI or ATM 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 3.7.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
atm	read

Examples

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

```
RP/0/RP0/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 2: 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.
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.

Field	Description
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 3.9.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/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 3: show atm class-link Field Descriptions, on page 51 describes the significant fields shown in the display.

Table 3: 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.
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.

Field	Description
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/RP0/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 16	Assigns a VC class to an ATM main interface.
vc-class atm, on page 79	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 3.9.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
atm	read

Examples

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

```
RP/0/RP0/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/RP0/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 4: 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.
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 3	Disables ILMI on an ATM interface.
atm ilmi-keepalive, on page 5	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 3.7.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
atm	read

Examples

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

```
RP/0/RP0/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 5: 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.
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.
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.

Field	Description
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 23	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 3.9.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
atm	read

Examples

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

```
RP/0/RP0/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 6: 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.
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.
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.

Field	Description
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/RP0/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 7: 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.
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 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.
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.

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. 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 39	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 3.7.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/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 8: 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.

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 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/RP0/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 9: 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.
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.

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.
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 43	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 3.9.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
atm	read

Examples

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

```
RP/0/RP0/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 10: 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.
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.

Field	Description
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.
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/RP0/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 18	Attaches a VC class to an ATM PVC.
vc-class atm, on page 79	Creates a VC class for an ATM PVC or an ATM interface and enters VC-class 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 3.7.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
interface	read

Examples

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

```
RP/0/RP0/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.
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.

Field	Description
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.
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.

Field	Description
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.
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 55	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 3.7.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface atm 0/2/0/0
RP/0/RP0/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/RP0/CPU0:router# no shutdown
```

Related Commands

Command	Description
show atm interface atm, on page 55	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 3.9.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router(config)# vc-class atm classA
RP/0/RP0/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/RP0/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/RP0/CPU0:router(config)# vc-class atm class1
RP/0/RP0/CPU0:router(config-vc-class-atm)#
```

Related Commands

Command	Description
class-vc, on page 18	Attaches a VC class to an ATM PVC.
show atm vc-class, on page 71	Displays information about all ATM VC classes on the router or for a specific ATM VC-class.

Dense Wavelength Division Multiplexing Commands

This module provides command line interface (CLI) commands for configuring dense wavelength division multiplexing (DWDM) on the Cisco CRS Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

admin-state

To configure the transport administration state on a DWDM port, use the **admin-state** command in DWDM configuration mode. To return the administration state from a DWDM port to the default, use the **no** form of this command.

admin-state in-service | maintenance | out-of-service

Syntax Description

in-service	Places the DWDM port in In Service (IS) state, to support all normal operation.
maintenance	Places the DWDM port in Out of Service Maintenance (OOS-MT) state to perform configuration, while the laser and G.709 framer remain up.
out-of-service	Places the DWDM port in Out of Service (OOS) state. The laser is turned off and all traffic flow is stopped. This is the default.

Command Default

Out-of-service is the default transport administration state.

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced. It replaced the **laser** and **shutdown (DWDM)** commands.
Release 3.9.1	The **maintenance** keyword was added.

Usage Guidelines

When you configure **admin-state maintenance**, the DWDM port is placed in OOS-MT state and any configuration of **maintenance disable** for the port can be overridden. The laser for the port and the G.709 framing remains enabled, and Fast Re-Route (FRR) is triggered. This form of the command is usually used in FRR context for traffic to move over backup path while maintenance is going on.

When you configure **admin-state out-of-service**, the DWDM port is placed in OOS state. The laser is turned off, traffic flow is stopped, and proactive protection is disabled. However, configuration changes can still be made on the port.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The following example shows how to turn on the laser and place a DWDM port in In Service (IS) state:

Note This is a required configuration beginning in Cisco IOS XR Software Release 3.9.0 and later releases. The DWDM cards will not operate without this configuration.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# controller dwdm 0/1/0/1
RP/0/RP0/CPU0:router(config-dwdm)# admin-state in-service
RP/0/RP0/CPU0:router(config-dwdm)# commit
```

The following example shows how to stop all operation on a DWDM port:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# controller dwdm 0/1/0/1
RP/0/RP0/CPU0:router(config-dwdm)# admin-state out-of-service
```

The following example shows how to enable the out-of-service maintenance transport administration state on a DWDM port:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# controller dwdm 0/1/0/1
RP/0/RP0/CPU0:router(config-dwdm)# admin-state maintenance
```

Related Commands

Command	Description
maintenance disable, on page 103	Provisions a maintenance embargo flag.

controller dwdm

To configure a DWDM controller, use the **controller dwdm** command in Global Configuration mode. To return to the default state, use the **no** form of this command.

controller dwdm *interface-path-id* [**vtxp-monitor**]

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.
vtxp-monitor	Enables VTXP (virtual transponder) attribute on the interface. The purpose of VTXP attribute tagging is to easily identify a set of interfaces (on which VTXP is enabled) and use them for further configuration or monitoring.

Command Default

No default behavior or values

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 5.3.0	**vtxp-monitor** keyword 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*/*subport*. 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.
  - *subport*: Physical port number of the sub-interface.
- If specifying a virtual interface, the number range varies, depending on interface type.

Task ID

Task ID	Operations
dwdm	read, write

Task ID	Operations
interface	read, write
sonet-sdh	read, write

Examples

This example shows how to configure a DWDM controller in slot 6:

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/6/0/0

RP/0/RP0/CPU0:router(config)# controller dwdm 0/6/0/0 vtxp-monitor
```

Related Commands

Command	Description
show controller dwdm, on page 126	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.
show vtxp-monitored ports, on page 140	Displays ports on which VTXP attribute is enabled.

g709 bdi-to-client-gais

To insert a Generic Alarm Indication Signal (GAIS) pattern to client on the detection of a backward defect indication (BDI), use the **g709 bdi-to-client-gais** command in DWDM configuration mode. To disable this feature, use the **no** form of this command.

g709 bdi-to-client-gais

Syntax Description

This command has no keywords or arguments.

Command Default

By default, no GAIS to client is inserted.

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

The **g709 bdi-to-client-gais** command is available on the 10-GE DWDM PLIM only.

Task ID

Task ID	Operations
dwdm	read, write

Examples

This example shows how to configure sending a Generic Alarm Indication Signal (GAIS) pattern signal to client when a BDI is received:

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/6/0/0
RP/0/RP0/CPU0:router(config-dwdm)# g709 bdi-to-client-gais
```

Related Commands

Command	Description
show controller dwdm, on page 126	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

g709 disable

To disable the ITU-T G.709 wrapper, use the **g709 disable** command in DWDM configuration mode. To enable the ITU-T G.709 wrapper, use the **no** form of this command.

g709 disable

Syntax Description

This command has no keywords or arguments.

Command Default

The G.709 wrapper is enabled.

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

Note The **g709 disable** command is available on the 10-GE DWDM PLIM only.

The G.709 wrapper must be enabled to enable forward error correction (FEC) mode on the controller.

To display the G.709 alarms and counters, use the **show controller dwdm g709** command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The G.709 wrapper is enabled by default. This example shows how to disable the G.709 wrapper on an interface:

```
RP/0/RP0/CPU0:Router(config)# controller dwdm 0/6/0/0
RP/0/RP0/CPU0:Router(config-dwdm)# g709 disable
```

If you have disabled the G.709 wrapper using the **g709 disable** command, use the **no g709 disable** command to re-enable it, as shown in the following example:

```
RP/0/RP0/CPU0:Router(config)# controller dwdm 0/6/0/0
RP/0/RP0/CPU0:Router(config-dwdm)# no g709 disable
```

Related Commands

Command	Description
g709 fec, on page 90	Configures the FEC mode for the DWDM controller.

Command	Description
show controller dwdm, on page 126	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

g709 fec

To configure the Forward Error Correction (FEC) mode for the DWDM controller, use the **g709 fec** command in DWDM configuration mode. To return to the default state, use the **no** form of this command.

g709 fec [**disable**] | **enhanced** | **standard** | **ci-bch** | **high-gain-hd-fec** | **high-gain-sd-fec** | **long-haul-hd-fec** | **long-haul-sd-fec**

Syntax Description

disable	Disables FEC.
enhanced	Enables ITU-T G.975.1 I.7 FEC. This is the default. Enables ITU-T G.975.1 I.4 FEC.
standard	Enables standard FEC mode.
ci-bch	Continuously Interleaved BCH FEC
high-gain-hd-fec	7% HD FEC. The default is T100 staircase FEC.
long-haul-hd-fec	20% HD FEC. The default is T100 staircase FEC.

Command Default

Enhanced FEC mode is enabled by default.

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 5.3.1	The **ci-bch** keyword was introduced.
Release 5.3.2	The high-gain-hd-fec and long-haul-hd-fec keywords were introduced.

Usage Guidelines

Note The enhanced FEC mode supported on the Cisco CRS Router (ITU-T G.975.1 I.7) and the Cisco ASR 9000 Series Router (ITU-T G.975.1 I.4) are different and therefore, incompatible. To support interoperability of DWDM between these routers, standard FEC must be configured. The OC-768c/STM-256c DWDM PLIM on the Cisco CRS Router supports enhanced FEC mode only. Disabling FEC or enabling standard FEC is not supported.

The **g709 fec** command can be used only when the DWDM controller port is not operational. In Cisco IOS XR releases prior to Cisco IOS XR Release 3.9.0, you stop operation using the **shutdown (DWDM)** command. Beginning in Cisco IOS XR Release 3.9.0, you stop operation using the **admin-state out-of-service** command.

The G.709 wrapper must be enabled to enable forward error correction (FEC) mode on the controller.

Enhanced FEC is the default mode; therefore, if you use the **no g709 fec** command, enhanced FEC is used.

To display the FEC mode, use the **show controller dwdm** command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

This example shows how to configure the FEC mode on a DWDM controller:

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/6/0/0
RP/0/RP0/CPU0:router(config-dwdm)# admin-state out-of-service
RP/0/RP0/CPU0:router(config-dwdm)# commit
RP/0/RP0/CPU0:router(config-dwdm)# g709 fec enhanced

RP/0/RP0/CPU0:router(config-dwdm)# commit
RP/0/RP0/CPU0:router(config-dwdm)# admin-state in-service
RP/0/RP0/CPU0:router(config-dwdm)# commit
```

Related Commands

Command	Description
admin-state, on page 83	Configures the transport administration state on a DWDM port.
show controller dwdm, on page 126	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.
g709 bdi-to-client-gais, on page 87	Inserts a GAIS pattern to client on the detection of a BDI.

g709 odu overhead tti

To configure the Trail Trace Identifier (TTI) level for an Optical Channel Data Unit (ODU), use the **g709 odu overhead tti** command in DWDM configuration mode. To return to the default, use the **no** form of this command.

g709 odu overhead tti **expected** | **sent** **ascii** | **hex***tti-string*

Syntax Description

expected	Configures the expected TTI string.
sent	Configures the transmit TTI string.
ascii	Indicates that the string is in ASCII format.
hex	Indicates that the string is in hexidecimal format.
tti-string	The TTI level string. You can configure the TTI level string in ASCII string format or hexadecimal format. The ASCII text string can be a maximum of 64 characters. The hexadecimal string length must be an even number and can be a maximum of 128 bytes.

Command Default

No TTI level string is configured.

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The following example shows how to configure the expected TTI string:

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/1/0/0
RP/0/RP0/CPU0:router(config-dwdm)# g709 odu overhead tti expected test OTU 5678
```

Related Commands

Command	Description
show controller dwdm, on page 126	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

g709 odu report disable

To disable the logging of selected Optical Channel Data Unit (ODU) alarms to the console for a DWDM controller, use the **g709 odu report disable** command in DWDM configuration mode. To return to the default state, use the **no** form of this command.

g709 odu report ais | bdi | eoc | lck | oci | ptim | sd-ber | sf-ber | tim disable

Syntax Description

ais	Alarm indication signal reporting status.
bdi	Backward defect indication reporting status.
eoc	GCC end of channel failure reporting status.
lck	Upstream connection locked reporting status.
oci	Open connection indication error reporting status.
pm-tca	Path monitoring BER TCA reporting status.
ptim	Payload type identifier mismatch reporting status.
sd-ber	Set SM BER in excess of SD threshold reporting status.
sf-ber	Set SM BER in excess of SF threshold reporting status.
tim	Set Trace Identifier Mismatch reporting status.

Command Default

Reporting is enabled for all keywords.

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.6.0	The **tim** keyword was added.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

This example shows how to disable ODU reporting for OCI:

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RP0/CPU0:router(config-dwdm)# g709 odu report oci disable
```

Related Commands

Command	Description
show controller dwdm, on page 126	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

g709 otu overhead tti

To configure the OTU Trail Trace Identifier (TTI) buffer for a DWDM controller, use the **g709 otu overhead tti** command in DWDM configuration mode. To return to the default state, use the **no** form of this command.

g709 otu overhead tti expected | **sent ascii** | **hex** *tti-string*

Syntax Description

expected	Configures the expected TTI string.
sent	Configures the transmit TTI string.
ascii	Indicates that the string is in ASCII format.
hex	Indicates that the string is in hexidecimal format.
tti-string	The TTI string. A maximum of 64 characters is allowed.

Command Default

No TTI string is configured

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

To display the TTI strings, use the **show controller dwdm g709** command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The following example shows how to configure the expected TTI string:

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RP0/CPU0:router(config-dwdm)# g709 otu overhead tti expected test OTU 5678
```

Related Commands

Command	Description
show controller dwdm, on page 126	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

g709 otu report disable

To disable the logging of selected Optical Channel Transport Unit (OTU) alarms to the console for a DWDM controller, use the **g709 otu report disable** command in DWDM configuration mode. To return to the default state, use the **no** form of this command.

g709 otu report ais | bdi | eoc | fecmismatch | iae | lof | lom | los | sd-ber | sf-ber | tim disable

Syntax Description

ais	Alarm indication signal reporting status.
bdi	Backward defect indication reporting status.
eoc	GCC end of channel failure reporting status.
fecmismatch	FEC mismatch alarm reporting status. **Note** FEC mismatch alarm is deprecated.
iae	Incoming alignment error reporting status.
lof	OTU loss of frame reporting status.
lom	Loss of multiple frame reporting status.
los	Loss of signal reporting status.
sd-ber	SM bit error rate (BER) is in excess of the signal degradation BER threshold.
sf-ber	SM BER is in excess of the signal failure BER threshold.
sm-tca	Section monitoring BER TCA reporting status.
tim	Trace Identifier Mismatch reporting status.

Command Default

Reporting is enabled for all keywords.

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.6.0	The **tim** keyword was added.

Usage Guidelines

Configuring two ends of an OTN link with different FEC modes is not supported. Even if different FEC modes are configured, the FEC mismatch alarm will not be raised. Interface may experience continuous port flap in addition to continuous bit interleaved parity (BIP) errors at both OTN and LAN level.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The following example shows how to disable OTU reporting for IAE:

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RP0/CPU0:router(config-dwdm)# g709 otu report iae disable
```

Related Commands

Command	Description
show controller dwdm, on page 126	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

g709 otu threshold

To configure thresholds for selected Optical Channel Transport Unit (OTU) bit error rate (BER) alarms, use the **g709 otu threshold** command in DWDM configuration mode. To return to the default state, use the **no** form of this command.

g709 otu threshold sd-ber | **sf-ber bit-error-rate**

Syntax Description

sd-ber *bit-error-rate*	Signal degradation bit error rate (BER) in the range 1 to 9, where *bit-error-rate* specifies a negative exponent of base 10 (10–*bit-error-rate*). The default is 6 (10–6).
sf-ber *bit-error-rate*	Signal failure BER above threshold in the range 1 to 9, where *bit-error-rate* specifies a negative exponent of base 10 (10–*bit-error-rate*). The default is 3 (10–3).

Command Default

The defalut bit error rate for **sd-ber** is 6.

The default bit error rate for **sf-ber** is 3.

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

This example shows how to set the signal fail BER rate to be 5:

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RP0/CPU0:router(config-dwdm)# g709 otu threshold sf-ber 5
```

Related Commands

Command	Description
show controller dwdm, on page 126	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

g709 tim-to-client-gais

To insert a Generic Alarm Indication Signal (GAIS) on the client side when a Trace Identifier Mismatch (TIM) is detected, use the **g709 tim-to-client-gais** command in DWDM configuration mode. To disable this feature, use the **no** form of this command.

g709 tim-to-client-gais

Syntax Description

This command has no keywords or arguments.

Command Default

By default, no GAIS to client is inserted.

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

Note The **g709 tim-to-client-gais** command is available on the 10-GE DWDM PLIM only.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The following example shows how to configure a GAIS to client when a TIM is received:

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/1/0/0
RP/0/RP0/CPU0:router(config-dwdm)# g709 tim-to-client-gais
```

Related Commands

Command	Description
show controller dwdm, on page 126	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

g709 tti-processing

To enable Trace Identifier Mismatch (TIM) alarms, use the **g709 tti-processing** command in DWDM configuration mode. To disable TIM alarms, use the **no** form of this command.

g709 tti-processing

Syntax Description

This command has no keywords or arguments.

Command Default

By default, trace identifier mismatch (TIM) alarms are disabled.

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

Note Trace identifier mismatch (TIM) alarms can be set only when TTI processing is enabled.

Task ID

Task ID	Operations
dwdm	read, write

Examples

This example shows how to configure the expected TTI string:

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/1/0/0
RP/0/RP0/CPU0:router(config-dwdm)# g709 tti-processing
```

Related Commands

Command	Description
show controller dwdm, on page 126	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

log signal

To enable 10 millisecond proactive monitoring of Forward Error Correction-Fast Re-Route (FEC-FRR), use the **log signal** command in DWDM configuration mode. To disable proactive monitoring, use the no form of this command.

log signal *file-name*

Syntax Description

file-name	Specifies the name of the log file.

Command Default

No default behavior or values

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

The proactive feature is used to trigger Forward Error Correction-Fast Re-Route (FEC-FRR).

Note The **log signal** command is supported on the legacy line cards but does not function on the A9K-8X100GE-SE line cards though it is supported on them.

To see the proactive status, use the **show controller dwdm proactive status** command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The following example shows how to enable 10 millisecond proactive monitoring of Forward Error Correction-Fast Re-Route (FEC-FRR).

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# controller dwdm 0/1/0/1
RP/0/RP0/CPU0:router(config-dwdm)# log signal LogFile1
```

Related Commands

Command	Description
show controller dwdm, on page 126	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

loopback (DWDM)

To configure the DWDM controller for loopback mode, use the **loopback** command in DWDM configuration mode. To remove the loopback DWDM command from the configuration file, use the **no** form of this command.

loopback internal | line

Syntax Description

internal	Specifies that all the packets be looped back to the router.
line	Specifies that the incoming network packets be looped back to the DWDM network.

Command Default

This command is disabled by default.

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

The DWDM controller supports two loopback operation modes for diagnostic purposes: internal and line. The terminal (internal) loopback mode allows the received data from the Layer 2 Framer (for example, a SONET/SDH framer for POS or Ethernet MAC for 10GE) of the PLIM to be looped back to the ingress side of the Framer. This allows the packets to be looped back to the PLIM. The line loopback mode allows the received trunk/DWDM line Rx to be connected to the trunk/DWDM line Tx towards the line. This is used for line diagnostics.

Task ID

Task ID	Operations
dwdm	read, write

Examples

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

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RP0/CPU0:router(config-dwdm)# loopback internal
```

maintenance disable

To provision a maintenance embargo flag, use the **maintenance disable** command in interface configuration mode. To remove a maintenance embargo flag, use the no form of this command.

maintenance disable

Syntax Description

This command has no keywords or arguments.

Command Default

Maintenance embargo flags are not provisioned.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

A maintenance embargo flag prevents maintenance activities from being performed on an interface.

To display the status of whether maintenance is enabled or disabled on an interface, use the **show interface pos** command or the **show interface tenGigE** command.

Task ID

Task ID	Operations
dwdm	read
interface	read, write

Examples

The following examples show how to provision a maintenance embargo flag:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface pos 1/0/1/1
RP/0/RP0/CPU0:Router(config-if)# maintenance disable
```

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:Router(config)# interface tengige 1/0/1/1
RP/0/RP0/CPU0:Router(config-if)# maintenance disable
```

Related Commands

Command	Description
admin-state, on page 83	Configures the transport administration state on a DWDM port.

network connection id

To configure a connection identifier for the Multi Service Transport Protocol (MSTP), use the **network connection id** command in DWDM configuration mode. To remove a connection identifier, use the no form of this command.

network connection id *id-number*

Syntax Description

id-number	Connection identifier.

Command Default

No default behavior or values

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The following example shows how to configure a connection identifier for the Multi Service Transport Protocol (MSTP).

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# controller dwdm 0/1/0/1
RP/0/RP0/CPU0:router(config-dwdm)# network connection id 1/1/1/1
```

Related Commands

Command	Description
network srlg , on page 106	Configures a SRLG on a DWDM controller.
network port id, on page 105	Assigns an identifier number to a port for the MSTP.

network port id

To assign an identifier number to a port for the Multi Service Transport Protocol (MSTP), use the **network port id** command in DWDM configuration mode. To remove an identifier number from a port, use the no form of this command.

network port id *id-number*

Syntax Description

id-number	Port identifier.

Command Default

No default behavior or values

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The following example shows how to assign an identifier number to a port for the Multi Service Transport Protocol (MSTP):

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# controller dwdm 0/1/0/1
RP/0/RP0/CPU0:router(config-dwdm)# network port id 1/0/1/1
```

Related Commands

Command	Description
network srlg , on page 106	Configures a SRLG on a DWDM controller.
network connection id, on page 104	Configures a connection identifier for the MSTP.

network srlg

To configure a Shared Risk Link Group (SRLG) on a DWDM controller, use the **network srlg** command in DWDM configuration mode. To remove an SRLG, use the no form of this command.

network srlg *value1 value2 value3*

Syntax Description

value1 value2 value3	Specifies the value.

Command Default

No default behavior or values

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

This example shows how to configure a Shared Risk Link Group (SRLG) on a DWDM controller:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# controller dwdm 0/1/0/1
RP/0/RP0/CPU0:router(config-dwdm)# network srlg value1 value2 value3
```

Related Commands

Command	Description
network port id, on page 105	Assigns an identifier number to a port for the MSTP.
network connection id, on page 104	Configures a connection identifier for the MSTP.

pm fec report enable

To enable Threshold Crossing Alert (TCA) generation for FEC, use the **pm fec report enable** command in DWDM configuration mode. To disable TCAs, use the **no** form of this command.

pm 15-min | 24-hour fec report ec-bits | uc-words enable

Syntax Description

15-min	Configures the TCA generation for 15-minute intervals.
24-hour	Configures TCA generation for 24-hour intervals.
ec-bits	Bit errors corrected (BIEC). Indicates the number of bit errors corrected in the DWDM trunk line during the performance monitoring time interval.
uc-words	Uncorrectable words. This is the number of uncorrectable words detected in the DWDM trunk line during the performance monitoring time interval.

Command Default

TCA is not enabled.

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

To display FEC performance measurement information, use the **show controller dwdm pm fec** command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The following example shows how to enable TCAs in FEC reporting for uncorrectable words:

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RP0/CPU0:router(config-dwdm)# pm 15-min fec report uc-words enable
```

Related Commands

Command	Description
show controller dwdm, on page 126	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

pm fec threshold

To configure performance monitoring thresholds on the FEC layer, use the **pm fec threshold** command in DWDM configuration mode. To return to the default state, use the **no** form of this command.

pm 15-min | **24-hour fec threshold ec-bits** | **uc-words** *threshold*

Syntax Description

15-min	Configures the performance monitoring thresholds for 15-minute intervals.
24-hour	Configures performance monitoring thresholds for 24-hour intervals.
ec-bits	Bit errors corrected (BIEC). Indicates the number of bit errors corrected in the DWDM trunk line during the performance monitoring time interval.
uc-words	Uncorrectable Words. This is the number of uncorrectable words detected in the DWDM trunk line during the performance monitoring time interval.
threshold	Threshold for the performance monitoring parameter in the range 1–4294967295.

Command Default

No threshold is configured.

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

To display performance measurement information for the FEC layer, use the **show controller dwdm pm fec** command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The following example shows how to configure an FEC layer performance monitoring threshold for uncorrectable words:

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RP0/CPU0:router(config-dwdm)# pm 15-min fec threshold uc-words 2000000
```

Related Commands

Command	Description
show controller dwdm pm, on page 135	Displays performance monitoring information for a DWDM controller.

pm optics report enable

To enable Threshold Crossing Alert (TCA) generation on the optics layer, use the **pm optics report enable** command in DWDM configuration mode. To disable TCA reporting, use the **no** form of this command.

pm 15-min | 24-hour optics report lbc | opr | opt max-tca | min-tca enable

Syntax Description

15-min	Configures TCA generation for 15-minute intervals.
24-hour	Configures TCA generation for 24-hour intervals.
lbc	Laser bias current.
opr	Optical power on the unidirectional port.
opt	Transmit optical power in dBm.
max-tca	Indicates that the maximum value of the parameter is compared against the threshold to determine if a TCA should be generated.
min-tca	Indicates that the minimum value of the parameter is compared against the threshold to determine if a TCA should be generated.

Command Default

TCA reporting is not enabled.

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

To display performance monitoring information for the optics, use the **show controller dwdm pm optics** command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The following example shows how to enable TCA reporting on the optics layer reporting for the maximum OPT:

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RP0/CPU0:router(config-dwdm)# pm 15-min optics report opt max-tca enable
```

Related Commands

Command	Description
show controller dwdm pm, on page 135	Displays performance monitoring information for a DWDM controller.

pm optics threshold

To configure performance monitoring thresholds on the optics layer, use the **pm optics threshold** command in DWDM configuration mode. To return to the default state, use the **no** form of this command.

pm 15-min | 24-hour optics threshold lbc | opr | optmax | min *threshold*

Syntax Description

15-min	Configures the performance monitoring thresholds for 15-minute intervals.
24-hour	Configures performance monitoring thresholds for 24-hour intervals.
lbc	Laser bias current.
opr	Optical power on the unidirectional port.
opt	Transmit optical power in dBm.
max	Indicates that the *threshold* is for the maximum value of the parameter.
min	Indicates that the *threshold* is for the minimum value of the parameter.
threshold	Threshold for the performance monitoring parameter.

Command Default

No thresholds are configured.

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

To display performance monitoring information for the optics layer, use the **show controller dwdm pm optics** command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The following example shows how to configure an optics layer performance monitoring threshold for maximum OPT:

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RP0/CPU0:router(config-dwdm)# pm 15-min optics threshold opt max 2000000
```

Related Commands

Command	Description
show controller dwdm pm, on page 135	Displays performance monitoring information for a DWDM controller.

pm otn report enable

To enable Threshold Crossing Alert (TCA) generation on the Optical Transport Network (OTN) layer, use the **pm otn report enable** command in DWDM configuration mode. To disable TCA reporting, use the **no** form of this command.

pm 15-min | 24-hour otn report *otn-parameter* **enable**

Syntax Description

15-min	Configures TCA generation for 15-minute intervals.
24-hour	Configures TCA generation for 24-hour intervals.
otn-parameter	Specific parameter for which to configure the threshold. OTN parameters can be as follows: • **bbe-pm-fe**—Far-end path monitoring background block errors (BBE-PM). Indicates the number of background block errors recorded in the optical transport network (OTN) path during the performance monitoring time interval. • **bbe-pm-ne**—Near-end path monitoring background block errors (BBE-PM). • **bbe-sm-fe**—Far-end section monitoring background block errors (BBE-SM). Indicates the number of background block errors recorded in the OTN section during the performance monitoring time interval. • **bbe-sm-ne**—Near-end section monitoring background block errors (BBE-SM). • **bber-pm-fe**—Far-end path monitoring background block errors ratio (BBER-PM). Indicates the background block errors ratio recorded in the OTN path during the performance monitoring time interval. • **bber-pm-ne**—Near-end path monitoring background block errors ratio (BBER-PM). • **bber-sm-fe**—Far-end section monitoring background block errors ratio (BBER-SM). Indicates the background block errors ratio recorded in the OTN section during the performance monitoring time interval. • **bber-sm-ne**—Near-end section monitoring background block errors ratio (BBER-SM) • **es-pm-fe**—Far-end path monitoring errored seconds (ES-PM). Indicates the errored seconds recorded in the OTN path during the performance monitoring time interval. • **es-pm-ne**—Near-end path monitoring errored seconds (ES-PM). • **es-sm-fe**—Far-end section monitoring errored seconds (ES-SM). Indicates the errored seconds recorded in the OTN section during the performance monitoring time interval. • **es-sm-ne**—Near-end section monitoring errored seconds (ES-SM). • **esr-pm-fe**—Far-end path monitoring errored seconds ratio (ESR-PM). Indicates the errored seconds ratio recorded in the OTN path during the performance monitoring time interval.

- **esr-pm-ne**—Near-end path monitoring errored seconds ratio (ESR-PM).
- **esr-sm-fe**—Far-end section monitoring errored seconds ratio (ESR-SM). Indicates the errored seconds ratio recorded in the OTN section during the performance monitoring time interval.
- **esr-sm-ne**—Near-end section monitoring errored seconds ratio (ESR-SM).
- **fc-pm-fe**—Far-end path monitoring failure counts (FC-PM). Indicates the failure counts recorded in the OTN path during the performance monitoring time interval.
- **fc-pm-ne**—Near-end path monitoring failure counts (FC-PM).
- **fc-sm-fe**—Far-end section monitoring failure counts (FC-SM). Indicates the failure counts recorded in the OTN section during the performance monitoring time interval.
- **fc-sm-ne**—Near-end section monitoring failure counts (FC-SM).
- **ses-pm-fe**—Far-end path monitoring severely errored seconds (SES-PM). Indicates the severely errored seconds recorded in the OTN path during the performance monitoring time interval.
- **ses-pm-ne**—Far-end path monitoring severely errored seconds (SES-PM).
- **ses-sm-fe**—Far-end section monitoring severely errored seconds (SES-SM). Indicates the severely errored seconds recorded in the OTN section during the performance monitoring time interval.
- **ses-sm-ne**—Near-end section monitoring severely errored seconds (SES-SM).
- **sesr-pm-fe**—Far-end path monitoring severely errored seconds ratio (SESR-PM). Indicates the severely errored seconds ratio recorded in the OTN path during the performance monitoring time interval.
- **sesr-pm-ne**—Near-end path monitoring severely errored seconds ratio (SESR-PM).
- **sesr-sm-fe**—Far-end section monitoring severely errored seconds ratio (SESR-SM). Indicates the severely errored seconds ratio recorded in the OTN section during the performance monitoring time interval.
- **sesr-sm-ne**—Near-end section monitoring severely errored seconds ratio (SESR-SM).
- **uas-pm-fe**—Far-end path monitoring unavailable seconds (UAS-PM). Indicates the unavailable seconds recorded in the OTN path during the performance monitoring time interval.
- **uas-pm-ne**—Near-end path monitoring unavailable seconds (UAS-PM).
- **uas-sm-fe**—Far-end section monitoring unavailable seconds (UAS-SM). Indicates the unavailable seconds recorded in the OTN section during the performance monitoring time interval.
- **uas-sm-ne**—Near-end section monitoring unavailable seconds (UAS-SM).

Command Default

TCA generation is not enabled.

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

To display performance measurement information for the OTN layer, use the **show controller dwdm pm otn** command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The following example shows how to enable TCA generation on the OTN layer reporting for the path monitoring errored seconds ratio (ESR-PM):

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RP0/CPU0:router(config-dwdm)# pm 15-min otn report esr-pm-fe enable
```

Related Commands

Command	Description
show controller dwdm pm, on page 135	Displays performance monitoring information for a DWDM controller.

pm otn threshold

To configure performance monitoring thresholds on the optical transport network (OTN) layer, use the **pm otn threshold** command in DWDM configuration mode. To disable TCA reporting, use the **no** form of this command.

pm 15-min | 24-hour otn threshold *otn-paramter* **enable**

Syntax Description

15-min	Configures performance monitoring thresholds for 15-minute intervals.
24-hour	Configures performance monitoring thresholds for 24-hour intervals.
otn-parameter	Specific parameter for which to configure the threshold. OTN parameters can be as follows: • **bbe-pm-fe**—Far-end path monitoring background block errors (BBE-PM). Indicates the number of background block errors recorded in the optical transport network (OTN) path during the performance monitoring time interval. • **bbe-pm-ne**—Near-end path monitoring background block errors (BBE-PM). • **bbe-sm-fe**—Far-end section monitoring background block errors (BBE-SM). Indicates the number of background block errors recorded in the OTN section during the performance monitoring time interval. • **bbe-sm-ne**—Near-end section monitoring background block errors (BBE-SM). • **bber-pm-fe**—Far-end path monitoring background block errors ratio (BBER-PM). Indicates the background block errors ratio recorded in the OTN path during the performance monitoring time interval. • **bber-pm-ne**—Near-end path monitoring background block errors ratio (BBER-PM). • **bber-sm-fe**—Far-end section monitoring background block errors ratio (BBER-SM). Indicates the background block errors ratio recorded in the OTN section during the performance monitoring time interval. • **bber-sm-ne**—Near-end section monitoring background block errors ratio (BBER-SM) • **es-pm-fe**—Far-end path monitoring errored seconds (ES-PM). Indicates the errored seconds recorded in the OTN path during the performance monitoring time interval. • **es-pm-ne**—Near-end path monitoring errored seconds (ES-PM). • **es-sm-fe**—Far-end section monitoring errored seconds (ES-SM). Indicates the errored seconds recorded in the OTN section during the performance monitoring time interval. • **es-sm-ne**—Near-end section monitoring errored seconds (ES-SM).

	• **esr-pm-fe**—Far-end path monitoring errored seconds ratio (ESR-PM). Indicates the errored seconds ratio recorded in the OTN path during the performance monitoring time interval. • **esr-pm-ne**—Near-end path monitoring errored seconds ratio (ESR-PM). • **esr-sm-fe**—Far-end section monitoring errored seconds ratio (ESR-SM). Indicates the errored seconds ratio recorded in the OTN section during the performance monitoring time interval. • **esr-sm-ne**—Near-end section monitoring errored seconds ratio (ESR-SM). • **fc-pm-fe**—Far-end path monitoring failure counts (FC-PM). Indicates the failure counts recorded in the OTN path during the performance monitoring time interval. • **fc-pm-ne**—Near-end path monitoring failure counts (FC-PM). • **fc-sm-fe**—Far-end section monitoring failure counts (FC-SM). Indicates the failure counts recorded in the OTN section during the performance monitoring time interval. • **fc-sm-ne**—Near-end section monitoring failure counts (FC-SM). • **ses-pm-fe**—Far-end path monitoring severely errored seconds (SES-PM). Indicates the severely errored seconds recorded in the OTN path during the performance monitoring time interval. • **ses-pm-ne**—Far-end path monitoring severely errored seconds (SES-PM). • **ses-sm-fe**—Far-end section monitoring severely errored seconds (SES-SM). Indicates the severely errored seconds recorded in the OTN section during the performance monitoring time interval. • **ses-sm-ne**—Near-end section monitoring severely errored seconds (SES-SM). • **sesr-pm-fe**—Far-end path monitoring severely errored seconds ratio (SESR-PM). Indicates the severely errored seconds ratio recorded in the OTN path during the performance monitoring time interval. • **sesr-pm-ne**—Near-end path monitoring severely errored seconds ratio (SESR-PM). • **sesr-sm-fe**—Far-end section monitoring severely errored seconds ratio (SESR-SM). Indicates the severely errored seconds ratio recorded in the OTN section during the performance monitoring time interval. • **sesr-sm-ne**—Near-end section monitoring severely errored seconds ratio (SESR-SM). • **uas-pm-fe**—Far-end path monitoring unavailable seconds (UAS-PM). Indicates the unavailable seconds recorded in the OTN path during the performance monitoring time interval. • **uas-pm-ne**—Near-end path monitoring unavailable seconds (UAS-PM).
	• **uas-sm-fe**—Far-end section monitoring unavailable seconds (UAS-SM). Indicates the unavailable seconds recorded in the OTN section during the performance monitoring time interval. • **uas-sm-ne**—Near-end section monitoring unavailable seconds (UAS-SM).
threshold	Threshold for the performance monitoring parameter.

Command Default No thresholds are configured.

Command Modes DWDM configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

To display performance measurement information for the OTN layer, use the **show controller dwdm pm otn** command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The following example shows how to configure an OTN layer performance monitoring threshold for path monitoring errored seconds ratio (ESR-PM):

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RP0/CPU0:router(config-dwdm)# pm 15-min otn threshold esr-pm-ne 500000
```

Related Commands

Command	Description
show controller dwdm pm, on page 135	Displays performance monitoring information for a DWDM controller.

proactive

To enable automatic triggering of Forward Error Correction-Fast Re-Route (FEC-FRR), use the **proactive** command in DWDM configuration mode. To disable automatic triggering, use the no form of this command.

proactive

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

The proactive feature is used to trigger Forward Error Correction-Fast Re-Route (FEC-FRR).

Note The **proactive** command is supported on the legacy line cards but does not function on the A9K-8X100GE-SE line cards though it is supported on them.

To see the proactive status, use the **show controller dwdm proactive status** command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The following example shows how to enable automatic triggering of Forward Error Correction-Fast Re-Route (FEC-FRR):

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# controller dwdm 0/1/0/1
RP/0/RP0/CPU0:router(config-dwdm)# proactive
```

Related Commands

Command	Description
show controller dwdm, on page 126	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

proactive revert threshold

To configure the revert threshold to trigger reverting from the Forward Error Correction-Fast Re-Route (FEC-FRR) route back to the original route, use the **proactive revert threshold** command in DWDM configuration mode. To remove the revert threshold, use the no form of this command.

proactive revert threshold *x-coefficient y-power*

Syntax Description

x-coefficient	Bit error rate coefficient (x of xE-y) . The range is 1 to 9. Default is 1.
y-power	Bit error rate exponent (y of xE-y). The range is 3 to 9.

Command Default

No default behavior or values

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

The proactive feature is used to trigger Forward Error Correction-Fast Re-Route (FEC-FRR).

Note The **proactive revert threshold** command is supported on the legacy line cards but does not function on the A9K-8X100GE-SE line cards though it is supported on them.

To see the proactive status, use the **show controller dwdm proactive status** command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The following example shows how to configure the revert threshold for FEC-FRR:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# controller dwdm 0/1/0/1
RP/0/RP0/CPU0:router(config-dwdm)# proactive revert threshold 1 9
```

Related Commands

Command	Description
show controller dwdm, on page 126	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

proactive revert window

To configure the revert window in which reverting from the Forward Error Correction-Fast Re-Route (FEC-FRR) route back to the original route is triggered, use the **proactive revert window** command in DWDM configuration mode. To remove the revert window, use the **no** form of this command.

proactive revert window *window*

Syntax Description

window	The length of time (in milliseconds) of the window in which reverting from FEC-FRR may be triggered. The range is 2000 to 100000.

Command Default

No default behavior or values

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

The proactive feature is used to trigger Forward Error Correction-Fast Re-Route (FEC-FRR).

Note The **proactive revert window** command is supported on the legacy line cards but does not function on the A9K-8X100GE-SE line cards though it is supported on them.

To see the proactive status, use the **show controller dwdm proactive status** command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The following example shows how to configure the window in which reverting from FEC-FRR may be triggered:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# controller dwdm 0/1/0/1
RP/0/RP0/CPU0:router(config-dwdm)# proactive revert window 100000
```

Related Commands

Command	Description
show controller dwdm, on page 126	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

proactive trigger threshold

To configure the trigger threshold of Forward Error Correction-Fast Re-Route (FEC-FRR), use the **proactive trigger threshold** command in DWDM configuration mode. To remove the trigger threshold, use the no form of this command.

proactive trigger threshold *x-coefficient y-power*

Syntax Description

x-coefficient	Bit error rate coefficient (x of xE-y) . The range is 1 to 9. Default is 1.
y-power	Bit error rate exponent (y of xE-y). The range is 3 to 9.

Command Default

No default behavior or values

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

The proactive feature is used to trigger Forward Error Correction-Fast Re-Route (FEC-FRR).

Note The **proactive trigger threshold** command is supported on the legacy line cards but does not function on the A9K-8X100GE-SE line cards though it is supported on them.

To see the proactive status, use the **show controller dwdm proactive status** command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The following example shows how to configure the trigger threshold of Forward Error Correction-Fast Re-Route (FEC-FRR)

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# controller dwdm 0/1/0/1
RP/0/RP0/CPU0:router(config-dwdm)# proactive trigger threshold 1 9
```

Related Commands

Command	Description
show controller dwdm, on page 126	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

proactive trigger window

To configure the trigger window (in milliseconds) in which Fast Re-Route may be triggered, use the **proactive trigger window** command in DWDM configuration mode. To remove the trigger window, use the no form of this command.

proactive trigger window *window*

Syntax Description

window	The length of time (in milliseconds) of the window in which FEC-FRR may be triggered. The range is 10 to 10000.

Command Default

No default behavior or values

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

The proactive feature is used to trigger Forward Error Correction-Fast Re-Route (FEC-FRR).

Note The **proactive trigger window** command is supported on the legacy line cards but does not function on the A9K-8X100GE-SE line cards though it is supported on them.

To see the proactive status, use the **show controller dwdm proactive status** command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The following example shows how to configure the trigger window (in milliseconds) in which triggering of Fast Re-Route may happen:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# controller dwdm 0/1/0/1
RP/0/RP0/CPU0:router(config-dwdm)# proactive trigger window 10000
```

Related Commands

Command	Description
show controller dwdm, on page 126	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

rx-los-threshold

To configure the transponder receive power threshold on a DWDM controller, use the **rx-los-threshold** command in DWDM configuration mode. To return the transponder receive power threshold to its default value, use the **no** form of this command.

rx-los-threshold power-level

Syntax Description

power-level	Receive power level in units of 0.1 dBm. Values can range from -350 to 50, which corresponds to a LOS threshold range of -35 dBm to 5 dBm.

Command Default

The default *power-level* is-19.5 dBm.

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced. It is supported only on the OC-768c/STM-256c DWDM PLIM.
Release 3.6.0	The value for the *power-level* argument was changed from -200 to 0, to -350 to 50.

Usage Guidelines

The **rx-los-threshold** command can be used only when the DWDM controller port is not operational. In Cisco IOS XR releases prior to Cisco IOS XR Release 3.9.0, you stop operation using the **shutdown (DWDM)** command. Beginning in Cisco IOS XR Release 3.9.0, you stop operation using the **admin-state out-of-service** command.

The **rx-los-threshold** command is applicable only to the OC-768c/STM-256c DWDM PLIM.

Task ID

Task ID	Operations
dwdm	read, write

Examples

This example shows how to configure the receive power threshold to -10 dBm:

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RP0/CPU0:router(config-dwdm)# rx-los-threshold -100
```

Related Commands

Command	Description
admin-state, on page 83	Configures the transport administration state on a DWDM port.
show controller dwdm, on page 126	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

Command	Description
transmit-power, on page 144	Configures the DWDM optics transmit laser power on a DWDM controller.

show controller dwdm

To display optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller, use the **show controller dwdm** command in EXEC mode.

show controller dwdm interface-path-id [**g709** [**registers**] | **log** | **optics** [**registers**] | **proactive status srlg tdc** | **wavelength-map**]

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.
g709	(Optional) Displays the G.709 Optical Transport Network (OTN) protocol alarms and counters for bit errors, along with the FEC statistics and threshold-based alerts. g709 mode and g709 fec set to enhanced by default.
log	(Optional) Displays information about signal logging.
optics	(Optional) Displays optical related information about the interface, such as output power level and wavelength.
registers	(Optional) For **g709**, displays platform-specific OTN framer registers; for **optics**, displays transponder registers.
proactive status	(Optional) Displays proactive status information.
srlg	(Optional) Displays Shared Risk Link Group (SRLG) information.
tdc	(Optional) Displays tunable dispersion compensator (TDC) information.
wavelength-map	(Optional) Displays the wavelength information.

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.4.0	The display of the TTI strings was added.
Release 3.6.0	Tunable dispersion compensator (TDC) information was added.
Release 3.9.0	The Transport Admin State output field was added, and the output for the FEC Mode field was modified to display the type of Enhanced FEC configured.
Release 3.9.1	The **srlg** and **proactive status** keywords were added.

Release	Modification
Release 5.3.0	The command output was enhanced to capture whether VTXP is enabled on an interface or not.

Usage Guidelines

DWDM interfaces with g709 capability(enabled) and FEC(enabled) would report with Threshold Crossing Alerts (TCA) for Error Correction based PREFEC version of SD and SF BER. The thresholds act independent of FRR thresholds. If FRR is also enabled, then PREFEC thresholds are expected to be manually tuned to provide an early warning before the protection is triggered. The information regarding PREFEC_SD and PREFEC_SF are made available for the **show controller dwdm interface-path-id g709** command. 10 GigE and 40 GigE DWDM interfaces support standard FEC and enhanced i.4 and i.7 FEC modes while 100GigE supports standard FEC.

Task ID

Task ID	Operations
dwdm	read
interface	read
sonet-sdh	read

Examples

This example shows the output from the **show controllers dwdm** command on a 10-GE DWDM PLIM (prior to Cisco IOS XR Release 3.9.0):

```
RP/0/RP0/CPU0:Router# show controller dwdm 0/6/0/0

Port dwdm 0/6/0/0

Controller State: up

Loopback: None

G709 Status


OTU
         LOS  = 0           LOF  = 0           LOM  = 0
         BDI  = 0           IAE  = 0           BIP  = 0
         BEI  = 0           TIM  = 0

ODU
         AIS  = 0           BDI  = 0           OCI  = 0
         LCK  = 0           BIP  = 0           BEI  = 0
         PTIM = 0           TIM  = 0

FEC Mode: Enhanced FEC(default)
         EC(current second) = 0           EC   = 0           UC   = 0
         pre-FEC BER < 2.35E-11           Q > 6.66           Q Margin > 7.52 dBQ

Remote FEC Mode: Unknown
         FECMISMATCH = 0

Detected Alarms: LOS
Asserted Alarms: LOS
Alarm Reporting Enabled for: LOS LOF LOM IAE OTU-BDI OTU-TIM OTU_SF_BER OTU_SD_BER ODU-AIS
 ODU-BDI OCI LCK PTIM ODU-TIM FECMISMATCH
```

```
BER Thresholds: OTU-SF = 10e-3  OTU-SD = 10e-6

OTU TTI Sent     String ASCII: Tx TTI Not Configured
OTU TTI Received String ASCII: Rx TTI Not Recieved
OTU TTI Expected String ASCII: Exp TTI Not Configured

ODU TTI Sent     String ASCII: Tx TTI Not Configured
ODU TTI Received String ASCII: Rx TTI Not Recieved
ODU TTI Expected String ASCII: Exp TTI Not Configured

Optics Status

         Optics Type:  DWDM
         Wavelength Info: C-Band, MSA ITU Channel=1, Frequency=196.10THz,
Wavelength=1528.773nm
         TX Power = 0.07 dBm
         RX Power = -43.35 dBm
         RX LOS Threshold = -17.00 dBm
TDC Info

        TDC Not Supported on the Plim
```

This example shows the output from the **show controllers dwdm** command on a OC-768c/STM-256c DWDM PLIM (prior to Cisco IOS XR Release 3.9.0):

```
RP/0/RP0/CPU0:Router# show controller dwdm 0/4/0/0

Port dwdm 0/4/0/0

Controller State: admin-down

Loopback: None

G709 Status


OTU
         LOS  = 0           LOF  = 0           LOM  = 0
         BDI  = 0           IAE  = 0           BIP  = 0
         BEI  = 0           TIM  = 0

ODU
         AIS  = 0           BDI  = 0           OCI  = 0
         LCK  = 0           BIP  = 0           BEI  = 0
         PTIM = 0           TIM  = 0

FEC Mode: Enhanced FEC(default)
         EC(current second) = 0          EC   = 0          UC   = 0
         pre-FEC BER < 2.35E-11          Q > 6.66          Q Margin > 7.52 dBQ

Remote FEC Mode: Unknown
         FECMISMATCH = 0

Detected Alarms: None
Asserted Alarms: None
Alarm Reporting Enabled for: LOS LOF LOM IAE OTU-BDI OTU-TIM OTU_SF_BER OTU_SD_BER ODU-AIS
 ODU-BDI OCI LCK PTIM ODU-TIM FECMISMATCH
BER Thresholds: OTU-SF = 10e-3  OTU-SD = 10e-6

OTU TTI Sent     String ASCII: Tx TTI Not Configured
OTU TTI Received String ASCII: Rx TTI Not Recieved
OTU TTI Expected String ASCII: Exp TTI Not Configured
```

```
ODU TTI Sent     String ASCII: Tx TTI Not Configured
ODU TTI Received String ASCII: Rx TTI Not Recieved
ODU TTI Expected String ASCII: Exp TTI Not Configured

Optics Status

         Optics Type:  DWDM
         Wavelength Info: C-Band, MSA ITU Channel=1, Frequency=196.10THz,
Wavelength=1528.773nm
         TX Power = 1.01 dBm
         RX Power = -99.99 dBm
         RX LOS Threshold = -17.00 dBm
TDC Info

        Operational Mode: AUTO
        Status :          AQUIRING
        Dispersion Setting : 0 ps/nm
```

The following example shows updated output from the **show controllers dwdm** command on a Cisco CRS-1 router in Cisco IOS XR Release 3.9.0:

```
RP/0/RP0/CPU0:Router(config-dwdm)# show controllers dwdm 0/0/0/0
Mon Aug  3 10:29:09.799 UTC

Port dwdm0/0/0/0

Controller State: up

Transport Admin State: OOS (Out-of-Service)

Loopback: None

G709 Status


OTU
         LOS  = 0           LOF  = 0           LOM  = 0
         BDI  = 0           IAE  = 0           BIP  = 0
         BEI  = 0           TIM  = 0

ODU
         AIS  = 0           BDI  = 0           OCI  = 0
         LCK  = 0           BIP  = 0           BEI  = 0
         PTIM = 0           TIM  = 0

FEC Mode: Enhanced FEC G.975.1 1.7 (Default)
         EC(current second) = 0           EC   = 0           UC   = 0
         pre-FEC BER < 9.00E-11           Q > 6.45           Q Margin > 7.25

Remote FEC Mode: Unknown
         FECMISMATCH = 0

Detected Alarms: None
Asserted Alarms: None
Alarm Reporting Enabled for: LOS LOF LOM IAE OTU-BDI OTU-TIM OTU_SF_BER OTU_SD_BER ODU-AIS
 ODU-BDI OCI LCK PTIM ODU-TIM FECMISMATCH
BER Thresholds: OTU-SF = E-3  OTU-SD = E-6

Connectivity Info

               Network Port ID:  Unavailable
               Network Connection ID:  Unavailable
```

```
OTU TTI Sent     String ASCII: Tx TTI Not Configured
OTU TTI Received String ASCII: Rx TTI Not Recieved
OTU TTI Expected String ASCII: Exp TTI Not Configured

ODU TTI Sent     String ASCII: Tx TTI Not Configured
ODU TTI Received String ASCII: Rx TTI Not Recieved
ODU TTI Expected String ASCII: Exp TTI Not Configured

Optics Status

         Optics Type:  10Gb MSA WDM (65km)
         Wavelength Info: C-Band, MSA ITU Channel=3, Frequency=196.00THz,
Wavelength=1529.553nm
         TX Power = -50.00 dBm
         RX Power = -47.19 dBm
TDC Info

        TDC Not Supported on the Plim

Network SRLG values:

        Not Configured
```

This table describes selected fields from the **show controllers dwdm** command output.

Table 12: show controllers dwdm Command Output Field Descriptions

Field	Description
AIS	Number of alarm indication signal (AIS) alarms. AIS is a signal sent downstream as an indication that an upstream defect has been detected.
Alarm reporting enabled for	Lists the alarms that are enabled for reporting.
Asserted Alarms	Alarms indicated to be reported by the user.
BDI	Number of backward defect indication (BDI) alarms. The BDI is a single bit that conveys information regarding signal failure in the upstream direction.
BER thresholds	Values of the configured bit error rate thresholds.
BIP	Number of bit interleaved parity alarms. The BIP is comprised of one byte and is used for error detection. It is computed over the entire optical channel payload unit (OPU).
Controller State	Status of the controller.
Detected Alarms	Alarms detected by the hardware.
EC	Corrected code words. This is the number of words corrected by the FEC and is displayed as a per second rate.
FEC Mode	Indicates the forward error correction (FEC) mode for the controller. This can be Disabled, Enhanced FEC G.975.1 1.7 (Default), or Standard FEC.
IAE	Number of incoming alignment errors (IAE).

Field	Description
LCK	Number of upstream connection locked alarms. LCK is a signal sent downstream as an indication that upstream the connection is locked, and no signal is passed through.
LOF	Number of OTU loss of frame (LOF) alarms.
LOM	Number of OTU loss of multiframe (LOM) alarms.
Loopback	Loopback status. Indicates whether or not loopback is enabled and the type of loopback enabled.
LOS	Number of OTU loss of signal (LOS) alarms. The LOS threshold is set using the **rx-los-threshold** command. If the receive optical power is less than or equal to this defined threshold, the optical LOS alarm is raised.
OCI	Number of open connection indication alarms. OCI is a signal sent downstream as an indication that upstream the signal is not connected to a trail termination source.
ODU	Optical channel data unit alarms.
OTU	Optical transport unit overhead alarms.
OTU TTI Expected	Value of the expected TTI.
OTU TTI Received	Value of the received TTI.
OTU TTI Sent	Value of the transmit trail trace identifier (TTI).
PTIM	Number of payload type identifier mismatch alarms. This occurs when there is a mismatch between the way the ITU-T G.709 option is configured on the PLIM at each end of the optical span.
TDC Info	Tunable Dispersion Compensator (TDC) information.
Transport Admin State	Current status of the port as set by the **admin-state** command. Possible values are: IS (In-Service) and OOS (Out-of-Service).
UC	Uncorrectable code words. This is a raw counter.
Pre-FEC BER	Pre - bit error rate (BER) forward error correction (FEC). The pre-FEC BER is calculated using pre-forward error correction (FEC) error counts.
Q	The general signal quality bit error rate (BER) per voltage. The Q and Q margin are calculated using the Pre-FEC BER.
Q Margin	The general signal quality bit error rate (BER) per voltage. The Q and Q margin are calculated using the Pre-FEC BER.
Operational Mode	Indicates whether the tunable dispersion compensator (TDC) operational mode option is set to Auto or Manual.

Field	Description
Status	Indicates whether the tunable dispersion compensator (TDC) is in the acquiring state or locked state. The status is invalid if there is a major alarm.
Dispersion Setting	Indicates a value between –700 and +700 packets per second (pps). The dispersion setting is read from the optics module after the tunable dispersion compensator (TDC) has locked.
Reroute Control	Not used.
Reroute BER	Not used.

See Table 13: show controllers dwdm optics Command Output Field Descriptions, on page 133 for a description of the optics fields.

The following example shows the output from the show controllers dwdm command with the **g709 registers** keywords:

```
RP/0/RP0/CPU0:router# show controller dwdm 0/3/0/0 g709 registers

Addr          Name                 Value
 0x00800030    Serial[0]            0x30303130
 0x00800034    Serial[1]            0x30353934
 0x00800038    Serial[2]            0x0
 0x0080003c    PartNum[0]           0x38303030
 0x00800040    PartNum[1]           0x3034312d
 0x00800044    PartNum[2]           0x30300010
 0x00800048    PartNum[3]           0x0
 0x0080004c    Version[0]           0x312e3041
 0x00800050    Version[1]           0x6c706861
 0x00800054    Version[2]           0x28423133
 0x00800058    Version[3]           0x35290000
 0x0080005c    Version[4]           0x0
 0x00800060    Version[5]           0x0
 0x0080002c    Band                 0x0
 0x0080001c    RefClock             0x0
 0x00800020    Loopback             0x0
 0x00800000    IntfStatus           0x5000000
 0x00800004    ModEnable            0x1
 0x0080000c    ModStatus            0x34010000
 0x00800010    ModIntrMask          0x7c000000
 0x00800014    ModIntr              0x0
 0x00800100    TxLineStat           0x80
 0x00800104    TxLineEvent          0x0
 0x00800108    TxLineIntrMask       0xc1
 0x00800114    TxOpticChan          0x1
 0x00800118    Wavelength           0x1753c5
 0x00800200    RxLineStat           0x8000
 0x00800208    RxLineEventMask      0xffe3
 0x00800204    RxLineEvent          0x0
```

The following example shows the output from the **show controllers dwdm** command with the **optics** keyword on a 10-GE PLIM:

```
RP/0/RP0/CPU0:router# show controller dwdm 0/3/0/0 optics

Optics Status
```

```
         Optics Type:  10Gb MSA WDM (65km)
         Clock Source: Internal
        Wavelength Band: C-Band, MSA ITU Channel = 3, Frequency = 196.00 THz,
Wavelength = 1529.553 nm
         TX Power = 3.79 dBm
         RX Power = -8.83 dBm
```

This table describes selected fields from the **show controllers dwdm** command output with the **optics** keyword.

Table 13: show controllers dwdm optics Command Output Field Descriptions

Field	Description
Optics Type	Indicates the optics type: GE or OC-768c/STM-256c DWDM.
Clock Source	Indicates whether the clock is internal or line.
Wavelength Band	Indicates the wavelength band: C-band or L-band.
MSA ITU Channel	Multi Source Agreement (MSA) ITU channel number.
Frequency	Frequency of the channel in terahertz.
Wavelength	Wavelength corresponding to the channel number in nanometers.
TX power	Value of the transmit power level. This is user configurable on the OC-768c/STM-256c DWDM PLIM using the **transmit-power** command.
RX Power	Actual optical power at the RX port.
RX LOS Threshold	Receive loss of signal threshold. This is user configurable on the OC-768c/STM-256c DWDM PLIM using the **rx-los-threshold** command. If the receive optical power is less than or equal to this defined threshold, the optical LOS alarm is raised.

This example shows sample output from the **show controllers dwdm** command with the **wavelength-map** keyword on a Gigabit Ethernet controller:

```
RP/0/RP0/CPU0:router# show controller dwdm 0/5/0/3 wavelength-map

Wavelength band: C-band
MSA ITU channel range supported: 3~84

Wavelength map table
 ----------------------------------------
 Channel Frequency       Wavelength
  Num      (THz)            (nm)
 ----------------------------------------
 03       196.00          1529.553
 ----------------------------------------
 04       195.95          1529.944
 ----------------------------------------
 05       195.90          1530.334
 ----------------------------------------
 06       195.85          1530.725
 ----------------------------------------
 07       195.80          1531.116
 ----------------------------------------
```

```
08       195.75          1531.507
----------------------------------------
09       195.70          1531.898
----------------------------------------
10       195.65          1532.290
----------------------------------------
11       195.60          1532.681
----------------------------------------
12       195.55          1533.073
----------------------------------------
13       195.50          1533.465
----------------------------------------
14       195.45          1533.858
----------------------------------------
15       195.40          1534.250
----------------------------------------
16       195.35          1534.643
----------------------------------------
17       195.30          1535.036
----------------------------------------
18       195.25          1535.429
----------------------------------------
19       195.20          1535.822
.
.
.
```

This table describes selected fields from the **show controllers dwdm** command output with the **wavelength-map** keyword.

Table 14: show controllers dwdm wavelength Command Output Field Descriptions

Field	Description
channel Num	Channel number.
frequency (THz)	Frequency of the wavelength in terahertz.
wavelength (nm)	Wavelength in nanometers.

Related Commands

Command	Description
admin-state, on page 83	Configures the transport administration state on a DWDM port.
rx-los-threshold, on page 124	Configures the transponder receive power threshold on a DWDM controller.
transmit-power, on page 144	Configures the DWDM optics transmit laser power on a DWDM controller.

show controller dwdm pm

To display performance monitoring information for a DWDM controller, use the **show controller dwdm pm** command in EXEC mode.

show controller dwdm *instance* **pm history** [**15-min** | **24-hour** | **fec** | **optics** | **otn**]
show controller dwdm *instance* **pm interval** [**15-min** | **24-hour**][**fec** | **optics** | **otn**] *index*

Syntax Description

instance	Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. • *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. Shared port adapters (SPAs) are referenced by their subslot number. • *port*: Physical port number of the interface. For more information about the syntax for the router, use the question mark (?) online help function.
history	Displays all performance monitoring data.
interval	Displays specific performance monitoring data in a particular interval.
15-min	Displays performance monitoring data in a 15-minute interval.
24-hour	Displays performance monitoring data in a 24-hour interval.
fec	Displays FEC performance parameters, such as bit errors corrected (BIEC) and uncorrectable words.
optics	Displays optics performance parameters, such as optical power.
otn	Displays OTN performance parameters, such as path monitoring failure counts (FC-PM) and section monitoring unavailable seconds (UAS-SM).
index	Interval for which to display the performance monitoring information.

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
dwdm	read

Task ID	Operations
interface	read
sonet-sdh	read

Examples

The following example shows the output from the **show controllers dwdm pm** command on a 10-GE DWDM PLIM:

```
RP/0/RP1/CPU0:Router# show controllers dwdm 0/2/0/0 pm interval 24-hour 0

g709 OTN in the current interval [00:00:00 - 08:05:58 Tue Jul 11 2006]
    ES-SM-NE    : 0         Threshold : -1       TCA(enable)  : NO
    ESR-SM-NE   : 0         Threshold : -1       TCA(enable)  : NO
    SES-SM-NE   : 0         Threshold : -1       TCA(enable)  : NO
    SESR-SM-NE  : 0         Threshold : -1       TCA(enable)  : NO
    UAS-SM-NE   : 0         Threshold : -1       TCA(enable)  : NO
    BBE-SM-NE   : 0         Threshold : -1       TCA(enable)  : NO
    BBER-SM-NE  : 0         Threshold : -1       TCA(enable)  : NO
    FC-SM-NE    : 0         Threshold : -1       TCA(enable)  : NO
    ES-PM-NE    : 0         Threshold : -1       TCA(enable)  : NO
    ESR-PM-NE   : 0         Threshold : -1       TCA(enable)  : NO
    SES-PM-NE   : 0         Threshold : -1       TCA(enable)  : NO
    SESR-PM-NE  : 0         Threshold : -1       TCA(enable)  : NO
    UAS-PM-NE   : 0         Threshold : -1       TCA(enable)  : NO
    BBE-PM-NE   : 0         Threshold : -1       TCA(enable)  : NO
    BBER-PM-NE  : 0         Threshold : -1       TCA(enable)  : NO
    FC-PM-NE    : 0         Threshold : -1       TCA(enable)  : NO
    ES-SM-FE    : 0         Threshold : -1       TCA(enable)  : NO
    ESR-SM-FE   : 0         Threshold : -1       TCA(enable)  : NO
    SES-SM-FE   : 0         Threshold : -1       TCA(enable)  : NO
    SESR-SM-FE  : 0         Threshold : -1       TCA(enable)  : NO
    UAS-SM-FE   : 106       Threshold : -1       TCA(enable)  : NO
    BBE-SM-FE   : 0         Threshold : -1       TCA(enable)  : NO
    BBER-SM-FE  : 0         Threshold : -1       TCA(enable)  : NO
    FC-SM-FE    : 0         Threshold : -1       TCA(enable)  : NO
    ES-PM-FE    : 0         Threshold : -1       TCA(enable)  : NO
    ESR-PM-FE   : 0         Threshold : -1       TCA(enable)  : NO
    SES-PM-FE   : 0         Threshold : -1       TCA(enable)  : NO
    SESR-PM-FE  : 0         Threshold : -1       TCA(enable)  : NO
    UAS-PM-FE   : 32327     Threshold : -1       TCA(enable)  : NO
    BBE-PM-FE   : 0         Threshold : -1       TCA(enable)  : NO
    BBER-PM-FE  : 0         Threshold : -1       TCA(enable)  : NO
    FC-PM-FE    : 0         Threshold : -1       TCA(enable)  : NO

g709 FEC in the current interval [00:00:00 - 08:05:58 Tue Jul 11 2006]
    EC-BITS   : 0               Threshold : 0             TCA(enable)  : NO
    UC-WORDS  : 0               Threshold : 0            TCA(enable)  : NO

Optics in the current interval [00:00:00 - 08:05:58 Tue Jul 11 2006]
             MIN     AVG     MAX  Threshold  TCA  Threshold  TCA
                                    (min)  (enable) (max)  (enable)
LBC[mA ] :  1163    4336    8487    -1         NO      -1       NO
OPT[uW]  :  2593    2593    2593    -1         NO      -1       NO
OPR[uW]  :  69      69      70      -1         NO      -1       NO
```

This table describes selected fields from the **show controllers dwdm pm** command output.

Table 15: show controllers dwdm pm Command Output Field Descriptions

Field	Description
EC-BITS	Bit errors corrected (BIEC). Indicates the number of bit errors corrected in the DWDM trunk line during the performance monitoring time interval.
UC-WORDS	Uncorrectable words. This is the number of uncorrectable words detected in the DWDM trunk line during the performance monitoring time interval.
LBC	Laser bias current.
OPR	Optical power on the unidirectional port.
OPT	Transmit optical power in dBm.
MAX	Indicates the maximum value of the parameter.
AVG	Indicates the average value of the parameter
MIN	Indicates the minimum value of the parameter.
THRESHOLD	Indicates the parameter's configured threshold.
TCA	Indicates if TCA reporting is enabled or not.
BBE-PM-FE	Far-end path monitoring background block errors (BBE-PM)—Indicates the number of background block errors recorded in the optical transport network (OTN) path during the performance monitoring time interval.
BBE-PM-NE	Near-end path monitoring background block errors (BBE-PM).
BBE-SM-FE	Far-end section monitoring background block errors (BBE-SM)—Indicates the number of background block errors recorded in the OTN section during the performance monitoring time interval.
BBE-SM-NE	Near-end section monitoring background block errors (BBE-SM).
BBER-PM-FE	Far-end path monitoring background block errors ratio (BBER-PM)—Indicates the background block errors ratio recorded in the OTN path during the performance monitoring time interval.
BBER-PM-NE	Near-end path monitoring background block errors ratio (BBER-PM).
BBER-SM-FE	Far-end section monitoring background block errors ratio (BBER-SM)—Indicates the background block errors ratio recorded in the OTN section during the performance monitoring time interval.
BBER-SM-NE	Near-end section monitoring background block errors ratio (BBER-SM).
ES-PM-FE	Far-end path monitoring errored seconds (ES-PM)—Indicates the errored seconds recorded in the OTN path during the performance monitoring time interval.
ES-PM-NE	Near-end path monitoring errored seconds (ES-PM).

Field	Description
ES-SM-FE	Far-end section monitoring errored seconds (ES-SM)—Indicates the errored seconds recorded in the OTN section during the performance monitoring time interval.
ES-SM-NE	Near-end section monitoring errored seconds (ES-SM).
ESR-PM-FE	Far-end path monitoring errored seconds ratio (ESR-PM)—Indicates the errored seconds ratio recorded in the OTN path during the performance monitoring time interval.
ESR-PM-NE	Near-end path monitoring errored seconds ratio (ESR-PM).
ESR-SM-FE	Far-end section monitoring errored seconds ratio (ESR-SM)—Indicates the errored seconds ratio recorded in the OTN section during the performance monitoring time interval.
ESR-SM-NE	Near-end section monitoring errored seconds ratio (ESR-SM).
FC-PM-FE	Far-end path monitoring failure counts (FC-PM)—Indicates the failure counts recorded in the OTN path during the performance monitoring time interval.
FC-PM-NE	Near-end path monitoring failure counts (FC-PM).
FC-SM-FE	Far-end section monitoring failure counts (FC-SM)—Indicates the failure counts recorded in the OTN section during the performance monitoring time interval.
FC-SM-NE	Near-end section monitoring failure counts (FC-SM).
SES-PM-FE	Far-end path monitoring severely errored seconds (SES-PM)—Indicates the severely errored seconds recorded in the OTN path during the performance monitoring time interval.
SES-PM-NE	Near-end path monitoring severely errored seconds (SES-PM).
SES-SM-FE	Far-end section monitoring severely errored seconds (SES-SM)—Indicates the severely errored seconds recorded in the OTN section during the performance monitoring time interval.
SES-SM-NE	Near-end section monitoring severely errored seconds (SES-SM).
SESR-PM-FE	Far-end path monitoring severely errored seconds ratio (SESR-PM)—Indicates the severely errored seconds ratio recorded in the OTN path during the performance monitoring time interval.
SESR-PM-NE	Near-end path monitoring severely errored seconds ratio (SESR-PM).
SESR-SM-FE	Far-end section monitoring severely errored seconds ratio (SESR-SM)—Indicates the severely errored seconds ratio recorded in the OTN section during the performance monitoring time interval.
SESR-SM-NE	Near-end section monitoring severely errored seconds ratio (SESR-SM).
UAS-PM-FE	Far-end path monitoring unavailable seconds (UAS-PM)—Indicates the unavailable seconds recorded in the OTN path during the performance monitoring time interval.
UAS-PM-NE	Near-end path monitoring unavailable seconds (UAS-PM).

Field	Description
UAS-SM-FE	Far-end section monitoring unavailable seconds (UAS-SM)—Indicates the unavailable seconds recorded in the OTN section during the performance monitoring time interval.
UAS-SM-NE	Near-end section monitoring unavailable seconds (UAS-SM).

show vtxp-monitored ports

To display the list of DWDM controller interfaces on which VTXP attribute is enabled, use the use the **show vtxp-monitored ports** command in Global Configuration mode.

show vtxp-monitored ports

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 5.3.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
dwdm	read, write
interface	read, write
sonet-sdh	read, write

Examples

The following example shows how to view the interfaces on which the VTXP attribute is enabled:

```
RP/0/RP0/CPU0:router# show vtxp-monitored ports

Thu Jan  8 17:01:29.931 IST
dwdm ifName : dwdm0/1/0/0
dwdm ifName : dwdm0/1/0/1
dwdm ifName : dwdm0/1/0/2
```

Related Commands

Command	Description
controller dwdm, on page 85	Configures a DWDM controller.

transport-mode (WAN/OTN)

To specify the transport mode for a 10-Gigabit Ethernet interface, use the **transport-mode** command in interface configuration mode. To return to the default mode, use the **no** form of this command.

transport-mode wan | otn bit-transparent opu1e | opu2e

Syntax Description

wan	Configures the interface for 10GBASE-W WAN SONET/SDH (9.95328Gb/s) transport.
otn bit-transparent	Configures the interface for 10-Gigabit Ethernet over Optical Transport Network (ITU-T G.709) with 10GBASE-R transparently mapped into OTU-2.
opu1e	Configures the interface for 10GBASE-R over OPU1e without fixed stuffing (11.0491Gb/s).
opu2e	Configures the interface for 10GBASE-R over OPU2e with fixed stuffing (11.0957Gb/s)

Command Default

The interface is in LAN mode. Neither WAN mode or OTN mode is configured.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

Three modes are supported for a 10-Gigabit Ethernet interface: LAN, WAN, or OTN on these Ethernet line cards and Modular Port Adaptors (MPAs):

- 2-Port 10-Gigabit Ethernet, 20-Port Gigabit Ethernet Combination line card (A9K-2T20GE-B and A9K-2T20GE-L)
- 8-Port 10-Gigabit Ethernet line card (A9K-8T-L, -B, or -E)
- 16-Port 10-Gigabit Ethernet SFP+ line card (A9K-16T/8-B and A9K-16T/8-B+AIP)
- 24-Port 10-Gigabit Ethernet line card (A9K-24X10GE-SE/TR)
- 36-Port 10-Gigabit Ethernet line card (A9K-36X10GE-SE/TR)
- 2-Port 10-Gigabit Ethernet Modular Port Adaptor (A9K-MPA-2x10GE)
- 4-Port 10-Gigabit Ethernet Modular Port Adaptor (A9K-MPA-4x10GE)
- 8-Port 10-Gigabit Ethernet Modular Port Adaptor (A9K-MPA-8x10GE)

Limitation:

On TenGig breakout interface of Cisco ASR 9000 High Density 100GE Ethernet (8x100G and 4x100G) line cards, configure same transport mode (OPU1E or OPU2E) on both ends of the interface. Different transport modes at both ends results in flapping of the interface status and the router console displays continuous interface UP/DOWN messages.

If you want to configure the interface for DWDM support, configure the 10-Gigabit Ethernet interface for OTN transport mode.

These 40GE MPAs support LAN and OTU3 modes:

- A9K-MPA-1x40GE
- A9K-MPA-2x40GE

Note Before Cisco IOS XR Software Release 4.2.0, only **transport-mode wan** was used under the interface configuration mode to set WAN PHY controller. Then, both Operational Mode and Configuration Mode would be changed to WAN Mode.

After Cisco IOS XR Software Release 4.2.0, you can use **transport-mode wan** under the interface configuration mode to use basic function of WAN PHY. In addition, we can use **wanmode on** under the wanphy controller mode to use alarm function and BIP counter.

Note On the Cisco A9K-4T16GE-TR and Cisco A9K-4T16GE-SE line cards, mixed use of LAN and WAN transport modes is not supported due to hardware limitation. In other words, WAN PHY is configured on all the four 10GigE ports to be operated either in LAN mode or WAN mode for 10 GigE ports 16, 17, 18 and 19.

On applying the configuration change from LAN to WAN or back on port 16, the same configuration shall be applied on all the other 10 GigE ports 17, 18, and 19. The ports 17, 18 or 19 cannot be used to make configuration changes using the **transport-mode** command. Also, the running configuration shows the configuration change only on port 16.

Task ID

Task ID	Operations
interface	read, write

Examples

This example shows how to configure the interface for WAN PHY mode:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface 10gigabitethernet 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# transport-mode wan
RP/0/RP0/CPU0:router(config-if)# commit
```

The following configuration is needed to operate in WAN PHY mode:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# controller wanphy <>
RP/0/RP0/CPU0:router(config)# wanmode on
RP/0/RP0/CPU0:router(config)# commit
```

This example shows how to configure a DWDM interface using OTN transport:

```
RP/0/RP0/CPU0:router# config
```

```
RP/0/RP0/CPU0:router(config)# interface 10gigabitethernet 0/5/0/7/0
RP/0/RP0/CPU0:router(config-if)# transport-mode otn bit-transparent opu1e
RP/0/RP0/CPU0:router(config-if)# commit
```

The following additional configuration is also needed:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# controller dwdm <>
RP/0/RP0/CPU0:router(config)# admin-state in-service
RP/0/RP0/CPU0:router(config)# commit
```

This example shows how to return the interface configuration to its default LAN mode from OTN or WAN PHY mode:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface 10gigabitethernet 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# no transport-mode
RP/0/RP0/CPU0:router(config-if)# commit
```

This configuration example shows how to configure the interface for OTU3 mode:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# controller dwdm <>
RP/0/RP0/CPU0:router(config)# g709 enable
RP/0/RP0/CPU0:router(config)# commit
```

Note The following QSFP+ Optics is required to support OTU3 mode:

- QSFP-40GE-LR4

Related Commands

Command	Description
controller wanphy, on page 926	Enters WAN physical controller configuration mode in which you can configure a 10-Gigabit Ethernet WAN PHY controller.

transmit-power

To configure the DWDM optics transmit laser power on a DWDM controller, use the **transmit-power** command in DWDM configuration mode. To return the transponder transmit power to its default value, use the **no** form of this command.

transmit-power power-level

Syntax Description

power-level	Transmit power level in units of 0.1 dBm. Values can range from -190 to +10, which corresponds to a power level range of -19 dBm to +1 dBm.

Command Default

power-level: 0 dBm

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the OC-768c/STM-256c DWDM PLIM.

Usage Guidelines

The controller must be in the shutdown state before you can use the **transmit-power** command. You can configure the transponder transmit power only on the OC-768c/STM-256c DWDM PLIM.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The following example shows how to configure the receive power threshold to -10 dBm:

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RP0/CPU0:router(config-dwdm)# transmit-power -100
```

Related Commands

Command	Description
rx-los-threshold, on page 124	Configures the transponder receive power threshold on a DWDM controller.
show controller dwdm, on page 126	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

wavelength

To set the wavelength on a DWDM controller to a specific ITU channel or to define a specific frequency or wavelength to a DWDM controller, use the **wavelength** command in DWDM configuration mode. To return the wavelength to its default value, use the **no** form of this command.

wavelength {**50GHz-grid** *channel-number* | **frequency** *frequency* | **update** *wavelength*} | **100MHz-grid frequency** *frequency*

Syntax Description

50GHz-grid	Specifies 50-GHz frequency grid.
100MHz-grid	Specifies 100-GHz frequency grid.
channel-number	ITU channel number. ITU channel numbers have predefined frequencies as defined by Multi Source Agreement (MSA) International Telecommunication Union (ITU) grid. • The range is 1 to 89 for conventional band (C-band) • The range is 106 to 185 for long band (L-band).
frequency *frequency*	Keyword that specifies the frequency for the DWDM controller. Enter the 5-digit frequency value in the range of 19170 to 19610 GHz. For example, enter **frequency 19580** to specify 195.8 THz.
update *wavelength*	Keyword that defines a specific wavelength for the DWDM controller. Enter the 7-digit frequency value in the range of 1528773-1563863 micrometers (mm). For example, enter **update 1532290** to specifiy 1532.29 nanometers (nm).

Command Default

The default for OC-768c/STM-256c DWDM PLIM, C-band is 1.

The default for 10-GE PLIM, C-band is 3.

The default for 10-GE PLIM, L-band is 106.

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 5.3.2	50 GHZ or 100 GHz options were introduced.

Usage Guidelines

You can set the wavelength to a specific ITU channel, that is represented by a channel number in the Multi Source Agreement (MSA) ITU grid.

- The default channel number for the 10-GE PLIM, C-band is 3, which corresponds to a frequency of 196.00 THz and wavelength of 1529.553 nm.
- The default channel number for the 10-GE PLIM, L-band is 106, which corresponds to a frequency of 190.85 THz and wavelength of 1570.83 nm.

- The default channel number for the OC-768c/STM-256c DWDM PLIM, C-band is 1, which corresponds to a frequency of 196.10 and a wavelength of 1528.773.

The spacing between wavelengths is 50 GHZ or 100 GHz. Use the **show controllers dwdm** command with the **wavelength-map** keyword to view the channel numbers and wavelengths that are supported for a particular controller.

The controller must be in the out-of-service state before you can use the **wavelength** command.

Task ID

Task ID	Operations
dwdm	read, write

Examples

The following example shows how to set the DWDM wavelength to ITU channel 10.

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/1/0/0
RP/0/RP0/CPU0:router(config-dwdm)# wavelength 50GHz-grid 10
```

The following example shows how to set the frequency of ITU channel 10 to 195.8 THz.

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/1/0/0
RP/0/RP0/CPU0:router(config-dwdm)# wavelength 50GHz-grid frequency 19580
```

The following example shows how to set the wavelength of ITU channel 10 to 1532.29 nm.

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/1/0/0
RP/0/RP0/CPU0:router(config-dwdm)# wavelength 10 update 1532290
```

Related Commands

Command	Description
show controller dwdm, on page 126	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

Ethernet Interface Commands

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

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

carrier-delay

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

Note

- The **carrier-delay** command is active only when both **up** and **down** are configured from the host.
- The range of carrier-delay on access port of CRS is 0 to 2147483648 msec.
- If this configuration is not used, the default value is determined by the underlying driver, and may vary depending on whether auto-negotiation is enabled. The default value is chosen to provide enough time for the hardware link to stabilize after state change and to protect the system from excessive link flaps.
- If a value of 0 is set, carrier-delay is disabled in that direction.

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 2147483648.
up *milliseconds*	Length of time, in milliseconds, to delay the processing of hardware link up notifications. Range is from 0 through 2147483648.

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 3.9.0	The default value used when there is no carrier-delay configuration changed from 0 to being defined by each driver.
Release 4.2.0	The range for both down and up was increased to 0 through 2147483648.
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 60000. The **up** keyword was added, and the value of the *milliseconds* argument was set at 0 through 60000.

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/RP0/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/RP0/CPU0:router(config-if)# carrier-delay up 100 down 100
```

Related Commands

Command	Description
dampening, on page 459	Turns on event dampening.

clear lldp

To reset Link Layer Discovery Protocol (LLDP) traffic counters or LLDP neighbor information, use the **clear lldp** command in EXEC mode.

clear lldp **counters** | **table**

Syntax Description

counters	Specifies that LLDP traffic counters are cleared.
table	Specifies that LLDP information in the neighbor table is cleared.

Command Default

LLDP traffic counters are not reset, and LLDP neighbor information is not cleared.

Command Modes

EXEC mode

Command History

Release	Modification
Release 4.2.3	This command was introduced.

Usage Guidelines

To reset counters from the **show lldp traffic** command, use the **clear lldp counters** command. To clear neighbor information displayed by the **show lldp neighbors** command, use the **clear lldp table** command.

Task ID

Task ID	Operation
ethernet-services	read, write

The following example shows how to clear the LLDP counters and display LLDP traffic. The output from the **show lldp traffic** command shows that all the traffic counters have been reset to zero.

```
RP/0/RP0/CPU0:router# clear lldp counters
RP/0/RP0/CPU0:router# show lldp traffic
LLDP traffic statistics:
        Total frames out: 0
        Total entries aged: 0
        Total frames in: 0
        Total frames received in error: 0
        Total frames discarded: 0
        Total TLVs discarded: 0
        Total TLVs unrecognized: 0
```

The following example shows how to clear the LLDP table. The output of the **show lldp neighbors** command shows that all information has been deleted from the table.

```
RP/0/RP0/CPU0:router# clear lldp table
RP/0/RP0/CPU0:router# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
```

```
Device ID           Local Intf     Hold-time  Capability      Port ID
```

Related Commands

Command	Description
show lldp neighbors, on page 232	Displays information about LLDP neighbors.
show lldp traffic, on page 235	Displays statistics for LLDP traffic.

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** *interface-path-id* [**location** *node-id*]

Syntax Description

{**GigabitEthernet** | **TenGigE**}	Type of Ethernet interface whose MAC accounting statistics you want to clear. Enter **GigabitEthernet**, **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.
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 mode

Command History

Release	Modification
Release 2.0	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/RP0/CPU0:router# clear mac-accounting TenGigE 0/1/5/0 location 1/0/0/1
```

Related Commands

Command	Description
mac-accounting, on page 166	Generates accounting information for IP traffic based on the source and destination MAC addresses on LAN interfaces.

Command	Description
show mac-accounting (Ethernet), on page 237	Displays MAC accounting statistics for an 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**

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 auto-negotiate is enabled on the interface, then the default is negotiated.

If auto-negotiate 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 3.0	This command was introduced.

Usage Guidelines

Note When you explicitly enable the sending of flow-control pause frames, the value you configured with the **flow-control** command overrides any auto-negotiated 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 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/RP0/CPU0:router(config)# interface TenGigE 0/3/0/0
RP/0/RP0/CPU0:router(config-if)# flow-control ingress
```

Related Commands

Command	Description
show interfaces, on page 469	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. Use the **no** form of the command to remove the configuration.

interface GigabitEthernet | **HundredGigE** | **TenGigE** *interface-path-id*

Syntax Description

GigabitEthernet	Specifies or creates a Gigabit Ethernet (1000 Mbps) interface.
HundredGigE	Specifies or creates a Hundred Gigabit Ethernet (100 Gbps) 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 mode

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.2	This command was modified. The **TenGigE** keyword was added.
Release 4.0.1	This command was modified. The **HundredGigE** 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

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

```
RP/0/RP0/CPU0:router(config)# interface TenGigE 0/4/0/0
RP/0/RP0/CPU0:router(config-if)#
```

Related Commands

Command	Description
interface (Ethernet), on page 156	Specifies or creates an Ethernet interface and enters interface configuration mode.

lldp

To enable the Link Layer Discovery Protocol (LLDP) globally for both transmit and receive operation on the system, use the **lldp** command in Global Configuration mode. To disable LLDP, use the **no** form of this command.

lldp

Syntax Description

This command has no keywords or arguments.

Command Default

LLDP is disabled.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.2.3	This command was introduced.
Release 5.3.1	The **lldp subinterfaces enable** was introduced.

Usage Guidelines

When you enable LLDP globally using the **lldp** command, LLDP is not enabled on subinterfaces or bundle subinterfaces by default. This is to prevent the LLDP process from consuming high CPU cycles. In order to enable LLDP on subinterfaces and bundle subinterfaces as well, the **lldp subinterfaces enable** command is introduced.

Note When you use this command, you must remember that as the scale of interfaces(with subinterfaces and bundle subinterfaces) becomes higher, it might cause the LLDP process to hog the CPU.

Task ID

Task ID	Operation
ethernet-services	read, write

This example shows how to enable LLDP globally on the router:

```
RP/0/RP0/CPU0:router(config)# lldp
```

This example shows how to enable LLDP on subinterfaces:

```
RP/0/RP0/CPU0:router(config)# lldp subinterfaces enable
```

Related Commands

Command	Description
show lldp, on page 225	Displays the global LLDP operational characteristics on the system.

lldp (interface)

To enter LLDP configuration mode, use the **lldp (interface)** command.

lldp

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 4.2.3	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
ethernet-services	read, write
interface	read, write

This example shows how to enter LLDP configuration mode from Ethernet interface configuration mode:

```
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# lldp
RP/0/RP0/CPU0:router(config-lldp)#
```

Related Commands

Command	Description
interface (Ethernet), on page 156	Specifies or creates an Ethernet interface and enters interface configuration mode.
lldp, on page 158	Enables LLDP globally for both transmit and receive operation on the system.

lldp enable (per-interface)

When LLDP is enabled globally, all interfaces that support LLDP are automatically enabled for both transmit and receive operations. However, if you want to enable LLDP per interface, use `lldp enable` command in interface configuration mode.

lldp enable

Command Default

None

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 6.5.1	This command was introduced.

Task ID

Task ID	Operation
ethernet-services	read, write
interface	read, write

To enable LLDP per interface:

```
RP/0/RSP0/CPU0:ios(config)# int gigabitEthernet 0/2/0/0
RP/0/RSP0/CPU0:ios(config-if)# no sh
RP/0/RSP0/CPU0:ios(config-if)#commit
RP/0/RSP0/CPU0:ios(config-if)#lldp ?
RP/0/RSP0/CPU0:ios(config-if)#lldp enable
RP/0/RSP0/CPU0:ios(config-if)#commit
```

lldp holdtime

To specify the length of time that information from a Link Layer Discovery Protocol (LLDP) packet should be held by the receiving device before aging and removing it, use the **lldp holdtime** command in Global Configuration mode. To return to the default, use the **no** form of this command.

lldp holdtime *seconds*

Syntax Description

seconds	Number from 0 to 65535 that specifies the amount of time (in seconds) to hold the packet information. The default is 120.

Command Default

The packet hold time is 120 seconds (2 minutes).

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.2.3	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
ethernet-services	read, write

This example shows how to change the default hold time to 1 minute:

```
RP/0/RP0/CPU0:router(config)# lldp holdtime 60
```

Related Commands

Command	Description
lldp, on page 158	Enables LLDP globally for both transmit and receive operation on the system.
show lldp, on page 225	Displays the global LLDP operational characteristics on the system.

lldp reinit

To specify the length of time to delay initialization of the Link Layer Discovery Protocol (LLDP) on an interface, use the **lldp reinit** command in Global Configuration mode. To return to the default, use the **no** form of this command.

lldp reinit *seconds*

Syntax Description

seconds	Number from 2 to 5 that specifies the length of time (in seconds) that LLDP should delay initialization. The default is 2.

Command Default

Initialization of LLDP is delayed for 2 seconds on an interface.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.2.3	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
ethernet-services	read, write

The following example shows how to change the default initialization delay from 2 to 4 seconds:

```
RP/0/RP0/CPU0:router(config)# lldp reinit 4
```

Related Commands

Command	Description
lldp, on page 158	Enables LLDP globally for both transmit and receive operation on the system.
show lldp, on page 225	Displays the global LLDP operational characteristics on the system.

lldp timer

To specify the Link Layer Discovery Protocol (LLDP) packet rate, use the **lldp timer** command in Global Configuration mode. To return to the default, use the **no** form of this command.

lldp timer *seconds*

Syntax Description

seconds	Number from 5 to 65534 that specifies the rate (in seconds) at which to send LLDP packets. The default is 30.

Command Default

LLDP packets are sent every 30 seconds.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.2.3	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
ethernet-services	read, write

The following example shows how to change the default LLDP packet rate from 30 seconds to 1 minute:

```
RP/0/RP0/CPU0:router(config)# lldp timer 60
```

Related Commands

Command	Description
lldp, on page 158	Enables LLDP globally for both transmit and receive operation on the system.
show lldp, on page 225	Displays the global LLDP operational characteristics on the system.

lldp tlv-select disable

To disable transmission of the selected Type Length Value (TLV) in Link Layer Discovery Protocol (LLDP) packets, use the **lld tlv-select disable** command in Global Configuration mode. To return to the default, use the **no** form of this command.

lldp tlv-select *tlv-name* **disable**

Syntax Description

tlv-name	Name of the TLV to be suppressed from LLDP packets. The *tlv-name* can be one of the following LLDP TLV types: • **management-address** • **port-description** • **system-capabilities** • **system-description** • **system-name**

Command Default

All TLVs are sent in LLDP packets.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.2.3	This command was introduced.

Usage Guidelines

Certain TLVs are classified as mandatory in LLDP packets, such as the Chassis ID, Port ID, and Time to Live (TTL) TLVs. These TLVs must be present in every LLDP packet. You can use the **lldp tlv-select disable** command to suppress transmission of certain other optional TLVs in LLDP packets.

Task ID

Task ID	Operation
ethernet-services	read, write

The following example shows how to disable transmission of the System Capabilities TLV from LLDP packets:

```
RP/0/RP0/CPU0:router(config)# lldp tlv-select system-capabilities disable
```

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

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 3.0	This command was introduced.

Usage Guidelines

The **loopback** command is available for all Ethernet interface types (Gigabit Ethernet, 10-Gigabit 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/RP0/CPU0:router(config)# interface TenGigE 0/3/0/0
RP/0/RP0/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**

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 3.0	This command was first introduced.
Release 4.3.2	The mac-accounting egress command was supported on Bundle Ethernet interfaces.

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/RP0/CPU0:routerconfigure
RP/0/RP0/CPU0:routerinterface bundle-ether <bundle-id>
RP/0/RP0/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/RP0/CPU0:routerconfigure
RP/0/RP0/CPU0:routerinterface bundle-ether <bundle-id>
RP/0/RP0/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 152	Clears MAC accounting statistics for an interface.
show mac-accounting (Ethernet), on page 237	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*

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 2.0	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) 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/RP0/CPU0:router(config)# interface TenGigE 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# mac-address 0001.2468.ABCD
```

negotiation auto

To enable link autonegotiation on Gigabit Ethernet interfaces, use the **negotiation auto** command in interface configuration mode. To disable link autonegotiation, use the **no** form of this command.

negotiation auto

Syntax Description

This command has no keywords or arguments.

Command Default

Link auto-negotiation is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

The **negotiation auto** command is available on Gigabit Ethernet interfaces only.

Task ID

Task ID	Operations
interface	read, write

Examples

This example shows how to enable link autonegotiation on an interface:

```
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/0/2/0
RP/0/RP0/CPU0:router(config-if)# negotiation auto
```

This example shows how to disable link autonegotiation on an interface:

```
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/0/2/0
RP/0/RP0/CPU0:router(config-if)# no negotiation auto
```

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

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 3.0	This command was first 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/RP0/CPU0:router(config)# interface TenGigE 0/3/0/0
RP/0/RP0/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 GigabitEthernet | **GigabitEthCtrlr** | **HundredGigE** | **HundredGigECtrlr** | **TenGigE** | **TenGigECtrlr** *interface-path-id* [**all** | **bert** | **control** | **internal** | **mac** | **periodic** | **phy** | **pm** | **regs** | **stats** | **xgxs**]

Syntax Description

{**GigabitEthernet** | **GigabitEthCtrlr | HundredGigE** | **HundredGigECtrlr** | **TenGigE** | **TenGigECtrlr**}	Specifies the type of Ethernet interface or controller whose status and configuration information you want to display. Enter GigabitEthernet, GigabitEthernetCtrlr, HundredGigE, HundredGigeCtrlr, TenGigE, or TenGigeCtrlr.
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. **Note** Not supported on the Cisco CRS 14-Port or Cisco CRS 20-Port or 10-Gigabit or 1-Port 100-Gigabit Ethernet LAN/WAN-PHY Interface Module.
control	Displays configuration and control information.
internal	Displays internal information for the interface.
periodic	Displays performance monitoring data periodically.
phy	Displays physical information for the interface.
pm	Displays Ethernet performance monitoring.
regs	Displays register information.
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 mode

Command History

Release	Modification
Release 3.0	This command was introduced.
Release 3.5.0	This command was modified. The **GigabitEthernet** and **TenGigE** keywords were added.
Release 4.0.1	This command was modified. The **HundredGigE** keyword was added.
Release 6.0.x	This command was modified. The **GigabitCtrlr**, **TenGigECtrlr**, and **HundredGigECtrlr** keywords were added. 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.

For controllers, use the following keywords only.

- all
- periodic
- pm
- stats

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

Examples

```
RP/0/RP0/CPU0:router# show controllers GigabitEthernet 0/0/0/1
Operational data for interface GigabitEthernet0/0/0/1:

State:
    Administrative state: enabled
    Operational state: Up
```

```
    LED state: Green On

Media:
    Media type: X fiber over short-wl laser PMD, full duplex
    Optics:
        Vendor: CISCO-FINISAR
        Part number: FTLF8519P2BNL-C6
        Serial number: FNS120304T9

MAC address information:
    Operational address: 001d.e5eb.88e1
    Burnt-in address: 001d.e5eb.88e1
    No unicast addresses in filter
    No multicast addresses in filter
Autonegotiation enabled:
    No restricted parameters

Operational values:
    Speed: 1Gbps
    Duplex: Full Duplex
    Flowcontrol: None
    Loopback: None (or external)
    MTU: 1526
    MRU: 1526
    Inter-packet gap: standard (12)
```

The following example shows sample output from the **show controllers TenGigE** command for the Cisco 8-Port 10-Gigabit Ethernet physical layer interface module (PLIM):

```
RP/0/RP0/CPU0:router# show controllers TenGigE 0/3/0/0

PHY:
XENPAK device registers:
========================

Vendor Name: CISCO-SUMITOMO
Vendor PN: SXP3101NV-C1
Vendor Rev: A1
Vendor SN: ECL120701L2

Package OUI: 0041f426
Vendor OUI: 00137b11
Vendor Date Code: 2004071200
nvr_control_status = 0x0007
nvr_version = 0x1e
nvr_size0 = 0x01
nvr_size1 = 0x00
mem_used0 = 0x01
mem_used1 = 0x00
basic_addr = 0x0b
cust_addr = 0x77
vend_addr = 0xa7
ext_vend_addr0= 0x00
ext_vend_addr1= 0xff
reserved0 = 0x00
tcvr_type = 0x01
connector = 0x01
encoding = 0x01
bitrate0 = 0x27
bitrate1 = 0x10
protocol = 0x01
x_gbe_code_byte_0 = 0x02
x_gbe_code_byte_1 = 0x00
```

```
sonet_sdh_code_byte_0 = 0x00
sonet_sdh_code_byte_1 = 0x00
sonet_sdh_code_byte_2 = 0x00
sonet_sdh_code_byte_3 = 0x00
x_gfc_code_byte_0 = 0x00
x_gfc_code_byte_1 = 0x00
x_gfc_code_byte_2 = 0x00
x_gfc_code_byte_3 = 0x00
range0 = 0x03
range1 = 0xe8
fibre_type_byte_0 = 0x20
fibre_type_byte_1 = 0x00
Center Wavelength:
chan0 = 1310.00 nm

chan1 =  0.00 nm
chan2 =  0.00 nm
chan3 =  0.00 nm

basic_checksum = 0x00

Link Alarm Status Registers:
rx_alarm_control = 0x0019
tx_alarm_control = 0x0059
lasi_control = 0x0000
rx_alarm_status = 0x0018
tx_alarm_status = 0x0058
lasi_status = 0x0005

Digital Optical Monitoring:
Transceiver Temp: 34.246 C
Laser Bias Current:  4.8640 mA
Laser Output Power: 0.5059 mW, -3.0 dBm
Receive Optical Power: 0.0000 mW, -inf dBm

Quake: devid 0x0043a400
10GE PMA/PMD Registers:
Control = 0x2040 Status = 0x0082 Dev ID 0 = 0x0043 Dev ID 1 = 0xa400 Speed Ability =
0x0001 Devices 1 = 0x001a Devices 2 = 0x0000 Control 2 = 0x0006 Status 2 = 0xb541 Tx
Disable = 0x0000 Rx Signal Detect = 0x0000 OUI 0 = 0x0041 OUI 1 = 0xf426

Quake (1.c001) = 0x0003

10GE PCS Registers:
Control = 0x2040 Status = 0x0082 Dev ID 0 = 0x0043 Dev ID 1 = 0xa400 Speed Ability =
0x0001 Devices 1 = 0x001a Devices 2 = 0x0000 Control 2 = 0x0000 Status 2 = 0x8401 PKG ID 0

= 0x0000 PKG ID 1 = 0x0000 Base X Status = 0x0000 Base X Control = 0x0000 Base R Status 1
= 0x0004 Base R Status 2 = 0x0000 Base R jitter seed a0 = 0x0000 Base R jitter seed a1 =
0x0000 Base R jitter seed a2 = 0x0000 Base R jitter seed a3 = 0x0000 Base R jitter seed b0

= 0x0000 Base R jitter seed b1 = 0x0000 Base R jitter seed b2 = 0x0000 Base R jitter seed
b3 = 0x0000 Base R jitter test control = 0x0000 Base R jitter test counter = 0x0000
10GE XS/XS Registers:
Control = 0x2040 Status = 0x0002
Dev ID 0 = 0x0043 Dev ID 1 = 0xa400
Speed Ability = 0x0001 Devices 1 = 0x001a Devices 2 = 0x0000 Status 2 = 0x8000 PKG ID 0 =
0x0000 PKG ID 1 = 0x0000 Lane Status = 0x1c0f Test Control = 0x0000

DTE XGXS (BCM8011):
Control = 0x0000 Status = 0x801f
Dev ID 0 = 0x0040 Dev ID 1 = 0x6092
Control 2 = 0x202f
Status 2 = 0x8b01
```

```
Speed Ability = 0x0001 Devices 1 = 0x001a Devices 2 = 0x0000 Status 2 = 0x8000 PKG ID 0 =
0x0000 PKG ID 1 = 0x0000 Lane Status = 0x1c0f Test Control = 0x0000

DTE XGXS (BCM8011):
Control = 0x0000 Status = 0x801f
Dev ID 0 = 0x0040 Dev ID 1 = 0x6092
Control 2 = 0x202f
Status 2 = 0x8b01

MAC (PLA):
Unicast MAC Address entries = 0
MAC (PLA) device is enabled
MAC (PLA) device is in promiscuous mode
MAC (PLA) device loopback is disabled

MAC (PLA) device MTU = 8226

8x10GE PLIM Registers:
local_regs_id = 0xa6602000 local_regs_inter_stat = 0x00000000 local_regs_inter_stat_alias
= 0x00000000 local_regs_inter_enbl_woset = 0x0000ff00 local_regs_inter_enbl_woclr =
0x0000ff00 local_regs_chip_reset = 0x00000000 local_regs_reset = 0xff000000
local_regs_misc_io = 0x00010000 sn_link_framed = 0x00000001 sn_link_crc_errors =
0x00000000 sn_link_force_reframe = 0x00000000 sn_link_error_reframe = 0x00000001
sn_link_force_error = 0x00000000 sn_link_error_cause = 0x00000000
sn_link_error_interrupt_mask = 0x00000003 channel0_control = 0x000000a6 channel1_control =

0x000000a6 channel2_control = 0x0000008e channel3_control = 0x0000008e channel4_control =
0x0000008e channel5_control = 0x000000a6 channel6_control = 0x000000a6 channel7_control =
0x0000008e
```

The following example shows sample output from the **show controllers TenGigE** command:

```
RP/0/RP0/CPU0:router# show controllers TenGigE 0/7/0/0
Tue Mar 22 15:32:35.491 UTC
Operational data for interface TenGigE0/7/0/0:

State:
    Administrative state: enabled
    Operational state: Up
    LED state: Green On

Phy:
    Media type: R fiber over 1310nm optics
    Optics:
        Vendor: CISCO-SUMITOMO
        Part number: SFCT-7081Z-CS2
        Serial number: AGA1447N4JE

MAC address information:
    Operational address: 0021.a03a.4744
    Burnt-in address: 0021.a03a.4744
    No unicast addresses in filter
    Operating in multicast promiscuous mode

Autonegotiation disabled.

Operational values:
    Speed: 10Gbps
    Duplex: Full Duplex
    Flowcontrol: None
    Loopback: None (or external)
    MTU: 1522
    MRU: 1522
    Inter-packet gap: standard (12)
```

The following example shows sample output from the base form of the **show controllers TenGigE** command for the Cisco CRS 14-Port 10-Gigabit Ethernet LAN/WAN-PHY Interface Module:

```
RP/0/RP0/CPU0:router# show controllers TenGigE 0/1/0/0
Thu Oct  7 16:18:32.348 EST
Operational data for interface TenGigE0/1/0/0:

State:
    Administrative state: disabled
    Operational state: Down (Reason: Link loss or low light, no loopback)
    LED state: Yellow On

Phy:
    Media type: R fiber over 1310nm optics
    Optics:
        Vendor: CISCO-SUMITOMO
        Part number: SXP3101NV-C1
        Serial number: ECL120701L2

MAC address information:
    Operational address: 0014.f294.6776
    Burnt-in address: 0014.f294.6776
    No unicast addresses in filter
    Operating in multicast promiscuous mode

Autonegotiation disabled.

Operational values:
    Speed: 10Gbps
    Duplex: Full Duplex
    Flowcontrol: None
    Loopback: None (or external)
    MTU: 1522
    MRU: 1522
    Inter-packet gap: standard (12)
```

The following example shows sample output from the **show controllers TenGigE all** form of the command:

```
RP/0/RP0/CPU0:router# show controllers TenGigE 0/7/0/0 all
ue Mar 22 15:32:45.685 UTC
Operational data for interface TenGigE0/7/0/0:

State:
    Administrative state: enabled
    Operational state: Up
    LED state: Green On

Phy:
    Media type: R fiber over 1310nm optics
    Optics:
        Vendor: CISCO-SUMITOMO
        Part number: SXP3101NV-C1
        Serial number: ECL120701L2

MAC address information:
    Operational address: 0021.a03a.4744
    Burnt-in address: 0021.a03a.4744
    No unicast addresses in filter
    Operating in multicast promiscuous mode

Autonegotiation disabled.

Operational values:
```

```
    Speed: 10Gbps
    Duplex: Full Duplex
    Flowcontrol: None
    Loopback: None (or external)
    MTU: 1522
    MRU: 1522
    Inter-packet gap: standard (12)

Statistics for interface TenGigE0/7/0/0 (cached values):

Ingress:
    Input total bytes           = 60
    Input good bytes            = 60

    Input total packets         = 1
    Input 802.1Q frames         = 0
    Input pause frames          = 0
    Input pkts 64 bytes         = 1
    Input pkts 65-127 bytes     = 0
    Input pkts 128-255 bytes    = 0
    Input pkts 256-511 bytes    = 0
    Input pkts 512-1023 bytes   = 0
    Input pkts 1024-1518 bytes  = 0
    Input pkts 1519-Max bytes   = 0

    Input good pkts             = 1
    Input unicast pkts          = 0
    Input multicast pkts        = 0
    Input broadcast pkts        = 1

    Input drop overrun          = 0
    Input drop abort            = 0
    Input drop invalid VLAN     = 0
    Input drop invalid DMAC     = 0
    Input drop invalid encap    = 0
    Input drop other            = 0

    Input error giant           = 0
    Input error runt            = 0
    Input error jabbers         = 0
    Input error fragments       = 0
    Input error CRC             = 0
    Input error collisions      = 0
    Input error symbol          = 0
    Input error other           = 0

    Input MIB giant             = 0
    Input MIB jabber            = 0
    Input MIB CRC               = 0

Egress:
    Output total bytes          = 0
    Output good bytes           = 0

    Output total packets        = 0
    Output 802.1Q frames        = 0
    Output pause frames         = 0
    Output pkts 64 bytes        = 0
    Output pkts 65-127 bytes    = 0
    Output pkts 128-255 bytes   = 0
    Output pkts 256-511 bytes   = 0
    Output pkts 512-1023 bytes  = 0
    Output pkts 1024-1518 bytes = 0
    Output pkts 1519-Max bytes  = 0
```

```
    Output good pkts            = 0
    Output unicast pkts         = 0
    Output multicast pkts       = 0
    Output broadcast pkts       = 0

    Output drop underrun        = 0
    Output drop abort           = 0
    Output drop other           = 0

    Output error other          = 0

Management information for interface TenGigE0/7/0/0:

Port number: 0
Bay number: 0
Interface handle: 0x1780200

Config:
    Auto-negotiation: Configuration not supported (Off)
    Carrier delay (up): Not configured
    Carrier delay (down): Not configured
    Speed: Configuration not supported (10Gbps)
    Duplex: Configuration not supported (Full Duplex)
    Flow Control: Not configured (None)
    IPG: Not configured (standard (12))
    Loopback: Not configured (None)
    MTU: Not configured
    Bandwidth: Not configured
    BER-SD Threshold: Configuration not supported
    BER-SD Report: Configuration not supported
    BER-SF Threshold: Configuration not supported
    BER-SF Report: Configuration not supported
    BER-SF Signal Remote Failure: Configuration not supported

Driver constraints:
    Min MTU: 64 bytes
    Max MTU: 9600 bytes
    Max speed: 10Gbps
    Interface type: TenGigE
    Management interface: No
    Promiscuous mode: Yes
    Default carrier delay up (auto-neg on): 0 ms
    Default carrier delay down (auto-neg on): 0 ms
    Default carrier delay up (auto-neg off): 0 ms
    Default carrier delay down (auto-neg off): 0 ms
    Allowed config mask: 0x27b

Cached driver state:
    MTU: 1522 bytes
    Burnt-in MAC address: 0021.a03a.4744

Operational carrier delay:
    Carrier delay (up): 0 ms
    Carrier delay (down): 0 ms

Bundle settings:
    Aggregated: No
    Bundle MTU: 1514 bytes
    Bundle MAC address: 0021.a03a.4744

Port FSM state:
    Port is enabled, link is up
Complete FSM state:
```

```
    Admin up
    Bundle admin up
    Client admin up
    Client admin tx not disabled
    Port enabled
    Port tx enabled
    Hardware link up
IDB interface state information:
    IDB bundle admin up
    IDB client admin up
    IDB client tx admin up
    IDB error disable not set

0 Unicast MAC Addresses:

0 Multicast MAC Addresses:

0 Unicast Bundle MAC Addresses:

0 Multicast Bundle MAC Addresses:


Operational address: 0021.a03a.4744
Burnt-in address: 0021.a03a.4744

PLA 0 port 0  MAC enabled  Rx MAC enabled
Administrative state: Up
Operational state: Up

0 HSRP/VRRP MAC addresses

VLAN Ethertype: 0x8100
QinQ Ethertype: 0x88a8
MTP  Ethertype: 0x88e7

4 VLAN UIDB entries
VLAN1   VLAN2      Packet Type Flags      UIDB Result Flags
   0        0          VLAN                   1 VLAN
   0        0               ARPA              1 ARPA
   0        0                    SAP          1 SAP
   0        0                                 1 SNAP


Total Power Available on PLIM for XFP's: 35000 mW
  Power used by Inserted XFP's: 1500 mW
  Power Available: 33500 mW

     Port        Power Used       State
      00          1500 mW         XFP Inserted and Powered On
      01          0000 mW         No XFP Inserted
      02          0000 mW         No XFP Inserted
      03          0000 mW         No XFP Inserted
      04          0000 mW         No XFP Inserted
      05          0000 mW         No XFP Inserted
      06          0000 mW         No XFP Inserted
      07          0000 mW         No XFP Inserted
      08          0000 mW         No XFP Inserted
      09          0000 mW         No XFP Inserted
      10          0000 mW         No XFP Inserted
      11          0000 mW         No XFP Inserted
      12          0000 mW         No XFP Inserted
      13          0000 mW         No XFP Inserted

802.3ae Sections
```

```
================

PMA/PMD
  Previous Alarm Status:
    PMA/PMD NOT Locked to Local Signal
  Current Alarm Status:
    PMA/PMD Locked to Local Signal
    SR Ability
    Loopback Ability

PCS
  Previous Alarm Status:
    PCS Rx Link DOWN
    PCS Rx NOT Block Locked
    PCS Rx Link Status DOWN
    PCS Error'd Block Counts: 0
    PCS BER Counts: 0
    PCS has NO Block Lock
  Current Alarm Status:
    PCS Rx Link UP
    PCS Rx Block Locked
    PCS Rx Link Status UP
    PCS Error'd Block Counts: 0
    PCS BER Counts: 0
    PCS has Block Lock

WIS: HW In LAN Mode - No Info


XFP General Info:
=================

PHY/XFP Status:  XFP is Working as expected


XFP Info:
=========
Max Power Dissipation: 1500 mW

XFP Type: 10GBASE-LR
Vendor Name: CISCO-SUMITOMO
Vendor Part Number: SFCT-7081Z-CS2
Vendor OUI: 0x00-0x17-0x6a
Vendor Hardware Revision: 01
Vendor Serial number: AGA1447N4JE
Date Code (yy/mm/dd): 10/11/27
Lot Code: 01

Cisco PID: XFP10GLR-192SR-L
Cisco VID: V01
Cisco PN: 10-2542-01

ID: XFP
Extended ID: 0x18
  TX ref clock input is not required
  CDP is supported
  Power Level 1 (1.5W max. power)
Minimum bit rate is 9900 MBits/s.
Maximum bit rate is 11100 MBits/s.


XFP Detail Info:
================
```

```
Temp: 30.119
Tx bias: 35.178 mA
Tx power: 0.5141 mW ( -2.9 dBm)
Rx power: 0.4612 mW ( -3.4 dBm)
AUX 1: Laser Temperature: 0x40
AUX 2: +3.3V Supply Voltage: 0x7

XFP Status: enabled.
 laser is enabled
 MOD NR is ready
 is powered on
 has interrupt(s)
 has no LOS
 data is ready
 TX path is ready
 TX laser is not in fault condition
 TX path CDR is locked
 RX path is ready
 RX path CDR is locked

Alarms:
  Low RX power alarm

Warnings:
  Low TX bias warning
  Low TX power warning
  Low RX power warning

THRESHOLDS
                      High Alarm     Low Alarm     High Warning      Low Warning
   Temperature     C       78.0          0.0            73.0            5.0
   Voltage         V     000.0000      000.0000       000.0000        000.0000
   Bias Current   mA     090.0000      005.0000       075.0000        015.0000
   Transmit power mW     022.3870      000.7580       011.2200        001.5130
   Receive power  mW     022.3870      000.1810       011.2200        000.3630
DTE XGXS
  Current Alarm Status:
    XGXS Lanes All Synchronized
    XGXS Lanes Aligned
PHY XGXS
  Previous Alarm Status:
    NO XGXS Local Fault
    TX Link Down
  Current Alarm Status:
    NO XGXS Local Fault
    TX Link UP

LASI 802.3ae Registers:
=======================
Previous: LASI Status = 0x0001 Rx Alarm Status = 0x0004 Tx Alarm Status = 0x0020
Current: LASI Status = 0x0000 Rx Alarm Status = 0x0000 Tx Alarm Status = 0x0000

PMA/PMD 802.3ae Registers:
==========================
Control = 0x2040 Status = 0x0006 Dev ID 0 = 0x0043 Dev ID 1 = 0xa400
Speed Ability = 0x0001 Devices 1 = 0x001e Devices 2 = 0x0000
Control 2 = 0x0007 Status 2 = 0xb181
Tx Disable = 0x0000 Rx Signal Detect = 0x0001
OUI 0 = 0x0000 OUI 1 = 0x0000
Current: Status = 0x0006 Status 2 = 0xb181

WIS 802.3ae Registers:
======================
Control = 0x2040 Status = 0x0082 Dev ID 0 = 0x0043 Dev ID 1 = 0xa400
```

```
Speed Ability = 0x0001 Devices 1 = 0x001e Devices 2 = 0x0000
Control 2 = 0x0000 Status 2 = 0x8003 Status 3 = 0x0008
Test Pattern Error Counter = 0x0000 Far End BLock Error Counter = 0x0000
J1 TX 1 = 0x0000 J1 TX 2 = 0x0000 J1 TX 3 = 0x0000 J1 TX 4 = 0x0000
J1 TX 5 = 0x0000 J1 TX 6 = 0x0000 J1 TX 7 = 0x0000 J1 TX 8 = 0x8900
J1 RX 1 = 0x0000 J1 RX 2 = 0x0000 J1 RX 3 = 0x0000 J1 RX 4 = 0x0000
J1 RX 5 = 0x0000 J1 RX 6 = 0x0000 J1 RX 7 = 0x0000 J1 RX 8 = 0x0000
Far End BIP Error 0 = 0x0000 Far End BIP Error 1 = 0x0000
Line BIP Error 0 = 0x0000 Line BIP Error 1 = 0x0000
Path BIP Error Count = 0x0000 Section BIP Error Count = 0x0000
J0 Tx 1 = 0x0000 J0 Tx 2 = 0x0000 J0 Tx 3 = 0x0000 J0 Tx 4 = 0x0000
J0 Tx 5 = 0x0000 J0 Tx 6 = 0x0000 J0 Tx 7 = 0x0000 J0 Tx 8 = 0x8900
J0 Rx 1 = 0x0000 J0 Rx 2 = 0x0000 J0 Rx 3 = 0x0000 J0 Rx 4 = 0x0000
J0 Rx 5 = 0x0000 J0 Rx 6 = 0x0000 J0 Rx 7 = 0x0000 J0 Rx 8 = 0x0000
Current: Status = 0x0082 Status 2 = 0x8003 Status 3 = 0x0008

PCS 802.3ae Registers:
======================
Control = 0x2040 Status = 0x0006 Dev ID 0 = 0x0043 Dev ID 1 = 0xa400
Speed Ability = 0x0001 Devices 1 = 0x001e Devices 2 = 0x0000
Control 2 = 0x0000 Status 2 = 0x8005
PKG ID 0 = 0x0000 PKG ID 1 = 0x0000
Base X Status = 0x0000 Base X Control = 0x0000
Base R Status 1 = 0x1005 Base R Status 2 = 0x8000
Base R jitter seed a0 = 0x0000 Base R jitter seed a1 = 0x0000
Base R jitter seed a2 = 0x0000 Base R jitter seed a3 = 0x0000
Base R jitter seed b0 = 0x0000 Base R jitter seed b1 = 0x0000
Base R jitter seed b2 = 0x0000 Base R jitter seed b3 = 0x0000
Base R jitter test control = 0x0000 Base R jitter test counter = 0x0000
Current: Status = 0x0006 Status 2 = 0x8005 Base R 1 = 0x1005 Base R 2 = 0x8000

PHY XS 802.3ae Registers:
=========================
Control = 0x2040 Status = 0x0006
Dev ID 0 = 0x0043 Dev ID 1 = 0xa400
Speed Ability = 0x0001 Devices 1 = 0x001e Devices 2 = 0x0000
Status 2 = 0x8000 PKG ID 0 = 0x0000 PKG ID 1 = 0x0000
Lane Status = 0x1c0f Test Control = 0x0000
Current: Status = 0x0006 Status 2 = 0x8000 Lane Status = 0x1c0f

XFP Register Info (MSA):
========================
(Reg 000 = 0x06)  (Reg 001 = 0x00)  (Reg 002 = 0x4e)  (Reg 003 = 0x00)
(Reg 004 = 0x00)  (Reg 005 = 0x00)  (Reg 006 = 0x49)  (Reg 007 = 0x00)
(Reg 008 = 0x05)  (Reg 009 = 0x00)  (Reg 010 = 0x00)  (Reg 011 = 0x00)
(Reg 012 = 0x00)  (Reg 013 = 0x00)  (Reg 014 = 0x00)  (Reg 015 = 0x00)
(Reg 016 = 0x00)  (Reg 017 = 0x00)  (Reg 018 = 0xaf)  (Reg 019 = 0xc8)
(Reg 020 = 0x09)  (Reg 021 = 0xc4)  (Reg 022 = 0x92)  (Reg 023 = 0x7c)
(Reg 024 = 0x1d)  (Reg 025 = 0x4c)  (Reg 026 = 0x57)  (Reg 027 = 0x73)
(Reg 028 = 0x02)  (Reg 029 = 0xf6)  (Reg 030 = 0x2b)  (Reg 031 = 0xd4)
(Reg 032 = 0x05)  (Reg 033 = 0xe9)  (Reg 034 = 0x57)  (Reg 035 = 0x73)
(Reg 036 = 0x00)  (Reg 037 = 0xb5)  (Reg 038 = 0x2b)  (Reg 039 = 0xd4)
(Reg 040 = 0x01)  (Reg 041 = 0x6b)  (Reg 042 = 0x5d)  (Reg 043 = 0x00)
(Reg 044 = 0x00)  (Reg 045 = 0x00)  (Reg 046 = 0x58)  (Reg 047 = 0x00)
(Reg 048 = 0x05)  (Reg 049 = 0x00)  (Reg 050 = 0x8d)  (Reg 051 = 0xcc)
(Reg 052 = 0x74)  (Reg 053 = 0x04)  (Reg 054 = 0x87)  (Reg 055 = 0x8c)
(Reg 056 = 0x7a)  (Reg 057 = 0x44)  (Reg 058 = 0x00)  (Reg 059 = 0x00)
(Reg 060 = 0x00)  (Reg 061 = 0x00)  (Reg 062 = 0x00)  (Reg 063 = 0x00)
(Reg 064 = 0x00)  (Reg 065 = 0x00)  (Reg 066 = 0x00)  (Reg 067 = 0x00)
(Reg 068 = 0x00)  (Reg 069 = 0x00)  (Reg 070 = 0x00)  (Reg 071 = 0x00)
(Reg 072 = 0x00)  (Reg 073 = 0x00)  (Reg 074 = 0x00)  (Reg 075 = 0x00)
(Reg 076 = 0x00)  (Reg 077 = 0x00)  (Reg 078 = 0x00)  (Reg 079 = 0x00)
(Reg 080 = 0x00)  (Reg 081 = 0x00)  (Reg 082 = 0x00)  (Reg 083 = 0x00)
(Reg 084 = 0x00)  (Reg 085 = 0x00)  (Reg 086 = 0x00)  (Reg 087 = 0x00)
```

```
(Reg 088 = 0x00)  (Reg 089 = 0x00)  (Reg 090 = 0x00)  (Reg 091 = 0x00)
(Reg 092 = 0x00)  (Reg 093 = 0x00)  (Reg 094 = 0x00)  (Reg 095 = 0x00)
(Reg 096 = 0x1e)  (Reg 097 = 0x77)  (Reg 098 = 0x00)  (Reg 099 = 0x00)
(Reg 100 = 0x44)  (Reg 101 = 0xb5)  (Reg 102 = 0x14)  (Reg 103 = 0x38)
(Reg 104 = 0x12)  (Reg 105 = 0x04)  (Reg 106 = 0x26)  (Reg 107 = 0xda)
(Reg 108 = 0x7e)  (Reg 109 = 0x32)  (Reg 110 = 0x04)  (Reg 111 = 0x00)
(Reg 112 = 0x00)  (Reg 113 = 0x00)  (Reg 114 = 0x00)  (Reg 115 = 0x00)
(Reg 116 = 0x00)  (Reg 117 = 0x00)  (Reg 118 = 0x00)  (Reg 119 = 0x00)
(Reg 120 = 0x00)  (Reg 121 = 0x00)  (Reg 122 = 0x00)  (Reg 123 = 0x00)
(Reg 124 = 0x00)  (Reg 125 = 0x00)  (Reg 126 = 0x00)  (Reg 127 = 0x01)

(Reg 128 = 0x06)  (Reg 129 = 0x18)  (Reg 130 = 0x07)  (Reg 131 = 0x40)
(Reg 132 = 0x00)  (Reg 133 = 0x00)  (Reg 134 = 0x00)  (Reg 135 = 0x40)
(Reg 136 = 0x00)  (Reg 137 = 0x00)  (Reg 138 = 0x00)  (Reg 139 = 0xb0)
(Reg 140 = 0x63)  (Reg 141 = 0x6f)  (Reg 142 = 0x0a)  (Reg 143 = 0x00)
(Reg 144 = 0x00)  (Reg 145 = 0x00)  (Reg 146 = 0x00)  (Reg 147 = 0x40)
(Reg 148 = 0x43)  (Reg 149 = 0x49)  (Reg 150 = 0x53)  (Reg 151 = 0x43)
(Reg 152 = 0x4f)  (Reg 153 = 0x2d)  (Reg 154 = 0x41)  (Reg 155 = 0x56)
(Reg 156 = 0x41)  (Reg 157 = 0x47)  (Reg 158 = 0x4f)  (Reg 159 = 0x20)
(Reg 160 = 0x20)  (Reg 161 = 0x20)  (Reg 162 = 0x20)  (Reg 163 = 0x20)
(Reg 164 = 0xf9)  (Reg 165 = 0x00)  (Reg 166 = 0x17)  (Reg 167 = 0x6a)
(Reg 168 = 0x53)  (Reg 169 = 0x46)  (Reg 170 = 0x43)  (Reg 171 = 0x54)
(Reg 172 = 0x2d)  (Reg 173 = 0x37)  (Reg 174 = 0x30)  (Reg 175 = 0x38)
(Reg 176 = 0x31)  (Reg 177 = 0x5a)  (Reg 178 = 0x2d)  (Reg 179 = 0x43)
(Reg 180 = 0x53)  (Reg 181 = 0x32)  (Reg 182 = 0x20)  (Reg 183 = 0x20)
(Reg 184 = 0x30)  (Reg 185 = 0x31)  (Reg 186 = 0x66)  (Reg 187 = 0x58)
(Reg 188 = 0x0f)  (Reg 189 = 0xa0)  (Reg 190 = 0x46)  (Reg 191 = 0x67)
(Reg 192 = 0x4b)  (Reg 193 = 0x1e)  (Reg 194 = 0x05)  (Reg 195 = 0x00)
(Reg 196 = 0x41)  (Reg 197 = 0x47)  (Reg 198 = 0x41)  (Reg 199 = 0x31)
(Reg 200 = 0x34)  (Reg 201 = 0x34)  (Reg 202 = 0x37)  (Reg 203 = 0x4e)
(Reg 204 = 0x34)  (Reg 205 = 0x4a)  (Reg 206 = 0x45)  (Reg 207 = 0x20)
(Reg 208 = 0x20)  (Reg 209 = 0x20)  (Reg 210 = 0x20)  (Reg 211 = 0x20)
(Reg 212 = 0x31)  (Reg 213 = 0x30)  (Reg 214 = 0x31)  (Reg 215 = 0x31)
(Reg 216 = 0x32)  (Reg 217 = 0x37)  (Reg 218 = 0x30)  (Reg 219 = 0x31)
(Reg 220 = 0x08)  (Reg 221 = 0x60)  (Reg 222 = 0x47)  (Reg 223 = 0xf4)
(Reg 224 = 0x00)  (Reg 225 = 0x00)  (Reg 226 = 0x06)  (Reg 227 = 0xef)
(Reg 228 = 0xfa)  (Reg 229 = 0xc9)  (Reg 230 = 0x9a)  (Reg 231 = 0x6c)
(Reg 232 = 0x5b)  (Reg 233 = 0x06)  (Reg 234 = 0x70)  (Reg 235 = 0xc5)
(Reg 236 = 0x2d)  (Reg 237 = 0xa5)  (Reg 238 = 0x7f)  (Reg 239 = 0xdf)
(Reg 240 = 0x9a)  (Reg 241 = 0x03)  (Reg 242 = 0xf6)  (Reg 243 = 0x00)
(Reg 244 = 0x00)  (Reg 245 = 0x00)  (Reg 246 = 0x00)  (Reg 247 = 0x00)
(Reg 248 = 0x00)  (Reg 249 = 0x00)  (Reg 250 = 0x00)  (Reg 251 = 0x00)
(Reg 252 = 0xf8)  (Reg 253 = 0x68)  (Reg 254 = 0x92)  (Reg 255 = 0xd1)
```

The following example shows sample output from the **show controllers TenGigE all** command for the Cisco CRS 14-Port 10-Gigabit Ethernet LAN/WAN-PHY Interface Module:

```
RP/0/RP0/CPU0:router# show controllers TenGigE 0/1/0/0 all

Thu Oct  7 18:23:49.231 EST
Operational data for interface TenGigE0/1/0/0:

State:
    Administrative state: disabled
    Operational state: Down (Reason: Link loss or low light, no loopback)
    LED state: Yellow On

Phy:
    Media type: R fiber over 1310nm optics
    Optics:
        Vendor: CISCO-SUMITOMO
        Part number: SXP3101NV-C1
        Serial number: ECL120701L2
```

```
MAC address information:
    Operational address: 0014.f294.6776
    Burnt-in address: 0014.f294.6776
    No unicast addresses in filter
    Operating in multicast promiscuous mode

Autonegotiation disabled.

Operational values:
    Speed: 10Gbps
    Duplex: Full Duplex
    Flowcontrol: None
    Loopback: None (or external)
    MTU: 1522
    MRU: 1522
    Inter-packet gap: standard (12)

Statistics for interface TenGigE0/1/0/0 (cached values):

Ingress:
    Input total bytes           = 0
    Input good bytes            = 0

    Input total packets         = 0
    Input 802.1Q frames         = 0
    Input pause frames          = 0
    Input pkts 64 bytes         = 0
    Input pkts 65-127 bytes     = 0
    Input pkts 128-255 bytes    = 0
    Input pkts 256-511 bytes    = 0
    Input pkts 512-1023 bytes   = 0
    Input pkts 1024-1518 bytes  = 0
    Input pkts 1519-Max bytes   = 0

    Input good pkts             = 0
    Input unicast pkts          = 0
    Input multicast pkts        = 0
    Input broadcast pkts        = 0

    Input drop overrun          = 0
    Input drop abort            = 0
    Input drop invalid VLAN     = 0
    Input drop invalid DMAC     = 0
    Input drop invalid encap    = 0
    Input drop other            = 0

    Input error giant           = 0
    Input error runt            = 0
    Input error jabbers         = 0
    Input error fragments       = 0
    Input error CRC             = 0
    Input error collisions      = 0
    Input error symbol          = 0
    Input error other           = 0

    Input MIB giant             = 0
    Input MIB jabber            = 0
    Input MIB CRC               = 0

Egress:
    Output total bytes          = 0
    Output good bytes           = 0

    Output total packets        = 0
```

```
    Output 802.1Q frames        = 0
    Output pkts 64 bytes        = 0
    Output pkts 65-127 bytes    = 0
    Output pkts 128-255 bytes   = 0
    Output pkts 256-511 bytes   = 0
    Output pkts 512-1023 bytes  = 0
    Output pkts 1024-1518 bytes = 0
    Output pkts 1519-Max bytes  = 0

    Output good pkts            = 0
    Output unicast pkts         = 0
    Output multicast pkts       = 0
    Output broadcast pkts       = 0

    Output drop underrun        = 0
    Output drop abort           = 0
    Output drop other           = 0

    Output error other          = 0

Management information for interface TenGigE0/1/0/0:

Port number: 0
Bay number: 0
Interface handle: 0x1180200

Config:
    Auto-negotiation: Configuration not supported (Off)
    Carrier delay (up): Not configured
    Carrier delay (down): Not configured
    Speed: Configuration not supported (10Gbps)
    Duplex: Configuration not supported (Full Duplex)
    Flow Control: Not configured (None)
    IPG: Not configured (standard (12))
    Loopback: Not configured (None)
    MTU: Not configured
    Bandwidth: Not configured --> This output field is changed
    BER-SD Threshold: Configuration not supported
    BER-SD Report: Configuration not supported
    BER-SF Threshold: Configuration not supported
    BER-SF Report: Configuration not supported
    BER-SF Signal Remote Failure: Configuration not supported

Driver constraints:
    Min MTU: 64 bytes
    Max MTU: 9600 bytes
    Max speed: 10Gbps
    Interface type: TenGigE
    Management interface: No
    Promiscuous mode: Yes
    Default carrier delay up (auto-neg on): 0 ms
    Default carrier delay down (auto-neg on): 0 ms
    Default carrier delay up (auto-neg off): 0 ms
    Default carrier delay down (auto-neg off): 0 ms
    Allowed config mask: 0x27b

Cached driver state:
    MTU: 1522 bytes
    Burnt-in MAC address: 0014.f294.6776

Operational carrier delay:
    Carrier delay (up): 0 ms
    Carrier delay (down): 0 ms
```

```
Bundle settings:
    Aggregated: No
    Bundle MTU: 1514 bytes
    Bundle MAC address: 0014.f294.6776

Port FSM state:
    Port is disabled, due to an admin down condition.
Complete FSM state:
    Admin down
    Bundle admin up
    Client admin up
    Client admin tx not disabled
    Port disabled
    Port tx disabled
    Hardware link down
IDB interface state information:
    IDB bundle admin up
    IDB client admin up
    IDB client tx admin up
    IDB error disable not set

0 Unicast MAC Addresses:

0 Multicast MAC Addresses:

0 Unicast Bundle MAC Addresses:

0 Multicast Bundle MAC Addresses:


Operational address: 0014.f294.6776
Burnt-in address: 0014.f294.6776

PLA 0 port 0  MAC enabled  Rx MAC disabled
Administrative state: Forced Remote fault
Operational state: Remote fault

0 HSRP/VRRP MAC addresses

VLAN Ethertype: 0x8100
QinQ Ethertype: 0x88a8
MTP  Ethertype: 0x88e7

4 VLAN UIDB entries
VLAN1   VLAN2      Packet Type Flags      UIDB Result Flags
   0        0          VLAN                   1 VLAN
   0        0               ARPA              1 ARPA
   0        0                    SAP          1 SAP
   0        0                                 1 SNAP


Total Power Available on PLIM for XFP's: 35000 mW
  Power used by Inserted XFP's: 33000 mW
  Power Available: 2000 mW

     Port        Power Used       State
      00          2500 mW         XFP Inserted and Powered On
      01          2500 mW         XFP Inserted and Powered On
      02          1500 mW         XFP Inserted and Powered On
      03          2500 mW         XFP Inserted and Powered On
      04          2500 mW         XFP Inserted and Powered On
      05          1500 mW         XFP Inserted and Powered On
      06          2500 mW         XFP Inserted and Powered On
      07          2500 mW         XFP Inserted and Powered On
```

```
      09          2500 mW         XFP Inserted and Powered On
      10          2500 mW         XFP Inserted and Powered On
      11          2500 mW         XFP Inserted and Powered On
      12          2500 mW         XFP Inserted and Powered On
      13          2500 mW         XFP Inserted and Powered On

802.3ae Sections
================

PMA/PMD
  Previous Alarm Status:
    PMA/PMD NOT Locked to Local Signal
  Current Alarm Status:
    PMA/PMD NOT Locked to Local Signal
    PMA/PMD Local Fault
    SR Ability
    Loopback Ability
    Rx Local Fault

PCS
  Previous Alarm Status:
    PCS Rx Link DOWN
    PCS Rx NOT Block Locked
    PCS Rx Link Status DOWN
    PCS Error'd Block Counts: 0
    PCS BER Counts: 0
    PCS has NO Block Lock
  Current Alarm Status:
    PCS Rx Link DOWN
    PCS Local Fault Detected
    PCS Rx Local Fault Detected
    PCS Rx NOT Block Locked
    PCS Rx Link Status DOWN
    PCS Error'd Block Counts: 0
    PCS BER Counts: 0
    PCS has NO Block Lock

WIS: HW In LAN Mode - No Info


XFP General Info:
=================

UDI Checking: Disabled
PHY/XFP Status: XFP Not UDI Compliant
 XFP is Working as expected


XFP Info:
=========
Max Power Dissipation: 2500 mW

XFP Type: 10GBASE-LR
Vendor Name: CISCO-SUMITOMO
Vendor Part Number: SXP3101NV-C1
Vendor OUI: 0x00-0x00-0x5f
Vendor Hardware Revision: C
Vendor Serial number: ECL120701L2
Date Code (yy/mm/dd): 08/02/27
Lot Code: D0

Cisco PID: XFP-10GLR-OC192SR
Cisco VID: V02
Cisco PN: 10-1989-02
```

```
ID: XFP
Extended ID: 0x58
  TX ref clock input is not required
  CDP is supported
  Power Level 2 (2.5W max. power)
Minimum bit rate is 9900 MBits/s.
Maximum bit rate is 10300 MBits/s.


XFP Detail Info:
================

Temp: 32.223
Tx bias: 0.0 mA
Tx power: 0.0 mW (-40 dBm)
Rx power: 0.33 mW (-24 dBm)
AUX 1: +3.3V Supply Voltage: 0x70
AUX 2: Auxiliary monitoring not implemented: 0x0

XFP Status: enabled.
 laser is enabled
 MOD NR is not ready
 is powered off
 doesn't have interrupt(s)
 has LOS
 data is ready
 TX path is ready
 TX laser is not in fault condition
 TX path CDR is locked
 RX path is not ready
 RX path CDR is not locked

Alarms:
  Low RX power alarm

Warnings:
  Low RX power warning

THRESHOLDS
                        High Alarm     Low Alarm     High Warning      Low Warng
   Temperature     C       80.0          -15.0           75.0            -10.0
   Voltage         V     000.0000        000.0000        000.0000        000.000
   Bias Current   mA     100.0000        000.0000        080.0000        000.000
   Transmit power mW     015.8480        001.2580        010.0000        001.990
   Receive power  mW     022.3870        000.1810        014.1250        000.280
DTE XGXS
  Current Alarm Status:
    XGXS Lanes All Synchronized
    XGXS Lanes Aligned
PHY XGXS
  Previous Alarm Status:
    NO XGXS Local Fault
    TX Link Down
  Current Alarm Status:
    NO XGXS Local Fault
    TX Link UP

LASI 802.3ae Registers:
=======================
Previous: LASI Status = 0x000d Rx Alarm Status = 0x0018 Tx Alarm Status = 0x0020
Current: LASI Status = 0x000c Rx Alarm Status = 0x0018 Tx Alarm Status = 0x0000

PMA/PMD 802.3ae Registers:
```

```
============================
Control = 0x2040 Status = 0x0082 Dev ID 0 = 0x0043 Dev ID 1 = 0xa400
Speed Ability = 0x0001 Devices 1 = 0x001e Devices 2 = 0x0000
Control 2 = 0x0007 Status 2 = 0xb581
Tx Disable = 0x0000 Rx Signal Detect = 0x0000
OUI 0 = 0x0000 OUI 1 = 0x0000
Current: Status = 0x0082 Status 2 = 0xb581

WIS 802.3ae Registers:
======================
Control = 0x2040 Status = 0x0082 Dev ID 0 = 0x0043 Dev ID 1 = 0xa400
Speed Ability = 0x0001 Devices 1 = 0x001e Devices 2 = 0x0000
Control 2 = 0x0000 Status 2 = 0x8003 Status 3 = 0x0048
Test Pattern Error Counter = 0x0000 Far End BLock Error Counter = 0x0000
J1 TX 1 = 0x0000 J1 TX 2 = 0x0000 J1 TX 3 = 0x0000 J1 TX 4 = 0x0000
J1 TX 5 = 0x0000 J1 TX 6 = 0x0000 J1 TX 7 = 0x0000 J1 TX 8 = 0x8900
J1 RX 1 = 0x0000 J1 RX 2 = 0x0000 J1 RX 3 = 0x0000 J1 RX 4 = 0x0000
J1 RX 5 = 0x0000 J1 RX 6 = 0x0000 J1 RX 7 = 0x0000 J1 RX 8 = 0x0000
Far End BIP Error 0 = 0x0000 Far End BIP Error 1 = 0x0000
Line BIP Error 0 = 0x0000 Line BIP Error 1 = 0x0000
Path BIP Error Count = 0x0000 Section BIP Error Count = 0x0000
J0 Tx 1 = 0x0000 J0 Tx 2 = 0x0000 J0 Tx 3 = 0x0000 J0 Tx 4 = 0x0000
J0 Tx 5 = 0x0000 J0 Tx 6 = 0x0000 J0 Tx 7 = 0x0000 J0 Tx 8 = 0x8900
J0 Rx 1 = 0x0000 J0 Rx 2 = 0x0000 J0 Rx 3 = 0x0000 J0 Rx 4 = 0x0000
J0 Rx 5 = 0x0000 J0 Rx 6 = 0x0000 J0 Rx 7 = 0x0000 J0 Rx 8 = 0x0000
Current: Status = 0x0082 Status 2 = 0x8003 Status 3 = 0x0048

PCS 802.3ae Registers:
======================
Control = 0x2040 Status = 0x0082 Dev ID 0 = 0x0043 Dev ID 1 = 0xa400
Speed Ability = 0x0001 Devices 1 = 0x001e Devices 2 = 0x0000
Control 2 = 0x0000 Status 2 = 0x8405
PKG ID 0 = 0x0000 PKG ID 1 = 0x0000
Base X Status = 0x0000 Base X Control = 0x0000
Base R Status 1 = 0x0004 Base R Status 2 = 0x0000
Base R jitter seed a0 = 0x0000 Base R jitter seed a1 = 0x0000
Base R jitter seed a2 = 0x0000 Base R jitter seed a3 = 0x0000
Base R jitter seed b0 = 0x0000 Base R jitter seed b1 = 0x0000
Base R jitter seed b2 = 0x0000 Base R jitter seed b3 = 0x0000
Base R jitter test control = 0x0000 Base R jitter test counter = 0x0000
Current: Status = 0x0082 Status 2 = 0x8405 Base R 1 = 0x0004 Base R 2 = 0x0000

PHY XS 802.3ae Registers:
=========================
Control = 0x2040 Status = 0x0006
Dev ID 0 = 0x0043 Dev ID 1 = 0xa400
Speed Ability = 0x0001 Devices 1 = 0x001e Devices 2 = 0x0000
Status 2 = 0x8000 PKG ID 0 = 0x0000 PKG ID 1 = 0x0000
Lane Status = 0x1c0f Test Control = 0x0000
Current: Status = 0x0006 Status 2 = 0x8000 Lane Status = 0x1c0f

XFP Register Info (MSA):
========================
(Reg 000 = 0x06)  (Reg 001 = 0x00)  (Reg 002 = 0x50)  (Reg 003 = 0x00)
(Reg 004 = 0xf1)  (Reg 005 = 0x00)  (Reg 006 = 0x4b)  (Reg 007 = 0x00)
(Reg 008 = 0xf6)  (Reg 009 = 0x00)  (Reg 010 = 0x00)  (Reg 011 = 0x00)
(Reg 012 = 0x00)  (Reg 013 = 0x00)  (Reg 014 = 0x00)  (Reg 015 = 0x00)
(Reg 016 = 0x00)  (Reg 017 = 0x00)  (Reg 018 = 0xc3)  (Reg 019 = 0x50)
(Reg 020 = 0x00)  (Reg 021 = 0x00)  (Reg 022 = 0x9c)  (Reg 023 = 0x40)
(Reg 024 = 0x00)  (Reg 025 = 0x00)  (Reg 026 = 0x3d)  (Reg 027 = 0xe8)
(Reg 028 = 0x04)  (Reg 029 = 0xea)  (Reg 030 = 0x27)  (Reg 031 = 0x10)
(Reg 032 = 0x07)  (Reg 033 = 0xcb)  (Reg 034 = 0x57)  (Reg 035 = 0x73)
(Reg 036 = 0x00)  (Reg 037 = 0xb5)  (Reg 038 = 0x37)  (Reg 039 = 0x2d)
(Reg 040 = 0x01)  (Reg 041 = 0x20)  (Reg 042 = 0x00)  (Reg 043 = 0x00)
```

```
(Reg 044 = 0x00)  (Reg 045 = 0x00)  (Reg 046 = 0x00)  (Reg 047 = 0x00)
(Reg 048 = 0x00)  (Reg 049 = 0x00)  (Reg 050 = 0x00)  (Reg 051 = 0x00)
(Reg 052 = 0x00)  (Reg 053 = 0x00)  (Reg 054 = 0x00)  (Reg 055 = 0x00)
(Reg 056 = 0x00)  (Reg 057 = 0x00)  (Reg 058 = 0x00)  (Reg 059 = 0x00)
(Reg 060 = 0x00)  (Reg 061 = 0x00)  (Reg 062 = 0x00)  (Reg 063 = 0x00)
(Reg 064 = 0x00)  (Reg 065 = 0x00)  (Reg 066 = 0x00)  (Reg 067 = 0x00)
(Reg 068 = 0x00)  (Reg 069 = 0x00)  (Reg 070 = 0x00)  (Reg 071 = 0x00)
(Reg 072 = 0x00)  (Reg 073 = 0x00)  (Reg 074 = 0x00)  (Reg 075 = 0x00)
(Reg 076 = 0x00)  (Reg 077 = 0x00)  (Reg 078 = 0x00)  (Reg 079 = 0x00)
(Reg 080 = 0x00)  (Reg 081 = 0x40)  (Reg 082 = 0x00)  (Reg 083 = 0x40)
(Reg 084 = 0x1e)  (Reg 085 = 0x00)  (Reg 086 = 0x00)  (Reg 087 = 0x00)
(Reg 088 = 0x00)  (Reg 089 = 0x00)  (Reg 090 = 0x00)  (Reg 091 = 0x00)
(Reg 092 = 0x00)  (Reg 093 = 0x00)  (Reg 094 = 0x00)  (Reg 095 = 0x00)
(Reg 096 = 0x20)  (Reg 097 = 0xdf)  (Reg 098 = 0x00)  (Reg 099 = 0x00)
(Reg 100 = 0x00)  (Reg 101 = 0x00)  (Reg 102 = 0x00)  (Reg 103 = 0x00)
(Reg 104 = 0x00)  (Reg 105 = 0x21)  (Reg 106 = 0x7e)  (Reg 107 = 0x44)
(Reg 108 = 0x00)  (Reg 109 = 0x00)  (Reg 110 = 0x32)  (Reg 111 = 0x18)
(Reg 112 = 0x00)  (Reg 113 = 0x00)  (Reg 114 = 0x00)  (Reg 115 = 0x00)
(Reg 116 = 0x00)  (Reg 117 = 0x00)  (Reg 118 = 0x00)  (Reg 119 = 0x00)
(Reg 120 = 0x00)  (Reg 121 = 0x00)  (Reg 122 = 0x00)  (Reg 123 = 0x00)
(Reg 124 = 0x00)  (Reg 125 = 0x00)  (Reg 126 = 0x00)  (Reg 127 = 0x01)

(Reg 128 = 0x06)  (Reg 129 = 0x58)  (Reg 130 = 0x07)  (Reg 131 = 0x40)
(Reg 132 = 0x00)  (Reg 133 = 0x00)  (Reg 134 = 0x00)  (Reg 135 = 0x40)
(Reg 136 = 0x00)  (Reg 137 = 0x00)  (Reg 138 = 0x00)  (Reg 139 = 0xb0)
(Reg 140 = 0x63)  (Reg 141 = 0x67)  (Reg 142 = 0x0a)  (Reg 143 = 0x00)
(Reg 144 = 0x00)  (Reg 145 = 0x00)  (Reg 146 = 0x00)  (Reg 147 = 0x40)
(Reg 148 = 0x43)  (Reg 149 = 0x49)  (Reg 150 = 0x53)  (Reg 151 = 0x43)
(Reg 152 = 0x4f)  (Reg 153 = 0x2d)  (Reg 154 = 0x53)  (Reg 155 = 0x55)
(Reg 156 = 0x4d)  (Reg 157 = 0x49)  (Reg 158 = 0x54)  (Reg 159 = 0x4f)
(Reg 160 = 0x4d)  (Reg 161 = 0x4f)  (Reg 162 = 0x20)  (Reg 163 = 0x20)
(Reg 164 = 0xc0)  (Reg 165 = 0x00)  (Reg 166 = 0x00)  (Reg 167 = 0x5f)
(Reg 168 = 0x53)  (Reg 169 = 0x58)  (Reg 170 = 0x50)  (Reg 171 = 0x33)
(Reg 172 = 0x31)  (Reg 173 = 0x30)  (Reg 174 = 0x31)  (Reg 175 = 0x4e)
(Reg 176 = 0x56)  (Reg 177 = 0x2d)  (Reg 178 = 0x43)  (Reg 179 = 0x31)
(Reg 180 = 0x20)  (Reg 181 = 0x20)  (Reg 182 = 0x20)  (Reg 183 = 0x20)
(Reg 184 = 0x43)  (Reg 185 = 0x20)  (Reg 186 = 0x66)  (Reg 187 = 0x58)
(Reg 188 = 0x0f)  (Reg 189 = 0xa0)  (Reg 190 = 0x46)  (Reg 191 = 0xbe)
(Reg 192 = 0x7d)  (Reg 193 = 0x96)  (Reg 194 = 0x08)  (Reg 195 = 0x00)
(Reg 196 = 0x45)  (Reg 197 = 0x43)  (Reg 198 = 0x4c)  (Reg 199 = 0x31)
(Reg 200 = 0x32)  (Reg 201 = 0x30)  (Reg 202 = 0x37)  (Reg 203 = 0x30)
(Reg 204 = 0x31)  (Reg 205 = 0x4c)  (Reg 206 = 0x32)  (Reg 207 = 0x20)
(Reg 208 = 0x20)  (Reg 209 = 0x20)  (Reg 210 = 0x20)  (Reg 211 = 0x20)
(Reg 212 = 0x30)  (Reg 213 = 0x38)  (Reg 214 = 0x30)  (Reg 215 = 0x32)
(Reg 216 = 0x32)  (Reg 217 = 0x37)  (Reg 218 = 0x44)  (Reg 219 = 0x30)
(Reg 220 = 0x08)  (Reg 221 = 0x60)  (Reg 222 = 0x70)  (Reg 223 = 0xb7)
(Reg 224 = 0x00)  (Reg 225 = 0x00)  (Reg 226 = 0x0b)  (Reg 227 = 0xd0)
(Reg 228 = 0xb4)  (Reg 229 = 0xd7)  (Reg 230 = 0x01)  (Reg 231 = 0x6d)
(Reg 232 = 0x35)  (Reg 233 = 0xbd)  (Reg 234 = 0x2c)  (Reg 235 = 0x22)
(Reg 236 = 0xe9)  (Reg 237 = 0xe2)  (Reg 238 = 0x49)  (Reg 239 = 0xc8)
(Reg 240 = 0xea)  (Reg 241 = 0x6a)  (Reg 242 = 0x2e)  (Reg 243 = 0x00)
(Reg 244 = 0x00)  (Reg 245 = 0x00)  (Reg 246 = 0x00)  (Reg 247 = 0x00)
(Reg 248 = 0x00)  (Reg 249 = 0x00)  (Reg 250 = 0x00)  (Reg 251 = 0x00)
(Reg 252 = 0xe6)  (Reg 253 = 0x39)  (Reg 254 = 0x8b)  (Reg 255 = 0x6e)
```

The following example shows sample output from the **show controllers TenGigE bert** command:

```
RP/0/RP0/CPU0:router# show controllers TenGigE 0/6/0/2 bert

BERT status for TenGigE0/6/0/2:

BERT State                      :       DISABLED
Test Pattern                    :       None test pattern
Time Remaining                  :       0
Time Interval                   :       0
```

The following example shows sample output from the **show controllers TenGigE bert** command that is unsupported on the Cisco CRS 14-Port or Cisco CRS 20-Port 10-Gigabit Ethernet LAN/WAN-PHY Interface Module:

```
RP/0/RP0/CPU0:router# show controllers TenGigE 0/1/0/0 bert
Thu Oct  7 18:26:01.108 EST
Command not supported on this interface
```

The following example shows sample output from the **show controllers TenGigE control** command for the Cisco CRS 14-Port 10-Gigabit Ethernet LAN/WAN-PHY Interface Module:

```
RP/0/RP0/CPU0:router# show controllers TenGigE 0/1/0/0 control

Thu Oct  7 18:26:11.815 EST
Management information for interface TenGigE0/1/0/0:

Port number: 0
Bay number: 0
Interface handle: 0x1180200

Config:
    Auto-negotiation: Configuration not supported (Off)
    Carrier delay (up): Not configured
    Carrier delay (down): Not configured
    Speed: Configuration not supported (10Gbps)
    Duplex: Configuration not supported (Full Duplex)
    Flow Control: Not configured (None)
    IPG: Not configured (standard (12))
    Loopback: Not configured (None)
    MTU: Not configured
    Bandwidth: Not configured
    BER-SD Threshold: Configuration not supported
    BER-SD Report: Configuration not supported
    BER-SF Threshold: Configuration not supported
    BER-SF Report: Configuration not supported
    BER-SF Signal Remote Failure: Configuration not supported

Driver constraints:
    Min MTU: 64 bytes
    Max MTU: 9600 bytes
    Max speed: 10Gbps
    Interface type: TenGigE
    Management interface: No
    Promiscuous mode: Yes
    Default carrier delay up (auto-neg on): 0 ms
    Default carrier delay down (auto-neg on): 0 ms
    Default carrier delay up (auto-neg off): 0 ms
    Default carrier delay down (auto-neg off): 0 ms
    Allowed config mask: 0x27b

Cached driver state:
    MTU: 1522 bytes
    Burnt-in MAC address: 0014.f294.6776

Operational carrier delay:
    Carrier delay (up): 0 ms
    Carrier delay (down): 0 ms

Bundle settings:
    Aggregated: No
    Bundle MTU: 1514 bytes
    Bundle MAC address: 0014.f294.6776

Port FSM state:
```

```
    Port is disabled, due to an admin down condition.
Complete FSM state:
    Admin down
    Bundle admin up
    Client admin up
    Client admin tx not disabled
    Port disabled
    Port tx disabled
    Hardware link down
IDB interface state information:
    IDB bundle admin up
    IDB client admin up
    IDB client tx admin up
    IDB error disable not set

0 Unicast MAC Addresses:

0 Multicast MAC Addresses:

0 Unicast Bundle MAC Addresses:

0 Multicast Bundle MAC Addresses:
```

The following example shows sample output from the **show controllers TenGigE internal** command for the Cisco CRS 14-Port 10-Gigabit Ethernet LAN/WAN-PHY Interface Module:

```
RP/0/RP0/CPU0:router# show controllers TenGigE 0/1/0/0 internal
Thu Oct  7 18:27:01.022 EST

Total Power Available on PLIM for XFP's: 35000 mW
  Power used by Inserted XFP's: 33000 mW
  Power Available: 2000 mW

     Port        Power Used       State
      00          2500 mW         XFP Inserted and Powered On
      01          2500 mW         XFP Inserted and Powered On
      02          1500 mW         XFP Inserted and Powered On
      03          2500 mW         XFP Inserted and Powered On
      04          2500 mW         XFP Inserted and Powered On
      05          1500 mW         XFP Inserted and Powered On
      06          2500 mW         XFP Inserted and Powered On
      07          2500 mW         XFP Inserted and Powered On
      08          2500 mW         XFP Inserted and Powered On
      09          2500 mW         XFP Inserted and Powered On
      10          2500 mW         XFP Inserted and Powered On
      11          2500 mW         XFP Inserted and Powered On
      12          2500 mW         XFP Inserted and Powered On
      13          2500 mW         XFP Inserted and Powered On
```

The following example shows sample output from the **show controllers TenGigE mac** command for the Cisco CRS 14-Port 10-Gigabit Ethernet LAN/WAN-PHY Interface Module:

```
RP/0/RP0/CPU0:router# show controllers TenGigE 0/1/0/0 mac
Thu Oct  7 18:27:34.289 EST

Operational address: 0014.f294.6776
Burnt-in address: 0014.f294.6776

PLA 0 port 0  MAC enabled  Rx MAC disabled
Administrative state: Forced Remote fault
Operational state: Remote fault

0 HSRP/VRRP MAC addresses

VLAN Ethertype: 0x8100
```

```
QinQ Ethertype: 0x88a8
MTP  Ethertype: 0x88e7

4 VLAN UIDB entries
VLAN1   VLAN2      Packet Type Flags      UIDB Result Flags
   0        0          VLAN                  1 VLAN
   0        0               ARPA             1 ARPA
   0        0                    SAP         1 SAP
   0        0                                1 SNAP
```

The following example shows sample output from the **show controllers TenGigE phy** command for the Cisco CRS 14-Port 10-Gigabit Ethernet LAN/WAN-PHY Interface Module:

```
RP/0/RP0/CPU0:router# show controllers TenGigE 0/1/0/0 phy
Thu Oct  7 18:27:51.884 EST

802.3ae Sections
================

PMA/PMD
  Previous Alarm Status:
    PMA/PMD NOT Locked to Local Signal
    PMA/PMD Local Fault
    SR Ability
    Loopback Ability
    Rx Local Fault
  Current Alarm Status:
    PMA/PMD NOT Locked to Local Signal
    PMA/PMD Local Fault
    SR Ability
    Loopback Ability
    Rx Local Fault

PCS
  Previous Alarm Status:
    PCS Rx Link DOWN
    PCS Local Fault Detected
    PCS Rx Local Fault Detected
    PCS Rx NOT Block Locked
    PCS Rx Link Status DOWN
    PCS Error'd Block Counts: 0
    PCS BER Counts: 0
    PCS has NO Block Lock
  Current Alarm Status:
    PCS Rx Link DOWN
    PCS Local Fault Detected
    PCS Rx Local Fault Detected
    PCS Rx NOT Block Locked
    PCS Rx Link Status DOWN
    PCS Error'd Block Counts: 0
    PCS BER Counts: 0
    PCS has NO Block Lock

WIS: HW In LAN Mode - No Info


XFP General Info:
=================

UDI Checking: Disabled
PHY/XFP Status: XFP Not UDI Compliant
 XFP is Working as expected
```

```
XFP Info:
=========
Max Power Dissipation: 2500 mW

XFP Type: 10GBASE-LR
Vendor Name: CISCO-SUMITOMO
Vendor Part Number: SXP3101NV-C1
Vendor OUI: 0x00-0x00-0x5f
Vendor Hardware Revision: C
Vendor Serial number: ECL120701L2
Date Code (yy/mm/dd): 08/02/27
Lot Code: D0

Cisco PID: XFP-10GLR-OC192SR
Cisco VID: V02
Cisco PN: 10-1989-02

ID: XFP
Extended ID: 0x58
  TX ref clock input is not required
  CDP is supported
  Power Level 2 (2.5W max. power)
Minimum bit rate is 9900 MBits/s.
Maximum bit rate is 10300 MBits/s.


XFP Detail Info:
================

Temp: 32.223
Tx bias: 0.0 mA
Tx power: 0.0 mW (-40 dBm)
Rx power: 0.33 mW (-24 dBm)
AUX 1: +3.3V Supply Voltage: 0x70
AUX 2: Auxiliary monitoring not implemented: 0x0

XFP Status: enabled.
 laser is enabled
 MOD NR is not ready
 is powered off
 doesn't have interrupt(s)
 has LOS
 data is ready
 TX path is ready
 TX laser is not in fault condition
 TX path CDR is locked
 RX path is not ready
 RX path CDR is not locked

Alarms:
  Low RX power alarm

Warnings:
  Low RX power warning

THRESHOLDS
                      High Alarm     Low Alarm     High Warning      Low Warng
   Temperature     C       80.0          -15.0            75.0           -10.0
   Voltage         V     000.0000        000.0000       000.0000       000.000
   Bias Current   mA     100.0000        000.0000       080.0000       000.000
   Transmit power mW     015.8480        001.2580       010.0000       001.990
   Receive power  mW     022.3870        000.1810       014.1250       000.280
```

The following example shows sample output from the **show controllers TenGigE regs** command:

```
RP/0/RP0/CPU0:router# show controllers GigabitEthernet 0/1/0/1 regs

MAC Registers for port: 1
 GE MAC CFG       (#0954): 704c5e5a
 GPCS Config      (#0147): 00000f08
 GPCS Status      (#0236): 000000ca
 GSERDES Status   (#0237): 0007fe09

RP/0/RP0/CPU0:router# show controllers GigabitEthernet 0/4/0/0 regs

MAC Registers for port: 0
 CONFIG1          (#1034): 03100a1a
 CONFIG2          (#1035): 040c2398
 CONTROL          (#1036): 00000000
 ADDRESS_LOW      (#1037): 53ffa780
 ADDRESS_HIGH     (#1038): 0000001b
 MII_MGMT_CONFIG  (#1039): 00000007
 MII_MGMT_CMD     (#1040): 00000000
 MII_MGMT_ADDRESS (#1041): 00000000
 MII_MGMT_DATA    (#1042): 40000000
 STAT_CONFIG      (#1043): 00000007
 MASK_R           (#1044): 00000000
 MASK_T           (#1045): 00000000
 COMP             (#1046): 00100d24
 MAC_CONFIG       (#1047): ffffffff
 INTERRUPT_C      (#1048): 00000000
```

The following example shows sample output from the **show controllers TenGigE regs** command for the Cisco CRS 14-Port 10-Gigabit Ethernet LAN/WAN-PHY Interface Module:

```
RP/0/RP0/CPU0:router# show controllers TenGigE 0/1/0/0 regs
Thu Oct  7 18:28:22.640 EST

LASI 802.3ae Registers:
=======================
Previous: LASI Status = 0x000c Rx Alarm Status = 0x0018 Tx Alarm Status = 0x0000
Current: LASI Status = 0x000c Rx Alarm Status = 0x0018 Tx Alarm Status = 0x0000

PMA/PMD 802.3ae Registers:
==========================
Control = 0x2040 Status = 0x0082 Dev ID 0 = 0x0043 Dev ID 1 = 0xa400
Speed Ability = 0x0001 Devices 1 = 0x001e Devices 2 = 0x0000
Control 2 = 0x0007 Status 2 = 0xb581
Tx Disable = 0x0000 Rx Signal Detect = 0x0000
OUI 0 = 0x0000 OUI 1 = 0x0000
Current: Status = 0x0082 Status 2 = 0xb581

WIS 802.3ae Registers:
======================
Control = 0x2040 Status = 0x0082 Dev ID 0 = 0x0043 Dev ID 1 = 0xa400
Speed Ability = 0x0001 Devices 1 = 0x001e Devices 2 = 0x0000
Control 2 = 0x0000 Status 2 = 0x8003 Status 3 = 0x0048
Test Pattern Error Counter = 0x0000 Far End BLock Error Counter = 0x0000
J1 TX 1 = 0x0000 J1 TX 2 = 0x0000 J1 TX 3 = 0x0000 J1 TX 4 = 0x0000
J1 TX 5 = 0x0000 J1 TX 6 = 0x0000 J1 TX 7 = 0x0000 J1 TX 8 = 0x8900
J1 RX 1 = 0x0000 J1 RX 2 = 0x0000 J1 RX 3 = 0x0000 J1 RX 4 = 0x0000
J1 RX 5 = 0x0000 J1 RX 6 = 0x0000 J1 RX 7 = 0x0000 J1 RX 8 = 0x0000
Far End BIP Error 0 = 0x0000 Far End BIP Error 1 = 0x0000
Line BIP Error 0 = 0x0000 Line BIP Error 1 = 0x0000
Path BIP Error Count = 0x0000 Section BIP Error Count = 0x0000
J0 Tx 1 = 0x0000 J0 Tx 2 = 0x0000 J0 Tx 3 = 0x0000 J0 Tx 4 = 0x0000
J0 Tx 5 = 0x0000 J0 Tx 6 = 0x0000 J0 Tx 7 = 0x0000 J0 Tx 8 = 0x8900
J0 Rx 1 = 0x0000 J0 Rx 2 = 0x0000 J0 Rx 3 = 0x0000 J0 Rx 4 = 0x0000
J0 Rx 5 = 0x0000 J0 Rx 6 = 0x0000 J0 Rx 7 = 0x0000 J0 Rx 8 = 0x0000
```

```
Current: Status = 0x0082 Status 2 = 0x8003 Status 3 = 0x0048

PCS 802.3ae Registers:
======================
Control = 0x2040 Status = 0x0082 Dev ID 0 = 0x0043 Dev ID 1 = 0xa400
Speed Ability = 0x0001 Devices 1 = 0x001e Devices 2 = 0x0000
Control 2 = 0x0000 Status 2 = 0x8405
PKG ID 0 = 0x0000 PKG ID 1 = 0x0000
Base X Status = 0x0000 Base X Control = 0x0000
Base R Status 1 = 0x0004 Base R Status 2 = 0x0000
Base R jitter seed a0 = 0x0000 Base R jitter seed a1 = 0x0000
Base R jitter seed a2 = 0x0000 Base R jitter seed a3 = 0x0000
Base R jitter seed b0 = 0x0000 Base R jitter seed b1 = 0x0000
Base R jitter seed b2 = 0x0000 Base R jitter seed b3 = 0x0000
Base R jitter test control = 0x0000 Base R jitter test counter = 0x0000
Current: Status = 0x0082 Status 2 = 0x8405 Base R 1 = 0x0004 Base R 2 = 0x0000

PHY XS 802.3ae Registers:
=========================
Control = 0x2040 Status = 0x0006
Dev ID 0 = 0x0043 Dev ID 1 = 0xa400
Speed Ability = 0x0001 Devices 1 = 0x001e Devices 2 = 0x0000
Status 2 = 0x8000 PKG ID 0 = 0x0000 PKG ID 1 = 0x0000
Lane Status = 0x1c0f Test Control = 0x0000
Current: Status = 0x0006 Status 2 = 0x8000 Lane Status = 0x1c0f

XFP Register Info (MSA):
========================
(Reg 000 = 0x06)  (Reg 001 = 0x00)  (Reg 002 = 0x50)  (Reg 003 = 0x00)
(Reg 004 = 0xf1)  (Reg 005 = 0x00)  (Reg 006 = 0x4b)  (Reg 007 = 0x00)
(Reg 008 = 0xf6)  (Reg 009 = 0x00)  (Reg 010 = 0x00)  (Reg 011 = 0x00)
(Reg 012 = 0x00)  (Reg 013 = 0x00)  (Reg 014 = 0x00)  (Reg 015 = 0x00)
(Reg 016 = 0x00)  (Reg 017 = 0x00)  (Reg 018 = 0xc3)  (Reg 019 = 0x50)
(Reg 020 = 0x00)  (Reg 021 = 0x00)  (Reg 022 = 0x9c)  (Reg 023 = 0x40)
(Reg 024 = 0x00)  (Reg 025 = 0x00)  (Reg 026 = 0x3d)  (Reg 027 = 0xe8)
(Reg 028 = 0x04)  (Reg 029 = 0xea)  (Reg 030 = 0x27)  (Reg 031 = 0x10)
(Reg 032 = 0x07)  (Reg 033 = 0xcb)  (Reg 034 = 0x57)  (Reg 035 = 0x73)
(Reg 036 = 0x00)  (Reg 037 = 0xb5)  (Reg 038 = 0x37)  (Reg 039 = 0x2d)
(Reg 040 = 0x01)  (Reg 041 = 0x20)  (Reg 042 = 0x00)  (Reg 043 = 0x00)
(Reg 044 = 0x00)  (Reg 045 = 0x00)  (Reg 046 = 0x00)  (Reg 047 = 0x00)
(Reg 048 = 0x00)  (Reg 049 = 0x00)  (Reg 050 = 0x00)  (Reg 051 = 0x00)
(Reg 052 = 0x00)  (Reg 053 = 0x00)  (Reg 054 = 0x00)  (Reg 055 = 0x00)
(Reg 056 = 0x00)  (Reg 057 = 0x00)  (Reg 058 = 0x00)  (Reg 059 = 0x00)
(Reg 060 = 0x00)  (Reg 061 = 0x00)  (Reg 062 = 0x00)  (Reg 063 = 0x00)
(Reg 064 = 0x00)  (Reg 065 = 0x00)  (Reg 066 = 0x00)  (Reg 067 = 0x00)
(Reg 068 = 0x00)  (Reg 069 = 0x00)  (Reg 070 = 0x00)  (Reg 071 = 0x00)
(Reg 072 = 0x00)  (Reg 073 = 0x00)  (Reg 074 = 0x00)  (Reg 075 = 0x00)
(Reg 076 = 0x00)  (Reg 077 = 0x00)  (Reg 078 = 0x00)  (Reg 079 = 0x00)
(Reg 080 = 0x00)  (Reg 081 = 0x40)  (Reg 082 = 0x00)  (Reg 083 = 0x40)
(Reg 084 = 0x1e)  (Reg 085 = 0x00)  (Reg 086 = 0x00)  (Reg 087 = 0x00)
(Reg 088 = 0x00)  (Reg 089 = 0x00)  (Reg 090 = 0x00)  (Reg 091 = 0x00)
(Reg 092 = 0x00)  (Reg 093 = 0x00)  (Reg 094 = 0x00)  (Reg 095 = 0x00)
(Reg 096 = 0x20)  (Reg 097 = 0xdf)  (Reg 098 = 0x00)  (Reg 099 = 0x00)
(Reg 100 = 0x00)  (Reg 101 = 0x00)  (Reg 102 = 0x00)  (Reg 103 = 0x00)
(Reg 104 = 0x00)  (Reg 105 = 0x21)  (Reg 106 = 0x7e)  (Reg 107 = 0x44)
(Reg 108 = 0x00)  (Reg 109 = 0x00)  (Reg 110 = 0x32)  (Reg 111 = 0x18)
(Reg 112 = 0x00)  (Reg 113 = 0x00)  (Reg 114 = 0x00)  (Reg 115 = 0x00)
(Reg 116 = 0x00)  (Reg 117 = 0x00)  (Reg 118 = 0x00)  (Reg 119 = 0x00)
(Reg 120 = 0x00)  (Reg 121 = 0x00)  (Reg 122 = 0x00)  (Reg 123 = 0x00)
(Reg 124 = 0x00)  (Reg 125 = 0x00)  (Reg 126 = 0x00)  (Reg 127 = 0x01)

(Reg 128 = 0x06)  (Reg 129 = 0x58)  (Reg 130 = 0x07)  (Reg 131 = 0x40)
(Reg 132 = 0x00)  (Reg 133 = 0x00)  (Reg 134 = 0x00)  (Reg 135 = 0x40)
(Reg 136 = 0x00)  (Reg 137 = 0x00)  (Reg 138 = 0x00)  (Reg 139 = 0xb0)
```

```
(Reg 140 = 0x63)  (Reg 141 = 0x67)  (Reg 142 = 0x0a)  (Reg 143 = 0x00)
(Reg 144 = 0x00)  (Reg 145 = 0x00)  (Reg 146 = 0x00)  (Reg 147 = 0x40)
(Reg 148 = 0x43)  (Reg 149 = 0x49)  (Reg 150 = 0x53)  (Reg 151 = 0x43)
(Reg 152 = 0x4f)  (Reg 153 = 0x2d)  (Reg 154 = 0x53)  (Reg 155 = 0x55)
(Reg 156 = 0x4d)  (Reg 157 = 0x49)  (Reg 158 = 0x54)  (Reg 159 = 0x4f)
(Reg 160 = 0x4d)  (Reg 161 = 0x4f)  (Reg 162 = 0x20)  (Reg 163 = 0x20)
(Reg 164 = 0xc0)  (Reg 165 = 0x00)  (Reg 166 = 0x00)  (Reg 167 = 0x5f)
(Reg 168 = 0x53)  (Reg 169 = 0x58)  (Reg 170 = 0x50)  (Reg 171 = 0x33)
(Reg 172 = 0x31)  (Reg 173 = 0x30)  (Reg 174 = 0x31)  (Reg 175 = 0x4e)
(Reg 176 = 0x56)  (Reg 177 = 0x2d)  (Reg 178 = 0x43)  (Reg 179 = 0x31)
(Reg 180 = 0x20)  (Reg 181 = 0x20)  (Reg 182 = 0x20)  (Reg 183 = 0x20)
(Reg 184 = 0x43)  (Reg 185 = 0x20)  (Reg 186 = 0x66)  (Reg 187 = 0x58)
(Reg 188 = 0x0f)  (Reg 189 = 0xa0)  (Reg 190 = 0x46)  (Reg 191 = 0xbe)
(Reg 192 = 0x7d)  (Reg 193 = 0x96)  (Reg 194 = 0x08)  (Reg 195 = 0x00)
(Reg 196 = 0x45)  (Reg 197 = 0x43)  (Reg 198 = 0x4c)  (Reg 199 = 0x31)
(Reg 200 = 0x32)  (Reg 201 = 0x30)  (Reg 202 = 0x37)  (Reg 203 = 0x30)
(Reg 204 = 0x31)  (Reg 205 = 0x4c)  (Reg 206 = 0x32)  (Reg 207 = 0x20)
(Reg 208 = 0x20)  (Reg 209 = 0x20)  (Reg 210 = 0x20)  (Reg 211 = 0x20)
(Reg 212 = 0x30)  (Reg 213 = 0x38)  (Reg 214 = 0x30)  (Reg 215 = 0x32)
(Reg 216 = 0x32)  (Reg 217 = 0x37)  (Reg 218 = 0x44)  (Reg 219 = 0x30)
(Reg 220 = 0x08)  (Reg 221 = 0x60)  (Reg 222 = 0x70)  (Reg 223 = 0xb7)
(Reg 224 = 0x00)  (Reg 225 = 0x00)  (Reg 226 = 0x0b)  (Reg 227 = 0xd0)
(Reg 228 = 0xb4)  (Reg 229 = 0xd7)  (Reg 230 = 0x01)  (Reg 231 = 0x6d)
(Reg 232 = 0x35)  (Reg 233 = 0xbd)  (Reg 234 = 0x2c)  (Reg 235 = 0x22)
(Reg 236 = 0xe9)  (Reg 237 = 0xe2)  (Reg 238 = 0x49)  (Reg 239 = 0xc8)
(Reg 240 = 0xea)  (Reg 241 = 0x6a)  (Reg 242 = 0x2e)  (Reg 243 = 0x00)
(Reg 244 = 0x00)  (Reg 245 = 0x00)  (Reg 246 = 0x00)  (Reg 247 = 0x00)
(Reg 248 = 0x00)  (Reg 249 = 0x00)  (Reg 250 = 0x00)  (Reg 251 = 0x00)
(Reg 252 = 0xe6)  (Reg 253 = 0x39)  (Reg 254 = 0x8b)  (Reg 255 = 0x6e)
```

The following example shows sample output from the **show controllers TenGigE stats** command:

```
RP/0/RP0/CPU0:router# show controllers TenGigE 0/4/0/0 stats

Statistics for interface TenGigE0/4/0/0 (cached values):

Ingress:
    Input total bytes           = 9614339316
    Input good bytes            = 9614339316

    Input total packets         = 106713557
    Input 802.1Q frames         = 0
    Input pause frames          = 0
    Input pkts 64 bytes         = 103907216
    Input pkts 65-127 bytes     = 2494185
    Input pkts 128-255 bytes    = 3410
    Input pkts 256-511 bytes    = 3406
    Input pkts 512-1023 bytes   = 2
    Input pkts 1024-1518 bytes  = 0
    Input pkts 1519-Max bytes   = 305338

    Input good pkts             = 106713557
    Input unicast pkts          = 105627141
    Input multicast pkts        = 1086414
    Input broadcast pkts        = 2

    Input drop overrun          = 0
    Input drop abort            = 0
    Input drop unknown 802.1Q   = 0
    Input drop other            = 0

    Input error giant           = 0
    Input error runt            = 0
    Input error jabbers         = 0
    Input error fragments       = 0
```

```
    Input error CRC             = 0
    Input error collisions      = 0
    Input error symbol          = 0
    Input error other           = 0

    Input MIB giant             = 305338
    Input MIB jabber            = 0
    Input MIB CRC               = 0

Egress:
    Output total bytes          = 15202682421
    Output good bytes           = 15202682421

    Output total packets        = 107534855
    Output 802.1Q frames        = 0
    Output pause frames         = 0
    Output pkts 64 bytes        = 103862713
    Output pkts 65-127 bytes    = 2448054
    Output pkts 128-255 bytes   = 308716
    Output pkts 256-511 bytes   = 6
    Output pkts 512-1023 bytes  = 13
    Output pkts 1024-1518 bytes = 0
    Output pkts 1519-Max bytes  = 915353

    Output good pkts            = 107534855
    Output unicast pkts         = 105321133
    Output multicast pkts       = 1298368
    Output broadcast pkts       = 1

    Output drop underrun        = 0
    Output drop abort           = 0
    Output drop other           = 0

    Output error other          = 0
```

The following example shows sample output from the **show controllers TenGigE stats** command for the Cisco CRS 14-Port 10-Gigabit Ethernet LAN/WAN-PHY Interface Module:

```
RP/0/RP0/CPU0:router# show controllers TenGigE 0/1/0/0 stats

Thu Oct  7 18:29:16.631 EST
Statistics for interface TenGigE0/1/0/0 (cached values):

Ingress:
    Input total bytes           = 0
    Input good bytes            = 0

    Input total packets         = 0
    Input 802.1Q frames         = 0
    Input pause frames          = 0
    Input pkts 64 bytes         = 0
    Input pkts 65-127 bytes     = 0
    Input pkts 128-255 bytes    = 0
    Input pkts 256-511 bytes    = 0
    Input pkts 512-1023 bytes   = 0
    Input pkts 1024-1518 bytes  = 0
    Input pkts 1519-Max bytes   = 0

    Input good pkts             = 0
    Input unicast pkts          = 0
    Input multicast pkts        = 0
    Input broadcast pkts        = 0

    Input drop overrun          = 0
```

```
    Input drop abort            = 0
    Input drop invalid VLAN     = 0
    Input drop invalid DMAC     = 0
    Input drop invalid encap    = 0
    Input drop other            = 0

    Input error giant           = 0
    Input error runt            = 0
    Input error jabbers         = 0
    Input error fragments       = 0
    Input error CRC             = 0
    Input error collisions      = 0
    Input error symbol          = 0
    Input error other           = 0

    Input MIB giant             = 0
    Input MIB jabber            = 0
    Input MIB CRC               = 0

Egress:
    Output total bytes          = 0
    Output good bytes           = 0

    Output total packets        = 0
    Output 802.1Q frames        = 0
    Output pause frames         = 0
    Output pkts 64 bytes        = 0
    Output pkts 65-127 bytes    = 0
    Output pkts 128-255 bytes   = 0
    Output pkts 256-511 bytes   = 0
    Output pkts 512-1023 bytes  = 0
    Output pkts 1024-1518 bytes = 0
    Output pkts 1519-Max bytes  = 0

    Output good pkts            = 0
    Output unicast pkts         = 0
    Output multicast pkts       = 0
    Output broadcast pkts       = 0

    Output drop underrun        = 0
    Output drop abort           = 0
    Output drop other           = 0

    Output error other          = 0
```

The following example shows sample output from the **show controllers TenGigE xgxs** command:

```
RP/0/RP0/CPU0:router# show controllers TenGigE 0/4/0/0 xgxs

Serdes Registers and info port: 0
  EDC Status    : 000000070 - EDC tracking
  Rx detected   : Yes
  Block lock    : Yes
  Tx aligned    : Yes
```

The following example shows sample output from the **show controllers TenGigE stats** command for the Cisco CRS 14-Port 10-Gigabit Ethernet LAN/WAN-PHY Interface Module:

```
RP/0/RP0/CPU0:router# show controllers TenGigE 0/1/0/0 xgxs

Thu Oct  7 18:30:03.732 EST
DTE XGXS
  Current Alarm Status:
    XGXS Lanes All Synchronized
    XGXS Lanes Aligned
```

```
PHY XGXS
  Previous Alarm Status:
    NO XGXS Local Fault
    TX Link UP
  Current Alarm Status:
    NO XGXS Local Fault
    TX Link UP
```

The following example shows sample output from the **show controllers HundredGigE** command for the Cisco CRS 1-Port 100-Gigabit Ethernet Interface Module:

```
RP/0/RP0/CPU0:router# show controllers HundredGigE 0/3/0/0
Tue Mar 22 06:00:35.411 UTC
Operational data for interface HundredGigE0/3/0/0:

State:
    Administrative state: enabled
    Operational state: Up
    LED state: Green On

Phy:
    Media type: fiber over 4 Lane optics
    Optics:
        Vendor: CISCO-SUMITOMO
        Part number: SXP3101NV-C1
        Serial number: ECL120701L2

MAC address information:
    Operational address: 001d.70b6.6810
    Burnt-in address: 001d.70b6.6810
    No unicast addresses in filter
    Operating in multicast promiscuous mode

Autonegotiation disabled.

Operational values:
    Speed: 100Gbps
    Duplex: Full Duplex
    Flowcontrol: None
    Loopback: None (or external)
    MTU: 9196
    MRU: 9196
    Inter-packet gap: standard (12)
```

The following example shows sample output from the **show controllers HundredGigE all** command for the Cisco CRS 1-Port 100-Gigabit Ethernet Interface Module:

```
RP/0/RP0/CPU0:router# show controllers HundredGigE 0/3/0/0 all
Tue Mar 22 06:00:57.557 UTC
Operational data for interface HundredGigE0/3/0/0:

State:
    Administrative state: enabled
    Operational state: Up
    LED state: Green On

Phy:
    Media type: fiber over 4 Lane optics
    Optics:
        Vendor: CISCO-SUMITOMO
        Part number: FTLC1181RDNS-C1
        Serial number: C22CSLA

MAC address information:
```

```
    Operational address: 001d.70b6.6810
    Burnt-in address: 001d.70b6.6810
    No unicast addresses in filter
    Operating in multicast promiscuous mode

Autonegotiation disabled.

Operational values:
    Speed: 100Gbps
    Duplex: Full Duplex
    Flowcontrol: None
    Loopback: None (or external)
    MTU: 9196
    MRU: 9196
    Inter-packet gap: standard (12)

Statistics for interface HundredGigE0/3/0/0 (cached values):

Ingress:
    Input total bytes           = 71105513310820
    Input good bytes            = 71074510205068

    Input total packets         = 7750770507
    Input 802.1Q frames         = 0
    Input pause frames          = 0
    Input pkts 64 bytes         = 895
    Input pkts 65-127 bytes     = 5118
    Input pkts 128-255 bytes    = 57
    Input pkts 256-511 bytes    = 2
    Input pkts 512-1023 bytes   = 1
    Input pkts 1024-1518 bytes  = 4
    Input pkts 1519-Max bytes   = 7750764430

    Input good pkts             = 7750770506
    Input unicast pkts          = 7750765816
    Input multicast pkts        = 4689
    Input broadcast pkts        = 1

    Input drop overrun          = 0
    Input drop abort            = 0
    Input drop invalid VLAN     = 0
    Input drop invalid DMAC     = 0
    Input drop invalid encap    = 0
    Input drop other            = 6947

    Input error giant           = 0
    Input error runt            = 0
    Input error jabbers         = 0
    Input error fragments       = 0
    Input error CRC             = 1
    Input error collisions      = 0
    Input error symbol          = 3
    Input error other           = 0

    Input MIB giant             = 0
    Input MIB jabber            = 0
    Input MIB CRC               = 0

Egress:
    Output total bytes          = 67727813126508
    Output good bytes           = 67698282738660

    Output total packets        = 7382593804
    Output 802.1Q frames        = 0
```

```
    Output pause frames         = 0
    Output pkts 64 bytes        = 702
    Output pkts 65-127 bytes    = 10272
    Output pkts 128-255 bytes   = 267
    Output pkts 256-511 bytes   = 5
    Output pkts 512-1023 bytes  = 0
    Output pkts 1024-1518 bytes = 6
    Output pkts 1519-Max bytes  = 7382582552

    Output good pkts            = 7382593804
    Output unicast pkts         = 7382590409
    Output multicast pkts       = 3391
    Output broadcast pkts       = 6

    Output drop underrun        = 0
    Output drop abort           = 2
    Output drop other           = 2373

    Output error other          = 0

Management information for interface HundredGigE0/3/0/0:

Port number: 0
Bay number: 0
Interface handle: 0x1380040

Config:
    Auto-negotiation: Configuration not supported (Off)
    Carrier delay (up): Not configured
    Carrier delay (down): Not configured
    Speed: Configuration not supported (100Gbps)
    Duplex: Configuration not supported (Full Duplex)
    Flow Control: Not configured (None)
    IPG: Configuration not supported (standard (12))
    Loopback: Not configured (None)
    MTU: 9188 bytes
    Bandwidth: Not configured
    BER-SD Threshold: Configuration not supported
    BER-SD Report: Configuration not supported
    BER-SF Threshold: Configuration not supported
    BER-SF Report: Configuration not supported
    BER-SF Signal Remote Failure: Configuration not supported

Driver constraints:
    Min MTU: 64 bytes
    Max MTU: 9600 bytes
    Max speed: 100Gbps
    Interface type: HundredGigE
    Management interface: No
    Promiscuous mode: Yes
    Default carrier delay up (auto-neg on): 0 ms
    Default carrier delay down (auto-neg on): 0 ms
    Default carrier delay up (auto-neg off): 0 ms
    Default carrier delay down (auto-neg off): 0 ms
    Allowed config mask: 0x26b

Cached driver state:
    MTU: 9196 bytes
    Burnt-in MAC address: 001d.70b6.6810

Operational carrier delay:
    Carrier delay (up): 0 ms
    Carrier delay (down): 0 ms
```

```
Bundle settings:
    Aggregated: No
    Bundle MTU: 1514 bytes
    Bundle MAC address: 001d.70b6.6810

Port FSM state:
    Port is enabled, link is up
Complete FSM state:
    Admin up
    Bundle admin up
    Client admin up
    Client admin tx not disabled
    Port enabled
    Port tx enabled
    Hardware link up
IDB interface state information:
    IDB bundle admin up
    IDB client admin up
    IDB client tx admin up
    IDB error disable not set

0 Unicast MAC Addresses:

0 Multicast MAC Addresses:

0 Unicast Bundle MAC Addresses:

0 Multicast Bundle MAC Addresses:


Operational address: 001d.70b6.6810
Burnt-in address: 001d.70b6.6810
MAC state for beluga 0 port 0

0 HSRP/VRRP MAC addresses

VLAN Ethertype: 0x8100
QinQ Ethertype: 0x88a8
MTP  Ethertype: 0x88e7

4 VLAN UIDB entries
VLAN1   VLAN2      Packet Type Flags      UIDB Result Flags
   0        0          VLAN                  1 VLAN
   0        0               ARPA             1 ARPA
   0        0                    SAP         1 SAP
   0        0                                1 SNAP

PLIM 1 Port HundredGigE Internal Information:
shmwin pointer: 0x581d4264
shmwin id     : 0x3c
shmwin initlization: complete
shmwin mac stats pointer: 0x603d3020
shmwin mac stats version: 0x1
shmwin ctx pointer: 0x603db07c
shmwin ctx version: 0x1
HW initilization: completed
Maximum CFP power class supported: 4
Maximum CFP power consumption supported: 30000 mW

802.3ba PCS
  Previous PCS Alarms:
    PCS Link had fault

  Current PCS Status:
```

```
    PCS is able to support 100GBASE-R
    PCS is Block Locked
    PCS Rx Link Status is UP
    PCS Errored Block Counts: 0
    PCS BER (Sync Header Error) Counts: 0

  PCS detailed information:

    RX Service Interface Lane Sync Header Lock Status:

    Lane-0 : Locked           Lane-10 : Locked
    Lane-1 : Locked           Lane-11 : Locked
    Lane-2 : Locked           Lane-12 : Locked
    Lane-3 : Locked           Lane-13 : Locked
    Lane-4 : Locked           Lane-14 : Locked
    Lane-5 : Locked           Lane-15 : Locked
    Lane-6 : Locked           Lane-16 : Locked
    Lane-7 : Locked           Lane-17 : Locked
    Lane-8 : Locked           Lane-18 : Locked
    Lane-9 : Locked           Lane-19 : Locked

    RX Service Interface Lane Marker Lock Status:

    Lane-0 : Locked           Lane-10 : Locked
    Lane-1 : Locked           Lane-11 : Locked
    Lane-2 : Locked           Lane-12 : Locked
    Lane-3 : Locked           Lane-13 : Locked
    Lane-4 : Locked           Lane-14 : Locked
    Lane-5 : Locked           Lane-15 : Locked
    Lane-6 : Locked           Lane-16 : Locked
    Lane-7 : Locked           Lane-17 : Locked
    Lane-8 : Locked           Lane-18 : Locked
    Lane-9 : Locked           Lane-19 : Locked

    Mapping of Service Interface Lane and RX PCS Lane:

    Rx Service Interface Lane 0 = PCS Lane 11
    Rx Service Interface Lane 1 = PCS Lane 1
    Rx Service Interface Lane 2 = PCS Lane 0
    Rx Service Interface Lane 3 = PCS Lane 12
    Rx Service Interface Lane 4 = PCS Lane 10
    Rx Service Interface Lane 5 = PCS Lane 3
    Rx Service Interface Lane 6 = PCS Lane 4
    Rx Service Interface Lane 7 = PCS Lane 14
    Rx Service Interface Lane 8 = PCS Lane 2
    Rx Service Interface Lane 9 = PCS Lane 13
    Rx Service Interface Lane 10 = PCS Lane 15
    Rx Service Interface Lane 11 = PCS Lane 7
    Rx Service Interface Lane 12 = PCS Lane 5
    Rx Service Interface Lane 13 = PCS Lane 16
    Rx Service Interface Lane 14 = PCS Lane 9
    Rx Service Interface Lane 15 = PCS Lane 6
    Rx Service Interface Lane 16 = PCS Lane 8
    Rx Service Interface Lane 17 = PCS Lane 17
    Rx Service Interface Lane 18 = PCS Lane 18
    Rx Service Interface Lane 19 = PCS Lane 19

    PCS Lane BIP Error Counters:

    Lane-0 : 0                Lane-10 : 0
    Lane-1 : 0                Lane-11 : 0
    Lane-2 : 0                Lane-12 : 0
    Lane-3 : 0                Lane-13 : 0
    Lane-4 : 0                Lane-14 : 0
```

```
    Lane-5 : 0                Lane-15 : 0
    Lane-6 : 0                Lane-16 : 0
    Lane-7 : 0                Lane-17 : 0
    Lane-8 : 0                Lane-18 : 0
    Lane-9 : 0                Lane-19 : 0

  Total PCS Lane BIP Error Count : 0
  Total PCS Lane Sync Header Error Count  : 0
  Total PCS Lane Bad 64/66 Code Count     : 3


Serdes section:
===============

None of 10 RX serial inputs detects loss of signal.
All of 10 Tx clock multiplication units are locked.
All of 10 Rx clock/data recovery units are locked.
None of 10 TX FIFO has underflow/overflow condition.
None of 10 RX FIFO has underflow/overflow condition.

CFP section:
==============

CFP General Information:

  Module Identifier:         CFP
  Ethernet Application Code: 100GBASE-LR4
  Module State:              Ready
  Power Class:               3
  Maximum Power Consumption: 23000 mW

CFP Vendor Information:

  Vendor Name:         CISCO-SUMITOMO CORP.
  Vendor PN:           FTLC1181RDNS-C1
  Vendor SN:           C22CSLA
  Vendor OUI:          0x0-0x90-0x65
  Lot Code:            00
  DATE CODE(YYYY/MM/DD): 2010/06/02
  CFP MSA Hardware Version:   1.0
  CFP MSA MDIO Version:       1.2
  Vendor Hardware Version:    1.2
  Vendor Firmware Version:    1.4

CFP UDI Information:

  UDI Compliant: Yes
  Cisco PID: CFP-100G-LR4
  Cisco VID: VES1

CFP Cisco Information:

  Vendor Name: CISCO
  Cisco PN   : 10-2549-01    Rev 01
  Cisco SN   : FNS14221PDX

CFP Detail Information:

  Number of lanes supoorted:

    Number of network lanes: 4
    Number of host lanes   : 10

  Time required by module:
```

```
    Maximum high-power-up time  :  15 s
    Maximum high-power-down time:   0 s
    Maximum tx-turn-on time     :   1 s
    Maximum tx-turn-off time    :   0 ms

  Module general control:

    Soft reset asserted     : No
    Soft low power asserted : No
    Soft tx disable asserted: No
    Soft program control 3 asserted: No
    Soft program control 2 asserted: No
    Soft program control 1 asserted: No
    Soft global alarm test asserted: No

    Tx disable pin asserted: No
    Low power pin asserted : No
    Program control 3 pin asserted: Yes
    Program control 2 pin asserted: Yes
    Program control 1 pin asserted: Yes

  Module Analog A/D value:

    Power supply voltage : 3.1939 V
    Temperature          : 38.5889 degC

  Network lane A/D value:

    Lane 0 Tx power: 1.2829 mW (  1.1 dBm)
    Lane 1 Tx power: 1.3931 mW (  1.4 dBm)
    Lane 2 Tx power: 1.4443 mW (  1.6 dBm)
    Lane 3 Tx power: 1.4791 mW (  1.7 dBm)

    Lane 0 Rx power: 1.1029 mW (  0.4 dBm)
    Lane 1 Rx power: 1.3673 mW (  1.4 dBm)
    Lane 2 Rx power: 1.3457 mW (  1.3 dBm)
    Lane 3 Rx power: 1.4423 mW (  1.6 dBm)

    Total Tx power : 5.5994 mW (  7.5 dBm)
    Total Rx power : 5.2582 mW (  7.2 dBm)

No XGXS present

PCS 802.3ba Registers:
======================
Control 1 = 0x0010
Status 1 = 0x0004
Dev ID 0 = 0x0000 Dev ID 1 = 0x0000
Speed Ability = 0x0008
Devices 1 = 0x0004 Devices 2 = 0x0000
Control 2 = 0x0005
Status 2 = 0x0020
PKG ID 0 = 0x0000 PKG ID 1 = 0x0000
Base R Status 1 = 0x1001
Base R Status 2 = 0x8000
BER high order counter = 0x0000
Errored blocks high order counter = 0x8000
Base R test pattern control = 0x0080
Base R test pattern error counter = 0x0000
Multi-lane BASE-R alignment status 1 = 0x10ff
Multi-lane BASE-R alignment status 2 = 0x0fff
Multi-lane BASE-R alignment status 3 = 0x00ff
Multi-lane BASE-R alignment status 4 = 0x0fff
```

```
BIP error counter lane 0 = 0x0000
BIP error counter lane 1 = 0x0000
BIP error counter lane 2 = 0x0000
BIP error counter lane 3 = 0x0000
BIP error counter lane 4 = 0x0000
BIP error counter lane 5 = 0x0000
BIP error counter lane 6 = 0x0000
BIP error counter lane 7 = 0x0000
BIP error counter lane 8 = 0x0000
BIP error counter lane 9 = 0x0000
BIP error counter lane 10 = 0x0000
BIP error counter lane 11 = 0x0000
BIP error counter lane 12 = 0x0000
BIP error counter lane 13 = 0x0000
BIP error counter lane 14 = 0x0000
BIP error counter lane 15 = 0x0000
BIP error counter lane 16 = 0x0000
BIP error counter lane 17 = 0x0000
BIP error counter lane 18 = 0x0000
BIP error counter lane 19 = 0x0000
Lane mapping register 0 = 0x000b
Lane mapping register 1 = 0x0001
Lane mapping register 2 = 0x0000
Lane mapping register 3 = 0x000c
Lane mapping register 4 = 0x000a
Lane mapping register 5 = 0x0003
Lane mapping register 6 = 0x0004
Lane mapping register 7 = 0x000e
Lane mapping register 8 = 0x0002
Lane mapping register 9 = 0x000d
Lane mapping register 10 = 0x000f
Lane mapping register 11 = 0x0007
Lane mapping register 12 = 0x0005
Lane mapping register 13 = 0x0010
Lane mapping register 14 = 0x0009
Lane mapping register 15 = 0x0006
Lane mapping register 16 = 0x0008
Lane mapping register 17 = 0x0011
Lane mapping register 18 = 0x0012
Lane mapping register 19 = 0x0013

Serdes registers:
==================

Chip id register: 0x8154
Chip revision id register: 0x1
Digital control 1 register register:
  serdes0:0x017a, serdes1:0x017a, serdes2:0x017a, serdes3:0x017a, serdes4:0x017a
  serdes5:0x017a, serdes6:0x017a, serdes7:0x017a, serdes8:0x017a, serdes9:0x017a
Digital control 2 register register:
  serdes0:0x0305, serdes1:0x0305, serdes2:0x0305, serdes3:0x0305, serdes4:0x0305
  serdes5:0x0305, serdes6:0x0305, serdes7:0x0305, serdes8:0x0305, serdes9:0x0305
Digital control 3 register register:
  serdes0:0x0d0f, serdes1:0x0d0f, serdes2:0x0d0f, serdes3:0x0d0f, serdes4:0x0d0f
  serdes5:0x0d0f, serdes6:0x0d0f, serdes7:0x0d0f, serdes8:0x0d0f, serdes9:0x0d0f
Digital control 5 register register:
  serdes0:0x6de0, serdes1:0x6de0, serdes2:0x6de0, serdes3:0x6de0, serdes4:0x6de0
  serdes5:0x6de0, serdes6:0x6de0, serdes7:0x6de0, serdes8:0x6de0, serdes9:0x6de0
Digital status 0 register register:
  serdes0:0x303b, serdes1:0x303b, serdes2:0x303b, serdes3:0x303b, serdes4:0x303b
  serdes5:0x303b, serdes6:0x303b, serdes7:0x303b, serdes8:0x303b, serdes9:0x303b
Line PRBS control register register:
  serdes0:0x0000, serdes1:0x0000, serdes2:0x0000, serdes3:0x0000, serdes4:0x0000
  serdes5:0x0000, serdes6:0x0000, serdes7:0x0000, serdes8:0x0000, serdes9:0x0000
```

```
Line PRBS status register register:
  serdes0:0x0000, serdes1:0x0000, serdes2:0x0000, serdes3:0x0000, serdes4:0x0000
  serdes5:0x0000, serdes6:0x0000, serdes7:0x0000, serdes8:0x0000, serdes9:0x0000
System PRBS control register register:
  serdes0:0x0000, serdes1:0x0000, serdes2:0x0000, serdes3:0x0000, serdes4:0x0000
  serdes5:0x0000, serdes6:0x0000, serdes7:0x0000, serdes8:0x0000, serdes9:0x0000
System PRBS status register register:
  serdes0:0x0000, serdes1:0x0000, serdes2:0x0000, serdes3:0x0000, serdes4:0x0000
  serdes5:0x0000, serdes6:0x0000, serdes7:0x0000, serdes8:0x0000, serdes9:0x0000
PRBS status 2 register register:
  serdes0:0x8008, serdes1:0x8008, serdes2:0x8008, serdes3:0x8008, serdes4:0x8008
  serdes5:0x8008, serdes6:0x8008, serdes7:0x8008, serdes8:0x8008, serdes9:0x8008
TX control 1 register register:
  serdes0:0x1884, serdes1:0x1884, serdes2:0x1884, serdes3:0x1884, serdes4:0x1884
  serdes5:0x1884, serdes6:0x1884, serdes7:0x1884, serdes8:0x1884, serdes9:0x1884
TX control 2 register register:
  serdes0:0x00a0, serdes1:0x00a0, serdes2:0x00a0, serdes3:0x00a0, serdes4:0x00a0
  serdes5:0x00a0, serdes6:0x00a0, serdes7:0x00a0, serdes8:0x00a0, serdes9:0x00a0
TX control 4 register register:
  serdes0:0x2412, serdes1:0x2412, serdes2:0x2412, serdes3:0x2412, serdes4:0x2412
  serdes5:0x2412, serdes6:0x2412, serdes7:0x2412, serdes8:0x2412, serdes9:0x2412
TX control 7 register register:
  serdes0:0x1077, serdes1:0x1077, serdes2:0x1077, serdes3:0x1077, serdes4:0x1077
  serdes5:0x1077, serdes6:0x1077, serdes7:0x1077, serdes8:0x1077, serdes9:0x1077
TX control 8 register register:
  serdes0:0xb800, serdes1:0xb800, serdes2:0xb800, serdes3:0xb800, serdes4:0xb800
  serdes5:0xb800, serdes6:0xb800, serdes7:0xb800, serdes8:0xb800, serdes9:0xb800
TX LVDS contrl 1 register register:
  serdes0:0x6050, serdes1:0x6050, serdes2:0x6050, serdes3:0x6050, serdes4:0x6050
  serdes5:0x6050, serdes6:0x6050, serdes7:0x6050, serdes8:0x6050, serdes9:0x6050
TX LVDS contrl 2 register register:
  serdes0:0x3bb1, serdes1:0x3ba1, serdes2:0x3ba9, serdes3:0x3ba9, serdes4:0x3bb1
  serdes5:0x3ba9, serdes6:0x3ba9, serdes7:0x3ba9, serdes8:0x3bb1, serdes9:0x3ba9
TX LVDS contrl 3 register register:
  serdes0:0x3bb1, serdes1:0x3ba1, serdes2:0x3ba9, serdes3:0x3ba9, serdes4:0x3bb1
  serdes5:0x3ba9, serdes6:0x3ba9, serdes7:0x3ba9, serdes8:0x3bb1, serdes9:0x3ba9
RX control 2 register register:
  serdes0:0x2220, serdes1:0x2220, serdes2:0x2224, serdes3:0x2224, serdes4:0x2222
  serdes5:0x2224, serdes6:0x2220, serdes7:0x2224, serdes8:0x2220, serdes9:0x2224
RX control 3 register register:
  serdes0:0x1631, serdes1:0x1631, serdes2:0x1631, serdes3:0x1631, serdes4:0x1631
  serdes5:0x1631, serdes6:0x1631, serdes7:0x1631, serdes8:0x1631, serdes9:0x1631
RX control 4 register register:
  serdes0:0x60c8, serdes1:0x40c8, serdes2:0x50c8, serdes3:0x50c8, serdes4:0x60c8
  serdes5:0x50c8, serdes6:0x50c8, serdes7:0x50c8, serdes8:0x60c8, serdes9:0x50c8
RX control 6 register register:
  serdes0:0x081a, serdes1:0x081a, serdes2:0x081a, serdes3:0x081a, serdes4:0x081a
  serdes5:0x081a, serdes6:0x081a, serdes7:0x081a, serdes8:0x081a, serdes9:0x081a
RX control 7 register register:
  serdes0:0x0000, serdes1:0x0000, serdes2:0x0000, serdes3:0x0000, serdes4:0x0000
  serdes5:0x0000, serdes6:0x0000, serdes7:0x0000, serdes8:0x0000, serdes9:0x0000
RX control 8 register register:
  serdes0:0x0000, serdes1:0x0000, serdes2:0x0000, serdes3:0x0000, serdes4:0x0000
  serdes5:0x0000, serdes6:0x0000, serdes7:0x0000, serdes8:0x0000, serdes9:0x0000
RX control 9 register register:
  serdes0:0x0000, serdes1:0x0000, serdes2:0x0000, serdes3:0x0000, serdes4:0x0000
  serdes5:0x0000, serdes6:0x0000, serdes7:0x0000, serdes8:0x0000, serdes9:0x0000
RX LVDS contrl 1 register register:
  serdes0:0x0bfa, serdes1:0x0bba, serdes2:0x0bba, serdes3:0x0bba, serdes4:0x0bba
  serdes5:0x0bba, serdes6:0x0bba, serdes7:0x0bba, serdes8:0x0bba, serdes9:0x0bba

CFP Registers:
================
```

```
NVR 1 Registers:

(Reg 0x8000=0x0e) (Reg 0x8001=0x95) (Reg 0x8002=0x01) (Reg 0x8003=0x01)
(Reg 0x8004=0x00) (Reg 0x8005=0x00) (Reg 0x8006=0x00) (Reg 0x8007=0x00)
(Reg 0x8008=0x08) (Reg 0x8009=0x4a) (Reg 0x800a=0x11) (Reg 0x800b=0x81)
(Reg 0x800c=0x34) (Reg 0x800d=0x0a) (Reg 0x800e=0x00) (Reg 0x800f=0x00)
(Reg 0x8010=0x01) (Reg 0x8011=0x04) (Reg 0x8012=0xca) (Reg 0x8013=0x45)
(Reg 0x8014=0xcc) (Reg 0x8015=0xb8) (Reg 0x8016=0x08) (Reg 0x8017=0x34)
(Reg 0x8018=0x21) (Reg 0x8019=0x44) (Reg 0x801a=0x40) (Reg 0x801b=0x70)
(Reg 0x801c=0x1c) (Reg 0x801d=0x73) (Reg 0x801e=0x64) (Reg 0x801f=0x46)
(Reg 0x8020=0x00) (Reg 0x8021=0x46) (Reg 0x8022=0x49) (Reg 0x8023=0x4e)
(Reg 0x8024=0x49) (Reg 0x8025=0x53) (Reg 0x8026=0x41) (Reg 0x8027=0x52)
(Reg 0x8028=0x20) (Reg 0x8029=0x43) (Reg 0x802a=0x4f) (Reg 0x802b=0x52)
(Reg 0x802c=0x50) (Reg 0x802d=0x2e) (Reg 0x802e=0x20) (Reg 0x802f=0x20)
(Reg 0x8030=0x20) (Reg 0x8031=0x00) (Reg 0x8032=0x90) (Reg 0x8033=0x65)
(Reg 0x8034=0x46) (Reg 0x8035=0x54) (Reg 0x8036=0x4c) (Reg 0x8037=0x43)
(Reg 0x8038=0x31) (Reg 0x8039=0x31) (Reg 0x803a=0x38) (Reg 0x803b=0x31)
(Reg 0x803c=0x52) (Reg 0x803d=0x44) (Reg 0x803e=0x4e) (Reg 0x803f=0x53)
(Reg 0x8040=0x2d) (Reg 0x8041=0x43) (Reg 0x8042=0x31) (Reg 0x8043=0x20)
(Reg 0x8044=0x43) (Reg 0x8045=0x32) (Reg 0x8046=0x32) (Reg 0x8047=0x43)
(Reg 0x8048=0x53) (Reg 0x8049=0x4c) (Reg 0x804a=0x41) (Reg 0x804b=0x20)
(Reg 0x804c=0x20) (Reg 0x804d=0x20) (Reg 0x804e=0x20) (Reg 0x804f=0x20)
(Reg 0x8050=0x20) (Reg 0x8051=0x20) (Reg 0x8052=0x20) (Reg 0x8053=0x20)
(Reg 0x8054=0x32) (Reg 0x8055=0x30) (Reg 0x8056=0x31) (Reg 0x8057=0x30)
(Reg 0x8058=0x30) (Reg 0x8059=0x36) (Reg 0x805a=0x30) (Reg 0x805b=0x32)
(Reg 0x805c=0x30) (Reg 0x805d=0x30) (Reg 0x805e=0x49) (Reg 0x805f=0x50)
(Reg 0x8060=0x55) (Reg 0x8061=0x49) (Reg 0x8062=0x42) (Reg 0x8063=0x48)
(Reg 0x8064=0x43) (Reg 0x8065=0x52) (Reg 0x8066=0x41) (Reg 0x8067=0x41)
(Reg 0x8068=0x0a) (Reg 0x8069=0x0c) (Reg 0x806a=0x01) (Reg 0x806b=0x02)
(Reg 0x806c=0x01) (Reg 0x806d=0x04) (Reg 0x806e=0x0c) (Reg 0x806f=0x03)
(Reg 0x8070=0x0f) (Reg 0x8071=0x68) (Reg 0x8072=0x0f) (Reg 0x8073=0x01)
(Reg 0x8074=0x01) (Reg 0x8075=0x00) (Reg 0x8076=0x00) (Reg 0x8077=0x00)
(Reg 0x8078=0x00) (Reg 0x8079=0x00) (Reg 0x807a=0x00) (Reg 0x807b=0x00)
(Reg 0x807c=0x00) (Reg 0x807d=0x00) (Reg 0x807e=0x00) (Reg 0x807f=0x1a)

NVR 2 Registers:

(Reg 0x8080=0x46) (Reg 0x8081=0x00) (Reg 0x8082=0x44) (Reg 0x8083=0x00)
(Reg 0x8084=0x02) (Reg 0x8085=0x00) (Reg 0x8086=0x00) (Reg 0x8087=0x00)
(Reg 0x8088=0x87) (Reg 0x8089=0x5a) (Reg 0x808a=0x86) (Reg 0x808b=0x10)
(Reg 0x808c=0x7b) (Reg 0x808d=0xc0) (Reg 0x808e=0x7a) (Reg 0x808f=0x75)
(Reg 0x8090=0x00) (Reg 0x8091=0x00) (Reg 0x8092=0x00) (Reg 0x8093=0x00)
(Reg 0x8094=0x00) (Reg 0x8095=0x00) (Reg 0x8096=0x00) (Reg 0x8097=0x00)
(Reg 0x8098=0x00) (Reg 0x8099=0x00) (Reg 0x809a=0x00) (Reg 0x809b=0x00)
(Reg 0x809c=0x00) (Reg 0x809d=0x00) (Reg 0x809e=0x00) (Reg 0x809f=0x00)
(Reg 0x80a0=0x00) (Reg 0x80a1=0x00) (Reg 0x80a2=0x00) (Reg 0x80a3=0x00)
(Reg 0x80a4=0x00) (Reg 0x80a5=0x00) (Reg 0x80a6=0x00) (Reg 0x80a7=0x00)
(Reg 0x80a8=0xea) (Reg 0x80a9=0x60) (Reg 0x80aa=0xe0) (Reg 0x80ab=0x9c)
(Reg 0x80ac=0x44) (Reg 0x80ad=0x5c) (Reg 0x80ae=0x3a) (Reg 0x80af=0x98)
(Reg 0x80b0=0x6e) (Reg 0x80b1=0x17) (Reg 0x80b2=0x62) (Reg 0x80b3=0x1e)
(Reg 0x80b4=0x10) (Reg 0x80b5=0x48) (Reg 0x80b6=0x0e) (Reg 0x80b7=0x83)
(Reg 0x80b8=0x37) (Reg 0x80b9=0x00) (Reg 0x80ba=0x35) (Reg 0x80bb=0x00)
(Reg 0x80bc=0x1b) (Reg 0x80bd=0x00) (Reg 0x80be=0x19) (Reg 0x80bf=0x00)
(Reg 0x80c0=0x6e) (Reg 0x80c1=0x17) (Reg 0x80c2=0x62) (Reg 0x80c3=0x1e)
(Reg 0x80c4=0x01) (Reg 0x80c5=0xf5) (Reg 0x80c6=0x00) (Reg 0x80c7=0xfb)
(Reg 0x80c8=0x00) (Reg 0x80c9=0x00) (Reg 0x80ca=0x00) (Reg 0x80cb=0x00)
(Reg 0x80cc=0x00) (Reg 0x80cd=0x00) (Reg 0x80ce=0x00) (Reg 0x80cf=0x00)
(Reg 0x80d0=0x00) (Reg 0x80d1=0x00) (Reg 0x80d2=0x00) (Reg 0x80d3=0x00)
(Reg 0x80d4=0x00) (Reg 0x80d5=0x00) (Reg 0x80d6=0x00) (Reg 0x80d7=0x00)
(Reg 0x80d8=0x00) (Reg 0x80d9=0x00) (Reg 0x80da=0x00) (Reg 0x80db=0x00)
(Reg 0x80dc=0x00) (Reg 0x80dd=0x00) (Reg 0x80de=0x00) (Reg 0x80df=0x00)
(Reg 0x80e0=0x00) (Reg 0x80e1=0x00) (Reg 0x80e2=0x00) (Reg 0x80e3=0x00)
(Reg 0x80e4=0x00) (Reg 0x80e5=0x00) (Reg 0x80e6=0x00) (Reg 0x80e7=0x00)
(Reg 0x80e8=0x00) (Reg 0x80e9=0x00) (Reg 0x80ea=0x00) (Reg 0x80eb=0x00)
```

```
(Reg 0x80ec=0x00) (Reg 0x80ed=0x00) (Reg 0x80ee=0x00) (Reg 0x80ef=0x00)
(Reg 0x80f0=0x00) (Reg 0x80f1=0x00) (Reg 0x80f2=0x00) (Reg 0x80f3=0x00)
(Reg 0x80f4=0x00) (Reg 0x80f5=0x00) (Reg 0x80f6=0x00) (Reg 0x80f7=0x00)
(Reg 0x80f8=0x00) (Reg 0x80f9=0x00) (Reg 0x80fa=0x00) (Reg 0x80fb=0x00)
(Reg 0x80fc=0x00) (Reg 0x80fd=0x00) (Reg 0x80fe=0x00) (Reg 0x80ff=0xe9)

NVR 3 Registers:

(Reg 0x8100=0x00) (Reg 0x8101=0x00) (Reg 0x8102=0x00) (Reg 0x8103=0x00)
(Reg 0x8104=0x00) (Reg 0x8105=0x00) (Reg 0x8106=0x00) (Reg 0x8107=0x00)
(Reg 0x8108=0x00) (Reg 0x8109=0x00) (Reg 0x810a=0x00) (Reg 0x810b=0x00)
(Reg 0x810c=0x00) (Reg 0x810d=0x00) (Reg 0x810e=0x00) (Reg 0x810f=0x00)
(Reg 0x8110=0x00) (Reg 0x8111=0x00) (Reg 0x8112=0x00) (Reg 0x8113=0x00)
(Reg 0x8114=0x00) (Reg 0x8115=0x00) (Reg 0x8116=0x00) (Reg 0x8117=0x00)
(Reg 0x8118=0x00) (Reg 0x8119=0x00) (Reg 0x811a=0x00) (Reg 0x811b=0x00)
(Reg 0x811c=0x00) (Reg 0x811d=0x00) (Reg 0x811e=0x00) (Reg 0x811f=0x00)
(Reg 0x8120=0x00) (Reg 0x8121=0x00) (Reg 0x8122=0x00) (Reg 0x8123=0x00)
(Reg 0x8124=0x00) (Reg 0x8125=0x00) (Reg 0x8126=0x00) (Reg 0x8127=0x00)
(Reg 0x8128=0x00) (Reg 0x8129=0x00) (Reg 0x812a=0x00) (Reg 0x812b=0x00)
(Reg 0x812c=0x00) (Reg 0x812d=0x00) (Reg 0x812e=0x00) (Reg 0x812f=0x00)
(Reg 0x8130=0x00) (Reg 0x8131=0x00) (Reg 0x8132=0x00) (Reg 0x8133=0x00)
(Reg 0x8134=0x00) (Reg 0x8135=0x00) (Reg 0x8136=0x00) (Reg 0x8137=0x00)
(Reg 0x8138=0x00) (Reg 0x8139=0x00) (Reg 0x813a=0x00) (Reg 0x813b=0x00)
(Reg 0x813c=0x00) (Reg 0x813d=0x00) (Reg 0x813e=0x00) (Reg 0x813f=0x00)
(Reg 0x8140=0x00) (Reg 0x8141=0x00) (Reg 0x8142=0x00) (Reg 0x8143=0x00)
(Reg 0x8144=0x00) (Reg 0x8145=0x00) (Reg 0x8146=0x00) (Reg 0x8147=0x00)
(Reg 0x8148=0x00) (Reg 0x8149=0x00) (Reg 0x814a=0x00) (Reg 0x814b=0x00)
(Reg 0x814c=0x00) (Reg 0x814d=0x00) (Reg 0x814e=0x00) (Reg 0x814f=0x00)
(Reg 0x8150=0x00) (Reg 0x8151=0x00) (Reg 0x8152=0x00) (Reg 0x8153=0x00)
(Reg 0x8154=0x00) (Reg 0x8155=0x00) (Reg 0x8156=0x00) (Reg 0x8157=0x00)
(Reg 0x8158=0x00) (Reg 0x8159=0x00) (Reg 0x815a=0x00) (Reg 0x815b=0x00)
(Reg 0x815c=0x00) (Reg 0x815d=0x00) (Reg 0x815e=0x00) (Reg 0x815f=0x00)
(Reg 0x8160=0x00) (Reg 0x8161=0x00) (Reg 0x8162=0x00) (Reg 0x8163=0x00)
(Reg 0x8164=0x00) (Reg 0x8165=0x00) (Reg 0x8166=0x00) (Reg 0x8167=0x00)
(Reg 0x8168=0x00) (Reg 0x8169=0x00) (Reg 0x816a=0x00) (Reg 0x816b=0x00)
(Reg 0x816c=0x00) (Reg 0x816d=0x00) (Reg 0x816e=0x00) (Reg 0x816f=0x00)
(Reg 0x8170=0x00) (Reg 0x8171=0x00) (Reg 0x8172=0x00) (Reg 0x8173=0x00)
(Reg 0x8174=0x00) (Reg 0x8175=0x00) (Reg 0x8176=0x00) (Reg 0x8177=0x00)
(Reg 0x8178=0x00) (Reg 0x8179=0x00) (Reg 0x817a=0x00) (Reg 0x817b=0x00)
(Reg 0x817c=0x00) (Reg 0x817d=0x00) (Reg 0x817e=0x00) (Reg 0x817f=0x00)

NVR 4 Registers:

(Reg 0x8180=0x00)

Vendor NVR1 Registers

(Reg 0x8400=0x00) (Reg 0x8401=0x00) (Reg 0x8402=0x00) (Reg 0x8403=0x00)
(Reg 0x8404=0x00) (Reg 0x8405=0x00) (Reg 0x8406=0x00) (Reg 0x8407=0x00)
(Reg 0x8408=0x00) (Reg 0x8409=0x00) (Reg 0x840a=0x00) (Reg 0x840b=0x00)
(Reg 0x840c=0x00) (Reg 0x840d=0x00) (Reg 0x840e=0x00) (Reg 0x840f=0x00)
(Reg 0x8410=0x43) (Reg 0x8411=0x49) (Reg 0x8412=0x53) (Reg 0x8413=0x43)
(Reg 0x8414=0x4f) (Reg 0x8415=0x20) (Reg 0x8416=0x20) (Reg 0x8417=0x20)
(Reg 0x8418=0x20) (Reg 0x8419=0x20) (Reg 0x841a=0x20) (Reg 0x841b=0x20)
(Reg 0x841c=0x20) (Reg 0x841d=0x20) (Reg 0x841e=0x20) (Reg 0x841f=0x20)
(Reg 0x8420=0x43) (Reg 0x8421=0x46) (Reg 0x8422=0x50) (Reg 0x8423=0x2d)
(Reg 0x8424=0x31) (Reg 0x8425=0x30) (Reg 0x8426=0x30) (Reg 0x8427=0x47)
(Reg 0x8428=0x2d) (Reg 0x8429=0x4c) (Reg 0x842a=0x52) (Reg 0x842b=0x34)
(Reg 0x842c=0x20) (Reg 0x842d=0x20) (Reg 0x842e=0x20) (Reg 0x842f=0x20)
(Reg 0x8430=0x56) (Reg 0x8431=0x45) (Reg 0x8432=0x53) (Reg 0x8433=0x31)
(Reg 0x8434=0x32) (Reg 0x8435=0x46) (Reg 0x8436=0x4e) (Reg 0x8437=0x53)
(Reg 0x8438=0x31) (Reg 0x8439=0x34) (Reg 0x843a=0x32) (Reg 0x843b=0x32)
(Reg 0x843c=0x31) (Reg 0x843d=0x50) (Reg 0x843e=0x44) (Reg 0x843f=0x58)
(Reg 0x8440=0x31) (Reg 0x8441=0x30) (Reg 0x8442=0x2d) (Reg 0x8443=0x32)
```

```
(Reg 0x8444=0x35) (Reg 0x8445=0x34) (Reg 0x8446=0x39) (Reg 0x8447=0x2d)
(Reg 0x8448=0x30) (Reg 0x8449=0x31) (Reg 0x844a=0x20) (Reg 0x844b=0x20)
(Reg 0x844c=0x30) (Reg 0x844d=0x31) (Reg 0x844e=0x20) (Reg 0x844f=0x20)
(Reg 0x8450=0x00) (Reg 0x8451=0x00) (Reg 0x8452=0x00) (Reg 0x8453=0x00)
(Reg 0x8454=0x00) (Reg 0x8455=0x00) (Reg 0x8456=0x00) (Reg 0x8457=0x00)
(Reg 0x8458=0x00) (Reg 0x8459=0x00) (Reg 0x845a=0x00) (Reg 0x845b=0x00)
(Reg 0x845c=0x00) (Reg 0x845d=0x00) (Reg 0x845e=0x00) (Reg 0x845f=0x00)
(Reg 0x8460=0x00) (Reg 0x8461=0x00) (Reg 0x8462=0x00) (Reg 0x8463=0x00)
(Reg 0x8464=0x00) (Reg 0x8465=0x00) (Reg 0x8466=0x00) (Reg 0x8467=0x00)
(Reg 0x8468=0x00) (Reg 0x8469=0x00) (Reg 0x846a=0x00) (Reg 0x846b=0x00)
(Reg 0x846c=0x00) (Reg 0x846d=0x00) (Reg 0x846e=0x00) (Reg 0x846f=0x00)
(Reg 0x8470=0x00) (Reg 0x8471=0x00) (Reg 0x8472=0x00) (Reg 0x8473=0x00)
(Reg 0x8474=0x00) (Reg 0x8475=0x00) (Reg 0x8476=0x00) (Reg 0x8477=0x00)
(Reg 0x8478=0x00) (Reg 0x8479=0x00) (Reg 0x847a=0x00) (Reg 0x847b=0x00)
(Reg 0x847c=0x00) (Reg 0x847d=0x00) (Reg 0x847e=0x00) (Reg 0x847f=0x1d)

VR 1 Registers:

(Reg 0xa000=0x0000) (Reg 0xa001=0x0000) (Reg 0xa002=0x0000) (Reg 0xa003=0x0000)
(Reg 0xa004=0x0000) (Reg 0xa005=0x0003) (Reg 0xa006=0x0002) (Reg 0xa007=0x0001)
(Reg 0xa008=0x0003) (Reg 0xa009=0x0002) (Reg 0xa00a=0x0001) (Reg 0xa00b=0x0000)
(Reg 0xa00c=0x0000) (Reg 0xa00d=0x0000) (Reg 0xa00e=0x0000) (Reg 0xa00f=0x0000)
(Reg 0xa010=0x000e) (Reg 0xa011=0x0200) (Reg 0xa012=0x0000) (Reg 0xa013=0x0000)
(Reg 0xa014=0x0000) (Reg 0xa015=0x0000) (Reg 0xa016=0x0020) (Reg 0xa017=0x0000)
(Reg 0xa018=0x0000) (Reg 0xa019=0x0000) (Reg 0xa01a=0x0000) (Reg 0xa01b=0x0000)
(Reg 0xa01c=0x0000) (Reg 0xa01d=0x0003) (Reg 0xa01e=0x0000) (Reg 0xa01f=0x0000)
(Reg 0xa020=0x0000) (Reg 0xa021=0x0000) (Reg 0xa022=0x0000) (Reg 0xa023=0x0000)
(Reg 0xa024=0x0000) (Reg 0xa025=0x0000) (Reg 0xa026=0x0000) (Reg 0xa027=0x0000)
(Reg 0xa028=0x0040) (Reg 0xa029=0x8070) (Reg 0xa02a=0x0062) (Reg 0xa02b=0x0999)
(Reg 0xa02c=0x0099) (Reg 0xa02d=0x0000) (Reg 0xa02e=0x0000) (Reg 0xa02f=0x26a6)
(Reg 0xa030=0x7cc3) (Reg 0xa031=0x0000) (Reg 0xa032=0x0000) (Reg 0xa033=0x0000)
(Reg 0xa034=0x0000) (Reg 0xa035=0x0000) (Reg 0xa036=0x0000) (Reg 0xa037=0x0000)
(Reg 0xa038=0x0000) (Reg 0xa039=0x0000) (Reg 0xa03a=0x0000)

NETWORK LANE VR 1 Registers:

(Reg 0xa200=0x0000) (Reg 0xa201=0x0000) (Reg 0xa202=0x0000) (Reg 0xa203=0x0000)
(Reg 0xa204=0x0000) (Reg 0xa205=0x0000) (Reg 0xa206=0x0000) (Reg 0xa207=0x0000)
(Reg 0xa208=0x0000) (Reg 0xa209=0x0000) (Reg 0xa20a=0x0000) (Reg 0xa20b=0x0000)
(Reg 0xa20c=0x0000) (Reg 0xa20d=0x0000) (Reg 0xa20e=0x0000) (Reg 0xa20f=0x0000)
(Reg 0xa210=0x0000) (Reg 0xa211=0x0000) (Reg 0xa212=0x0000) (Reg 0xa213=0x0000)
(Reg 0xa214=0x0000) (Reg 0xa215=0x0000) (Reg 0xa216=0x0000) (Reg 0xa217=0x0000)
(Reg 0xa218=0x0000) (Reg 0xa219=0x0000) (Reg 0xa21a=0x0000) (Reg 0xa21b=0x0000)
(Reg 0xa21c=0x0000) (Reg 0xa21d=0x0000) (Reg 0xa21e=0x0000) (Reg 0xa21f=0x0000)
(Reg 0xa220=0x0000) (Reg 0xa221=0x0000) (Reg 0xa222=0x0000) (Reg 0xa223=0x0000)
(Reg 0xa224=0x0000) (Reg 0xa225=0x0000) (Reg 0xa226=0x0000) (Reg 0xa227=0x0000)
(Reg 0xa228=0x0000) (Reg 0xa229=0x0000) (Reg 0xa22a=0x0000) (Reg 0xa22b=0x0000)
(Reg 0xa22c=0x0000) (Reg 0xa22d=0x0000) (Reg 0xa22e=0x0000) (Reg 0xa22f=0x0000)
(Reg 0xa230=0x0000) (Reg 0xa231=0x0000) (Reg 0xa232=0x0000) (Reg 0xa233=0x0000)
(Reg 0xa234=0x0000) (Reg 0xa235=0x0000) (Reg 0xa236=0x0000) (Reg 0xa237=0x0000)
(Reg 0xa238=0x0000) (Reg 0xa239=0x0000) (Reg 0xa23a=0x0000) (Reg 0xa23b=0x0000)
(Reg 0xa23c=0x0000) (Reg 0xa23d=0x0000) (Reg 0xa23e=0x0000) (Reg 0xa23f=0x0000)
(Reg 0xa240=0x9999) (Reg 0xa241=0x9999) (Reg 0xa242=0x9999) (Reg 0xa243=0x9999)
(Reg 0xa244=0x0000) (Reg 0xa245=0x0000) (Reg 0xa246=0x0000) (Reg 0xa247=0x0000)
(Reg 0xa248=0x0000) (Reg 0xa249=0x0000) (Reg 0xa24a=0x0000) (Reg 0xa24b=0x0000)
(Reg 0xa24c=0x0000) (Reg 0xa24d=0x0000) (Reg 0xa24e=0x0000) (Reg 0xa24f=0x0000)
(Reg 0xa250=0xe058) (Reg 0xa251=0xe058) (Reg 0xa252=0xe058) (Reg 0xa253=0xe058)
(Reg 0xa254=0x0000) (Reg 0xa255=0x0000) (Reg 0xa256=0x0000) (Reg 0xa257=0x0000)
(Reg 0xa258=0x0000) (Reg 0xa259=0x0000) (Reg 0xa25a=0x0000) (Reg 0xa25b=0x0000)
(Reg 0xa25c=0x0000) (Reg 0xa25d=0x0000) (Reg 0xa25e=0x0000) (Reg 0xa25f=0x0000)
(Reg 0xa260=0x0000)

NETWORK LANE VR 2 Registers:
```

```
(Reg 0xa280=0x0000) (Reg 0xa281=0x0000) (Reg 0xa282=0x0000) (Reg 0xa283=0x0000)
(Reg 0xa284=0x0000) (Reg 0xa285=0x0000) (Reg 0xa286=0x0000) (Reg 0xa287=0x0000)
(Reg 0xa288=0x0000) (Reg 0xa289=0x0000) (Reg 0xa28a=0x0000) (Reg 0xa28b=0x0000)
(Reg 0xa28c=0x0000) (Reg 0xa28d=0x0000) (Reg 0xa28e=0x0000) (Reg 0xa28f=0x0000)
(Reg 0xa290=0x0000) (Reg 0xa291=0x0000) (Reg 0xa292=0x0000) (Reg 0xa293=0x0000)
(Reg 0xa294=0x0000) (Reg 0xa295=0x0000) (Reg 0xa296=0x0000) (Reg 0xa297=0x0000)
(Reg 0xa298=0x0000) (Reg 0xa299=0x0000) (Reg 0xa29a=0x0000) (Reg 0xa29b=0x0000)
(Reg 0xa29c=0x0000) (Reg 0xa29d=0x0000) (Reg 0xa29e=0x0000) (Reg 0xa29f=0x0000)
(Reg 0xa2a0=0xb766) (Reg 0xa2a1=0x98aa) (Reg 0xa2a2=0x922b) (Reg 0xa2a3=0x882c)
(Reg 0xa2a4=0x0000) (Reg 0xa2a5=0x0000) (Reg 0xa2a6=0x0000) (Reg 0xa2a7=0x0000)
(Reg 0xa2a8=0x0000) (Reg 0xa2a9=0x0000) (Reg 0xa2aa=0x0000) (Reg 0xa2ab=0x0000)
(Reg 0xa2ac=0x0000) (Reg 0xa2ad=0x0000) (Reg 0xa2ae=0x0000) (Reg 0xa2af=0x0000)
(Reg 0xa2b0=0x3238) (Reg 0xa2b1=0x364a) (Reg 0xa2b2=0x38b5) (Reg 0xa2b3=0x39c7)
(Reg 0xa2b4=0x0000) (Reg 0xa2b5=0x0000) (Reg 0xa2b6=0x0000) (Reg 0xa2b7=0x0000)
(Reg 0xa2b8=0x0000) (Reg 0xa2b9=0x0000) (Reg 0xa2ba=0x0000) (Reg 0xa2bb=0x0000)
(Reg 0xa2bc=0x0000) (Reg 0xa2bd=0x0000) (Reg 0xa2be=0x0000) (Reg 0xa2bf=0x0000)
(Reg 0xa2c0=0x2fc0) (Reg 0xa2c1=0x2fae) (Reg 0xa2c2=0x2fc0) (Reg 0xa2c3=0x2fd1)
(Reg 0xa2c4=0x0000) (Reg 0xa2c5=0x0000) (Reg 0xa2c6=0x0000) (Reg 0xa2c7=0x0000)
(Reg 0xa2c8=0x0000) (Reg 0xa2c9=0x0000) (Reg 0xa2ca=0x0000) (Reg 0xa2cb=0x0000)
(Reg 0xa2cc=0x0000) (Reg 0xa2cd=0x0000) (Reg 0xa2ce=0x0000) (Reg 0xa2cf=0x0000)
(Reg 0xa2d0=0x2b06) (Reg 0xa2d1=0x3579) (Reg 0xa2d2=0x3462) (Reg 0xa2d3=0x3867)
(Reg 0xa2d4=0x0000) (Reg 0xa2d5=0x0000) (Reg 0xa2d6=0x0000) (Reg 0xa2d7=0x0000)
(Reg 0xa2d8=0x0000) (Reg 0xa2d9=0x0000) (Reg 0xa2da=0x0000) (Reg 0xa2db=0x0000)
(Reg 0xa2dc=0x0000) (Reg 0xa2dd=0x0000) (Reg 0xa2de=0x0000) (Reg 0xa2df=0x0000)
(Reg 0xa2e0=0x0000)

HOST LANE VR 1 Registers:

(Reg 0xa400=0x0000) (Reg 0xa401=0x0000) (Reg 0xa402=0x0000) (Reg 0xa403=0x0000)
(Reg 0xa404=0x0000) (Reg 0xa405=0x0000) (Reg 0xa406=0x0000) (Reg 0xa407=0x0000)
(Reg 0xa408=0x0000) (Reg 0xa409=0x0000) (Reg 0xa40a=0x0000) (Reg 0xa40b=0x0000)
(Reg 0xa40c=0x0000) (Reg 0xa40d=0x0000) (Reg 0xa40e=0x0000) (Reg 0xa40f=0x0000)
(Reg 0xa410=0x0000) (Reg 0xa411=0x0000) (Reg 0xa412=0x0000) (Reg 0xa413=0x0000)
(Reg 0xa414=0x0000) (Reg 0xa415=0x0000) (Reg 0xa416=0x0000) (Reg 0xa417=0x0000)
(Reg 0xa418=0x0000) (Reg 0xa419=0x0000) (Reg 0xa41a=0x0000) (Reg 0xa41b=0x0000)
(Reg 0xa41c=0x0000) (Reg 0xa41d=0x0000) (Reg 0xa41e=0x0000) (Reg 0xa41f=0x0000)
(Reg 0xa420=0x0001) (Reg 0xa421=0x0001) (Reg 0xa422=0x0001) (Reg 0xa423=0x0001)
(Reg 0xa424=0x0001) (Reg 0xa425=0x0001) (Reg 0xa426=0x0001) (Reg 0xa427=0x0001)
(Reg 0xa428=0x0001) (Reg 0xa429=0x0001) (Reg 0xa42a=0x0000) (Reg 0xa42b=0x0000)
(Reg 0xa42c=0x0000) (Reg 0xa42d=0x0000) (Reg 0xa42e=0x0000) (Reg 0xa42f=0x0000)
(Reg 0xa430=0x0000) (Reg 0xa431=0x0000) (Reg 0xa432=0x0000) (Reg 0xa433=0x0000)
(Reg 0xa434=0x0000) (Reg 0xa435=0x0000) (Reg 0xa436=0x0000) (Reg 0xa437=0x0000)
(Reg 0xa438=0x0000) (Reg 0xa439=0x0000) (Reg 0xa43a=0x0000) (Reg 0xa43b=0x0000)
(Reg 0xa43c=0x0000) (Reg 0xa43d=0x0000) (Reg 0xa43e=0x0000) (Reg 0xa43f=0x0000)
(Reg 0xa440=0x0001) (Reg 0xa441=0x0001) (Reg 0xa442=0x0001) (Reg 0xa443=0x0001)
(Reg 0xa444=0x0001) (Reg 0xa445=0x0001) (Reg 0xa446=0x0001) (Reg 0xa447=0x0001)
(Reg 0xa448=0x0001) (Reg 0xa449=0x0001) (Reg 0xa44a=0x0000) (Reg 0xa44b=0x0000)
(Reg 0xa44c=0x0000) (Reg 0xa44d=0x0000) (Reg 0xa44e=0x0000) (Reg 0xa44f=0x0000)
(Reg 0xa450=0x0000)
```

The following example shows sample output from the **show controllers HundredGigE bert** command for the Cisco CRS 1-Port 100-Gigabit Ethernet Interface Module:

```
RP/0/RP0/CPU0:router# show controllers HundredGigE 0/3/0/0 bert
Tue Mar 22 06:01:53.201 UTC
Command not supported on this interface
```

The following example shows sample output from the **show controllers HundredGigE control** command for the Cisco CRS 1-Port 100-Gigabit Ethernet Interface Module:

```
RP/0/RP0/CPU0:router# show controllers HundredGigE 0/3/0/0 control
Tue Mar 22 06:02:02.882 UTC
Management information for interface HundredGigE0/3/0/0:

Port number: 0
```

```
Bay number: 0
Interface handle: 0x1380040

Config:
    Auto-negotiation: Configuration not supported (Off)
    Carrier delay (up): Not configured
    Carrier delay (down): Not configured
    Speed: Configuration not supported (100Gbps)
    Duplex: Configuration not supported (Full Duplex)
    Flow Control: Not configured (None)
    IPG: Configuration not supported (standard (12))
    Loopback: Not configured (None)
    MTU: 9188 bytes
    Bandwidth: Not configured
    BER-SD Threshold: Configuration not supported
    BER-SD Report: Configuration not supported
    BER-SF Threshold: Configuration not supported
    BER-SF Report: Configuration not supported
    BER-SF Signal Remote Failure: Configuration not supported

Driver constraints:
    Min MTU: 64 bytes
    Max MTU: 9600 bytes
    Max speed: 100Gbps
    Interface type: HundredGigE
    Management interface: No
    Promiscuous mode: Yes
    Default carrier delay up (auto-neg on): 0 ms
    Default carrier delay down (auto-neg on): 0 ms
    Default carrier delay up (auto-neg off): 0 ms
    Default carrier delay down (auto-neg off): 0 ms
    Allowed config mask: 0x26b

Cached driver state:
    MTU: 9196 bytes
    Burnt-in MAC address: 001d.70b6.6810

Operational carrier delay:
    Carrier delay (up): 0 ms
    Carrier delay (down): 0 ms

Bundle settings:
    Aggregated: No
    Bundle MTU: 1514 bytes
    Bundle MAC address: 001d.70b6.6810

Port FSM state:
    Port is enabled, link is up
Complete FSM state:
    Admin up
    Bundle admin up
    Client admin up
    Client admin tx not disabled
    Port enabled
    Port tx enabled
    Hardware link up
IDB interface state information:
    IDB bundle admin up
    IDB client admin up
    IDB client tx admin up
    IDB error disable not set

0 Unicast MAC Addresses:
```

```
0 Multicast MAC Addresses:

0 Unicast Bundle MAC Addresses:

0 Multicast Bundle MAC Addresses:
```

The following example shows sample output from the **show controllers HundredGigE internal** command for the Cisco CRS 1-Port 100-Gigabit Ethernet Interface Module:

```
RP/0/RP0/CPU0:router# show controllers HundredGigE 0/3/0/0 internal
Tue Mar 22 06:02:47.254 UTC
PLIM 1 Port HundredGigE Internal Information:
shmwin pointer: 0x581d4264
shmwin id     : 0x3c
shmwin initlization: complete
shmwin mac stats pointer: 0x603d3020
shmwin mac stats version: 0x1
shmwin ctx pointer: 0x603db07c
shmwin ctx version: 0x1
HW initilization: completed
Maximum CFP power class supported: 4
Maximum CFP power consumption supported: 30000 mW
```

The following example shows sample output from the **show controllers HundredGigE mac** command for the Cisco CRS 1-Port 100-Gigabit Ethernet Interface Module:

```
RP/0/RP0/CPU0:router# show controllers HundredGigE 0/3/0/0 mac
Tue Mar 22 06:02:56.722 UTC

Operational address: 001d.70b6.6810
Burnt-in address: 001d.70b6.6810
MAC state for beluga 0 port 0

0 HSRP/VRRP MAC addresses

VLAN Ethertype: 0x8100
QinQ Ethertype: 0x88a8
MTP  Ethertype: 0x88e7

4 VLAN UIDB entries
VLAN1   VLAN2      Packet Type Flags      UIDB Result Flags
   0        0          VLAN                  1 VLAN
   0        0               ARPA             1 ARPA
   0        0                    SAP         1 SAP
   0        0                                1 SNAP
```

The following example shows sample output from the **show controllers HundredGigE phy** command for the Cisco CRS 1-Port 100-Gigabit Ethernet Interface Module:

```
RP/0/RP0/CPU0:router# show controllers HundredGigE 0/3/0/0 phy
Tue Mar 22 06:03:04.371 UTC

802.3ba PCS
  Previous PCS Alarms:
    None

  Current PCS Status:
    PCS is able to support 100GBASE-R
    PCS is Block Locked
    PCS Rx Link Status is UP
    PCS Errored Block Counts: 0
    PCS BER (Sync Header Error) Counts: 0

PCS detailed information:
```

```
RX Service Interface Lane Sync Header Lock Status:

  Lane-0 : Locked           Lane-10 : Locked
  Lane-1 : Locked           Lane-11 : Locked
  Lane-2 : Locked           Lane-12 : Locked
  Lane-3 : Locked           Lane-13 : Locked
  Lane-4 : Locked           Lane-14 : Locked
  Lane-5 : Locked           Lane-15 : Locked
  Lane-6 : Locked           Lane-16 : Locked
  Lane-7 : Locked           Lane-17 : Locked
  Lane-8 : Locked           Lane-18 : Locked
  Lane-9 : Locked           Lane-19 : Locked

RX Service Interface Lane Marker Lock Status:

  Lane-0 : Locked           Lane-10 : Locked
  Lane-1 : Locked           Lane-11 : Locked
  Lane-2 : Locked           Lane-12 : Locked
  Lane-3 : Locked           Lane-13 : Locked
  Lane-4 : Locked           Lane-14 : Locked
  Lane-5 : Locked           Lane-15 : Locked
  Lane-6 : Locked           Lane-16 : Locked
  Lane-7 : Locked           Lane-17 : Locked
  Lane-8 : Locked           Lane-18 : Locked
  Lane-9 : Locked           Lane-19 : Locked

Mapping of Service Interface Lane and RX PCS Lane:

  Rx Service Interface Lane 0 = PCS Lane 11
  Rx Service Interface Lane 1 = PCS Lane 1
  Rx Service Interface Lane 2 = PCS Lane 0
  Rx Service Interface Lane 3 = PCS Lane 12
  Rx Service Interface Lane 4 = PCS Lane 10
  Rx Service Interface Lane 5 = PCS Lane 3
  Rx Service Interface Lane 6 = PCS Lane 4
  Rx Service Interface Lane 7 = PCS Lane 14
  Rx Service Interface Lane 8 = PCS Lane 2
  Rx Service Interface Lane 9 = PCS Lane 13
  Rx Service Interface Lane 10 = PCS Lane 15
  Rx Service Interface Lane 11 = PCS Lane 7
  Rx Service Interface Lane 12 = PCS Lane 5
  Rx Service Interface Lane 13 = PCS Lane 16
  Rx Service Interface Lane 14 = PCS Lane 9
  Rx Service Interface Lane 15 = PCS Lane 6
  Rx Service Interface Lane 16 = PCS Lane 8
  Rx Service Interface Lane 17 = PCS Lane 17
  Rx Service Interface Lane 18 = PCS Lane 18
  Rx Service Interface Lane 19 = PCS Lane 19

PCS Lane BIP Error Counters:

  Lane-0 : 0                Lane-10 : 0
  Lane-1 : 0                Lane-11 : 0
  Lane-2 : 0                Lane-12 : 0
  Lane-3 : 0                Lane-13 : 0
  Lane-4 : 0                Lane-14 : 0
  Lane-5 : 0                Lane-15 : 0
  Lane-6 : 0                Lane-16 : 0
  Lane-7 : 0                Lane-17 : 0
  Lane-8 : 0                Lane-18 : 0
  Lane-9 : 0                Lane-19 : 0

Total PCS Lane BIP Error Count : 0
Total PCS Lane Sync Header Error Count  : 0
```

```
  Total PCS Lane Bad 64/66 Code Count     : 3


Serdes section:
===============

None of 10 RX serial inputs detects loss of signal.
All of 10 Tx clock multiplication units are locked.
All of 10 Rx clock/data recovery units are locked.
None of 10 TX FIFO has underflow/overflow condition.
None of 10 RX FIFO has underflow/overflow condition.

CFP section:
==============

CFP General Information:

  Module Identifier:         CFP
  Ethernet Application Code: 100GBASE-LR4
  Module State:              Ready
  Power Class:               3
  Maximum Power Consumption: 23000 mW

CFP Vendor Information:

  Vendor Name:         CISCO-SUMITOMO
  Vendor PN:           FTLC1181RDNS-C1
  Vendor SN:           C22CSLA
  Vendor OUI:          0x0-0x90-0x65
  Lot Code:            00
  DATE CODE(YYYY/MM/DD): 2010/06/02
  CFP MSA Hardware Version:   1.0
  CFP MSA MDIO Version:       1.2
  Vendor Hardware Version:    1.2
  Vendor Firmware Version:    1.4

CFP UDI Information:

  UDI Compliant: Yes
  Cisco PID: CFP-100G-LR4
  Cisco VID: VES1

CFP Cisco Information:

  Vendor Name: CISCO
  Cisco PN   : 10-2549-01    Rev 01
  Cisco SN   : FNS14221PDX

CFP Detail Information:

  Number of lanes supoorted:

    Number of network lanes: 4
    Number of host lanes   : 10

  Time required by module:

    Maximum high-power-up time  :  15 s
    Maximum high-power-down time:   0 s
    Maximum tx-turn-on time     :   1 s
    Maximum tx-turn-off time    :   0 ms

  Module general control:
```

```
    Soft reset asserted     : No
    Soft low power asserted : No
    Soft tx disable asserted: No
    Soft program control 3 asserted: No
    Soft program control 2 asserted: No
    Soft program control 1 asserted: No
    Soft global alarm test asserted: No

    Tx disable pin asserted: No
    Low power pin asserted : No
    Program control 3 pin asserted: Yes
    Program control 2 pin asserted: Yes
    Program control 1 pin asserted: Yes

  Module Analog A/D value:

    Power supply voltage : 3.1969 V
    Temperature          : 38.4290 degC

  Network lane A/D value:

    Lane 0 Tx power: 1.2776 mW (  1.1 dBm)
    Lane 1 Tx power: 1.3995 mW (  1.5 dBm)
    Lane 2 Tx power: 1.4517 mW (  1.6 dBm)
    Lane 3 Tx power: 1.4856 mW (  1.7 dBm)

    Lane 0 Rx power: 1.1044 mW (  0.4 dBm)
    Lane 1 Rx power: 1.3834 mW (  1.4 dBm)
    Lane 2 Rx power: 1.3426 mW (  1.3 dBm)
    Lane 3 Rx power: 1.4456 mW (  1.6 dBm)

    Total Tx power : 5.6144 mW (  7.5 dBm)
    Total Rx power : 5.2760 mW (  7.2 dBm)
```

The following example shows sample output from the **show controllers HundredGigE regs** command for the Cisco CRS 1-Port 100-Gigabit Ethernet Interface Module:

```
RP/0/RP0/CPU0:router# show controllers HundredGigE 0/3/0/0 regs
Tue Mar 22 06:03:25.597 UTC

PCS 802.3ba Registers:
======================
Control 1 = 0x0010
Status 1 = 0x0004
Dev ID 0 = 0x0000 Dev ID 1 = 0x0000
Speed Ability = 0x0008
Devices 1 = 0x0004 Devices 2 = 0x0000
Control 2 = 0x0005
Status 2 = 0x0020
PKG ID 0 = 0x0000 PKG ID 1 = 0x0000
Base R Status 1 = 0x1001
Base R Status 2 = 0x8000
BER high order counter = 0x0000
Errored blocks high order counter = 0x8000
Base R test pattern control = 0x0080
Base R test pattern error counter = 0x0000
Multi-lane BASE-R alignment status 1 = 0x10ff
Multi-lane BASE-R alignment status 2 = 0x0fff
Multi-lane BASE-R alignment status 3 = 0x00ff
Multi-lane BASE-R alignment status 4 = 0x0fff
BIP error counter lane 0 = 0x0000
BIP error counter lane 1 = 0x0000
BIP error counter lane 2 = 0x0000
BIP error counter lane 3 = 0x0000
```

```
BIP error counter lane 4 = 0x0000
BIP error counter lane 5 = 0x0000
BIP error counter lane 6 = 0x0000
BIP error counter lane 7 = 0x0000
BIP error counter lane 8 = 0x0000
BIP error counter lane 9 = 0x0000
BIP error counter lane 10 = 0x0000
BIP error counter lane 11 = 0x0000
BIP error counter lane 12 = 0x0000
BIP error counter lane 13 = 0x0000
BIP error counter lane 14 = 0x0000
BIP error counter lane 15 = 0x0000
BIP error counter lane 16 = 0x0000
BIP error counter lane 17 = 0x0000
BIP error counter lane 18 = 0x0000
BIP error counter lane 19 = 0x0000
Lane mapping register 0 = 0x000b
Lane mapping register 1 = 0x0001
Lane mapping register 2 = 0x0000
Lane mapping register 3 = 0x000c
Lane mapping register 4 = 0x000a
Lane mapping register 5 = 0x0003
Lane mapping register 6 = 0x0004
Lane mapping register 7 = 0x000e
Lane mapping register 8 = 0x0002
Lane mapping register 9 = 0x000d
Lane mapping register 10 = 0x000f
Lane mapping register 11 = 0x0007
Lane mapping register 12 = 0x0005
Lane mapping register 13 = 0x0010
Lane mapping register 14 = 0x0009
Lane mapping register 15 = 0x0006
Lane mapping register 16 = 0x0008
Lane mapping register 17 = 0x0011
Lane mapping register 18 = 0x0012
Lane mapping register 19 = 0x0013

Serdes registers:
==================

Chip id register: 0x8154
Chip revision id register: 0x1
Digital control 1 register register:
  serdes0:0x017a, serdes1:0x017a, serdes2:0x017a, serdes3:0x017a, serdes4:0x017a
  serdes5:0x017a, serdes6:0x017a, serdes7:0x017a, serdes8:0x017a, serdes9:0x017a
Digital control 2 register register:
  serdes0:0x0305, serdes1:0x0305, serdes2:0x0305, serdes3:0x0305, serdes4:0x0305
  serdes5:0x0305, serdes6:0x0305, serdes7:0x0305, serdes8:0x0305, serdes9:0x0305
Digital control 3 register register:
  serdes0:0x0d0f, serdes1:0x0d0f, serdes2:0x0d0f, serdes3:0x0d0f, serdes4:0x0d0f
  serdes5:0x0d0f, serdes6:0x0d0f, serdes7:0x0d0f, serdes8:0x0d0f, serdes9:0x0d0f
Digital control 5 register register:
  serdes0:0x6de0, serdes1:0x6de0, serdes2:0x6de0, serdes3:0x6de0, serdes4:0x6de0
  serdes5:0x6de0, serdes6:0x6de0, serdes7:0x6de0, serdes8:0x6de0, serdes9:0x6de0
Digital status 0 register register:
  serdes0:0x303b, serdes1:0x303b, serdes2:0x303b, serdes3:0x303b, serdes4:0x303b
  serdes5:0x303b, serdes6:0x303b, serdes7:0x303b, serdes8:0x303b, serdes9:0x303b
Line PRBS control register register:
  serdes0:0x0000, serdes1:0x0000, serdes2:0x0000, serdes3:0x0000, serdes4:0x0000
  serdes5:0x0000, serdes6:0x0000, serdes7:0x0000, serdes8:0x0000, serdes9:0x0000
Line PRBS status register register:
  serdes0:0x0000, serdes1:0x0000, serdes2:0x0000, serdes3:0x0000, serdes4:0x0000
  serdes5:0x0000, serdes6:0x0000, serdes7:0x0000, serdes8:0x0000, serdes9:0x0000
System PRBS control register register:
```

```
  serdes0:0x0000, serdes1:0x0000, serdes2:0x0000, serdes3:0x0000, serdes4:0x0000
  serdes5:0x0000, serdes6:0x0000, serdes7:0x0000, serdes8:0x0000, serdes9:0x0000
System PRBS status register register:
  serdes0:0x0000, serdes1:0x0000, serdes2:0x0000, serdes3:0x0000, serdes4:0x0000
  serdes5:0x0000, serdes6:0x0000, serdes7:0x0000, serdes8:0x0000, serdes9:0x0000
PRBS status 2 register register:
  serdes0:0x8008, serdes1:0x8008, serdes2:0x8008, serdes3:0x8008, serdes4:0x8008
  serdes5:0x8008, serdes6:0x8008, serdes7:0x8008, serdes8:0x8008, serdes9:0x8008
TX control 1 register register:
  serdes0:0x1884, serdes1:0x1884, serdes2:0x1884, serdes3:0x1884, serdes4:0x1884
  serdes5:0x1884, serdes6:0x1884, serdes7:0x1884, serdes8:0x1884, serdes9:0x1884
TX control 2 register register:
  serdes0:0x00a0, serdes1:0x00a0, serdes2:0x00a0, serdes3:0x00a0, serdes4:0x00a0
  serdes5:0x00a0, serdes6:0x00a0, serdes7:0x00a0, serdes8:0x00a0, serdes9:0x00a0
TX control 4 register register:
  serdes0:0x2412, serdes1:0x2412, serdes2:0x2412, serdes3:0x2412, serdes4:0x2412
  serdes5:0x2412, serdes6:0x2412, serdes7:0x2412, serdes8:0x2412, serdes9:0x2412
TX control 7 register register:
  serdes0:0x1077, serdes1:0x1077, serdes2:0x1077, serdes3:0x1077, serdes4:0x1077
  serdes5:0x1077, serdes6:0x1077, serdes7:0x1077, serdes8:0x1077, serdes9:0x1077
TX control 8 register register:
  serdes0:0xb800, serdes1:0xb800, serdes2:0xb800, serdes3:0xb800, serdes4:0xb800
  serdes5:0xb800, serdes6:0xb800, serdes7:0xb800, serdes8:0xb800, serdes9:0xb800
TX LVDS contrl 1 register register:
  serdes0:0x6050, serdes1:0x6050, serdes2:0x6050, serdes3:0x6050, serdes4:0x6050
  serdes5:0x6050, serdes6:0x6050, serdes7:0x6050, serdes8:0x6050, serdes9:0x6050
TX LVDS contrl 2 register register:
  serdes0:0x3bb1, serdes1:0x3ba1, serdes2:0x3ba9, serdes3:0x3ba9, serdes4:0x3bb1
  serdes5:0x3ba9, serdes6:0x3ba9, serdes7:0x3ba9, serdes8:0x3bb1, serdes9:0x3ba9
TX LVDS contrl 3 register register:
  serdes0:0x3bb1, serdes1:0x3ba1, serdes2:0x3ba9, serdes3:0x3ba9, serdes4:0x3bb1
  serdes5:0x3ba9, serdes6:0x3ba9, serdes7:0x3ba9, serdes8:0x3bb1, serdes9:0x3ba9
RX control 2 register register:
  serdes0:0x2220, serdes1:0x2220, serdes2:0x2224, serdes3:0x2224, serdes4:0x2222
  serdes5:0x2224, serdes6:0x2220, serdes7:0x2224, serdes8:0x2220, serdes9:0x2224
RX control 3 register register:
  serdes0:0x1631, serdes1:0x1631, serdes2:0x1631, serdes3:0x1631, serdes4:0x1631
  serdes5:0x1631, serdes6:0x1631, serdes7:0x1631, serdes8:0x1631, serdes9:0x1631
RX control 4 register register:
  serdes0:0x60c8, serdes1:0x40c8, serdes2:0x50c8, serdes3:0x50c8, serdes4:0x60c8
  serdes5:0x50c8, serdes6:0x50c8, serdes7:0x50c8, serdes8:0x60c8, serdes9:0x50c8
RX control 6 register register:
  serdes0:0x081a, serdes1:0x081a, serdes2:0x081a, serdes3:0x081a, serdes4:0x081a
  serdes5:0x081a, serdes6:0x081a, serdes7:0x081a, serdes8:0x081a, serdes9:0x081a
RX control 7 register register:
  serdes0:0x0000, serdes1:0x0000, serdes2:0x0000, serdes3:0x0000, serdes4:0x0000
  serdes5:0x0000, serdes6:0x0000, serdes7:0x0000, serdes8:0x0000, serdes9:0x0000
RX control 8 register register:
  serdes0:0x0000, serdes1:0x0000, serdes2:0x0000, serdes3:0x0000, serdes4:0x0000
  serdes5:0x0000, serdes6:0x0000, serdes7:0x0000, serdes8:0x0000, serdes9:0x0000
RX control 9 register register:
  serdes0:0x0000, serdes1:0x0000, serdes2:0x0000, serdes3:0x0000, serdes4:0x0000
  serdes5:0x0000, serdes6:0x0000, serdes7:0x0000, serdes8:0x0000, serdes9:0x0000
RX LVDS contrl 1 register register:
  serdes0:0x0bfa, serdes1:0x0bba, serdes2:0x0bba, serdes3:0x0bba, serdes4:0x0bba
  serdes5:0x0bba, serdes6:0x0bba, serdes7:0x0bba, serdes8:0x0bba, serdes9:0x0bba

CFP Registers:
==============

NVR 1 Registers:

(Reg 0x8000=0x0e) (Reg 0x8001=0x95) (Reg 0x8002=0x01) (Reg 0x8003=0x01)
(Reg 0x8004=0x00) (Reg 0x8005=0x00) (Reg 0x8006=0x00) (Reg 0x8007=0x00)
```

```
(Reg 0x8008=0x08) (Reg 0x8009=0x4a) (Reg 0x800a=0x11) (Reg 0x800b=0x81)
(Reg 0x800c=0x34) (Reg 0x800d=0x0a) (Reg 0x800e=0x00) (Reg 0x800f=0x00)
(Reg 0x8010=0x01) (Reg 0x8011=0x04) (Reg 0x8012=0xca) (Reg 0x8013=0x45)
(Reg 0x8014=0xcc) (Reg 0x8015=0xb8) (Reg 0x8016=0x08) (Reg 0x8017=0x34)
(Reg 0x8018=0x21) (Reg 0x8019=0x44) (Reg 0x801a=0x40) (Reg 0x801b=0x70)
(Reg 0x801c=0x1c) (Reg 0x801d=0x73) (Reg 0x801e=0x64) (Reg 0x801f=0x46)
(Reg 0x8020=0x00) (Reg 0x8021=0x46) (Reg 0x8022=0x49) (Reg 0x8023=0x4e)
(Reg 0x8024=0x49) (Reg 0x8025=0x53) (Reg 0x8026=0x41) (Reg 0x8027=0x52)
(Reg 0x8028=0x20) (Reg 0x8029=0x43) (Reg 0x802a=0x4f) (Reg 0x802b=0x52)
(Reg 0x802c=0x50) (Reg 0x802d=0x2e) (Reg 0x802e=0x20) (Reg 0x802f=0x20)
(Reg 0x8030=0x20) (Reg 0x8031=0x00) (Reg 0x8032=0x90) (Reg 0x8033=0x65)
(Reg 0x8034=0x46) (Reg 0x8035=0x54) (Reg 0x8036=0x4c) (Reg 0x8037=0x43)
(Reg 0x8038=0x31) (Reg 0x8039=0x31) (Reg 0x803a=0x38) (Reg 0x803b=0x31)
(Reg 0x803c=0x52) (Reg 0x803d=0x44) (Reg 0x803e=0x4e) (Reg 0x803f=0x53)
(Reg 0x8040=0x2d) (Reg 0x8041=0x43) (Reg 0x8042=0x31) (Reg 0x8043=0x20)
(Reg 0x8044=0x43) (Reg 0x8045=0x32) (Reg 0x8046=0x32) (Reg 0x8047=0x43)
(Reg 0x8048=0x53) (Reg 0x8049=0x4c) (Reg 0x804a=0x41) (Reg 0x804b=0x20)
(Reg 0x804c=0x20) (Reg 0x804d=0x20) (Reg 0x804e=0x20) (Reg 0x804f=0x20)
(Reg 0x8050=0x20) (Reg 0x8051=0x20) (Reg 0x8052=0x20) (Reg 0x8053=0x20)
(Reg 0x8054=0x32) (Reg 0x8055=0x30) (Reg 0x8056=0x31) (Reg 0x8057=0x30)
(Reg 0x8058=0x30) (Reg 0x8059=0x36) (Reg 0x805a=0x30) (Reg 0x805b=0x32)
(Reg 0x805c=0x30) (Reg 0x805d=0x30) (Reg 0x805e=0x49) (Reg 0x805f=0x50)
(Reg 0x8060=0x55) (Reg 0x8061=0x49) (Reg 0x8062=0x42) (Reg 0x8063=0x48)
(Reg 0x8064=0x43) (Reg 0x8065=0x52) (Reg 0x8066=0x41) (Reg 0x8067=0x41)
(Reg 0x8068=0x0a) (Reg 0x8069=0x0c) (Reg 0x806a=0x01) (Reg 0x806b=0x02)
(Reg 0x806c=0x01) (Reg 0x806d=0x04) (Reg 0x806e=0x0c) (Reg 0x806f=0x03)
(Reg 0x8070=0x0f) (Reg 0x8071=0x68) (Reg 0x8072=0x0f) (Reg 0x8073=0x01)
(Reg 0x8074=0x01) (Reg 0x8075=0x00) (Reg 0x8076=0x00) (Reg 0x8077=0x00)
(Reg 0x8078=0x00) (Reg 0x8079=0x00) (Reg 0x807a=0x00) (Reg 0x807b=0x00)
(Reg 0x807c=0x00) (Reg 0x807d=0x00) (Reg 0x807e=0x00) (Reg 0x807f=0x1a)

NVR 2 Registers:

(Reg 0x8080=0x46) (Reg 0x8081=0x00) (Reg 0x8082=0x44) (Reg 0x8083=0x00)
(Reg 0x8084=0x02) (Reg 0x8085=0x00) (Reg 0x8086=0x00) (Reg 0x8087=0x00)
(Reg 0x8088=0x87) (Reg 0x8089=0x5a) (Reg 0x808a=0x86) (Reg 0x808b=0x10)
(Reg 0x808c=0x7b) (Reg 0x808d=0xc0) (Reg 0x808e=0x7a) (Reg 0x808f=0x75)
(Reg 0x8090=0x00) (Reg 0x8091=0x00) (Reg 0x8092=0x00) (Reg 0x8093=0x00)
(Reg 0x8094=0x00) (Reg 0x8095=0x00) (Reg 0x8096=0x00) (Reg 0x8097=0x00)
(Reg 0x8098=0x00) (Reg 0x8099=0x00) (Reg 0x809a=0x00) (Reg 0x809b=0x00)
(Reg 0x809c=0x00) (Reg 0x809d=0x00) (Reg 0x809e=0x00) (Reg 0x809f=0x00)
(Reg 0x80a0=0x00) (Reg 0x80a1=0x00) (Reg 0x80a2=0x00) (Reg 0x80a3=0x00)
(Reg 0x80a4=0x00) (Reg 0x80a5=0x00) (Reg 0x80a6=0x00) (Reg 0x80a7=0x00)
(Reg 0x80a8=0xea) (Reg 0x80a9=0x60) (Reg 0x80aa=0xe0) (Reg 0x80ab=0x9c)
(Reg 0x80ac=0x44) (Reg 0x80ad=0x5c) (Reg 0x80ae=0x3a) (Reg 0x80af=0x98)
(Reg 0x80b0=0x6e) (Reg 0x80b1=0x17) (Reg 0x80b2=0x62) (Reg 0x80b3=0x1e)
(Reg 0x80b4=0x10) (Reg 0x80b5=0x48) (Reg 0x80b6=0x0e) (Reg 0x80b7=0x83)
(Reg 0x80b8=0x37) (Reg 0x80b9=0x00) (Reg 0x80ba=0x35) (Reg 0x80bb=0x00)
(Reg 0x80bc=0x1b) (Reg 0x80bd=0x00) (Reg 0x80be=0x19) (Reg 0x80bf=0x00)
(Reg 0x80c0=0x6e) (Reg 0x80c1=0x17) (Reg 0x80c2=0x62) (Reg 0x80c3=0x1e)
(Reg 0x80c4=0x01) (Reg 0x80c5=0xf5) (Reg 0x80c6=0x00) (Reg 0x80c7=0xfb)
(Reg 0x80c8=0x00) (Reg 0x80c9=0x00) (Reg 0x80ca=0x00) (Reg 0x80cb=0x00)
(Reg 0x80cc=0x00) (Reg 0x80cd=0x00) (Reg 0x80ce=0x00) (Reg 0x80cf=0x00)
(Reg 0x80d0=0x00) (Reg 0x80d1=0x00) (Reg 0x80d2=0x00) (Reg 0x80d3=0x00)
(Reg 0x80d4=0x00) (Reg 0x80d5=0x00) (Reg 0x80d6=0x00) (Reg 0x80d7=0x00)
(Reg 0x80d8=0x00) (Reg 0x80d9=0x00) (Reg 0x80da=0x00) (Reg 0x80db=0x00)
(Reg 0x80dc=0x00) (Reg 0x80dd=0x00) (Reg 0x80de=0x00) (Reg 0x80df=0x00)
(Reg 0x80e0=0x00) (Reg 0x80e1=0x00) (Reg 0x80e2=0x00) (Reg 0x80e3=0x00)
(Reg 0x80e4=0x00) (Reg 0x80e5=0x00) (Reg 0x80e6=0x00) (Reg 0x80e7=0x00)
(Reg 0x80e8=0x00) (Reg 0x80e9=0x00) (Reg 0x80ea=0x00) (Reg 0x80eb=0x00)
(Reg 0x80ec=0x00) (Reg 0x80ed=0x00) (Reg 0x80ee=0x00) (Reg 0x80ef=0x00)
(Reg 0x80f0=0x00) (Reg 0x80f1=0x00) (Reg 0x80f2=0x00) (Reg 0x80f3=0x00)
(Reg 0x80f4=0x00) (Reg 0x80f5=0x00) (Reg 0x80f6=0x00) (Reg 0x80f7=0x00)
(Reg 0x80f8=0x00) (Reg 0x80f9=0x00) (Reg 0x80fa=0x00) (Reg 0x80fb=0x00)
```

```
(Reg 0x80fc=0x00) (Reg 0x80fd=0x00) (Reg 0x80fe=0x00) (Reg 0x80ff=0xe9)

NVR 3 Registers:

(Reg 0x8100=0x00) (Reg 0x8101=0x00) (Reg 0x8102=0x00) (Reg 0x8103=0x00)
(Reg 0x8104=0x00) (Reg 0x8105=0x00) (Reg 0x8106=0x00) (Reg 0x8107=0x00)
(Reg 0x8108=0x00) (Reg 0x8109=0x00) (Reg 0x810a=0x00) (Reg 0x810b=0x00)
(Reg 0x810c=0x00) (Reg 0x810d=0x00) (Reg 0x810e=0x00) (Reg 0x810f=0x00)
(Reg 0x8110=0x00) (Reg 0x8111=0x00) (Reg 0x8112=0x00) (Reg 0x8113=0x00)
(Reg 0x8114=0x00) (Reg 0x8115=0x00) (Reg 0x8116=0x00) (Reg 0x8117=0x00)
(Reg 0x8118=0x00) (Reg 0x8119=0x00) (Reg 0x811a=0x00) (Reg 0x811b=0x00)
(Reg 0x811c=0x00) (Reg 0x811d=0x00) (Reg 0x811e=0x00) (Reg 0x811f=0x00)
(Reg 0x8120=0x00) (Reg 0x8121=0x00) (Reg 0x8122=0x00) (Reg 0x8123=0x00)
(Reg 0x8124=0x00) (Reg 0x8125=0x00) (Reg 0x8126=0x00) (Reg 0x8127=0x00)
(Reg 0x8128=0x00) (Reg 0x8129=0x00) (Reg 0x812a=0x00) (Reg 0x812b=0x00)
(Reg 0x812c=0x00) (Reg 0x812d=0x00) (Reg 0x812e=0x00) (Reg 0x812f=0x00)
(Reg 0x8130=0x00) (Reg 0x8131=0x00) (Reg 0x8132=0x00) (Reg 0x8133=0x00)
(Reg 0x8134=0x00) (Reg 0x8135=0x00) (Reg 0x8136=0x00) (Reg 0x8137=0x00)
(Reg 0x8138=0x00) (Reg 0x8139=0x00) (Reg 0x813a=0x00) (Reg 0x813b=0x00)
(Reg 0x813c=0x00) (Reg 0x813d=0x00) (Reg 0x813e=0x00) (Reg 0x813f=0x00)
(Reg 0x8140=0x00) (Reg 0x8141=0x00) (Reg 0x8142=0x00) (Reg 0x8143=0x00)
(Reg 0x8144=0x00) (Reg 0x8145=0x00) (Reg 0x8146=0x00) (Reg 0x8147=0x00)
(Reg 0x8148=0x00) (Reg 0x8149=0x00) (Reg 0x814a=0x00) (Reg 0x814b=0x00)
(Reg 0x814c=0x00) (Reg 0x814d=0x00) (Reg 0x814e=0x00) (Reg 0x814f=0x00)
(Reg 0x8150=0x00) (Reg 0x8151=0x00) (Reg 0x8152=0x00) (Reg 0x8153=0x00)
(Reg 0x8154=0x00) (Reg 0x8155=0x00) (Reg 0x8156=0x00) (Reg 0x8157=0x00)
(Reg 0x8158=0x00) (Reg 0x8159=0x00) (Reg 0x815a=0x00) (Reg 0x815b=0x00)
(Reg 0x815c=0x00) (Reg 0x815d=0x00) (Reg 0x815e=0x00) (Reg 0x815f=0x00)
(Reg 0x8160=0x00) (Reg 0x8161=0x00) (Reg 0x8162=0x00) (Reg 0x8163=0x00)
(Reg 0x8164=0x00) (Reg 0x8165=0x00) (Reg 0x8166=0x00) (Reg 0x8167=0x00)
(Reg 0x8168=0x00) (Reg 0x8169=0x00) (Reg 0x816a=0x00) (Reg 0x816b=0x00)
(Reg 0x816c=0x00) (Reg 0x816d=0x00) (Reg 0x816e=0x00) (Reg 0x816f=0x00)
(Reg 0x8170=0x00) (Reg 0x8171=0x00) (Reg 0x8172=0x00) (Reg 0x8173=0x00)
(Reg 0x8174=0x00) (Reg 0x8175=0x00) (Reg 0x8176=0x00) (Reg 0x8177=0x00)
(Reg 0x8178=0x00) (Reg 0x8179=0x00) (Reg 0x817a=0x00) (Reg 0x817b=0x00)
(Reg 0x817c=0x00) (Reg 0x817d=0x00) (Reg 0x817e=0x00) (Reg 0x817f=0x00)

NVR 4 Registers:

(Reg 0x8180=0x00)

Vendor NVR1 Registers

(Reg 0x8400=0x00) (Reg 0x8401=0x00) (Reg 0x8402=0x00) (Reg 0x8403=0x00)
(Reg 0x8404=0x00) (Reg 0x8405=0x00) (Reg 0x8406=0x00) (Reg 0x8407=0x00)
(Reg 0x8408=0x00) (Reg 0x8409=0x00) (Reg 0x840a=0x00) (Reg 0x840b=0x00)
(Reg 0x840c=0x00) (Reg 0x840d=0x00) (Reg 0x840e=0x00) (Reg 0x840f=0x00)
(Reg 0x8410=0x43) (Reg 0x8411=0x49) (Reg 0x8412=0x53) (Reg 0x8413=0x43)
(Reg 0x8414=0x4f) (Reg 0x8415=0x20) (Reg 0x8416=0x20) (Reg 0x8417=0x20)
(Reg 0x8418=0x20) (Reg 0x8419=0x20) (Reg 0x841a=0x20) (Reg 0x841b=0x20)
(Reg 0x841c=0x20) (Reg 0x841d=0x20) (Reg 0x841e=0x20) (Reg 0x841f=0x20)
(Reg 0x8420=0x43) (Reg 0x8421=0x46) (Reg 0x8422=0x50) (Reg 0x8423=0x2d)
(Reg 0x8424=0x31) (Reg 0x8425=0x30) (Reg 0x8426=0x30) (Reg 0x8427=0x47)
(Reg 0x8428=0x2d) (Reg 0x8429=0x4c) (Reg 0x842a=0x52) (Reg 0x842b=0x34)
(Reg 0x842c=0x20) (Reg 0x842d=0x20) (Reg 0x842e=0x20) (Reg 0x842f=0x20)
(Reg 0x8430=0x56) (Reg 0x8431=0x45) (Reg 0x8432=0x53) (Reg 0x8433=0x31)
(Reg 0x8434=0x32) (Reg 0x8435=0x46) (Reg 0x8436=0x4e) (Reg 0x8437=0x53)
(Reg 0x8438=0x31) (Reg 0x8439=0x34) (Reg 0x843a=0x32) (Reg 0x843b=0x32)
(Reg 0x843c=0x31) (Reg 0x843d=0x50) (Reg 0x843e=0x44) (Reg 0x843f=0x58)
(Reg 0x8440=0x31) (Reg 0x8441=0x30) (Reg 0x8442=0x2d) (Reg 0x8443=0x32)
(Reg 0x8444=0x35) (Reg 0x8445=0x34) (Reg 0x8446=0x39) (Reg 0x8447=0x2d)
(Reg 0x8448=0x30) (Reg 0x8449=0x31) (Reg 0x844a=0x20) (Reg 0x844b=0x20)
(Reg 0x844c=0x30) (Reg 0x844d=0x31) (Reg 0x844e=0x20) (Reg 0x844f=0x20)
(Reg 0x8450=0x00) (Reg 0x8451=0x00) (Reg 0x8452=0x00) (Reg 0x8453=0x00)
```

```
(Reg 0x8454=0x00) (Reg 0x8455=0x00) (Reg 0x8456=0x00) (Reg 0x8457=0x00)
(Reg 0x8458=0x00) (Reg 0x8459=0x00) (Reg 0x845a=0x00) (Reg 0x845b=0x00)
(Reg 0x845c=0x00) (Reg 0x845d=0x00) (Reg 0x845e=0x00) (Reg 0x845f=0x00)
(Reg 0x8460=0x00) (Reg 0x8461=0x00) (Reg 0x8462=0x00) (Reg 0x8463=0x00)
(Reg 0x8464=0x00) (Reg 0x8465=0x00) (Reg 0x8466=0x00) (Reg 0x8467=0x00)
(Reg 0x8468=0x00) (Reg 0x8469=0x00) (Reg 0x846a=0x00) (Reg 0x846b=0x00)
(Reg 0x846c=0x00) (Reg 0x846d=0x00) (Reg 0x846e=0x00) (Reg 0x846f=0x00)
(Reg 0x8470=0x00) (Reg 0x8471=0x00) (Reg 0x8472=0x00) (Reg 0x8473=0x00)
(Reg 0x8474=0x00) (Reg 0x8475=0x00) (Reg 0x8476=0x00) (Reg 0x8477=0x00)
(Reg 0x8478=0x00) (Reg 0x8479=0x00) (Reg 0x847a=0x00) (Reg 0x847b=0x00)
(Reg 0x847c=0x00) (Reg 0x847d=0x00) (Reg 0x847e=0x00) (Reg 0x847f=0x1d)

VR 1 Registers:

(Reg 0xa000=0x0000) (Reg 0xa001=0x0000) (Reg 0xa002=0x0000) (Reg 0xa003=0x0000)
(Reg 0xa004=0x0000) (Reg 0xa005=0x0003) (Reg 0xa006=0x0002) (Reg 0xa007=0x0001)
(Reg 0xa008=0x0003) (Reg 0xa009=0x0002) (Reg 0xa00a=0x0001) (Reg 0xa00b=0x0000)
(Reg 0xa00c=0x0000) (Reg 0xa00d=0x0000) (Reg 0xa00e=0x0000) (Reg 0xa00f=0x0000)
(Reg 0xa010=0x000e) (Reg 0xa011=0x0200) (Reg 0xa012=0x0000) (Reg 0xa013=0x0000)
(Reg 0xa014=0x0000) (Reg 0xa015=0x0000) (Reg 0xa016=0x0020) (Reg 0xa017=0x0000)
(Reg 0xa018=0x0000) (Reg 0xa019=0x0000) (Reg 0xa01a=0x0000) (Reg 0xa01b=0x0000)
(Reg 0xa01c=0x0000) (Reg 0xa01d=0x0003) (Reg 0xa01e=0x0000) (Reg 0xa01f=0x0000)
(Reg 0xa020=0x0000) (Reg 0xa021=0x0000) (Reg 0xa022=0x0000) (Reg 0xa023=0x0000)
(Reg 0xa024=0x0000) (Reg 0xa025=0x0000) (Reg 0xa026=0x0000) (Reg 0xa027=0x0000)
(Reg 0xa028=0x0040) (Reg 0xa029=0x8070) (Reg 0xa02a=0x0062) (Reg 0xa02b=0x0999)
(Reg 0xa02c=0x0099) (Reg 0xa02d=0x0000) (Reg 0xa02e=0x0000) (Reg 0xa02f=0x265f)
(Reg 0xa030=0x7cc3) (Reg 0xa031=0x0000) (Reg 0xa032=0x0000) (Reg 0xa033=0x0000)
(Reg 0xa034=0x0000) (Reg 0xa035=0x0000) (Reg 0xa036=0x0000) (Reg 0xa037=0x0000)
(Reg 0xa038=0x0000) (Reg 0xa039=0x0000) (Reg 0xa03a=0x0000)

NETWORK LANE VR 1 Registers:

(Reg 0xa200=0x0000) (Reg 0xa201=0x0000) (Reg 0xa202=0x0000) (Reg 0xa203=0x0000)
(Reg 0xa204=0x0000) (Reg 0xa205=0x0000) (Reg 0xa206=0x0000) (Reg 0xa207=0x0000)
(Reg 0xa208=0x0000) (Reg 0xa209=0x0000) (Reg 0xa20a=0x0000) (Reg 0xa20b=0x0000)
(Reg 0xa20c=0x0000) (Reg 0xa20d=0x0000) (Reg 0xa20e=0x0000) (Reg 0xa20f=0x0000)
(Reg 0xa210=0x0000) (Reg 0xa211=0x0000) (Reg 0xa212=0x0000) (Reg 0xa213=0x0000)
(Reg 0xa214=0x0000) (Reg 0xa215=0x0000) (Reg 0xa216=0x0000) (Reg 0xa217=0x0000)
(Reg 0xa218=0x0000) (Reg 0xa219=0x0000) (Reg 0xa21a=0x0000) (Reg 0xa21b=0x0000)
(Reg 0xa21c=0x0000) (Reg 0xa21d=0x0000) (Reg 0xa21e=0x0000) (Reg 0xa21f=0x0000)
(Reg 0xa220=0x0000) (Reg 0xa221=0x0000) (Reg 0xa222=0x0000) (Reg 0xa223=0x0000)
(Reg 0xa224=0x0000) (Reg 0xa225=0x0000) (Reg 0xa226=0x0000) (Reg 0xa227=0x0000)
(Reg 0xa228=0x0000) (Reg 0xa229=0x0000) (Reg 0xa22a=0x0000) (Reg 0xa22b=0x0000)
(Reg 0xa22c=0x0000) (Reg 0xa22d=0x0000) (Reg 0xa22e=0x0000) (Reg 0xa22f=0x0000)
(Reg 0xa230=0x0000) (Reg 0xa231=0x0000) (Reg 0xa232=0x0000) (Reg 0xa233=0x0000)
(Reg 0xa234=0x0000) (Reg 0xa235=0x0000) (Reg 0xa236=0x0000) (Reg 0xa237=0x0000)
(Reg 0xa238=0x0000) (Reg 0xa239=0x0000) (Reg 0xa23a=0x0000) (Reg 0xa23b=0x0000)
(Reg 0xa23c=0x0000) (Reg 0xa23d=0x0000) (Reg 0xa23e=0x0000) (Reg 0xa23f=0x0000)
(Reg 0xa240=0x9999) (Reg 0xa241=0x9999) (Reg 0xa242=0x9999) (Reg 0xa243=0x9999)
(Reg 0xa244=0x0000) (Reg 0xa245=0x0000) (Reg 0xa246=0x0000) (Reg 0xa247=0x0000)
(Reg 0xa248=0x0000) (Reg 0xa249=0x0000) (Reg 0xa24a=0x0000) (Reg 0xa24b=0x0000)
(Reg 0xa24c=0x0000) (Reg 0xa24d=0x0000) (Reg 0xa24e=0x0000) (Reg 0xa24f=0x0000)
(Reg 0xa250=0xe058) (Reg 0xa251=0xe058) (Reg 0xa252=0xe058) (Reg 0xa253=0xe058)
(Reg 0xa254=0x0000) (Reg 0xa255=0x0000) (Reg 0xa256=0x0000) (Reg 0xa257=0x0000)
(Reg 0xa258=0x0000) (Reg 0xa259=0x0000) (Reg 0xa25a=0x0000) (Reg 0xa25b=0x0000)
(Reg 0xa25c=0x0000) (Reg 0xa25d=0x0000) (Reg 0xa25e=0x0000) (Reg 0xa25f=0x0000)
(Reg 0xa260=0x0000)

NETWORK LANE VR 2 Registers:

(Reg 0xa280=0x0000) (Reg 0xa281=0x0000) (Reg 0xa282=0x0000) (Reg 0xa283=0x0000)
(Reg 0xa284=0x0000) (Reg 0xa285=0x0000) (Reg 0xa286=0x0000) (Reg 0xa287=0x0000)
(Reg 0xa288=0x0000) (Reg 0xa289=0x0000) (Reg 0xa28a=0x0000) (Reg 0xa28b=0x0000)
(Reg 0xa28c=0x0000) (Reg 0xa28d=0x0000) (Reg 0xa28e=0x0000) (Reg 0xa28f=0x0000)
```

```
(Reg 0xa290=0x0000) (Reg 0xa291=0x0000) (Reg 0xa292=0x0000) (Reg 0xa293=0x0000)
(Reg 0xa294=0x0000) (Reg 0xa295=0x0000) (Reg 0xa296=0x0000) (Reg 0xa297=0x0000)
(Reg 0xa298=0x0000) (Reg 0xa299=0x0000) (Reg 0xa29a=0x0000) (Reg 0xa29b=0x0000)
(Reg 0xa29c=0x0000) (Reg 0xa29d=0x0000) (Reg 0xa29e=0x0000) (Reg 0xa29f=0x0000)
(Reg 0xa2a0=0xb766) (Reg 0xa2a1=0x98ea) (Reg 0xa2a2=0x91eb) (Reg 0xa2a3=0x882c)
(Reg 0xa2a4=0x0000) (Reg 0xa2a5=0x0000) (Reg 0xa2a6=0x0000) (Reg 0xa2a7=0x0000)
(Reg 0xa2a8=0x0000) (Reg 0xa2a9=0x0000) (Reg 0xa2aa=0x0000) (Reg 0xa2ab=0x0000)
(Reg 0xa2ac=0x0000) (Reg 0xa2ad=0x0000) (Reg 0xa2ae=0x0000) (Reg 0xa2af=0x0000)
(Reg 0xa2b0=0x321d) (Reg 0xa2b1=0x36cb) (Reg 0xa2b2=0x38da) (Reg 0xa2b3=0x3a08)
(Reg 0xa2b4=0x0000) (Reg 0xa2b5=0x0000) (Reg 0xa2b6=0x0000) (Reg 0xa2b7=0x0000)
(Reg 0xa2b8=0x0000) (Reg 0xa2b9=0x0000) (Reg 0xa2ba=0x0000) (Reg 0xa2bb=0x0000)
(Reg 0xa2bc=0x0000) (Reg 0xa2bd=0x0000) (Reg 0xa2be=0x0000) (Reg 0xa2bf=0x0000)
(Reg 0xa2c0=0x2fc0) (Reg 0xa2c1=0x2fd1) (Reg 0xa2c2=0x2fd1) (Reg 0xa2c3=0x2fd1)
(Reg 0xa2c4=0x0000) (Reg 0xa2c5=0x0000) (Reg 0xa2c6=0x0000) (Reg 0xa2c7=0x0000)
(Reg 0xa2c8=0x0000) (Reg 0xa2c9=0x0000) (Reg 0xa2ca=0x0000) (Reg 0xa2cb=0x0000)
(Reg 0xa2cc=0x0000) (Reg 0xa2cd=0x0000) (Reg 0xa2ce=0x0000) (Reg 0xa2cf=0x0000)
(Reg 0xa2d0=0x2b33) (Reg 0xa2d1=0x360a) (Reg 0xa2d2=0x3453) (Reg 0xa2d3=0x37f2)
(Reg 0xa2d4=0x0000) (Reg 0xa2d5=0x0000) (Reg 0xa2d6=0x0000) (Reg 0xa2d7=0x0000)
(Reg 0xa2d8=0x0000) (Reg 0xa2d9=0x0000) (Reg 0xa2da=0x0000) (Reg 0xa2db=0x0000)
(Reg 0xa2dc=0x0000) (Reg 0xa2dd=0x0000) (Reg 0xa2de=0x0000) (Reg 0xa2df=0x0000)
(Reg 0xa2e0=0x0000)

HOST LANE VR 1 Registers:

(Reg 0xa400=0x0000) (Reg 0xa401=0x0000) (Reg 0xa402=0x0000) (Reg 0xa403=0x0000)
(Reg 0xa404=0x0000) (Reg 0xa405=0x0000) (Reg 0xa406=0x0000) (Reg 0xa407=0x0000)
(Reg 0xa408=0x0000) (Reg 0xa409=0x0000) (Reg 0xa40a=0x0000) (Reg 0xa40b=0x0000)
(Reg 0xa40c=0x0000) (Reg 0xa40d=0x0000) (Reg 0xa40e=0x0000) (Reg 0xa40f=0x0000)
(Reg 0xa410=0x0000) (Reg 0xa411=0x0000) (Reg 0xa412=0x0000) (Reg 0xa413=0x0000)
(Reg 0xa414=0x0000) (Reg 0xa415=0x0000) (Reg 0xa416=0x0000) (Reg 0xa417=0x0000)
(Reg 0xa418=0x0000) (Reg 0xa419=0x0000) (Reg 0xa41a=0x0000) (Reg 0xa41b=0x0000)
(Reg 0xa41c=0x0000) (Reg 0xa41d=0x0000) (Reg 0xa41e=0x0000) (Reg 0xa41f=0x0000)
(Reg 0xa420=0x0001) (Reg 0xa421=0x0001) (Reg 0xa422=0x0001) (Reg 0xa423=0x0001)
(Reg 0xa424=0x0001) (Reg 0xa425=0x0001) (Reg 0xa426=0x0001) (Reg 0xa427=0x0001)
(Reg 0xa428=0x0001) (Reg 0xa429=0x0001) (Reg 0xa42a=0x0000) (Reg 0xa42b=0x0000)
(Reg 0xa42c=0x0000) (Reg 0xa42d=0x0000) (Reg 0xa42e=0x0000) (Reg 0xa42f=0x0000)
(Reg 0xa430=0x0000) (Reg 0xa431=0x0000) (Reg 0xa432=0x0000) (Reg 0xa433=0x0000)
(Reg 0xa434=0x0000) (Reg 0xa435=0x0000) (Reg 0xa436=0x0000) (Reg 0xa437=0x0000)
(Reg 0xa438=0x0000) (Reg 0xa439=0x0000) (Reg 0xa43a=0x0000) (Reg 0xa43b=0x0000)
(Reg 0xa43c=0x0000) (Reg 0xa43d=0x0000) (Reg 0xa43e=0x0000) (Reg 0xa43f=0x0000)
(Reg 0xa440=0x0001) (Reg 0xa441=0x0001) (Reg 0xa442=0x0001) (Reg 0xa443=0x0001)
(Reg 0xa444=0x0001) (Reg 0xa445=0x0001) (Reg 0xa446=0x0001) (Reg 0xa447=0x0001)
(Reg 0xa448=0x0001) (Reg 0xa449=0x0001) (Reg 0xa44a=0x0000) (Reg 0xa44b=0x0000)
(Reg 0xa44c=0x0000) (Reg 0xa44d=0x0000) (Reg 0xa44e=0x0000) (Reg 0xa44f=0x0000)
(Reg 0xa450=0x0000)
```

The following example shows sample output from the **show controllers HundredGigE stats** command for the Cisco CRS 1-Port 100-Gigabit Ethernet Interface Module:

```
RP/0/RP0/CPU0:router# show controllers HundredGigE 0/3/0/0 stats
Tue Mar 22 06:04:08.484 UTC
Statistics for interface HundredGigE0/3/0/0 (cached values):

Ingress:
    Input total bytes           = 73475628362976
    Input good bytes            = 73443591856352

    Input total packets         = 8009121965
    Input 802.1Q frames         = 0
    Input pause frames          = 0
    Input pkts 64 bytes         = 925
    Input pkts 65-127 bytes     = 5220
    Input pkts 128-255 bytes    = 59
    Input pkts 256-511 bytes    = 2
```

```
    Input pkts 512-1023 bytes   = 1
    Input pkts 1024-1518 bytes  = 4
    Input pkts 1519-Max bytes   = 8009115754

    Input good pkts             = 8009121964
    Input unicast pkts          = 8009117183
    Input multicast pkts        = 4780
    Input broadcast pkts        = 1

    Input drop overrun          = 0
    Input drop abort            = 0
    Input drop invalid VLAN     = 0
    Input drop invalid DMAC     = 0
    Input drop invalid encap    = 0
    Input drop other            = 6947

    Input error giant           = 0
    Input error runt            = 0
    Input error jabbers         = 0
    Input error fragments       = 0
    Input error CRC             = 1
    Input error collisions      = 0
    Input error symbol          = 3
    Input error other           = 0

    Input MIB giant             = 0
    Input MIB jabber            = 0
    Input MIB CRC               = 0

Egress:
    Output total bytes          = 70097928185720
    Output good bytes           = 70067364389772

    Output total packets        = 7640945487
    Output 802.1Q frames        = 0
    Output pause frames         = 0
    Output pkts 64 bytes        = 725
    Output pkts 65-127 bytes    = 10602
    Output pkts 128-255 bytes   = 275
    Output pkts 256-511 bytes   = 5
    Output pkts 512-1023 bytes  = 0
    Output pkts 1024-1518 bytes = 6
    Output pkts 1519-Max bytes  = 7640933874

    Output good pkts            = 7640945487
    Output unicast pkts         = 7640941982
    Output multicast pkts       = 3501
    Output broadcast pkts       = 6

    Output drop underrun        = 0
    Output drop abort           = 2
    Output drop other           = 2373

    Output error other          = 0
```

The following example shows sample output from the **show controllers HundredGigE xgxs** command for the Cisco CRS 1-Port 100-Gigabit Ethernet Interface Module:

```
RP/0/RP0/CPU0:router# show controllers HundredGigE 0/3/0/0 xgxs
Tue Mar 22 06:04:19.546 UTC
No XGXS present
```

show lldp

To display the global Link Layer Discovery Protocol (LLDP) operational characteristics on the system, use the **show lldp** command in EXEC mode.

show lldp

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 4.2.3	This command was introduced.

Usage Guidelines

The **show lldp** command displays the LLDP operational characteristics when LLDP is enabled globally on the system using the **lldp** command. The settings for the following commands are displayed:

- **lldp timer**
- **lldp holdtime**
- **lldp reinit**

Task ID

Task ID	Operation
ethernet-services	read

Example 1

The following example shows the default LLDP operational characteristics when LLDP is enabled globally on the system:

```
RP/0/RP0/CPU0:router# show lldp
Wed Apr 13 06:16:45.510 DST
Global LLDP information:
        Status: ACTIVE
        LLDP advertisements are sent every 30 seconds
        LLDP hold time advertised is 120 seconds
        LLDP interface reinitialisation delay is 2 seconds
```

Example 2

The following example shows the output when LLDP is not enabled globally on the system:

```
RP/0/RP0/CPU0:router# show lldp
Wed Apr 13 06:42:48.221 DST
% LLDP is not enabled
```

Related Commands

Command	Description
lldp, on page 158	Enables LLDP globally for both transmit and receive operation on the system.
lldp timer, on page 163	Specifies the LLDP packet rate.
lldp holdtime, on page 161	Specifies the length of time that information from an LLDP packet should be held by the receiving device before aging and removing it.
lldp reinit, on page 162	Specifies the length of time to delay initialization of LLDP on an interface.

show lldp entry

To display detailed information about LLDP neighbors, use the **show lldp entry** command in EXEC mode.

show lldp entry * *name*

Syntax Description

*	Displays detailed information about all LLDP neighbors.
name	Name of a specific LLDP neighbor for which detailed information is displayed.

Syntax Description

This command has no keywords or arguments.

Command Modes

EXEC mode

Command History

Release	Modification
Release 4.2.3	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
ethernet-services	read

The following example shows sample output for all LLDP neighbor table entries on the system:

```
RP/0/RP0/CPU0:router# show lldp entry *
Wed Apr 13 10:29:40.342 UTC
Capability codes:
        (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
        (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

------------------------------------------------
Local Interface: GigabitEthernet0/0/0/8
Chassis id: 0026.9815.c3e6
Port id: Gi0/0/0/8
Port Description: GigabitEthernet0/0/0/8
System Name: asr9k-5

System Description:
Cisco IOS XR Software, Version 4.1.0.32I[Default]
Copyright (c) 2011 by Cisco Systems, Inc.

Time remaining: 102 seconds
Hold Time: 120 seconds
System Capabilities: R
Enabled Capabilities: R
Management Addresses:
  IPv4 address: 10.5.173.110



------------------------------------------------
Local Interface: GigabitEthernet0/0/0/8
```

```
Chassis id: 0026.9815.c3e6
Port id: Gi0/0/0/8.1
Port Description: GigabitEthernet0/0/0/8.1
System Name: asr9k-5

System Description:
Cisco IOS XR Software, Version 4.1.0.32I[Default]
Copyright (c) 2011 by Cisco Systems, Inc.

Time remaining: 96 seconds
Hold Time: 120 seconds
System Capabilities: R
Enabled Capabilities: R
Management Addresses:
  IPv4 address: 10.5.173.110


Total entries displayed: 2
```

Related Commands

Command	Description
lldp, on page 158	Enables LLDP globally for both transmit and receive operation on the system.

show lldp errors

To display Link Layer Discovery Protocol (LLDP) error and overflow statistics, use the **show lldp errors** command in EXEC mode.

show lldp errors [**location** *location*]

Syntax Description

location	*location*	(Optional) Displays information about LLDP neighbors for the specified location. The *location* argument is entered in the *rack/slot/module* notation.

Command Default

Totals of LLDP error and overflow statistics for the system are displayed.

Command Modes

EXEC mode

Command History

Release	Modification
Release 4.2.3	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
ethernet-services	read

The following example shows sample output for the **show lldp errors** command:

```
RP/0/RP0/CPU0:router# show lldp errors
Wed Apr 13 06:17:08.321 DST

LLDP errors/overflows:
        Total memory allocation failures: 0
        Total encapsulation failures: 0
        Total input queue overflows: 0
        Total table overflows: 0
```

Related Commands

Command	Description
lldp, on page 158	Enables LLDP globally for both transmit and receive operation on the system.
show lldp traffic, on page 235	Displays statistics for LLDP traffic.

show lldp interface

To display Link Layer Discovery Protocol (LLDP) configuration and status information on an interface, use the **show lldp interface** command in EXEC mode.

show lldp interface [*type interface-path-id* | **location** *location*]

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 *location*	(Optional) Displays information about LLDP neighbors for the specified location. The *location* argument is entered in the *rack/slot/module* notation.

Command Default

LLDP configuration and status information for all interfaces is displayed.

Command Modes

EXEC mode

Command History

Release	Modification
Release 4.2.3	This command was introduced.

Usage Guidelines

When LLDP is enabled globally on the system, all supported interfaces are automatically enabled for both LLDP receive and transmit operations. You can individually disable interfaces for either LLDP receive or transmit operations using the **receive disable** command or **transmit disable** command in LLDP configuration mode under the interface.

Task ID

Task ID	Operation
ethernet-services	read

The following example shows sample output for the **show lldp interface** command for the Gigabit Ethernet interface at 0/1/0/7:

```
RP/0/RP0/CPU0:router# show lldp interface gigabitethernet 0/1/0/7
Wed Apr 13 13:22:30.501 DST


GigabitEthernet0/1/0/7:
        Tx: enabled
        Rx: enabled
        Tx state: IDLE
        Rx state: WAIT FOR FRAME
```

Table 16: show lldp interface Field Descriptions

Field	Description
Tx:	Configuration status of the interface to transmit LLDP advertisements.
Rx:	Configuration status of the interface to receive LLDP advertisements.
Tx state:	Status of the LLDP transmit process on the interface.
Rx state:	Status of the LLDP receive process on the interface.

Related Commands

Command	Description
lldp, on page 158	Enables LLDP globally for both transmit and receive operation on the system.
lldp (interface), on page 159	Enters LLDP configuration mode.

show lldp neighbors

To display information about Link Layer Discovery Protocol (LLDP) neighbors, use the **show lldp neighbors** command in EXEC mode.

show lldp neighbors [*type interface-path-id* | **location** *location*] [**detail**]

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 *location*	(Optional) Displays information about LLDP neighbors for the specified location. The *location* argument is entered in the *rack/slot/module* notation.
detail	(Optional) Displays all available information about LLDP neighbors.

Command Default

Basic device information for LLDP neighbors is displayed.

Command Modes

EXEC mode

Command History

Release	Modification
Release 4.2.3	This command was introduced.

Usage Guidelines

To clear the neighbor information displayed by the **show lldp neighbors** command, use the **clear lldp table** command.

Task ID

Task ID	Operation
ethernet-services	read

The following example show sample output for the **show lldp neighbors** command:

```
RP/0/RP0/CPU0:router# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID           Local Intf     Hold-time  Capability      Port ID
R1                  Et1/0          150        R               Et1/0

Total entries displayed: 1
```

Table 17: show lldp neighbors Field Descriptions

Field	Description
Device ID	Name of the neighbor device. **Note** If the device ID has more than 20 characters, the ID will be truncated to 20 characters in command output because of display constraints.
Local Intf	Local interface through which this neighbor is connected.
Hold-time	Amount of time (in seconds) that the local device will hold the LLDP advertisement from a sending device before discarding it.
Capability	The device type of the neighbor, whose values correspond to the characters and definition displayed in the "Capability codes" section.
Port ID	Interface and port number of the neighboring device.

The following example shows sample output for the **show lldp neighbors detail** command:

```
RP/0/RP0/CPU0:router# show lldp neighbors detail
Wed Apr 13 10:29:40.342 UTC
Capability codes:
        (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
        (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

------------------------------------------------
Local Interface: GigabitEthernet0/0/0/8
Chassis id: 0026.9815.c3e6
Port id: Gi0/0/0/8
Port Description: GigabitEthernet0/0/0/8
System Name: asr9k-5

System Description:
Cisco IOS XR Software, Version 4.1.0.32I[Default]
Copyright (c) 2011 by Cisco Systems, Inc.

Time remaining: 102 seconds
Hold Time: 120 seconds
System Capabilities: R
Enabled Capabilities: R
Management Addresses:
  IPv4 address: 10.5.173.110



------------------------------------------------
Local Interface: GigabitEthernet0/0/0/8
Chassis id: 0026.9815.c3e6
Port id: Gi0/0/0/8.1
Port Description: GigabitEthernet0/0/0/8.1
System Name: asr9k-5

System Description:
Cisco IOS XR Software, Version 4.1.0.32I[Default]
```

```
Copyright (c) 2011 by Cisco Systems, Inc.

Time remaining: 96 seconds
Hold Time: 120 seconds
System Capabilities: R
Enabled Capabilities: R
Management Addresses:
  IPv4 address: 10.5.173.110


Total entries displayed: 2
```

Related Commands

Command	Description
lldp, on page 158	Enables LLDP globally for both transmit and receive operation on the system.
clear lldp, on page 150	Resets LLDP traffic counters or LLDP neighbor information.

show lldp traffic

To display statistics for Link Layer Discovery Protocol (LLDP) traffic, use the **show lldp traffic** command in EXEC mode.

show lldp traffic [**location** *location*]

Syntax Description

location	*location*	(Optional) Displays LLDP statistics for traffic at the specified location. The *location* argument is entered in the *rack/slot/module* notation.

Command Default

Totals of LLDP statistics for the system are displayed.

Command Modes

EXEC mode

Command History

Release	Modification
Release 4.2.3	This command was introduced.

Usage Guidelines

To reset the counters displayed by the **show lldp traffic** command, use the **clear lldp counters** command.

Task ID

Task ID	Operation
ethernet-services	read

The following example shows sample output for statistics for all LLDP traffic on the system:

```
RP/0/RP0/CPU0:router# show lldp traffic
LLDP traffic statistics:
    Total frames out: 277
    Total entries aged: 0
    Total frames in: 328
    Total frames received in error: 0
    Total frames discarded: 0
    Total TLVs discarded: 0
    Total TLVs unrecognized: 0
```

Table 18: show lldp traffic Field Descriptions

Field	Description
Total frames out:	Number of LLDP advertisements sent from the device.
Total entries aged:	Number of LLDP neighbor entries removed due to expiration of the hold time.
Total frames in:	Number of LLDP advertisements received by the device.
Total frames received in error:	Number of times the LLDP advertisements contained errors of any type.

Field	Description
Total frames discarded:	Number of times the LLDP process discarded an incoming advertisement.
Total TLVs discarded:	Number of times the LLDP process discarded a Type Length Value (TLV) from an LLDP frame.
Total TLVs unrecognized:	Number of TLVs that could not be processed because the content of the TLV was not recognized by the device or the contents of the TLV were incorrectly specified.

Related Commands

Command	Description
lldp, on page 158	Enables LLDP globally for both transmit and receive operation on the system.
clear lldp, on page 150	Resets LLDP traffic counters or LLDP neighbor information.

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** *interface-path-id* **bundle-ether***bundle-id*[**location node-id**]

Syntax Description

{**GigabitEthernet** | **TenGigEHundred GigEbundle-ether** }	Indicates the type of Ethernet interface whose MAC accounting statistics you want to display. Enter **GigabitEthernet**, **TenGigE** , **bundle-ether**.
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 mode

Command History

Release	Modification
Release 3.0	This command was introduced.
Release 4.3.2	The **bundle-ether** keyword was included.

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/RP0/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 19: 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 152	Clears MAC accounting statistics for an interface.
mac-accounting, on page 166	Generates accounting information for IP traffic based on the source and destination MAC addresses on LAN interfaces.

Ethernet OAM Commands

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

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

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**

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

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ethernet oam
RP/0/RP0/CPU0:router(config-if-eoam)# action capabilities-conflict log
```

Related Commands

Command	Description
ethernet oam profile, on page 309	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 306	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 370	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

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 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
```

```
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ethernet oam
RP/0/RP0/CPU0:router(config-if-eoam)# action critical-event log
```

Related Commands

Command	Description
ethernet oam profile, on page 309	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 306	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 370	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

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 3.9.0	This command was introduced.
Release 4.0.0	The **efd** keyword was added.
Release 6.1.2	Removed restriction disallowing default value (log) in Ethernet OAM configuration mode.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ethernet oam
RP/0/RP0/CPU0:router(config-if-eoam)# action discovery-timeout log
```

Related Commands

Command	Description
ethernet oam profile, on page 309	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 306	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 370	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**

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 3.9.0	This command was introduced.
Release 6.1.2	Removed restriction disallowing default value (log) in Ethernet OAM configuration mode.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
```

```
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ethernet oam
RP/0/RP0/CPU0:router(config-if-eoam)# action dying-gasp log
```

Related Commands

Command	Description
ethernet oam profile, on page 309	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 306	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 370	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

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 3.9.0	This command was introduced.
Release 6.1.2	Removed restriction disallowing default value (disable) in Ethernet OAM configuration mode.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
```

```
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ethernet oam
RP/0/RP0/CPU0:router(config-if-eoam)# action high-threshold disable
```

Related Commands

Command	Description
ethernet oam profile, on page 309	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 306	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 370	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

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 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ethernet oam
RP/0/RP0/CPU0:router(config-if-eoam)# action remote-loopback log
```

Related Commands

Command	Description
ethernet oam profile, on page 309	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 306	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 370	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**

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

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ethernet oam
RP/0/RP0/CPU0:router(config-if-eoam)# action session-down log
```

Related Commands

Command	Description
ethernet oam profile, on page 309	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 306	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 370	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**

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 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ethernet oam
RP/0/RP0/CPU0:router(config-if-eoam)# action session-up log
```

Related Commands

Command	Description
ethernet oam profile, on page 309	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 306	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 370	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**

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. This command replaces the **action link-fault** command.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ethernet oam
RP/0/RP0/CPU0:router(config-if-eoam)# action uni-directional link-fault log
```

Related Commands

Command	Description
ethernet oam profile, on page 309	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 306	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 370	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

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

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ethernet oam
(config-if-eoam)# action wiring-conflict error-disable-interface
```

Related Commands

Command	Description
ethernet oam profile, on page 309	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 306	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 370	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**

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). For loss measurements, the size of each bin in percentage points (range 1-100). 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.

For loss measurements, the default is aggregation disabled.

Command Modes

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

Command History

Release	Modification
Release 4.0.0	This command was introduced.
Release 4.3.0	The measurement statistics for Y.1731 Synthetic Loss Measurement (SLM) was included.

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).

For synthetic loss 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 25 for loss measurements yields 4 bins of statistics for these sample ranges:

- Bin 1—Samples with loss ranges 0 to < 25 percentage points.
- Bin 2—Samples with loss ranges greater than or equal to 25 and < 50 percentage points.

- Bin 3—Samples with loss ranges greater than or equal to 50 and < 75 percentage points.
- Bin 4—Samples with loss ranges greater than or equal to 75 and <100 percentage points.

Note For delay and jitter measurements (round-trip or one-way), the lower bound of the first bin is zero, and the last bin is effectively of infinite width. If aggregation is disabled, each individual delay value is stored. For loss measurements, the lower bound of the first bin is zero, and the upper bound of the last bin is 100. The last bin may be wider than the other bins. If aggregation is disabled, each calculated FLR value is stored.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet sla
RP/0/RP0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RP/0/RP0/CPU0:router(config-sla-prof)# statistics measure round-trip-delay
RP/0/RP0/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*]

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 3.9.1	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet cfm
RP/0/RP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/RP0/CPU0:router(config-cfm-dmn-svc)# ais transmission interval 1m cos 7
```

Related Commands

Command	Description
log ais, on page 347	Configures AIS logging for a CFM domain service to indicate when AIS or LCK packets are received.
ais transmission up, on page 266	Configures AIS transmission on a CFM interface.
show ethernet cfm interfaces ais, on page 391	Displays the information about interfaces that are currently transmitting AIS.
show ethernet cfm local meps, on page 397	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*]

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 3.9.1	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/2
RP/0/RP0/CPU0:router(config-if)# ethernet cfm
RP/0/RP0/CPU0:router(config-if-cfm)# ais transmission up interval 1m cos 7
```

Related Commands

Command	Description
ais transmission, on page 264	Configures AIS transmission for a CFM domain service.
log ais, on page 347	Configures AIS logging for a CFM domain service to indicate when AIS or LCK packets are received.
show ethernet cfm interfaces ais, on page 391	Displays the information about interfaces that are currently transmitting AIS.
show ethernet cfm local meps, on page 397	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 4.0.0	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 269 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet sla
RP/0/RP0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/RP0/CPU0:router(config-sla-prof)# statistics measure round-trip-delay
RP/0/RP0/CPU0:router(config-sla-prof-stat-cfg)# buckets archive 50
```

Related Commands

Command	Description
buckets size, on page 269	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*

Syntax Description

number	Specifies the size of each bucket. The number of probes that each buckets may contain. The range is 1 to 100.
per-probe	Probes span multiple buckets.
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 4.0.0	This command was introduced.
Release 4.3.0	The **per-probe** keyword was deprecated.

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 369, send (SLA), on page 378, and schedule (SLA), on page 375 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet sla
RP/0/RP0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RP/0/RP0/CPU0:router(config-sla-prof)# statistics measure round-trip-delay
RP/0/RP0/CPU0:router(config-sla-prof-stat-cfg)# buckets size 100 per-probe
```

Related Commands

Command	Description
buckets archive, on page 268	Configures the number of buckets to store in memory.
probe, on page 369	Enters SLA profile probe configuration mode.
schedule (SLA), on page 375	
send (SLA), on page 378	Configures the number and timing of packets sent by a probe in an operations profile.

clear error-disable

To clear error-disable reason of an interface, use the **clear error-disable** command in the EXEC mode.

clear error-disable {**interface**<*interface*>| {**all** |<*location* > }}

Syntax Description

interface	The interface for which you want to clear the error-disable reason.
location	Clear error-disable for all interfaces on a specific card, or on all cards.

Command Default

An interface, location o

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
interface	exec

Example

The following example shows how to clear error-disable reason for an interface:

```
RP/0/0/CPU0:ios#sh error-disable
Interface            Error-Disable reason            Retry (s)  Time disabled
-------------------  ------------------------------  ---------  --------------
Gi0/0/0/0            ethernet-oam-link-fault               ---  01:00 01 Jan

RP/0/0/CPU0:ios#
RP/0/0/CPU0:ios#clear error-disable interface G 0/0/0/0
```

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 *r ack*/*slot*/*module* notation.

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router# clear ethernet cfm ccm-learning-database location all
```

Related Commands

Command	Description
show ethernet cfm ccm-learning-database, on page 387	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 mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router# clear ethernet cfm interface statistics location all
```

Related Commands

Command	Description
show ethernet cfm interfaces statistics, on page 393	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 3.9.0	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/RP0/CPU0:router# clear ethernet cfm local meps all
```

Related Commands

Command	Description
show ethernet cfm local meps, on page 397	Displays information about local MEPs.

clear ethernet cfm offload

To trigger the re-application of Maintenance End Points (MEPs) that have been disabled due to exceeding offload resource limits, use the **clear ethernet cfm offload** command in the EXEC mode.

Note This command does not clear any counters or stored statistics for the MEPs.

clear ethernet cfm offloadlocation*node-id*

Syntax Description

location *node-id*	(Optional) Specifies the location for which the re-application of MEPs needs to be triggered.

Command Default

The default action is to clear the CFM offload information for all nodes.

Command Modes

EXEC mode

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ethernet-services	execute

Example

This example shows how to execute the **clear ethernet cfm offload** command:

```
RP/0/RP0/CPU0:router# clear ethernet cfm offload
```

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 mode

Command History

Release	Modification
Release 3.9.0	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/RP0/CPU0:router# clear ethernet cfm peer meps all
```

Related Commands

Command	Description
show ethernet cfm peer meps, on page 403	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 mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

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

```
RP/0/RP0/CPU0:router# clear ethernet cfm traceroute-cache all
```

Related Commands

Command	Description
traceroute cache, on page 450	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 411	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 mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router# clear ethernet oam statistics interface gigabitethernet 0/1/5/1
```

Related Commands

Command	Description
show ethernet oam statistics, on page 426	Displays the local and remote Ethernet OAM statistics for interfaces.
show ethernet oam interfaces, on page 424	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 mode

Command History

Release	Modification
Release 4.0.0	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 269 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/RP0/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/RP0/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/RP0/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 mode

Command History

Release	Modification
Release 4.0.0	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 269 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/RP0/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/RP0/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/RP0/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 280	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 311	Executes an on-demand Ethernet SLA operation probe for CFM delay measurement.
ethernet sla on-demand operation type cfm-synthetic-loss-measurement probe, on page 333	Executes an on-demand Ethernet SLA operation probe for CFM synthetic loss measurement.
show ethernet sla operations, on page 432	Displays information about configured Ethernet SLA operations.
show ethernet sla statistics, on page 435	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 mode

Command History

Release	Modification
Release 4.0.0	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 269 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/RP0/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/RP0/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/RP0/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/RP0/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/RP0/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 269	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 number of lost periodic information OAMPDUs. 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 3.9.0	This command was introduced.

Usage Guidelines

If no packets are received from the OAM peer in the specified connection timeout period which is measured in number of lost periodic Information OAMPDUs, then the OAM session is brought down, and the negotiation phase starts again.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

This example shows how to configure the connection timeout value of an Ethernet OAM session:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/CPU0:router(config-eoam)# connection timeout 20
```

Related Commands

Command	Description
action discovery-timeout, on page 246	Configures what action is taken on an interface when a connection timeout occurs.
ethernet oam, on page 306	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
ethernet oam profile, on page 309	Creates an EOAM profile and enters EOAM configuration mode.
show ethernet oam configuration, on page 417	Displays the current active Ethernet OAM configuration on an interface.

Command	Description
show ethernet oam discovery, on page 420	Displays the current status of Ethernet OAM sessions.
show ethernet oam interfaces, on page 424	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*

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 3.9.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet cfm
RP/0/RP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/RP0/CPU0:router(config-cfm-dmn-svc)# continuity-check archive hold-time 100
```

Related Commands

Command	Description
show ethernet cfm peer meps, on page 403	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*]

Syntax Description

time	Interval at which continuity-check messages are transmitted. Valid values are: • 3.3ms: 3.3 milliseconds • 10ms: 10 milliseconds • 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 3.9.0	This command was introduced.
Release 4.3.1	The **continuity-check interval** command was updated to allow CCM time interval of 10ms.
Release 7.1.15	The command was updated to allow CCM time interval of 3.3ms.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet cfm
RP/0/RP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/RP0/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

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 3.9.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet cfm
RP/0/RP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/RP0/CPU0:router(config-cfm-dmn-svc)# continuity-check loss auto-traceroute
```

Related Commands

Command	Description
show ethernet cfm traceroute-cache, on page 411	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*

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 3.9.0	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.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ethernet cfm mep domain Dm1 service Sv1 mep-id 1
RP/0/RP0/CPU0:router(config-if-cfm-mep)# cos 7
```

Related Commands

Command	Description
ethernet cfm (interface), on page 304	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 mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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/RP0/CPU0:router# debug ethernet cfm packets hexdump

RP/0/RP0/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/RP0/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/RP0/CPU0:May 29 14:15:39.621 : cfmd[150]: PKT-RX:   CCM: MAID: MDID String 'dom4',
SMAN String 'ser4'
RP/0/RP0/CPU0:May 29 14:15:39.621 : cfmd[150]: PKT-RX:   CCM: Sender ID: Chassis ID Local
'hpr', Mgmt Addr <none>
RP/0/RP0/CPU0:May 29 14:15:39.621 : cfmd[150]: PKT-RX:   CCM: Port status: Up, interface
status Up
RP/0/RP0/CPU0:May 29 14:15:39.622 : cfmd[150]: PKT-RX:   Raw Frame:
RP/0/RP0/CPU0:May 29 14:15:39.622 : cfmd[150]: PKT-RX:     0x40010546 00000001 00100404
646F6D34 02047365 72340000 00000000 00000000
RP/0/RP0/CPU0:May 29 14:15:39.622 : cfmd[150]: PKT-RX:     0x00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000
RP/0/RP0/CPU0:May 29 14:15:39.622 : cfmd[150]: PKT-RX:     0x00000000 00000000 00000200
01020400 01010100 05030768 707200
RP/0/RP0/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/RP0/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/RP0/CPU0:May 29 14:15:43.625 : cfmd[150]: PKT-TX:   CCM: MAID: MDID String 'foo', SMAN
```

```
 String 'foo'
RP/0/RP0/CPU0:May 29 14:15:43.625 : cfmd[150]: PKT-TX:   CCM: Sender ID: Chassis ID Local
'ios', Mgmt Addr <none>
RP/0/RP0/CPU0:May 29 14:15:43.625 : cfmd[150]: PKT-TX:   CCM: Port status: Up, interface
status Up
RP/0/RP0/CPU0:May 29 14:15:43.625 : cfmd[150]: PKT-TX:   Raw Frame:
RP/0/RP0/CPU0:May 29 14:15:43.625 : cfmd[150]: PKT-TX:     0x40018546 00000010 00010403
666F6F02 03666F6F 00000000 00000000 00000000
RP/0/RP0/CPU0:May 29 14:15:43.625 : cfmd[150]: PKT-TX:     0x00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000
RP/0/RP0/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 295	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 mode

Command History

Release	Modification
Release 3.9.0	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/RP0/CPU0:router# debug ethernet cfm protocol-state

RP/0/RP0/CPU0:May 29 14:41:49.966 : cfmd[150]: CFM: Created 1 local MEPs in PM and Engine
RP/0/RP0/CPU0:May 29 14:41:49.967 : cfmd[150]: CFM: State changes notification for 1 EFPs
RP/0/RP0/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/RP0/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/RP0/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 292	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*]]

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 3.9.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet cfm
RP/0/RP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0/CPU0:router(config-cfm-dmn)#
```

Related Commands

Command	Description
ethernet cfm (global), on page 303	Enters CFM configuration mode.
ethernet cfm (interface), on page 304	Enters interface CFM configuration mode.
mep domain, on page 356	Creates a MEP on an interface.
service, on page 381	
show ethernet cfm configuration-errors, on page 389	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 395	Displays a list of local maintenance points.
show ethernet cfm local meps, on page 397	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.

efdprotection-switching
no efd

Syntax Description

protection-switching	Enables protection switching, which causes high-priority notifications to be sent when peer MEPs specified for cross-check time out, or when CCMs are received with the RDI bit set.

Note The high-priority notifications only apply to MEPs that are offloaded. In the case of non-offloaded MEPs, enabling protection switching has no effect, and the command only enables EFD.

Command Default

EFD is disabled.

Command Modes

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

Command History

Release	Modification
Release 3.9.1	This command was introduced.
Release 4.3.1	The **protection-switching** keyword was included.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet cfm
RP/0/RP0/CPU0:router(config-cfm)# domain D1 level 1
RP/0/RP0/CPU0:router(config-cfm-dmn)# service S1 down-meps
RP/0/RP0/CPU0:router(config-cfm-dmn-svc)# efd
```

Related Commands

Command	Description
show efd interface, on page 386	Displays all interfaces that are shut down because of EFD.
show ethernet cfm local meps, on page 397	Displays information about local MEPs.

error-disable recovery cause

To configure error-disable to automatically attempt recovery, use the **error-disable recovery cause** command.

error-disable recovery cause { **ethernet-oam-critical-event** | **ethernet-oam-link-fault** | **. . .** } [**interval**<**30 – 1,000,000** >]

Syntax Description

link-oam-critical-event	Used when a critical event is detected by Ethernet Link OAM.
cause	One of the defined error-disable causes, for example: ethernet-oam-link-fault.
interval	Specifies the interval, in seconds, at which retries are attempted. The range is 30 to 1,000,000.
link-oam-link-fault	Used when a unidirectional link is detected by Ethernet Link OAM.

Command Default

Default interval period is 300 seconds.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.3	This command was introduced.

Usage Guidelines

When error disable recovery is enabled, the interface automatically recovers from the error-disabled state, and the device retries bringing the interface up.

Task ID

Task ID	Operation
interface	write

Example

The following example shows the full list of error-disable recovery causes:

```
RP/0/0/CPU0:ios(config)#error-disable recovery cause ?
cluster-udld                    Used when UDLD is enabled on a Cluster port and UDLD is in
 aggressive mode and UDLD goes uni directional
link-oam-capabilities-conflict  Used when Ethernet Link OAM configuration conflicts with
the peer
link-oam-critical-event        Used when a critical event is detected by Ethernet Link OAM
link-oam-discovery-timeout      Used when an Ethernet Link OAM session fails to come up in
 time
link-oam-dying-gasp             Used when a dying gasp is detected by Ethernet Link OAM
link-oam-link-fault             Used when a unidirectional link is detected by Ethernet
Link OAM
link-oam-miswired               Used when a mis-wiring is detected with Ethernet Link OAM
link-oam-session-down           Used when an Ethernet Link OAM session goes down
link-oam-threshold-breached     Used when a configured error threshold has been breached
pvrst-pvid-mismatch            Used when a PVRST BPDU packet is tagged with a VLAN ID which
 is different from the VLAN ID on which it was sent.
stp-bpdu-guard                  Used when an STP BPDU is received on a port on which BPDU
```

```
Guard is configured
stp-legacy-bpdu                 Used when a legacy BPDU is received on a port. Only MSTP
and RSTP BPDUs are supported
udld-loopback                 Used when UDLD detects that the port is in loopback mode(i.e.
 its Tx is directly connected to its Rx)
udld-neighbor-mismatch          Used when mismatched neighbors are detected by UDLD
udld-timeout                    Used when all UDLD neigbors on the link have timed out
udld-unidirectional             Used when a link is detected to be unidirectional
```

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 mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enter the CFM configuration mode.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet cfm
RP/0/RP0/CPU0:router(config-cfm)#
```

Related Commands

Command	Description
domain, on page 297	
ethernet cfm (interface), on page 304	Enters interface CFM configuration mode.
show ethernet cfm configuration-errors, on page 389	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 395	Displays a list of local maintenance points.
show ethernet cfm local meps, on page 397	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 3.9.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enter interface CFM configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ethernet cfm
RP/0/RP0/CPU0:router(config-if-cfm)#
```

Related Commands

Command	Description
cos (CFM), on page 291	Configures the CoS for all CFM packets generated by the MEP on an interface.
ethernet cfm (global), on page 303	Enters CFM configuration mode.
mep domain, on page 356	Creates a MEP on an interface.
show ethernet cfm configuration-errors, on page 389	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 395	Displays a list of local maintenance points.

Command	Description
show ethernet cfm local meps, on page 397	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

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 3.9.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/5/6
RP/0/RP0/CPU0:router(config-if)# ethernet oam
RP/0/RP0/CPU0:router(config-if-eoam)#
```

ethernet oam loopback

To start or stop a loopback at the remote end of an Ethernet OAM interface, use the **ethernet oam loopback** command in EXEC mode.

ethernet oam loopback enable | **disable** *type interface-path-id*

Syntax Description

enable	Starts a loopback at the remote end.
disable	Stops the loopback at the remote end.
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

Loopback is not enabled.

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

This command puts the remote peer device into loopback mode. This means that all traffic sent to the peer is looped back, which means that it is sent back from the peer and received by the router. All traffic received from the peer device is discarded.

This command returns when the OAM client receives confirmation from the remote end that the remote loopback has been enabled or disabled. If no response or a failure response is received, an error is returned.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to start a loopback at the far end of an Ethernet OAM interface.

```
RP/0/RP0/CPU0:router# ethernet oam loopback enable tengigabitethernet 0/6/1/0
```

Related Commands

Command	Description
action remote-loopback, on page 252	Configures what action is taken on an interface when a remote-loopback event occurs.
snmp-server traps ethernet oam events, on page 444	
show ethernet oam configuration, on page 417	Displays the current active Ethernet OAM configuration on an interface.

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*

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 3.9.0	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/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/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 mode

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enter the Ethernet SLA configuration mode.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet sla
RP/0/RP0/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.

<groupcomp >
<kwd >ethernet</kwd>
<sep> </sep>
<kwd >sla</kwd>
<sep> </sep>
<kwd >on-demand</kwd>
<sep> </sep>
<kwd >operation</kwd>
<sep> </sep>
<kwd >type</kwd>
<sep> </sep>
<groupchoice >
<kwd >cfm-delay-measurement</kwd>
<kwd >cfm-delay-measurement-v0</kwd>
</groupchoice>
<sep> </sep>
<kwd >probe</kwd>
<sep> </sep>
<groupcomp importance='optional' >
<kwd >priority</kwd>
<sep> </sep>
<kwd >number</kwd>
</groupcomp>
<sep> </sep>
<groupcomp importance='optional' >
<kwd >send</kwd>
<sep> </sep>
<groupchoice >
<groupcomp >

<kwd >packet</kwd>
<sep> </sep>
<groupchoice >
<kwd >once</kwd>
<groupcomp >
<kwd >every</kwd>
<sep> </sep>
<kwd >number</kwd>
<sep> </sep>
<groupchoice >
<kwd >milliseconds</kwd>
<kwd >seconds</kwd>
<kwd >minutes</kwd>
<kwd >hours</kwd>
</groupchoice>
</groupcomp>
</groupchoice>
</groupcomp>
<groupcomp >
<kwd >burst</kwd>
<sep> </sep>
<groupchoice >
<kwd >once</kwd>
<groupcomp >
<kwd >every</kwd>
<sep> </sep>
<kwd >number</kwd>
<sep> </sep>
<groupchoice >
<kwd >seconds</kwd>
<kwd >minutes</kwd>
<kwd >hours</kwd>
</groupchoice>
</groupcomp>

```
</groupchoice>
</groupcomp>
</groupchoice>
<sep> </sep>
<kwd >packet</kwd>
<sep> </sep>
<kwd >count</kwd>
<sep> </sep>
<kwd >number</kwd>
<sep> </sep>
<kwd >interval</kwd>
<sep> </sep>
<kwd >number</kwd>
<sep> </sep>
<groupchoice >
<kwd >milliseconds</kwd>
<kwd >seconds</kwd>
</groupchoice>
</groupcomp>
<sep> </sep>
<groupcomp importance='optional' >
<kwd >packet</kwd>
<sep> </sep>
<kwd >size</kwd>
<sep> </sep>
<kwd >bytes</kwd>
<sep> </sep>
<groupcomp importance='optional' >
<kwd >test</kwd>
<sep> </sep>
<kwd >pattern</kwd>
<sep> </sep>
<groupchoice >
<groupcomp >
```

<kwd >hex</kwd>
<sep> </sep>
<kwd >0x</kwd>
<sep> </sep>
<kwd >HHHHHHHH</kwd>
</groupcomp>
<kwd >pseudo-random</kwd>
</groupchoice>
</groupcomp>
</groupcomp>
<sep> </sep>
<kwd >domain</kwd>
<sep> </sep>
<kwd >domain_name</kwd>
<sep> </sep>
<kwd >source</kwd>
<sep> </sep>
<kwd >interface</kwd>
<sep> </sep>
<kwd >type</kwd>
<sep> </sep>
<kwd >interface-path-id</kwd>
<sep> </sep>
<kwd >target</kwd>
<sep> </sep>
<groupchoice >
<groupcomp >
<kwd >mac-address</kwd>
<sep> </sep>
<kwd >H</kwd>
<sep> </sep>
<groupcomp >
<delim>.</delim>
<kwd >H</kwd>

```
</groupcomp>
<sep> </sep>
<groupcomp >
<delim>.</delim>
<kwd >H</kwd>
</groupcomp>
<sep> </sep>
<groupcomp >
<delim>.</delim>
<kwd >H</kwd>
</groupcomp>
</groupcomp>
<groupcomp >
<kwd >mep-id</kwd>
<sep> </sep>
<kwd >id_number</kwd>
</groupcomp>
</groupchoice>
<sep> </sep>
<groupcomp importance='optional' >
<kwd >statistics</kwd>
<sep> </sep>
<kwd >measure</kwd>
<sep> </sep>
<groupchoice >
<kwd >one-way-delay-ds</kwd>
<kwd >one-way-delay-sd</kwd>
<kwd >one-way-jitter-ds</kwd>
<kwd >one-way-jitter-sd</kwd>
<kwd >round-trip-delay</kwd>
<kwd >round-trip-jitter</kwd>
</groupchoice>
<sep> </sep>
<groupcomp importance='optional' >
```

<kwd >aggregate</kwd>
<sep> </sep>
<groupchoice >
<kwd >none</kwd>
<groupcomp >
<kwd >bins</kwd>
<sep> </sep>
<kwd >number</kwd>
<sep> </sep>
<kwd >width</kwd>
<sep> </sep>
<kwd >milliseconds</kwd>
</groupcomp>
</groupchoice>
</groupcomp>
</groupcomp>
<sep> </sep>
<groupcomp importance='optional' >
<kwd >buckets</kwd>
<sep> </sep>
<groupchoice >
<groupcomp >
<kwd >archive</kwd>
<sep> </sep>
<kwd >number</kwd>
</groupcomp>
<groupcomp >
<kwd >size</kwd>
<sep> </sep>
<kwd >number</kwd>
<sep> </sep>
<groupchoice >
<kwd >per-probe</kwd>
<kwd >probes</kwd>

```
</groupchoice>
</groupcomp>
</groupchoice>
</groupcomp>
<sep> </sep>
<groupcomp importance='optional' >
<kwd >schedule</kwd>
<sep> </sep>
<groupchoice >
<kwd >now</kwd>
<groupcomp >
<kwd >at</kwd>
<sep> </sep>
<kwd >hh</kwd>
<sep> </sep>
<groupcomp >
<delim>:</delim>
<kwd >mm</kwd>
</groupcomp>
<sep> </sep>
<groupcomp importance='optional' >
<delim>.</delim>
<kwd >ss</kwd>
</groupcomp>
<sep> </sep>
<groupcomp importance='optional' >
<kwd >day</kwd>
<sep> </sep>
<groupcomp importance='optional' >
<kwd >month</kwd>
<sep> </sep>
<kwd importance='optional' >year</kwd>
</groupcomp>
</groupcomp>
```

```
</groupcomp>
<groupcomp >
<kwd >in</kwd>
<sep> </sep>
<kwd >number</kwd>
<sep> </sep>
<groupchoice >
<kwd >seconds</kwd>
<kwd >minutes</kwd>
<kwd >hours</kwd>
</groupchoice>
</groupcomp>
</groupchoice>
<sep> </sep>
<groupcomp importance='optional' >
<kwd >for</kwd>
<sep> </sep>
<kwd >duration</kwd>
<sep> </sep>
<groupchoice >
<kwd >seconds</kwd>
<kwd >minutes</kwd>
<kwd >hours</kwd>
</groupchoice>
</groupcomp>
<sep> </sep>
<groupcomp importance='optional' >
<kwd >repeat</kwd>
<sep> </sep>
<kwd >every</kwd>
<sep> </sep>
<kwd >number</kwd>
<sep> </sep>
<groupchoice >
```

<kwd >seconds</kwd>

<kwd >minutes</kwd>

<kwd >hours</kwd>

</groupchoice>

<sep> </sep>

<kwd >count</kwd>

<sep> </sep>

<kwd >probes</kwd>

</groupcomp>

</groupcomp>

<sep> </sep>

<kwd importance='optional' >asynchronous</kwd>

</groupcomp>

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.
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 mode

Command History

Release	Modification
Release 4.0.0	This command was introduced.
Release 4.3.0	The **cfm-delay-measurement-v0** option was included.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/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 280	Deletes the contents of buckets containing SLA statistics collected by all operations probes.
clear ethernet sla statistics on-demand, on page 281	Deletes the contents of buckets containing SLA statistics collected by on-demand probes.
show ethernet sla operations, on page 432	Displays information about configured Ethernet SLA operations.

Command	Description
show ethernet sla statistics, on page 435	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 mode.

ethernet sla on-demand operation type cfm-delay-measurement cfm-delay-measurement-v0probe [**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* | **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 mode

Command History

Release	Modification
Release 4.0.0	This command was introduced.
Release 4.3.0	The **cfm-delay-measurement-v0** keyword was included.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/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 280	Deletes the contents of buckets containing SLA statistics collected by all operations probes.
clear ethernet sla statistics on-demand, on page 281	Deletes the contents of buckets containing SLA statistics collected by on-demand probes.
show ethernet sla operations, on page 432	Displays information about configured Ethernet SLA operations.
show ethernet sla statistics, on page 435	Displays the contents of buckets containing Ethernet SLA metrics collected by probes.

ethernet sla on-demand operation type cfm-synthetic-loss-measurement probe

To execute an on-demand Ethernet SLA operation probe for CFM synthetic loss measurement, use the **ethernet sla on-demand operation type cfm-synthetic-loss-measurement probe** command in EXEC mode.

ethernet sla on-demand operation type cfm-synthetic-loss-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**]**synthetic loss calculation packets** *number* [**packet size** *bytes* [**test pattern hex 0x** *HHHHHHHH*]] **domain** *domain_name* **source interface** *type interface-path-id* **target mac-address H.H.H** | **mep-id** *id_number* [**statistics measure one-way-loss-sd** | **one-way-loss-ds** [**aggregate none** | **bins** *number* **width** *count*] [**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.
synthetic loss calculation packets*number*	Defines the number of packets that must be used to make each FLR calculation for synthetic loss measurements. It ranges from 10 to 12096000.
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-loss-ds**—One-way loss statistics from destination to source. • **one-way-loss-sd**—One-way loss statistics from source to destination.

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 *count*	Specifies the range of the samples to be collected within each bin in percentage points, from 1 to 100.
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 these 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 these 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 these 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 mode

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ethernet-services	execute

Example

This example shows a minimum configuration, that specifies the local domain and source interface and target MEP, using these defaults:

- Send a burst once for a packet count of 100 and interval of 100 milliseconds .
- The number of packets to be used for FLR calculation is 100.
- Measure the one way loss statistics in both the directions .
- Aggregate statistics into one bin.
- Schedule now.
- Display results on the console.

```
RP/0/RP0/CPU0:routerethernet sla on-demand operation type cfm-synthetic-loss-measurement
probe
domain D1 source interface TenGigE 0/6/1/0 target mac-address 2.3.4
```

Related Commands

Command	Description
clear ethernet sla statistics all, on page 280	Deletes the contents of buckets containing SLA statistics collected by all operations probes.
clear ethernet sla statistics on-demand, on page 281	Deletes the contents of buckets containing SLA statistics collected by on-demand probes.
show ethernet sla operations, on page 432	Displays information about configured Ethernet SLA operations.
show ethernet sla statistics, on page 435	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 {**frames** [**low** *threshold* [**thousand** | **million** | **billion**]][**high** *threshold* [**thousand** | **million** | **billion**]] | **ppm** [**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 ppm.

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 6.1.32	This command was introduced.

Usage Guidelines

The frame period window is defined in the IEEE specification as a number of received frames, in our implementation it is x milliseconds.

To obtain the number of frames, the configured time interval is converted to a window size in frames using the interface speed. For example, for a 1Gbps interface, the IEEE defines minimum frame size as 512 bits. So, we get a maximum of approximately 1.5 million frames per second. If the window size is configured to be 8 seconds (8000ms) then this would give us a Window of 12 million frames in the specification's definition of Errored Frame Window.

The thresholds for frame-period are measured in errors per million frames. Hence, if you configure a window of 8000ms (that is a window of 12 million frames) and a high threshold of 100, then the threshold would be crossed if there are 1200 errored frames in that period (that is, 100 per million for 12 million).

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.

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/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/CPU0:router(config-eoam)# link-monitor
RP/0/RP0/CPU0:router(config-eoam-lm)# frame-period threshold ppm 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 milliseconds *window* | **frames** *window*[**thousand | million | billion**]

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 milliseconds.

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 6.1.32	This command was introduced.

Usage Guidelines

The IEEE 802.3 standard defines the window size as number of frames rather than a time duration. These two formats can be converted either way by using a knowledge of the interface speed. Note that the conversion assumes that all frames are of the minimum size.

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/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/CPU0:router(config-eoam)# link-monitor
RP/0/RP0/CPU0:router(config-eoam-lm)# frame-period window milliseconds 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*]

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 3.9.0	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/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/CPU0:router(config-eoam)# link-monitor (config-eoam)#  link-monitor
RP/0/RP0/CPU0:router(config-eoam-lm)# frame-seconds threshold low 10 high 900
```

Related Commands

Command	Description
ethernet oam profile, on page 309	Creates an EOAM profile and enters EOAM configuration mode.
link-monitor, on page 346	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*

Syntax Description

window Size of the window for a frame-seconds error in milliseconds. The range is 10000 to 900000.

Note The only accepted values are multiples of the line card-specific polling interval, that is, 1000 milliseconds for most line cards.

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 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/CPU0:router(config-eoam)# link-monitor
RP/0/RP0/CPU0:router(config-eoam-lm)#
```

Related Commands

Command	Description
ethernet oam profile, on page 309	Creates an EOAM profile and enters EOAM configuration mode.
link-monitor, on page 346	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*]

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. (Optional, at least one of high and low must be specified) High threshold, in symbols, that causes a frame error event to trigger an action. The range is 1 to 12000000.

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 3.9.0	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/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/CPU0:router(config-eoam)# link-monitor
RP/0/RP0/CPU0:router(config-eoam-lm)# frame threshold low 100 high 60000
```

Related Commands

Command	Description
ethernet oam profile, on page 309	Creates an EOAM profile and enters EOAM configuration mode.
link-monitor, on page 346	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*

Syntax Description

window	Size of the window for a frame error in milliseconds. 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 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/CPU0:router(config-eoam)# link-monitor
RP/0/RP0/CPU0:router(config-eoam-lm)# frame window 60
```

Related Commands

Command	Description
ethernet oam profile, on page 309	Creates an EOAM profile and enters EOAM configuration mode.
link-monitor, on page 346	Enters Ethernet OAM link monitor configuration mode.

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 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/CPU0:router(config-eoam)# link-monitor
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/5/6
RP/0/RP0/CPU0:router(config-if)# ethernet oam
RP/0/RP0/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

Command Default

Logging is disabled.

Command Modes

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

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet cfm
RP/0/RP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/RP0/CPU0:router(config-cfm-dmn-svc)# log ais
```

Related Commands

Command	Description
ais transmission, on page 264	Configures AIS transmission for a CFM domain service.
ais transmission up, on page 266	Configures AIS transmission on a CFM interface.
show ethernet cfm interfaces ais, on page 391	Displays the information about interfaces that are currently transmitting AIS.
show ethernet cfm local meps, on page 397	Displays information about local MEPs.

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

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 3.9.0	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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet cfm
RP/0/RP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/RP0/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

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 3.9.0	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.

Note If a Local MEP is receiving Wrong Level CCMs, then a transient timeout might occur when correct Level CCMs are received again.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet cfm
RP/0/RP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/RP0/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

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 3.9.0	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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet cfm
RP/0/RP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/RP0/CPU0:router(config-cfm-dmn-svc)# log crosscheck errors
```

Related Commands

Command	Description
mep crosscheck, on page 354	Enters CFM MEP crosscheck configuration mode.
mep-id, on page 355	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

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 3.9.1	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet cfm
RP/0/RP0/CPU0:router(config-cfm)# domain D1 level 1
RP/0/RP0/CPU0:router(config-cfm-dmn)# service S1 down-meps
RP/0/RP0/CPU0:router(config-cfm-dmn-svc)# log efd
```

Related Commands

Command	Description
efd, on page 299	Enables EFD on all down MEPs in a down MEPs service.
show efd interface, on page 386	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 3.9.0	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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet cfm
RP/0/RP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/RP0/CPU0:router(config-cfm-dmn-svc)# maximum-meps 4000
```

Related Commands

Command	Description
domain, on page 297	
ethernet cfm (global), on page 303	Enters CFM configuration mode.
ethernet cfm (interface), on page 304	Enters interface CFM configuration mode.
service, on page 381	

Command	Description
show ethernet cfm configuration-errors, on page 389	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 395	Displays a list of local maintenance points.
show ethernet cfm local meps, on page 397	Displays information about local MEPs.
show ethernet cfm peer meps, on page 403	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 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet cfm
RP/0/RP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/RP0/CPU0:router(config-cfm-dmn-svc)# mep crosscheck
RP/0/RP0/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*]

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 3.9.0	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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet cfm
RP/0/RP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/RP0/CPU0:router(config-cfm-dmn-svc)# mep crosscheck
RP/0/RP0/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*

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 3.9.1	This command was introduced. This command replaces the **ethernet cfm mep** command.

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 381 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ethernet cfm
RP/0/RP0/CPU0:router(config-if-cfm)# mep domain Dm1 service Sv1 mep-id 1
```

Related Commands

Command	Description
ethernet cfm (interface), on page 304	Enters interface CFM configuration mode.
show ethernet cfm configuration-errors, on page 389	Displays information about errors that are preventing configured CFM operations from becoming active, as well as any warnings that have occurred.

mib-retrieval

mib-retrieval [**disable**]

Syntax Description

disable	Disables MIB retrieval on 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 3.9.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/5/6
RP/0/RP0/CPU0:router(config-if)# ethernet oam
RP/0/RP0/CPU0:router(config-if-eoam)# mib-retrieval
```

Related Commands

Command	Description
ethernet oam profile, on page 309	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 306	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 370	Attaches an Ethernet OAM profile to an interface.
show ethernet oam configuration, on page 417	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam interfaces, on page 424	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-onlyccm-learning**

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.
ccm-learning	[Optional] Enables CCM learning for MIPs created in this service. This must be used only in services with a relatively long CCM interval of at least 100 ms. CCM learning at MIPs is disabled by default.

Command Default

None

Command Modes

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

Command History

Release	Modification
Release 3.9.0	This command was introduced.
Release 4.3.1	The **ccm-learning** keyword 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

Related Commands

Command	Description
domain, on page 297	
ethernet cfm (global), on page 303	Enters CFM configuration mode.
service, on page 381	
show ethernet cfm configuration-errors, on page 389	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 395	Displays a list of local maintenance points.
show ethernet cfm local meps, on page 397	Displays information about local MEPs.
show ethernet cfm peer meps, on page 403	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 3.9.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/5/6
RP/0/RP0/CPU0:router(config-if)# ethernet oam
RP/0/RP0/CPU0:router(config-if-eoam)# profile Profile_1
RP/0/RP0/CPU0:router(config-if-eoam)# mode passive
```

Related Commands

Command	Description
ethernet oam profile, on page 309	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 306	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 370	Attaches an Ethernet OAM profile to an interface.

Command	Description
show ethernet oam configuration, on page 417	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam interfaces, on page 424	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**]

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 6.1.32	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/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/CPU0:router(config-eoam)# link-monitor
RP/0/RP0/CPU0:router(config-eoam-lm)# monitoring disable
```

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**]

Syntax Description

bytes	(Optional) Minimum size of the packet including padding when necessary. The range is 1 to 9000 bytes. This value refers to the total frame size including the Layer 2 or Layer 3 packet header. Optional TLVs, such as the End TLV, are only included when the requested packet size allows.
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 4.0.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet sla
RP/0/RP0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/RP0/CPU0:router(config-sla-prof)# probe
RP/0/RP0/CPU0:router(config-sla-prof-pb)# packet size 9000
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet sla
RP/0/RP0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/RP0/CPU0:router(config-sla-prof)# probe
RP/0/RP0/CPU0:router(config-sla-prof-pb)# packet size 9000 test pattern hex 0xabcdabcd
RP/0/RP0/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 read 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 mode

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

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to send an Ethernet CFM loopback message:

```
RP/0/RP0/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*

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 4.0.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet sla
RP/0/RP0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/RP0/CPU0:router(config-sla-prof)# probe
RP/0/RP0/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

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 4.0.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet sla
RP/0/RP0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/RP0/CPU0:router(config-sla-prof)# probe
RP/0/RP0/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*

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 3.9.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/5/6
RP/0/RP0/CPU0:router(config-if)# ethernet oam
RP/0/RP0/CPU0:router(config-if-eoam)# profile Profile_1
```

Related Commands

Command	Description
ethernet oam profile, on page 309	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 306	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
show ethernet oam configuration, on page 417	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam interfaces, on page 424	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-delay-measurement-v0** | **cfm-loopback** | **cfm-synthetic-loss-measurement**

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-delay-measurement-v0**: CFM delay measurement version 0 packets • **cfm-loopback**: CFM loopback packets • **cfm-synthetic-loss-measurement**: CFM synthetic loss measurement packets

Command Default

No default behavior or values

Command Modes

Ethernet SLA configuration (config-sla)

Command History

Release	Modification
Release 4.0.0	This command was introduced.
Release 4.3.0	The **cfm-delay-measurement-v0** and **cfm-synthetic-loss-measurement** keyword was introduced.

Usage Guidelines

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.

Note You can configure the Ethernet SLA profile to use Y.1731 DMM frames. The restriction of 150 configured Ethernet SLA operations for each CFM MEP is removed not only for profiles using DMM frames, but also for profiles using the other supported Y.1731 frame types, such as loopback measurement and synthetic loss measurement. For interoperability purposes, it is still possible to configure profiles to use DMM v0 frames. This is done by specifying a type of **cfm-delay-measurement-v0** on the **profile(SLA)** command. The limit of 150 configured operations for each CFM MEP still applies in this case.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet sla
RP/0/RP0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/RP0/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 | remote-loopback | 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.
remote-loopback	Requires that remote-loopback 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 behaviour or values

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 3.9.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/CPU0:router(config-eoam)# require-remote mode active
RP/0/RP0/CPU0:router(config-eoam)# require-remote mib-retrieval
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/6/5/0
RP/0/RP0/CPU0:router(config-if)# ethernet oam
RP/0/RP0/CPU0:router(config-if-eoam)# require-remote mode active disabled
RP/0/RP0/CPU0:router(config-if-eoam)# require-remote mib-retrieval disabled
RP/0/RP0/CPU0:router(config-if-eoam)# require-remote link-monitoring disabled
```

Related Commands

Command	Description
ethernet oam profile, on page 309	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 306	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 370	Attaches an Ethernet OAM profile to an interface.
action capabilities-conflict, on page 242	Configures what action is taken on an interface when a capabilities-conflict event occurs.
show ethernet oam configuration, on page 417	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam discovery, on page 420	Displays the current status of Ethernet OAM sessions.
show ethernet oam interfaces, on page 424	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**]

Daily Scheduling
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**]

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 4.0.0	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.

Note The schedule start time starts after the configuration is committed and not at the time when the operation is configured.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following examples show how to schedule operation probes in a profile:

Example 1: Weekly Scheduling on a Specified Day at a Specified Time and Duration

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet sla
RP/0/RP0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/RP0/CPU0:router(config-sla-prof)# schedule every week on Monday at 23:30 for 1 hour
```

Example 2: Daily Scheduling at a Specified Time and Duration

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet sla
RP/0/RP0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/RP0/CPU0:router(config-sla-prof)# schedule every day at 11:30 for 5 minutes
```

Example 3: Hourly Scheduling Beginning at a Specified Time

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet sla
RP/0/RP0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/RP0/CPU0:router(config-sla-prof)# schedule every 2 hours first at 13:45:01
```

Example 4: Hourly Scheduling for a Specified Duration

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet sla
RP/0/RP0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/RP0/CPU0:router(config-sla-prof)# schedule every 6 hours for 2 hours
```

Related Commands

Command	Description
send (SLA), on page 378	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**
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 4.0.0	This command was introduced.
Release 4.3.0	The statistics measurement for Y.1731 Synthetic Loss Measurement was included.

Usage Guidelines

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:

Example 1: Sending a Burst of a Number of Packets With a Specified Interval Every Specified Number of Seconds

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet sla
RP/0/RP0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/RP0/CPU0:router(config-sla-prof)# probe
RP/0/RP0/CPU0:router(config-sla-prof-pb)# send burst every 60 seconds packet count 30
interval 1 second
RP/0/RP0/CPU0:router(config-sla-prof-pb)#
```

Example 2: Sending a Burst of a Number of Packets With a Specified Interval One Time

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet sla
RP/0/RP0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/RP0/CPU0:router(config-sla-prof)# probe
RP/0/RP0/CPU0:router(config-sla-prof-pb)# send burst once packet count 2 interval 1 second

RP/0/RP0/CPU0:router(config-sla-prof-pb)#
```

Example 3: Sending a Single Packet Every Specified Number of Seconds

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet sla
RP/0/RP0/CPU0:router(config-sla)# profile  Prof1  type  cfm-loopback
RP/0/RP0/CPU0:router(config-sla-prof)# probe
```

```
RP/0/RP0/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*]]

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 or mp2mp. **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.
mp2mp *xconnect-name*	Specifies the name of the multipoint-to-multipoint cross connect and enters the Ethernet CFM domain service mode.
ce-id *ce-id-value*	Specifies the local Customer Edge (CE) identifier.
remote-ce-id *remote-ce-id-value*	Specifies the remote Customer Edge (CE) identifier.
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 3.9.0	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:

  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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet cfm
RP/0/RP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0/CPU0:router(config-cfm-dmn)# service Serv_1 down-meps
RP/0/RP0/CPU0:router(config-cfm-dmn-svc)#
```

The following example shows how to associate a p2p cross connect service to a domain and enter CFM domain service configuration mode.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet cfm
RP/0/RP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/RP0/CPU0:router(config-cfm-dmn-svc)#
```

The following example shows how to enable CFM on a multipoint-to-multipoint cross connect.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet cfm
RP/0/RP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0/CPU0:router(config-cfm-dmn)# service Cross_Connect_2 xconnect group XG2 mp2mp X2
ce-id 201 remote-ce-id 202
RP/0/RP0/CPU0:router(config-cfm-dmn-svc)#
```

Related Commands

Command	Description
domain, on page 297	Creates and names a container for all domain configurations and enter the CFM domain configuration mode.
ethernet cfm (global), on page 303	Enters Ethernet CFM configuration mode.
p2p	Enters p2p configuration mode to configure point-to-point cross-connects.
show ethernet cfm configuration-errors, on page 389	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 395	Displays all the maintenance points that have been created.
show ethernet cfm local meps, on page 397	Displays information about local MEPs.
show ethernet cfm peer meps, on page 403	Displays other MEPs detected by a local MEP.
xconnect group	Configures a cross-connect group.

show error-disable

To display the error-disabled state of interfaces, use the **show error-disable** command in the EXEC mode.

show error-disable [**recovery**] [**interface** <*interface*>]

Syntax Description

recovery	Enables error disabled recovery on an interface.
interface	Displays error-disable state for a single interface.

Command Default

This command includes all the error-disabled interfaces.

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
interface	read

Example

The following example shows how to display the error disable information.

```
show error-disable
    [ recovery ]
    [ interface <interface> ]

Interface             Error-Disable reason            Retry (s)  Time disabled
--------------------  ------------------------------  ---------  --------------
           Gi0/1/0/3  ethernet-oam-link-fault           1020000  17:12:23 04/31
           Gi0/2/0/1  ethernet-oam-critical-event           ---  20:04 04/31/06
   Gi10/11/0/12.1234  ethernet-oam-high-threshold           245  20:02:42
show error-disable trace
    [ essential | non-essential ]
```

Related Commands

Command	Description
error-disable recovery cause , on page 301	Enables error disabled recovery on an interface.
clear error-disable, on page 271	Clears all error disabled conditions on an interface.

show efd database

To display complete information about all interfaces brought down due to **EFD**, use the show efd database command in EXEC mode.

show efd database [**server**|**client**][**interface**]

Syntax Description

client	Displays all interfaces brought down by EFD filtered by a specific client protocol.
server	Displays all interfaces brought down by EFD filtered by interface owner.
interface	Displays a specific EFD state for the EFD state, if applicable.

Command Default

This command display all interfaces brought down by EFD.

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ethernet-services	read

Example

The following example shows how to display the error disable information.

```
# show efd database
Client CFM
==========
Interface         Since             Success  Msg Req  Del
-----------------------------------------------------------
GigE0/0/0/0.0     07/08/09 14:53    Yes      No       No

Server VLAN MA
==============
Interface         Clients
-------------------------
GigE0/0/0/0.0     CFM
```

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 mode

Command History

Release	Modification
Release 3.9.1	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/RP0/CPU0:router# show efd interfaces

Server VLAN MA
==============
Interface         Clients
--------------------------
GigE0/0/0/0.0     CFM
```

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 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 mode

Command History

Release	Modification
Release 3.9.0	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/RP0/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 20: 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 mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows how to display all the CFM configuration errors on all domains:

```
RP/0/RP0/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.
```

Related Commands

Command	Description
ethernet cfm (global), on page 303	Enters CFM configuration mode.
ethernet cfm (interface), on page 304	Enters interface CFM configuration mode.
traceroute ethernet cfm, on page 451	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 mode

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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/RP0/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 21: 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 264	Configures AIS transmission for a CFM domain service.
log ais, on page 347	Configures AIS logging for a CFM domain service to indicate when AIS or LCK packets are received.
ais transmission up, on page 266	Configures AIS transmission on a CFM interface.
show ethernet cfm local meps, on page 397	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 mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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/RP0/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 22: 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 273	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 mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ethernet-services	read

Examples

This example shows how to display maintenance points:

```
RP/0/RP0/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 23: 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 397	Displays information about local MEPs.
show ethernet cfm peer meps, on page 403	Displays information about maintenance end points (MEPs) for peer MEPs.
traceroute cache, on page 450	Sets the maximum limit of traceroute cache entries or the maximum time limit to hold the traceroute cache entries.
traceroute ethernet cfm, on page 451	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 mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.
Release 3.9.1	New output fields were added for AIS.

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

Example 1: show ethernet cfm local meps Command

This example shows sample output of the default statistics for local MEPs without any filtering:

```
RP/0/RP0/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 24: 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.

Example 2: show ethernet cfm local meps Command Filtered by Domain and Service

```
RP/0/RP0/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
```

Example 3: show ethernet cfm local meps detail Command

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/RP0/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
```

Example 4: show ethernet cfm local meps verbose Command

This example shows sample output of detailed statistics for local MEPs:

```
RP/0/RP0/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)
  EFD triggered:           No

  Packet        Sent      Received
  ------  ----------  ----------------------------------------------------
  AIS           5576             0
  SLM              0            11
  SLR             11             0
  DMM              0             6
  DMR              5             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 errors: 0 missing (0 auto), 0 unexpected

  CCM generation enabled:  Yes, 1s (Remote Defect detected: Yes)
                             CCM processing offloaded to software
  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
  LMM              3             4
  LMR              5             3

Domain gaz (level 4), Service baz
Up MEP on Standby Bundle-Ether 1, MEP-ID 3
================================================================================
  Interface state: Up      MAC address: 6655.4433.2211
  Peer MEPs: 1 up, 0 with errors, 0 timed out (archived)

  CCM generation enabled:  Yes, 1s (Remote Defect detected: No)
                             CCM processing offloaded to software
)
                           Sending disabled on local standby MEP
  CCM defects detected:    Defects below ignored on local standby MEP
                           I - Wrong interval
                           V - Wrong level
```

```
  AIS generation enabled:  No
  Sending AIS:             No
  Receiving AIS:           No

  Packet        Sent      Received
  ------  ----------  ------------------------------------------------------------
  CCM              0         67890  (out of seq: 6, discarded: 10)
  LBM              0             1
  LBR              0             2  (out of seq: 0, with bad data: 0)
  AIS              0             3
  LCK              -             4

Domain bar (level 3), Service boz
Down MEP on GigabitEthernet102/1/0/0.345, MEP-ID 200
================================================================================
  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

  No packets sent/received
```

Related Commands

Command	Description
show ethernet cfm local maintenance-points, on page 395	Displays a list of local maintenance points.
show ethernet cfm peer meps, on page 403	Displays information about maintenance end points (MEPs) for peer MEPs.
traceroute ethernet cfm, on page 451	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 mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

If a Local MEP is receiving Wrong Level CCMs, and if the Remote MEP has its CCM processing offloaded, then the last CCM cannot be displayed.

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows sample output of MEPs detected by a local MEP:

```
RP/0/RP0/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 25: 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/RP0/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
   Received CCM handling offloaded to software
   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 26: 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.
Offload status	Offload status of received CCM handling.

Related Commands

Command	Description
show ethernet cfm local maintenance-points, on page 395	Displays a list of local maintenance points.
show ethernet cfm local meps, on page 397	Displays information about local MEPs.
traceroute ethernet cfm, on page 451	Sends Ethernet CFM traceroute messages to generate a basic.

show ethernet cfm summary

To display summary information about CFM, use the **show ethernet cfm summary** command in the EXEC mode.

show ethernet cfm summary location*node-id*

Syntax Description

location *node-id*	(Optional) Specifies the location for which CFM summary is required. If the location is not specified, an overall summary for all nodes is displayed, followed by information for each node. If the location is specified, only information from that node is displayed.

Command Default

An overall summary for all nodes is displayed.

Command Modes

EXEC mode

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ethernet-services	read

Example

This example shows how to display ethernet CFM summary:

```
RP/0/RP0/CPU0:router# show ethernet cfm summary

CFM System Summary
==================

Domains                                4
Services                           10000
Local MEPS                         10000
  Operational                       9997
    Down MEPs                       9997
    Up MEPs                            0
    Offloaded                        200
      3.3ms                          100
      10ms                           100
  Disabled (misconfiguration)          2
  Disabled (resource limit)            1
  Disabled (operational error)         0
Peer MEPs                          9997
  Operational                      9990
    Defect detected                    5
    No defect detected              9985
  Timed out                            7
MIPs                                   0
```

```
Interfaces                          10000
Bridge domains/Xconnects            10000
Traceroute Cache entries                3
Traceroute Cache replies               11
CCM Learning Database entries       10000


CFM Summary for 0/0/CPU0
========================

Initial resynchronization: complete

Domains                                 4
Services                            10000
Local MEPS                           1000
  Operational                         999
    Down MEPs                         999
    Up MEPs                             0
    Offloaded                         100
      3.3ms                           100
      10ms                              0
  Disabled (misconfiguration)           1
  Disabled (offload resource limit)     0
  Disabled (operational error)          0
Peer MEPs                            999
  Operational                        998
    Defect detected                    2
    No defect detected               996
  Timed out                            1
MIPs                                   0
Interfaces                           1000
Bridge domains/Xconnects            10000
Traceroute Cache entries                1
Traceroute Cache replies                3
CCM Learning Database entries        1000
```

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 mode

Command History

Release	Modification
Release 3.9.0	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/RP0/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 27: 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.
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.

Field	Description
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.
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/RP0/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 450	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 278	Removes the contents of the traceroute cache.
traceroute ethernet cfm, on page 451	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 mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.
Release 4.0.0	The “Uni-directional link-fault detection enabled” output field was added. 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/RP0/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/RP0/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 420	Displays the current status of Ethernet OAM sessions.
show ethernet oam statistics, on page 426	Displays the local and remote Ethernet OAM statistics for interfaces.
show ethernet oam interfaces, on page 424	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 mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/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/RP0/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 417	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam statistics, on page 426	Displays the local and remote Ethernet OAM statistics for interfaces.
show ethernet oam interfaces, on page 424	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

No specific guidelines impact the use of this command.

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/RP0/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 417	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam discovery, on page 420	Displays the current status of Ethernet OAM sessions.
show ethernet oam interfaces, on page 424	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 mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows how to display the current state for all Ethernet OAM interfaces:

```
RP/0/RP0/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 28: 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.
EFD triggered	Indicates if an Ethernet Fault Detection (EFD) event has occurred on the interface and the type of fault that triggered the interface to be moved to the down state for the line protocol. The possible EFD trigger events are: • capabilities-conflict • discovery-timeout • • session-down • wiring-conflict

Related Commands

Command	Description
show ethernet oam configuration, on page 417	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam discovery, on page 420	Displays the current status of Ethernet OAM sessions.
show ethernet oam statistics, on page 426	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 mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/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 417	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam discovery, on page 420	Displays the current status of Ethernet OAM sessions.
show ethernet oam interfaces, on page 424	Displays the current state of Ethernet OAM interfaces.

show ethernet oam summary

To display the summary of all the active OAM sessions across all the interfaces, use the **show ethernet oam summary** command in EXEC mode.

The summary output hides the fields for which the field count is zero (0).

show ethernet oam summary

Command Default

This command displays summary of all the active OAM sessions for all the interfaces.

Command Modes

EXEC mode

Command History

Release	Modification
Release 5.2.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows how to display the summary for all the active OAM sessions across all the interfaces.

```
Router#show ethernet oam summary
Wed Apr 29 09:32:19.874 PDT
Link OAM System Summary
=======================
Profiles:                               1
Interfaces:                             4
  Interface states
    Port down:                          4
    Passive wait:                       0
    Active send:                        0
    Operational:                        0
     Loopback mode:                     0
  Miswired connections:                 1
Events:                                 0
  Local:                                0
    Symbol period:                      0
    Frame:                              0
    Frame period:                       0
    Frame seconds:                      0
  Remote:                               0
    Symbol period:                      0
    Frame:                              0
    Frame period:                       0
    Frame seconds:                      0

Event Logs
================================================================================
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

Interface           Time                       Type           Loc'n  Action
------------------- -------------------------- -------------- ------ ------
Gi0/0/0/0           Wed Apr 29 08:56:54 PDT    Dying gasp     Local  Err.D
Gi0/0/0/0           Wed Apr 29 08:56:54 PDT    Link fault     Remote Err.D
Gi0/0/0/1           Wed Apr 29 08:56:51 PDT    Dying gasp     Local  Err.D
Gi0/0/0/1           Wed Apr 29 08:56:51 PDT    Link fault     Remote Err.D
Gi0/0/0/2           Wed Apr 29 08:56:50 PDT    Dying gasp     Local  Err.D
Gi0/0/0/2           Wed Apr 29 08:56:50 PDT    Dying gasp     Remote Err.D
Gi0/0/0/3           Wed Apr 29 08:56:46 PDT    Dying gasp     Local  Err.D
Gi0/0/0/3           Wed Apr 29 08:56:46 PDT    Link fault     Remote Err.D
```

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 mode

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/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 mode

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

Examples

The following example shows how to display information about configured SLA operations in brief:

```
RP/0/RP0/CPU0:router# show ethernet sla operations

Profile               Instance
--------------------  ------------------------------------------------------------
gold                  Gi0/0/0/0, dom d,     to MEP-ID 200                       !
business-gold         Gi0/0/0/0, dom mydom, to 00ab.cdef.1234
business-gold         Gi0/0/0/0, dom mydom, to MEP-ID 2
```

Note If the SLA operation has a configuration error, an exclamation point (!) is displayed at the end of the line in the command output.

The following example shows how to display information about configured SLA operations in detail:

```
RP/0/RP0/CPU0:router# show ethernet sla operations detail

Source: Interface GigabitEthernet0/0/0/0, Domain d
Destination: Target MEP-ID 200
================================================================================
Profile 'gold'
Profile is not configured

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/RP0/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/RP0/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 mode

Command History

Release	Modification
Release 4.0.0	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/RP0/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/RP0/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/RP0/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/RP0/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/RP0/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 269	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*

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 4.0.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ethernet cfm
RP/0/RP0/CPU0:router(config-if-cfm)# mep domain Dm1 service Sv1 mep-id 1
```

```
RP/0/RP0/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 403	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 mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

If a Local MEP is receiving Wrong Level CCMs, then a transient timeout might occur when correct Level CCMs are received again.

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/RP0/CPU0:router #configure
RP/0/RP0/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 mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router# configure
RP/0/RP0/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 4.0.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet sla
RP/0/RP0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RP/0/RP0/CPU0:router(config-sla-prof)# statistics measure round-trip-delay
RP/0/RP0/CPU0:router(config-sla-prof-stat-cfg)#
```

Related Commands

Command	Description
ethernet sla, on page 310	Enters the Ethernet SLA configuration mode.
profile (SLA), on page 371	Creates an SLA operation profile and enter the SLA profile configuration mode.

symbol-period threshold

To configure the thresholds that trigger an Ethernet OAM symbol-period error event, use the **symbol-period threshold** command in Ethernet OAM link monitor configuration mode. To return the threshold to the default value, use the **no** form of this command.

symbol-period threshold low *threshold* [**high** *threshold*]

Syntax Description

low *threshold*	Low threshold value, in symbols, that triggers a symbol-period error event. The range is 0 to 60000000.
high *threshold*	(Optional) High threshold value, in symbols, that triggers a symbol-period error event. The range is 0 to 60000000. The high threshold value can be configured only in conjunction with the low threshold value.

Command Default

The default low threshold is 1 symbol.

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 3.9.0	This command was introduced.
Release 6.1.2	Allowed high threshold without low threshold. Added choice of units.

Usage Guidelines

When the low threshold is passed, a symbol-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 symbol-period low and high thresholds that trigger a symbol-period error event:

```
Router(config)# ethernet oam profile Profile_1
Router(config-eoam)# link-monitor
Router(config-eoam-lm)# symbol-period threshold low 100 high 6000
```

symbol-period window

To configure the window size for an Ethernet OAM symbol-period error event, use the **symbol-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.

symbol-period window *window*

Syntax Description

window	Size of the window for symbol-period error in milliseconds. The range is 1000 to 60000.

Command Default

The default value is 1000 milliseconds.

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 3.9.0	This command was introduced.

Usage Guidelines

The IEEE 802.3 standard defines the window size as a number of symbols rather than a time duration. These two formats can be converted either way by using a knowledge of the interface speed and encoding.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the window size for a symbol-period error.

```
RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RP0/CPU0:router(config-eoam)# link-monitor
RP/0/RP0/CPU0:router(config-eoam-lm)# symbol-period window 60000
```

synthetic loss calculation packets

To configure the number of packets that must be used to calculate each Frame Loss Ratio (FLR) calculation, use the **synthetic loss calculation packets** command in the Ethernet SLA profile probe configuration mode.

synthetic loss calculation packets *number*

Syntax Description

number	Specifies the number of packets that must be used to calculate each FLR. The range is 10 – 12096000.

Note The value must be a divisor of the number of packets per probe. If bursts are configured, the value must be a multiple of the number of packets per burst.

Command Default

The default value is the number of packets in the probe, that is each probe results in a single FLR calculation.

Command Modes

SLA profile probe configuration (config-sla-prof-pb)

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

The **synthetic loss calculation packets** command can only be configured for packet types that support synthetic loss measurement.

Note An FLR value is calculated for each discrete block of packets. For instance, if a value of 10 is configured, then the first FLR value is calculated based on packets 0 to 9, the second FLR value is calculated based on packets 10 to 19, and so on.

Task ID

Task ID	Operation
ethernet-services	read, write

Example

This example shows how to configure the number of packets to be used to calculate FLR using the **synthetic loss calculation packets** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet sla
RP/0/RP0/CPU0:router(config-sla)# profile  Prof1  type  cfm-synthetic-loss-measurement
RP/0/RP0/CPU0:router(config-sla-prof)# probe
RP/0/RP0/CPU0:router(config-sla-prof-pb)# synthetic loss calculation packets 1250
```

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*

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 3.9.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ethernet cfm
RP/0/RP0/CPU0:router(config-cfm)# traceroute cache hold-time 1 size 3000
```

Related Commands

Command	Description
ethernet cfm (global), on page 303	Enters CFM configuration mode.
traceroute ethernet cfm, on page 451	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 mode

Command History

Release	Modification
Release 3.9.0	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/RP0/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 450	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 278	Removes the contents of the traceroute cache.
show ethernet cfm traceroute-cache, on page 411	Displays the contents of the traceroute cache.

Global Interface Commands

This module describes the global command line interface (CLI) commands for configuring interfaces on the Cisco CRS Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

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 2.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router# interface TenGigE 0/4/1/0
RP/0/RP0/CPU0:router# bandwidth 4000000
```

Related Commands

Command	Description
shutdown (global), on page 479	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 2.0	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
basic-services	read, write

Examples

This example shows how to use the **clear interface** command to clear the loopback interface 2:

```
RP/0/RP0/CPU0:router# clear interface loopback 2
```

Related Commands

Command	Description
shutdown (global), on page 479	Disables an interface (forces an interface to be administratively down).

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*]]

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 2.0	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/RP0/CPU0:router(config)# interface TenGigE 0/4/0/0
RP/0/RP0/CPU0:router(config-if))# dampening
```

Related Commands

Command	Description
show im dampening, on page 466	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*

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 2.0	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 **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).

Until Release 6.5.1, when you create an interface with some configurations, upon router or interface reload, interface configurations are lost. From Release 6.5.1, onwards, automatic shutdown config behavior is persistent and no shutdown configs are lost on interface or router reload.

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/RP0/CPU0:router(config)# interface POS 0/2/0/1
```

Related Commands

Command	Description
clear interface, on page 457	Clears interface statistics or packet counters.
shutdown (global), on page 479	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*

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 2.0	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 encapsulations 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.

Note For the 10x10GigE CPAK (10 ports with only 8 profiles), it is not possible to support 10 different MTUs on 10 different 10GigE ports. One of the profiles needs to be reserved for the default MTU, in case you need to change the configured MTU back to the default MTU. Therefore on the 10x10g CPAK, you can configure different MTU sizes on 7 ports and the other 3 ports have the default MTU size. If you configure the 8th port, the configuration command succeeds but an error appears on the console.

Task ID

Task ID	Operations
interface	read, write

Examples

In this example, the MTU value for all interfaces is verified. The MTU value is shown in the next-to-last column:

```
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface TenGigE 6/0/0/0
RP/0/RP0/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/RP0/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 479	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 2.0	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/RP0/CPU0:router(config)# interface TenGigE 0/4/0/0
RP/0/RP0/CPU0:router(config-if)# no shutdown
RP/0/RP0/CPU0:router(config-if)# dampening
```

```
RP/0/RP0/CPU0:router# show im dampening

Interface               Proto              Caps               Penalty Suppressed

---------               -----              ----               ----------------
TenGigE0/4/0/0              0                 0                   0       NO

RP/0/RP0/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/RP0/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/RP0/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/RP0/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 29: 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 459	Turns on event dampening.
shutdown (global), on page 479	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 2.0	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.
Release 4.0.0	Added QoS drops to total input drops and total output drops statistics.

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/RP0/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/RP0/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/RP0/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/RP0/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/RP0/CPU0/0          up          up               ARPA  1514     100000
     Mg0/RP0/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 30: 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.
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.
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.

Field	Description
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.
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.

Field	Description
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.
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 terminated 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.
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.

Field	Description
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

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 2.0	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/RP0/CPU0:router(config)# interface TenGigE 0/4/0/2
RP/0/RP0/CPU0:router(config-if)# shutdown
```

Related Commands

Command	Description
show interfaces, on page 469	Displays statistics for all interfaces configured on the router or on a specific node.
show ip interface	Displays IPv4 interface status and configuration.

Internal Ethernet Control Network Commands

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

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

clear controller backplane ethernet clients

To clear the aggregate client statistics of traffic sent and received over the control Ethernet, use the **clear controller backplane ethernet clients** command in administration EXEC mode.

clear controller backplane ethernet clients client-id statistics | all statistics location *node-id*

Syntax Description

client-id	Client ID. Range is from 1 through 33.
statistics	Clears a list of client statistics for the specified client ID.
all	Clears a list of all client applications and their IDs.
location *node-id*	Clears the node or the controller information. **Note** Use the **show platform** command to see a list of all nodes currently in the system.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced. This command replaces the **clear controller backplane ethernet location statistics** command.

Usage Guidelines

Enter the **location** *node-id* argument in the *rack*/*slot*/*module* notation.

Task ID

Task ID	Operations
system	execute

Examples

The following example shows how to clear client statistics for client ID 1 on the node at 0/1/1:

```
RP/0/RP0/CPU0:router(admin)# clear controller backplane ethernet clients 1 statistics
location 0/1/1
```

The following example shows how to clear all client statistics on the node at 0/1/1:

```
RP/0/RP0/CPU0:router(admin)# clear controller backplane ethernet clients all statistics
location 0/1/1
```

Related Commands

Command	Description
show controllers backplane ethernet clients, on page 487	Displays information about client applications in a particular location.
show controllers backplane ethernet detail, on page 492	Displays detailed information about the backplane interfaces in a particular location.

clear controller backplane ethernet statistics

To clear the aggregate statistics of traffic sent and received over the control Ethernet, use the **clear controller backplane ethernet statistics** command in administration EXEC mode.

clear controller backplane ethernet statistics location *node-id*

Syntax Description

location *node-id*	Clears the node of statistics. **Note** Use the **show platform** command to see a list of all nodes currently in the system.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced. This command replaces the **clear controller backplane ethernet location statistics** command.

Usage Guidelines

No specific guidelines impact the use of this command.

Enter the **location** *node-id* argument in the *rack*/*slot*/*module* notation.

Task ID

Task ID	Operations
system	execute

Examples

The following example shows how to clear all statistics on the node at 0/1/1:

```
RP/0/RP0/CPU0:router(admin)# clear controller backplane ethernet statistics location 0/1/1
```

Related Commands

Command	Description
show controllers backplane ethernet brief, on page 485	Displays brief information about backplane Ethernet interfaces in a particular location.

show controllers backplane ethernet brief

To display brief information about backplane Ethernet interfaces in a particular location, use the **show controllers backplane ethernet brief** command in administration EXEC mode.

show controllers backplane ethernet brief location *node-id*

Syntax Description

location *node-id*	Displays brief backplane Ethernet information for a specified location. **Note** Use the **show platform** command to see a list of all nodes currently in the system.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced. This command replaces the **show controllers backplane ethernet local brief** and **show controllers backplane ethernet location brief** commands.

Usage Guidelines

Enter the **location** *node-id* argument in the *rack*/*slot*/*module* notation.

Task ID

Task ID	Operations
fabric	read
system	read

Examples

The following example shows the output from the **show controllers backplane ethernet brief** command:

```
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet brief location 0/1/0

FastEthernet0_0_CPU0 (local) is up, MTU 1514 bytes
    57569 packets input, 5999749 bytes
    36963 packets output, 4105673 bytes
```

Table 31: show controllers backplane ethernet brief Field Descriptions

Field	Description
MTU	Maximum packet size, in bytes, that a particular interface can handle.
packets input	Total number of packets received.

Field	Description
packets output	Total number of packets transmitted.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets transmitted by the system.

Related Commands

Command	Description
show controllers backplane ethernet clients, on page 487	Displays information about client applications in a particular location.
show controllers backplane ethernet detail, on page 492	Displays detailed information about the backplane interfaces in a particular location.
show controllers backplane ethernet manageability bridge list, on page 504	Displays the CE bridges distributed across a Cisco CRS system.

show controllers backplane ethernet clients

To display information about client applications in a particular location, use the **show controllers backplane ethernet clients** command in administration EXEC mode.

show controllers backplane ethernet clients *client-id* **statistics** | **all location** *node-id*

Syntax Description

client-id	Client ID. Range is from 1 through 33.
statistics	Displays a list of client statistics for the specified client ID.
all	Displays a list of all client applications and their IDs.
location *node-id*	Displays a list of all client applications and their IDs for a specified location. **Note** Use the **show platform** command to see a list of all nodes currently in the system.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced. This command replaces the **show controllers backplane ethernet local clients** and **show controllers backplane ethernet location clients** commands.

Usage Guidelines

Enter the **location** *node-id* argument in the *rack/slot/module* notation.

Task ID

Task ID	Operations
fabric	read
system	read

Examples

The following example shows the output from the **show controllers backplane ethernet clients** command, which displays detailed statistics for a specified backplane client application:

```
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet clients 2 statistics
location 0/rp0/cpu0

  Client GSP, ES Client Id 2, PID 127057 running on FastEthernet0_RP0_CPU0
    LWM calls 1 open, 0 close, 0 close callback, 0 unblocks
    1610 packets input, 531492 bytes
    1601 packets delivered,518082 bytes
    0 packets discarded (0 bytes) in garbage collection
    0 (0 bytes) unicast packets filtered
    9 (3750 bytes) multicast packets filtered
    0 (0 bytes) buffer mgmt policy discards
```

```
    0 (0 bytes) locking error discards
    0 packets waiting for client

    1846 packets output, 905259 bytes, 0 could not be transmitted
    Packets output at high priority : 251
    Packets output at med  priority : 0
    Packets output at low  priority : 1595
    Out-of-packet write rejects (high) : 0
    Out-of-packet write rejects (med ) : 0
    Out-of-packet write rejects (low ) : 0
    DMA write rejects (high) : 0
    DMA write rejects (med ) : 0
    DMA write rejects (low ) : 0

    Async calls open 1, close 0 (Number of async open calls by the client with eth_server)

    Rx pkts at high level : produced 246, lipc 0, depth 0, drops 0 (Rx packets produced,
consumed, queue depth, drops at various levels)
    Rx pkts at high level : consumed 246, fails 0, wakeups 240
    Rx pkts at med  level : produced 0, lipc 0, depth 0, drops 0
    Rx pkts at med  level : consumed 0, fails 0, wakeups 0
    Rx pkts at low  level : produced 1355, lipc 0, depth 0, drops 0
    Rx pkts at low  level : consumed 1355, fails 0, wakeups 1032

    Rx mem score 0, alloc fails 0, free fails 0      (Rx mem score for this client, alloc
free fails)
    Rx mem threshold exceeded rejects 0, mutex lock fails 0 (Rx mem drops due to non-avail
 of buffers, mutex lock fails)

    Tx pkts at high level : produced 251, depth 0, fails 0, drops 0 (Tx packets produced,
consumed, queue depth, drops at various levels)
    Tx pkts at high level : consumed 251, drops 0, wakeups 251
    Tx pkts at med  level : produced 0, depth 0, fails 0, drops 0
    Tx pkts at med  level : consumed 0, drops 0, wakeups 0
    Tx pkts at low  level : produced 1595, depth 0, fails 0, drops 0
    Tx pkts at low  level : consumed 1595, drops 0, wakeups 1110

   Tx mem score 0, server held 0, alloc fails 0, free fails 0 (Tx mem score for this client,
 alloc free fails)
    Tx mem threshold exceeded rejects 0, mutex lock fails 0
```

Table 32: show controllers backplane ethernet clients Field Descriptions (For a Specified Client)

Field	Description
Client GSP	Name of the Ethernet server client.
ES Client Id *number*	Numerical identifier of the Ethernet server client.
PID *number* running on Fast Ethernet *location*	Process identifier of the Ethernet server client.
LWM calls	Number of corresponding lightweight messaging (LWM) calls performed by the client.
packets input, bytes	Total packet bytes received by the Ethernet server for this client.
packets delivered, bytes	Total packet bytes delivered by the Ethernet server to the client.

Field	Description
packets discarded (bytes) in garbage collection	Number of packets and packet bytes discarded because the client did not pick up the packet in 10 seconds.
(bytes) unicast packets filtered	Number of unicast packets and unicast packet bytes not destined for this client.
(bytes) multicast packets filtered	Number of multicast packets and multicast packet bytes not destined for this client.
(bytes) buffer mgmt policy discards	Number of packets and packet bytes dropped because the client used too many Ethernet server buffers.
(bytes) locking error discards	Number of packets and packet bytes discarded because of locking error discards.
packets waiting for client	Number of packets waiting to be picked up by the client.
packet output, bytes	Number of packets and packet bytes output by the Ethernet server for this client.
could not be transmitted	Number of packets that could not be transmitted by the Ethernet server for this client.
Packets output at high, medium, low priority	Number of packets output at high, medium, and low priorities.
Out-of-packet write rejects (high, medium, low)	Number of packet write failures at high, medium, and low priorities.
DMA write rejects (high, medium, low)	Number of packet write failures by the driver at high, medium, and low priorities.
Async calls open, close	Number of asynchronous calls performed by the client.
Rx pkts at high, med, low levels (produced, consumed, queue depth, drops at various levels)	Number of packets received by the Ethernet server and produced onto the queueing and dispatching (QAD) queue for the client. Also, number of packets consumed by the client, depth off the queue, and dropped.
Rx pkts at high, med, low levels (consumed, fails, wakeups)	Number of packets consumed by the client from the QAD queue. Also, number of packets that failed and number of wakeups.
Rx mem score	Number of buffers currently held by the client on the receive side.
alloc fails	Number of receive allocation failures for the client.
free fails	Number of free failures for the client.
Rx mem threshold exceeded rejects	Number of packets dropped because the client exceeded its threshold.
mutex lock fails	Number of mutex lock failures on the receive side.

Field	Description
Tx pkts at high, med, low levels (produced, depth, fails, drops)	Number of packets enqueued onto the QAD queue by the client. Also, the depth off the queue and number of packets that failed and were dropped.
Tx pkts at high, med, low levels (consumed, drops, wakeups)	Number of packets dequeued from the QAD queue by the Ethernet server. Also, number of packets that were dropped and number of wakeups.
Tx mem score	Number of buffers currently held by the client on the transmit side.
server held	Number of packets given by the client and not yet transmitted by the Ethernet server.
alloc fails	Number of allocation failures for the client on the transmit side.
free fails	Number of free failures on the transmit side.
Tx mem threshold exceeded rejects	Number of transmit packet failures because the client exceeded its quota.
mutex lock fails	Number of mutex lock failures on the transmit side.

The following example shows the output from the **show controllers backplane ethernet clients** command, which displays a summary of statistics for all of the backplane client applications:

```
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet clients all location
0/0/CPU0

    Intf           Client ethernet         Client              Description
    Name              server id            Process Id
-------------------------------------------------------------------------------
 FE0_0_CPU0              1                  12307          QNX network manager
                         2                  28726               Group services
                         3                      0          Reserved for Attach
                         4                      0            Plugin controller
                         5                      0                Designated SC
                         6                      0                HFR H/W diags
                         7                      0            IP packet handler
                         8                  16415        Redundancy controller
                         9                      0          HFR Virtual console
                        10                  12312         HFR Virtual terminal
                        11                  12305        Control ethernet echo
                        12                      0       Control eth echo reply
                        13                      0  Card Configuration Protocol
                        14                      0          Reserved for Attach
                        15                      0           Chassis controller
                        16                      0            Forwarding driver
                        17                  16414                    MBI hello
                        18                      0       MBI Boot Server Source
                        19                      0                HSR ES client
                        20                      0           Test application 1
                        21                      0           Test application 2
                        22                      0      Test client out-of-band
```

Table 33: show controllers backplane ethernet clients Field Descriptions (For All Clients)

Field	Description
Intf Name	Identifies the Ethernet interface.
Client ethernet server id	Identifies the Ethernet server for the specified interface.
Client process id	Identifies the client process running on the specified interface.
Description	Describes the backplane client application.

Related Commands

Command	Description
show controllers backplane ethernet brief, on page 485	Displays brief information about backplane Ethernet interfaces in a particular location.
show controllers backplane ethernet detail, on page 492	Displays detailed information about the backplane interfaces in a particular location.
show controllers backplane ethernet manageability bridge list, on page 504	Displays the CE bridges distributed across a Cisco CRS system.

show controllers backplane ethernet detail

To display detailed information about the backplane interfaces in a particular location, use the **show controllers backplane ethernet detail** command in administration EXEC mode.

show controllers backplane ethernet detail location *node-id*

Syntax Description

location *node-id*	Displays detailed information about backplane interfaces for a specified location. **Note** Use the **show platform** command to see a list of all nodes currently in the system.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced. This command replaces the **show controllers backplane ethernet local detail** and **show controllers backplane ethernet location detail** commands.

Usage Guidelines

Enter the **location** *node-id* argument in the *rack*/*slot*/*module* notation.

Task ID

Task ID	Operations
fabric	read
system	read

Examples

The following example shows the output from the **show controllers backplane ethernet detail** command:

```
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet detail location 0/rp0/cpu0

FastEthernet0_RP0_CPU0 is up
  Hardware is 10/100 Ethernet, H/W address is 5246.4800.0201
  Internet address is 10.0.2.1
  MTU 1514 bytes
  Encapsulation HFRIES (Platform Internal Ethernet Server)
  Mode : Full Duplex,  Rate : 100Mb/s
    11576 packets input, 809064 bytes, 0 total input drops
    11346 driver inputs,11175 driver callbacks
    0 packets discarded (0 bytes) in garbage collection
    12 packets discarded (5784 bytes) in recv processing
    0 incomplete frames discarded
    0 packets discarded due to bad headers
    0 packets waiting for clients
    0 packets waiting on Rx
    Packets waiting at high priority : 0
    Packets waiting at med  priority : 0
```

```
    Packets waiting at low  priority : 0
    Received 3 broadcast packets, 54 multicast packets
    Input errors: 0 CRC, 0 overrun, 0 alignment, 0 length, 0 collision
    12105 packets output, 17021692 bytes, 0 total output drops
    Output 0 broadcast packets, 555 multicast packets
    Output errors: 0 underruns, 0 aborts, 0 loss of carrier
    Write rejects : 0
    Rx mem score 1000, alloc fails 0, free fails 0, retrieved buffers 0 (memory score on
Rx side, 1000 is expected, alloc, free fails on Rx side)
    Rx mem threshold exceeded rejects 0, mutex lock fails 0 (Memory threshold exceeded due
 to lack of buffers on Rx)
    Tx mem score 1, server held 0, alloc fails 0, free fails 0 (memory score on Tx side)
    Tx mem threshold exceeded rejects 0, mutex lock fails 0, retrieved buffers 0
    Tx quota for         high :  100  med  :  100  low  :  799  (Buffer quota on tx side,
expected is  arnd 100, 100, 800)
    Tx waits for         high :    0  med  :    0  low  :    0 (tx stalls (lwm+qad) due to
 non-avail of buffers)
    Tx (QAD) waits for   high :    0  med  :    0  low  :    0 (tx stalls (qad only))
    Tx (QAD) wakeups for high :  146  med  :    0  low  :   22 (tx wakeups)
```

Table 34: show controllers backplane ethernet detail Field Descriptions

Field	Description
FastEthernet*node* is *status*	Status of the node, which can be up or down.
Hardware	Hardware type, followed by the hardware address.
Internet address	IP address of the interface.
MTU	Maximum packet size, in bytes, that a particular interface can handle.
Encapsulation	Encapsulation method assigned to the interface.
Mode	Operating mode of the interface, followed by transmission data.
packets input	Total number of packets received.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
total input drops	Total number of packets dropped from the input queue because the queue was full.
driver inputs	Number of packets input inside the software driver.
driver callbacks	Number of callback invocations by the software driver.
packets discarded (bytes) in garbage collection	Number of packets and bytes discarded.
packets discarded (bytes) in recv processing	Number of packets and bytes discarded.
incomplete frames discarded	Number of incomplete frames dropped in the receive direction.
packets discarded due to bad headers	Number of packets dropped because of bad headers.

Field	Description
packets waiting for clients	Number of packets to be picked up by the client.
packets waiting on Rx	Number of packets to be processed by the Ethernet server.
Packets waiting at high/med/low priority	Number of high-, medium-, and low-priority packets to be processed by the Ethernet server.
Received broadcast packets, multicast packets	Total number of broadcast and multicast packets received by the interface.
Input errors	Number of errors received by the interface. Input errors occur when incoming cells are dropped or corrupted. The possible input errors are as follows: • CRC—Number of times that the checksum calculated from the data received did not match the checksum from the transmitted data. • overrun—Number of times that the receiver hardware was incapable of handing received data to a hardware buffer because the input rate exceeded the receiver's capability to handle the data. • alignment—Number of nonoctets received. • length—Number of times the interface prevented the ASIC from overrunning a maximum transmission unit (MTU) size. • collision—Number of messages retransmitted because of an Ethernet collision.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets transmitted by the system.
total output drops	Total number of packets dropped from the output queue because the queue was full.
Output broadcast packets, multicast packets	Total number of broadcast and multicast packets transmitted by the interface.
Output errors	Number of errors transmitted on the interface. Output errors occur when outgoing cells are dropped or corrupted. The possible types output errors are as follows: • underruns—Number of times that the far-end transmitter has been running faster than the near-end receiver can handle. • aborts—Number of illegal sequences of one bits on the interface. • loss of carrier—Number of times the interface was reset because the carrier detect line of that interface was up, but the line protocol was down.
Write rejects	Number of software driver errors on the transmit side.
Rx mem score	Number of overall outstanding Ethernet server receive buffers.

Field	Description
alloc fails	Number of allocation failures in the receive direction.
free fails	Number of free failures in the receive direction.
retrieved buffers	Number of receive buffers retrieved.
Rx mem threshold exceeded rejects	Number of receive buffer rejects because of a threshold overrun.
mutex lock fails	Number of mutex lock failures in the receive direction.
Tx mem score	Number of outstanding transmit buffers for all clients.
server held	Number of buffers, with packets not yet transmitted, held by the Ethernet server.
alloc fails	Number of allocation failures in the transmit direction.
free fails	Number of free failures in the transmit direction.
Tx mem threshold exceeded rejects	Number of transmit buffer rejects because of a threshold overrun.
mutex lock fails	Number of mutex lock failures in the transmit direction.
retrieved buffers	Number of transmit buffers retrieved.
Tx quota for high/med/low	Total number of buffers available for transmission on the ring.
Tx waits for high/med/low	Number of times the transmit thread had to wait because of a buffer quota shortage for LWM clients.
Tx (QAD) waits for high/med/low	Number of times queueing and dispatching (QAD) clients had to wait because of a quota shortage.
Tx (QAD) wakeups for high/med/low	Number of times the transmit thread was woken up.

Related Commands

Command	Description
show controllers backplane ethernet brief, on page 485	Displays brief information about backplane Ethernet interfaces in a particular location.
show controllers backplane ethernet clients, on page 487	Displays information about client applications in a particular location.
show controllers backplane ethernet manageability bridge list, on page 504	Displays the CE bridges distributed across a Cisco CRS system.

show controllers backplane ethernet manageability bridge basic

To display basic information for a Control Ethernet (CE) bridge, use the **show controllers backplane ethernet manageability bridge** command in administration EXEC mode.

show controllers backplane ethernet manageability bridge *bridge-name* **basic**

Syntax Description

bridge-name Identifies the bridge whose information you want to display. For the *bridge-name* argument, use the following naming notation:

ControlEthernet *rack_slot_module_* [S0 | S1]

The underscore between values is required as part of the notation. A sample bridge name is ControlEthernet0_RP0_CPU0_S0.

Note To view a list of CE bridges currently in the system, enter the **show controllers backplane ethernet manageability bridge list** command.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

An explanation of each component of the bridge naming notation (ControlEthernet*rack_slot_module_*[S0 | S1]) is as follows:

- *rack*: Chassis number of the rack.
- *slot*: Physical slot number of the card.
- *module*: Processor module number is always CPU0.
- [S0 | S1]: S0 indicates an intra-rack bridge, and S1 indicates an inter-rack bridge.

Each route processor (RP) card has one S0 bridge, and each system controller (SC) card has one S0 bridge and one S1 bridge.

Task ID

Task ID	Operations
fabric	read
system	read

Examples

The following example shows how to display basic information for a bridge named ControlEthernet0_RP0_CPU0_S0:

```
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet manageability bridge
ControlEthernet0_RP0_CPU0_S0 basic

Bridge Base Information
-----------------------------------------
Bridge Name      : ControlEthernet0_RP0_CPU0_S0
Bridge Address   : 00 11 93 ef e8 e2
Number of Ports  : 18
Bridge Type      : Transparent Only
-----------------------------------------
```

Table 35: show controllers backplane ethernet manageability bridge basic Field Descriptions

Field	Description
Bridge Name	Displays the name of the bridge in the ControlEthernet*rack_slot_module*_[S0 | S1] naming notation.
Bridge Address	Displays the MAC address of the bridge.
Number of Ports	Displays the number of ports controlled by the bridge.
Bridge Type	Indicates the type of bridging that is being performed. Valid values include the following: • Unknown • Transparent Only • Sourceroute Only • SRT

Related Commands

Command	Description
show controllers backplane ethernet manageability bridge list, on page 504	Displays the CE bridges distributed across a Cisco CRS system.

show controllers backplane ethernet manageability bridge fdb-entry

To display the forwarding table entry for a Control Ethernet (CE) bridge port, use the **show controllers backplane ethernet manageability bridge fdb-entry** command in administration EXEC mode.

show controllers backplane ethernet manageability bridge *bridge-name* **fdb-entry** *mac-address*

Syntax Description

bridge-name	Identifies the bridge whose information you want to display. For the *bridge-name* argument, use the following naming notation: ControlEthernet*rack_slot_module_*[S0 | S1] The underscore between values is required as part of the notation. A sample bridge name is ControlEthernet0_RP0_CPU0_S0. **Note** To view a list of CE bridges currently in the system, enter the **show controllers backplane ethernet manageability bridge list** command.
mac-address	Identifies a bridge port with the specified 48-bit MAC address. You must enter the address in the *H.H.H* format. **Note** To view the forwarding table of a CE bridge, which includes 48-bit MAC addresses, enter the **show controllers backplane ethernet manageability bridge forwarding** command

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

An explanation of each component of the bridge naming notation (ControlEthernet*rack_slot_module_*[S0 | S1]) is as follows:

- *rack*: Chassis number of the rack.
- *slot*: Physical slot number of the card.
- *module*: Processor module number is always CPU0.
- [S0 | S1]: S0 indicates an intra-rack bridge, and S1 indicates an inter-rack bridge.

Each route processor (RP) card has one S0 bridge, and each system controller (SC) card has one S0 bridge and one S1 bridge.

Task ID

Task ID	Operations
fabric	read
system	read

Examples

The following example shows how to display the forwarding table entry for a bridge port with the MAC address of 5246.4800.0040:

```
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet manageability bridge
ControlEthernet0_RP0_CPU0_S0 fdb-entry 5246.4800.0040

-------------------------------------------------------
Bridge Name      : ControlEthernet0_RP0_CPU0_S0
      Trasparent Bridging Forwarding Table
-------------------------------------------------------
Mac_Address     Ingress_Port    Status
-------------------------------------------------------
5246.4800.0040          12      Learned
```

Table 36: show controllers backplane ethernet manageability bridge fdb-entry Field Descriptions

Field	Description
Bridge Name	Displays the name of the bridge in the ControlEthernet*rack_slot_module*_[S0 | S1] naming notation.
MAC Address	Displays a unicast 48-bit MAC address for which the bridge has forwarding and/or filtering information.
Ingress Port	Displays the number of the port. A value of 0 indicates that the port number has not been learned, but that the bridge does have some forwarding/filtering information about this address.
Status	Displays the status of the port, which can be one of the following: • Other—None of the other values applies. • Invalid—The forwarding table entry is no longer valid (for example, it was learned and has since aged out), but has not yet been flushed from the table. • Learned—The port was learned and is being used. • Self—The MAC address of the port represents one of the addresses. • Mgmt—The MAC address of the port is also the value of an existing instance of dot1dStaticAddress.

Related Commands

Command	Description
show controllers backplane ethernet manageability bridge forwarding, on page 501	Displays a forwarding database table for a CE bridge.

Command	Description
show controllers backplane ethernet manageability bridge list, on page 504	Displays the CE bridges distributed across a Cisco CRS system.
show controllers backplane ethernet manageability bridge port, on page 506	Displays information for a CE bridge port.

show controllers backplane ethernet manageability bridge forwarding

To display a forwarding database table for a Control Ethernet (CE) bridge, use the **show controllers backplane ethernet manageability bridge forwarding** command in administration EXEC mode.

show controllers backplane ethernet manageability bridge *bridge-name* **forwarding**

Syntax Description

bridge-name Identifies the bridge whose information you want to display. For the *bridge-name* argument, use the following naming notation:

ControlEthernet*rack_slot_module*_[S0 | S1]

The underscore between values is required as part of the notation. A sample bridge name is ControlEthernet0_RP0_CPU0_S0.

Note To view a list of CE bridges currently in the system, enter the **show controllers backplane ethernet manageability bridge list** command.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

An explanation of each component of the bridge naming notation (ControlEthernet*rack_slot_module*_[S0 | S1]) is as follows:

- *rack*: Chassis number of the rack.
- *slot*: Physical slot number of the card.
- *module*: Processor module number is always CPU0.
- [S0 | S1]: S0 indicates an intra-rack bridge, and S1 indicates an inter-rack bridge.

Each route processor (RP) card has one S0 bridge, and each system controller (SC) card has one S0 bridge and one S1 bridge.

Task ID

Task ID	Operations
fabric	read
system	read

Examples

The following example shows how to display forwarding database information a bridge named ControlEthernet0_RP0_CPU0_S0:

```
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet manageability bridge
ControlEthernet0_RP0_CPU0_S0 forwarding

-------------------------------------------------------
Bridge Name      : ControlEthernet0_RP0_CPU0_S0
      Trasparent Bridging Forwarding Table
-------------------------------------------------------
Mac_Address     Ingress_Port    Status
-------------------------------------------------------
0000.0000.0000          0       Learned
0000.000f.ffff          0       Learned
0000.0102.0304          1       Learned
0249.4450.0000          0       Learned
0249.4450.0001          0       Learned
0249.4450.0002          0       Learned
5246.4800.0010          9       Learned
5246.4800.0011          9       Learned
5246.4800.0040          12      Learned
5246.4800.0041          12      Learned
5246.4800.0042          12      Learned
5246.4800.0060          14      Learned
5246.4800.0061          14      Learned
5246.4800.0201          0       Learned
5246.4800.0211          1       Learned
5246.4800.0800          2       Learned
5246.4800.0810          3       Learned
5246.4800.0820          4       Learned
5246.4800.0830          5       Learned
ffff.ffff.ffff          0       Learned
```

Table 37: show controllers backplane ethernet manageability bridge forwarding Field Descriptions

Field	Description
Bridge Name	Displays the name of the bridge in the ControlEthernet*rack_slot_module*_[S0 | S1] naming notation.
MAC Address	Displays a unicast 48-bit MAC address for which the bridge has forwarding and/or filtering information.
Ingress Port	Displays the number of the port. A value of 0 indicates that the port number has not been learned, but that the bridge does have some forwarding/filtering information about this address.

Field	Description
Status	Displays the status of the port, which can be one of the following: • Other—None of the other values applies. • Invalid—The forwarding table entry is no longer valid (for example, it was learned and has since aged out), but has not yet been flushed from the table. • Learned—The port was learned and is being used. • Self—The MAC address of the port represents one of the addresses. • Mgmt—The MAC address of the port is also the value of an existing instance of dot1dStaticAddress.

Related Commands

Command	Description
show controllers backplane ethernet manageability bridge fdb-entry, on page 498	Displays the forwarding table entry for a CE bridge port.
show controllers backplane ethernet manageability bridge list, on page 504	Displays the CE bridges distributed across a Cisco CRS system.

show controllers backplane ethernet manageability bridge list

To display the Control Ethernet (CE) bridges distributed across a Cisco CRS system, use the **show controllers backplane ethernet manageability bridge list** command in administration EXEC mode.

show controllers backplane ethernet manageability bridge list

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

The Cisco CRS system is comprised of multiple CE bridges. Each route processor (RP) card has one S0 bridge, and each system controller (SC) card has one S0 bridge and one S1 bridge.

Task ID

Task ID	Operations
fabric	read
system	read

Examples

The following example displays a list of CE bridges that comprise a routing system:

```
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet manageability bridge list

ControlEthernet0_RP0_CPU0_S0
ControlEthernet0_RP1_CPU0_S0
ControlEthernet1_RP0_CPU0_S0
ControlEthernet1_RP1_CPU0_S0
ControlEthernetF0_SC0_CPU0_S0
ControlEthernetF0_SC0_CPU0_S1
ControlEthernetF0_SC1_CPU0_S0
ControlEthernetF0_SC1_CPU0_S1
ControlEthernetF1_SC0_CPU0_S0
ControlEthernetF1_SC0_CPU0_S1
```

Table 38: show controllers backplane ethernet manageability bridge list Field Descriptions

Field	Description
bridge-name	Displays the name of each bridge in the ControlEthernet*rack_slot_module*_S0 | S1 naming notation where an explanation of each components is as follows: • *rack* = Chassis number of the rack. • *slot* = Physical slot number of the card. • *module* = Processor module number is always CPU0. • S0 | S1 = S0 indicates an intra-rack bridge, and S1 indicates an inter-rack bridge.

Related Commands

Command	Description
show platform	Displays information and status for each node in the system.

show controllers backplane ethernet manageability bridge port

To display information for a Control Ethernet (CE) bridge port, use the **show controllers backplane ethernet manageability bridge port** command in administration EXEC mode.

show controllers backplane ethernet manageability bridge *bridge-name* **port** *port-number* **basic** | **span-tree** | **transparent**

Syntax Description

bridge-name	Identifies the bridge whose information you want to display. For the *bridge-name* argument, use the following naming notation: ControlEthernet*rack_slot_module_*[S0 | S1] The underscore between values is required as part of the notation. A sample bridge name is ControlEthernet0_RP0_CPU0_S0. **Note** To view a list of CE bridges currently in the system, enter the **show controllers backplane ethernet manageability bridge list** command.
port-number	Specify a bridge port number. The range is from 1 to 50.
basic	Displays basic information for a bridge port.
span-tree	Displays Spanning Tree Protocol (STP) information for a bridge port.
transparent	Displays transparent bridging information for a bridge port.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

An explanation of each component of the bridge naming notation (ControlEthernet*rack_slot_module_*[S0 | S1]) is as follows:

- *rack*: Chassis number of the rack.
- *slot*: Physical slot number of the card.
- *module*: Processor module number is always CPU0.
- [S0 | S1]: S0 indicates an intra-rack bridge, and S1 indicates an inter-rack bridge.

The Cisco CRS system is comprised of multiple bridges. Each route processor (RP) card has one S0 bridge, and each system controller (SC) card has one S0 bridge and one S1 bridge. STP is implemented to avoid bridging loops within the control plane network.

Task ID

Task ID	Operations
fabric	read
system	read

Examples

The following example shows how to display basic information for port 12 on bridge ControlEthernet0_RP0_CPU0_S0:

```
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet manageability bridge
ControlEthernet0_RP0_CPU0_S0 port 12 basic

Bridge Base Port Information
----------------------------------------
Bridge Name             : ControlEthernet0_RP0_CPU0_S0
Port Id                 : 12
InterfaceName           : ControlEthernet0_RP0_CPU0_S0_12
Circuit                 : NULL
Delay Discards          : 0
MTU Discards            : 0
----------------------------------------
```

Table 39: show controllers backplane ethernet manageability bridge port basic Field Descriptions

Field	Description
Bridge Name	Displays the name of the bridge in the ControlEthernet*rack_slot_module*_[S0 | S1] naming notation.
Port ID	Displays the number of the port for which you are displaying information.
Interface Name	Displays the name of the interface associated with the port in the ControlEthernet*rack_slot_module*_[S0 | S1]_*port* naming notation.
Circuit	Displays a unique name (NULL) for a port that potentially has the same value as another port on the same bridge.
Delay Discards	Displays the number of frames discarded by the port because of excessive transit delays through the bridge. This counter is incremented by both transparent and source route bridges.
MTU Discards	Displays the number of frames discarded by the port because they are too large. This counter is incremented by both transparent and source route bridges.

The following example shows how to display STP information for port 12 on bridge ControlEthernet0_RP0_CPU0_S0:

```
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet manageability bridge
ControlEthernet0_RP0_CPU0_S0 port 12 span-tree

Bridge stp Port Information
----------------------------------------
Bridge Name             : ControlEthernet0_RP0_CPU0_S0
Port Id                 : 12
```

```
Port Priority           : 128
Port State              : forwarding(5)
Port Enabled            : enabled(1)
Path Cost               : 200000
Port Designated Root    : 90 01 00 11 93 ef e8 e2
Port Designated Cost    : 0
Port Designated Bridge  : 90 01 00 11 93 ef e8 e2
Designated Port         : 32770
Forward Transport count : 2
----------------------------------------
```

Table 40: show controllers backplane ethernet manageability bridge port span-tree Field Descriptions

Field	Description
Bridge Name	Displays the name of the bridge in the ControlEthernet*rack_slot_module*_[S0 | S1] naming notation.
Port ID	Displays the number of the port for which you are displaying information.
Port Priority	Displays the value of the priority field, which is contained in the first octet (in network byte order) of the Port ID (2 octet long).
Port State	Displays the current state of the port as defined by STP. Valid values are disabled(1), blocking(2), listening(3), learning(4), forwarding(5), and broken(6).
Port Enabled	Indicates whether the port is enabled or disabled.
Path Cost	Displays the contribution of the port to the cost of paths towards its spanning tree root.
Port Designated Root	Displays the unique identifier of the bridge, which is recorded as the root in the bridge protocol data units (BPDUs). The BPDUs are transmitted by the designated bridge for the segment to which the port is attached.
Port Designated Cost	Displays the path cost of the designated port for the segment connected to this port.
Port Designated Bridge	Displays the identifier of the bridge that a port considers to be the designated bridge for the segment connected to this port.
Designated Port	Displays the identifier of the port on the designated bridge for the segment connected to this port.
Forward Transport Count	Displays the number of times this port has transitioned from the learning to the forwarding states.

The following example shows how to display transparent bridging information for port 12 on bridge ControlEthernet0_RP0_CPU0_S0:

```
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet manageability bridge
ControlEthernet0_RP0_CPU0_S0 port 12 transparent

Bridge tp Port Information
----------------------------------------
Bridge Name             : ControlEthernet0_RP0_CPU0_S0
```

```
Port Id                 : 12
Maximum                 : 1504
Receive Count           : 1
Transmit Count          : 123
Received Discards       : 0
----------------------------------------
```

Table 41: show controllers backplane ethernet manageability bridge port transparent Field Descriptions

Field	Description
Bridge Name	Displays the name of the bridge in the ControlEthernet*rack_slot_module*_[S0 | S1] naming notation.
Port ID	Displays the number of the port for which you are displaying information.
Maximum	Displays the maximum size, in bytes, of the INFO (non-MAC) field that the port receives or transmits.
Receive Count	Displays the number of frames received by the port from the segment to which it is connected.
Transmit Count	Displays the number of frames transmitted by the port to the segment to which it is connected.
Received Discards	Displays the number of received valid frames that were discarded.

Related Commands

Command	Description
show controllers backplane ethernet manageability bridge list, on page 504	Displays the CE bridges distributed across a Cisco CRS system.
show controllers backplane ethernet manageability bridge fdb-entry, on page 498	Displays the forwarding table entry for a CE bridge port.

show controllers backplane ethernet manageability bridge span-tree

To display Spanning Tree Protocol (STP) information for a Control Ethernet (CE) bridge, use the **show controllers backplane ethernet manageability bridge span-tree** command in administration EXEC mode.

show controllers backplane ethernet manageability bridge *bridge-name* **span-tree**

Syntax Description

bridge-name Identifies the bridge whose information you want to display. For the *bridge-name* argument, use the following naming notation:

ControlEthernet*rack_slot_module*_[S0 | S1]

The underscore between values is required as part of the notation. A sample bridge name is ControlEthernet0_RP0_CPU0_S0.

Note To view a list of CE bridges currently in the system, enter the **show controllers backplane ethernet manageability bridge list** command.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

An explanation of each component of the bridge naming notation (ControlEthernet*rack_slot_module*_[S0 | S1]) is as follows:

- *rack*: Chassis number of the rack.
- *slot*: Physical slot number of the card.
- *module*: Processor module number is always CPU0.
- [S0 | S1]: S0 indicates an intra-rack bridge, and S1 indicates an inter-rack bridge.

The Cisco CRS system is comprised of multiple bridges. Each route processor (RP) card has one S0 bridge, and each system controller (SC) card has one S0 bridge and one S1 bridge. STP is implemented to avoid bridging loops within the control plane network.

Task ID

Task ID	Operations
fabric	read
system	read

Examples

The following example shows how to display STP information for bridge ControlEthernet0_RP0_CPU0_S0:

```
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet manageability bridge
ControlEthernet0_RP0_CPU0_S0 span-tree

Spanning Tree Protocol Information
------------------------------------------
Bridge Name              : ControlEthernet0_RP0_CPU0_S0
STP Version              : IEEE8021D
STP Priority             : 36864
STP Topology Change      : 1793743
STP Topology Change Count: 2
Designated Root          : 90 00 00 11 93 ef e8 e2
STP Root Cost            : 0
STP Root Port            : 0
Maximum Age              : 8
Hello Time               : 1
STP Hold Time            : 1
STP Forward Delay        : 6
Bridge Maximum Age       : 8
Bridge Hello Time        : 1
Bridge Forward Delay     : 6
------------------------------------------
```

Table 42: show controllers backplane ethernet manageability bridge span-tree Field Descriptions

Field	Description
Bridge Name	Displays the name of the bridge in the ControlEthernet*rack_slot_module*_[S0 | S1] naming notation.
STP Version	Displays the STP version that is currently running.
STP Priority	Displays the value of the writable portion of the bridge ID (the first two octets of the bridge ID). The valid range is 0 through 65535.
STP Topology Change	Displays the time, in hundredths of a second, since a topology change was last detected by the bridge.
STP Topology Change Count	Displays the number of topology changes detected by the bridge since the management entity was last reset or initialized.
Designated Root	Displays the bridge identifier of the root of the spanning tree as determined by STP.
STP Root Cost	Displays the path cost from the bridge to the root.
STP Root Port	Displays the number of the port that offers the lowest cost path from the bridge to the root bridge.
Maximum Age	Displays the maximum age, in hundredths of a second, of STP information learned from the network on any port before it is discarded.

Field	Description
Hello Time	Displays the time, in hundredths of a second, between the transmission of bridge protocol data units (BPDUs) by any port that is the root of the spanning tree or trying to become the root.
STP Hold Time	Displays the amount of time, in hundredths of a second, that determines the interval during which no more than two BPDUs are transmitted by the node.
STP Forward Delay	Displays a time value, in hundredths of a second, that determines how fast a port changes its spanning state when moving toward the forwarding state.
Bridge Maximum Age	Displays a maximum age value used by all bridges when this bridge is acting as the root.
Bridge Hello Time	Displays a hello time value used by all bridges when this bridge is acting as the root.
Bridge Forward Delay	Displays a forward delay value used by all bridges when this bridge is acting as the root.

Related Commands

Command	Description
show controllers backplane ethernet manageability bridge list, on page 504	Displays the CE bridges distributed across a Cisco CRS system.
show controllers backplane ethernet manageability bridge port, on page 506	Displays information for a CE bridge port.

show controllers backplane ethernet manageability bridge transparent

To display transparent bridging information for a Control Ethernet (CE) bridge, use the **show controllers backplane ethernet manageability bridge transparent** command in administration EXEC mode.

show controllers backplane ethernet manageability bridge *bridge-name* **transparent**

Syntax Description

bridge-name Identifies the bridge whose information you want to display. For the *bridge-name* argument, use the following naming notation:

ControlEthernet*rack_slot_module*_[S0 | S1]

The underscore between values is required as part of the notation. A sample bridge name is ControlEthernet0_RP0_CPU0_S0.

Note To view a list of CE bridges currently in the system, enter the **show controllers backplane ethernet manageability bridge list** command.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

An explanation of each component of the bridge naming notation (ControlEthernet*rack_slot_module*_[S0 | S1]) is as follows:

- *rack*: Chassis number of the rack.
- *slot*: Physical slot number of the card.
- *module*: Processor module number is always CPU0.
- [S0 | S1]: S0 indicates an intra-rack bridge, and S1 indicates an inter-rack bridge.

Each route processor (RP) card has one S0 bridge, and each system controller (SC) card has one S0 bridge and one S1 bridge.

Task ID

Task ID	Operations
fabric	read
system	read

Examples

The following example shows how to display transparent bridging information for bridge ControlEthernet0_RP0_CPU0_S0:

```
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet manageability bridge
ControlEthernet0_RP0_CPU0_S0 transparent

Spanning Tree Protocol Information
-----------------------------------------
Bridge Name             : ControlEthernet0_RP0_CPU0_S0
Learned Discards        : 0
Aging Time              : 300
-----------------------------------------
```

Table 43: show controllers backplane ethernet manageability bridge transparent Field Descriptions

Field	Description
Bridge Name	Displays the name of the bridge in the ControlEthernet*rack_slot_module*_[S0 | S1] naming notation.
Learned Discards	Displays the number of forwarding database entries that were learned or would have been learned but have been discarded because of a storage space shortage in the forwarding database.
Aging Time	Displays the time-out period, in seconds, for aging out dynamically learned forwarding information.

Related Commands

Command	Description
show controllers backplane ethernet manageability bridge list, on page 504	Displays the CE bridges distributed across a Cisco CRS system.
show controllers backplane ethernet manageability bridge port, on page 506	Displays information for a CE bridge port.

show controllers backplane ethernet manageability interface attributes

To display attribute information for a Control Ethernet (CE) interface, use the **show controllers backplane ethernet manageability interface attributes** command in administration EXEC mode.

show controllers backplane ethernet manageability interface *interface-name* **attributes**

Syntax Description

interface-name Identifies the CE interface whose information you want to display. For the *interface-name* argument, use the following naming notation:

ControlEthernet*rack/slot/module/*[S0 | S1]/*port*

The slash between values is required as part of the notation. A sample CE interface name is ControlEthernet0/RP0/CPU0/S0/1.

Note To view a list of the CE interfaces for a node, enter the **show controllers backplane ethernet manageability interface list** command.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

An explanation of each component of the interface naming notation (ControlEthernet*rack/slot/module/*[S0 | S1]/*port*) is as follows:

- *rack*: Chassis number of the rack.
- *slot*: Physical slot number of the card.
- *module*: Processor module number is always CPU0.
- [S0 | S1]: S0 indicates an intra-rack switch, and S1 indicates an inter-rack switch.
- *port*: Physical port number of the interface.

Task ID

Task ID	Operations
fabric	read
system	read

Examples

The following example shows how to display attribute information for a specified CE interface:

```
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet manageability interface
ControlEthernet0/RP0/CPU0/S0/10 attributes

Control Ether Interface Attributes
-----------------------------------
Interface Name      : ControlEthernet0_RP0_CPU0_S0_10
Interface Type      : Fast Ethernet
Interface Speed      : 100000000
Interface High Speed : 100
Admin Status         : 1
Oper  Status         : 1
Connector Present    : 0
Physical Address     : NA
---------------------------------
```

Table 44: show controllers backplane ethernet manageability interface attributes Field Descriptions

Field	Description
Interface Name	Displays the name of the CE interface in the ControlEthernet*rack_slot_module*_[S0 | S1]_*port* naming notation.
Interface Type	Displays the type of interface.
Interface Speed	Displays the current bandwidth, in bits per second, of the interface.
Interface High Speed	Displays the current bandwidth, in units of 1,000,000 bits per second, of the interface.
Admin Status	Displays the state of the interface. Valid values are 1 (up), 2 (down), and 3 (testing). While the interface is in a testing state, operational packets cannot be passed.
Oper Status	Displays the current operational state of the interface. Valid values are 1 (up), 2 (down), 3 (testing), 4 (unknown), 5 (dormant), 6 (not present), 7 (lower layer down).
Connector Present	Indicates whether the interface sublayer has a physical connector. Valid values include 0 (a physical connector is present), and 1 (a physical connector is not present).
Physical Address	The address of the interface at its protocol sublayer, if one is present.

Related Commands

Command	Description
show controllers backplane ethernet manageability interface list, on page 517	Displays a list of CE interfaces for a node.

show controllers backplane ethernet manageability interface list

To display a list of Control Ethernet (CE) interfaces for a node, use the **show controllers backplane ethernet manageability interface list** command in administration EXEC mode.

show controllers backplane ethernet manageability interface list [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays CE interfaces for a specified location. Enter the *node-id* argument in the *rack*/*slot*/*module* notation.

Note Use the **show platform** command to see a list of all nodes currently in the system.

Command Default

No default behavior or values

Command Default

CE interfaces for the active route processor (RP) are displayed.

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
fabric	read
system	read

Examples

The following example shows how to display a list of the CE interfaces for the active RP, which in this case includes 18 ports.

```
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet manageability interface
list

ControlEthernet0/RP0/CPU0
ControlEthernet0/RP0/CPU0/S0/1
ControlEthernet0/RP0/CPU0/S0/2
ControlEthernet0/RP0/CPU0/S0/3
ControlEthernet0/RP0/CPU0/S0/4
ControlEthernet0/RP0/CPU0/S0/5
ControlEthernet0/RP0/CPU0/S0/6
ControlEthernet0/RP0/CPU0/S0/7
ControlEthernet0/RP0/CPU0/S0/8
ControlEthernet0/RP0/CPU0/S0/9
```

```
ControlEthernet0/RP0/CPU0/S0/10
ControlEthernet0/RP0/CPU0/S0/11
ControlEthernet0/RP0/CPU0/S0/12
ControlEthernet0/RP0/CPU0/S0/13
ControlEthernet0/RP0/CPU0/S0/14
ControlEthernet0/RP0/CPU0/S0/15
ControlEthernet0/RP0/CPU0/S0/16
ControlEthernet0/RP0/CPU0/S0/49
ControlEthernet0/RP0/CPU0/S0/50
```

The following example shows how to display a list of the CE interfaces for the standby RP, which in this case also includes 18 ports.

```
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet manageability interface
list location 0/RP1/CPU0

ControlEthernet0/RP1/CPU0
ControlEthernet0/RP1/CPU0/S0/1
ControlEthernet0/RP1/CPU0/S0/2
ControlEthernet0/RP1/CPU0/S0/3
ControlEthernet0/RP1/CPU0/S0/4
ControlEthernet0/RP1/CPU0/S0/5
ControlEthernet0/RP1/CPU0/S0/6
ControlEthernet0/RP1/CPU0/S0/7
ControlEthernet0/RP1/CPU0/S0/8
ControlEthernet0/RP1/CPU0/S0/9
ControlEthernet0/RP1/CPU0/S0/10
ControlEthernet0/RP1/CPU0/S0/11
ControlEthernet0/RP1/CPU0/S0/12
ControlEthernet0/RP1/CPU0/S0/13
ControlEthernet0/RP1/CPU0/S0/14
ControlEthernet0/RP1/CPU0/S0/15
ControlEthernet0/RP1/CPU0/S0/16
ControlEthernet0/RP1/CPU0/S0/49
ControlEthernet0/RP1/CPU0/S0/50
```

Table 45: show controllers backplane ethernet manageability interface list Field Descriptions

Field	Description
interface-name	Displays the name of each interface in the ControlEthernet*rack/slot/module/*S0 | S1/*port* naming notation, where an explanation of each components is as follows: • *rack* = Chassis number of the rack. • *slot* = Physical slot number of the card. • *module* = Processor module number is always CPU0. • S0 | S1 = S0 indicates an intra-rack bridge, and S1 indicates an inter-rack bridge. • *port*: Physical port number of the interface.

Related Commands

Command	Description
show platform	Displays information and status for each node in the system.

show controllers backplane ethernet manageability interface mau-autonet-info

To display medium attachment unit (MAU) auto negotiation information for a Control Ethernet (CE) interface, use the **show controllers backplane ethernet manageability interface mau-autonet-info** command in administration EXEC mode.

show controllers backplane ethernet manageability interface *interface-name* **mau-autonet-info**

Syntax Description

interface-name Identifies the CE interface whose information you want to display. For the *interface-name* argument, use the following naming notation:

ControlEthernet*rack/slot/module/*[S0 | S1]/*port*

The slash between values is required as part of the notation. A sample CE interface name is ControlEthernet0/RP0/CPU0/S0/1.

Note To view a list of the CE interfaces for a node, enter the **show controllers backplane ethernet manageability interface list** command.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

An explanation of each component of the interface naming notation (ControlEthernet*rack/slot/module/*[S0 | S1]/*port*) is as follows:

- *rack*: Chassis number of the rack.
- *slot*: Physical slot number of the card.
- *module*: Processor module number is always CPU0.
- [S0 | S1]: S0 indicates an intra-rack switch, and S1 indicates an inter-rack switch.
- *port*: Physical port number of the interface.

Task ID

Task ID	Operations
fabric	read
system	read

Examples

The following example shows how to display information about MAU auto negotiation for interface ControlEthernet0/RP0/CPU0/S0/49:

```
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet manageability interface
ControlEthernet0/RP0/CPU0/S0/49 mau-autoneg-info

Control Ether MAU Auto Neg Information
--------------------------------------
Interface Name             : ControlEthernet0_RP0_CPU0_S0_49
AutoNeg Admin Status       : Enabled
AutoNeg Remote Signal      : Not Detected
AutoNeg Config             : Other
AutoNeg Restart            : No Restart
Local Capability Bits      : b1000baseXFD
Advertised Capability Bits : b1000baseXFD
Received Capability Bits   : b1000baseXFD
--------------------------------------
```

Table 46: show controllers backplane ethernet manageability interface mau-autoneg-info Field Descriptions

Field	Description
Interface Name	Displays the name of the CE interface in the ControlEthernet*rack_slot_module*_[S0 | S1]_*port* naming notation.
AutoNeg Admin Status	Displays the status of the auto-negotiation function (enabled or disabled).
AutoNeg Remote Signal	Indicates whether or not auto-negotiation signaling is detected on the remote end of the link.
AutoNeg Config	Indicates the current status of the auto-negotiation process, which can be one of the following: other, configuring, complete, disabled, parallel detect fail.
AutoNeg Restart	Displays whether or not the auto-negotiation function is restarting link negotiation.

Field	Description
Local Capability Bits	Displays a value that uniquely identifies the set of capabilities of the local auto-negotiation entity, which can be one of the following: • bOther—Other or unknown • b10baseT—10BASE-T half-duplex mode • b10baseTFD—10BASE-T full-duplex mode • b100baseT4—100BASE-T4 • b100baseTX—100BASE-TX half-duplex mode • b100baseTXFD—100BASE-TX full-duplex mode • b100baseT2—100BASE-T2 half-duplex mode • b100baseT2FD—100BASE-T2 full-duplex mode • bfdxPause—PAUSE for full-duplex links • bfdxAPause—Asymmetric PAUSE for full-duplex links • bfdxSPause—Symmetric PAUSE for full-duplex links • bfdxBPause—Asymmetric and symmetric PAUSE for full-duplex links • b1000baseX—1000BASE-X, -LX, -SX, -CX half-duplex mode • b1000baseXFD—1000BASE-X, -LX, -SX, -CX full-duplex mode • b1000baseT—1000BASE-T half-duplex mode • b1000baseTFD—1000BASE-T full-duplex mode
Advertised Capability Bits	Displays a value that uniquely identifies the set of capabilities advertised by the local auto-negotiation entity. For a list of valid values, refer to the Local Capability Bits entry in this table.
Received Capability Bits	Displays a value that uniquely identifies the set of capabilities received from the remote auto-negotiation entity. For a list of valid values, refer to the Local Capability Bits entry in this table.

Related Commands

Command	Description
show controllers backplane ethernet manageability interface list, on page 517	Displays a list of CE interfaces for a node.
show controllers backplane ethernet manageability interface mau-info, on page 522	Displays medium attachment unit (MAU) information for a Control Ethernet (CE) interface.
show controllers backplane ethernet manageability interface mau-jack-type, on page 527	Displays the medium attachment unit (MAU) jack type for a CE interface.

show controllers backplane ethernet manageability interface mau-info

To display medium attachment unit (MAU) information for a Control Ethernet (CE) interface, use the **show controllers backplane ethernet manageability interface mau-info** command in administration EXEC mode.

show controllers backplane ethernet manageability interface *interface-name* **mau-info**

Syntax Description

interface-name Identifies the CE interface whose information you want to display. For the *interface-name* argument, use the following naming notation:

ControlEthernet*rack/slot/module/*[S0 | S1]/*port*

The slash between values is required as part of the notation. A sample CE interface name is ControlEthernet0/RP0/CPU0/S0/1.

Note To view a list of the CE interfaces for a node, enter the **show controllers backplane ethernet manageability interface list** command.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

An explanation of each component of the interface naming notation (ControlEthernet*rack/slot/module/*[S0 | S1]/*port*) is as follows:

- *rack*: Chassis number of the rack.
- *slot*: Physical slot number of the card.
- *module*: Processor module number is always CPU0.
- [S0 | S1]: S0 indicates an intra-rack switch, and S1 indicates an inter-rack switch.
- *port*: Physical port number of the interface.

Task ID

Task ID	Operations
fabric	read
system	read

Examples

The following example shows how to display MAU information for interface ControlEthernet0/RP0/CPU0/S0/10:

```
RP/0/RP0/CPU0:router(admin)#show controllers backplane ethernet manageability interface
ControlEthernet0/RP0/CPU0/S0/10 mau-info

Control Ether MAU Information
---------------------------------
Interface Name        : ControlEthernet0_RP0_CPU0_S0_10
MAU Type              : dot3MauTypeAUI
MAU Status            : Operational
Media Available       : Available
Media Avail St Exits  : 0
MAU Jabber state      : No Jabber
Jabber State Enters   : 0
False Carrier Events  : 3
MAU DefaultType       : dot3MauTypeAUI
Auto Neg Supported    : 0
MAU TypeList Bits     : bOther
HCFalse Carriers        : 3
```

Table 47: show controllers backplane ethernet manageability interface mau-info Field Descriptions

Field	Description
Interface Name	Displays the name of the CE interface in the ControlEthernet*rack_slot_module*_[S0 | S1]_*port* naming notation.
MAU Type	Displays the MAU type, which can be one of the following: • dot3MauTypeAUI—No internal MAU, view from AUI • dot3MauType100BaseT4—4 pair category 3 UTP • dot3MauType1000BaseLXFD—Fiber over long-wavelength laser, full duplex mode • dot3MauType1000BaseSXFD—Fiber over short-wavelength laser, full duplex mode
MAU Status	Displays the current state of the MAU. Valid values are other, unknown, operational, standby, shutdown, and reset.
Media Available	Displays the state of the available MAU, which can be one of the following: • Other—The state of the MAU is not one of the other valid values. • Unknown—The state of the MAU is unknown; for example, the MAU is being initialized. • Available—The link, light, or loopback states are normal. • Not Available—The MAU is experiencing link loss or is in a low light or no loopback state. • Remote Fault—A fault is detected at the remote end of the link.

Field	Description
Media Avail St Exits	Displays the number of times that the MAU leaves the Available state.
MAU Jabber State	Displays the MAU jabber state, which can be one of the following: • Other—The jabber state of the MAU is not one of the other valid values. • Unknown—The jabber state of the MAU is unknown; for example, the MAU is being initialized. • No Jabber—The MAU is not jabbering. • Jabbering—The MAU is jabbering.
Jabber State Enters	Displays the number of times that the MAU enters the jabbering state.
False Carrier Events	Displays the number of false carrier events during idle in 100BASE-X links (dot3MauType100BaseT4, dot3MauType100BaseTX, dot3MauType100BaseFX, and all 1000Mbps types). For all other MAU types, this counter displays 0.
MAU Default Type	Displays the default administrative baseband MAU type to be used in conjunction with the operational MAU type.
Auto Neg Supported	Indicates whether or not auto negotiation is supported on the MAU. Valid values are 0 (auto negotiation is not supported), and 0 (auto negotiation is supported).
MAU Type List Bits	Displays a set of possible IEEE 802.3 types of the MAU, which can be one of the following: • bOther—Other or unknown • bAUI—AUI • b10base5—10BASE-5 • bFoirl—FOIRL • b10base2—10BASE-2 • b10baseT—10BASE-T duplex mode unknown • b10baseFP—10BASE-FP • b10baseFB—10BASE-FB • b10baseFL—10BASE-FL duplex mode unknown • b10broad36—10BROAD36

Field	Description
	• b10baseTHD—10BASE-T half duplex mode • b10baseTFD—10BASE-T full duplex mode • b10baseFLHD—10BASE-FL half duplex mode • b10baseFLFD—10BASE-FL full duplex mode • b100baseT4—100BASE-T4 • b100baseTXHD—100BASE-TX half duplex mode • b100baseTXFD—100BASE-TX full duplex mode • b100baseFXHD—100BASE-FX half duplex mode • b100baseFXFD—100BASE-FX full duplex mode • b100baseT2HD—100BASE-T2 half duplex mode
	• b100baseT2FD—100BASE-T2 full duplex mode • b1000baseXHD—1000BASE-X half duplex mode • b1000baseXFD—1000BASE-X full duplex mode • b1000baseLXHD—1000BASE-LX half duplex mode • b1000baseLXFD—1000BASE-LX full duplex mode • b1000baseSXHD—1000BASE-SX half duplex mode • b1000baseSXFD—1000BASE-SX full duplex mode • b1000baseCXHD—1000BASE-CX half duplex mode • b1000baseCXFD—1000BASE-CX full duplex mode • b1000baseTHD—1000BASE-T half duplex mode

Field	Description
	• b1000baseTFD—1000BASE-T full duplex mode • b10GbaseX—10GBASE-X • b10GbaseLX4—10GBASE-LX4 • b10GbaseR—10GBASE-R • b10GbaseER—10GBASE-ER • b10GbaseLR—10GBASE-LR • b10GbaseSR—10GBASE-SR • b10GbaseW—10GBASE-W • b10GbaseEW—10GBASE-EW • b10GbaseLW—10GBASE-LW • b10GbaseSW—10GBASE-SW
HC False Carriers	Displays the number of false carrier events during idle in 100BASE-X and 1000BASE-X links. For all other MAU types, this counter displays 0.

Related Commands

Command	Description
show controllers backplane ethernet manageability interface list, on page 517	Displays a list of CE interfaces for a node.
show controllers backplane ethernet manageability interface mau-autonet-info, on page 519	Displays medium attachment unit (MAU) auto negotiation information for a CE interface.
show controllers backplane ethernet manageability interface mau-jack-type, on page 527	Displays the medium attachment unit (MAU) jack type for a CE interface.

show controllers backplane ethernet manageability interface mau-jack-type

To display the medium attachment unit (MAU) jack type for a Control Ethernet (CE) interface, use the **show controllers backplane ethernet manageability interface mau-jack-type** command in administration EXEC mode.

show controllers backplane ethernet manageability interface *interface-name* **mau-jack-type**

Syntax Description

interface-name	Identifies the CE interface whose information you want to display. For the *interface-name* argument, use the following naming notation: ControlEthernet*rack/slot/module/*[S0 | S1]/*port* The slash between values is required as part of the notation. A sample CE interface name is ControlEthernet0/RP0/CPU0/S0/1. **Note** To view a list of the CE interfaces for a node, enter the **show controllers backplane ethernet manageability interface list** command.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

An explanation of each component of the interface naming notation (ControlEthernet*rack/slot/module/*[S0 | S1]/*port*) is as follows:

- *rack*: Chassis number of the rack.
- *slot*: Physical slot number of the card.
- *module*: Processor module number is always CPU0.
- [S0 | S1]: S0 indicates an intra-rack switch, and S1 indicates an inter-rack switch.
- *port*: Physical port number of the interface.

Task ID

Task ID	Operations
fabric	read
system	read

Examples

The following example shows how to display the MAU jack type for interface ControlEthernet0/RP0/CPU0/S0/10:

```
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet manageability interface
ControlEthernet0/RP0/CPU0/S0/10 mau-jack-type

Control Ether MAU Jack Type
-------------------------------------
Interface Name          : ControlEthernet0_RP0_CPU0_S0_10
MAU Jack Type           : undefined or unknown
```

Table 48: show controllers backplane ethernet manageability interface mau-jack-type Field Descriptions

Field	Description
Interface Name	Displays the name of the interface in the ControlEthernet*rack_slot_module*_[S0 | S1]_*port* naming notation.
MAU Jack Type	Displays the jack connector type, which can be undefined or unknown.

Related Commands

Command	Description
show controllers backplane ethernet manageability interface list, on page 517	Displays a list of CE interfaces for a node.
show controllers backplane ethernet manageability interface mau-autonet-info, on page 519	Displays medium attachment unit (MAU) auto negotiation information for a CE interface.
show controllers backplane ethernet manageability interface mau-info, on page 522	Displays medium attachment unit (MAU) information for a Control Ethernet (CE) interface.

show controllers backplane ethernet manageability interface statistics

To display statistics for a Control Ethernet (CE) interface, use the **show controllers backplane ethernet manageability interface statistics** command in administration EXEC mode.

show controllers backplane ethernet manageability interface *interface-name* **statistics**

Syntax Description

interface-name Identifies the CE interface whose information you want to display. For the *interface-name* argument, use the following naming notation:

ControlEthernet *rack/slot/module/* [S0 | S1]/ *port*

The slash between values is required as part of the notation. A sample CE interface name is ControlEthernet0/RP0/CPU0/S0/1.

Note To view a list of the CE interfaces for a node, enter the **show controllers backplane ethernet manageability interface list** command.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

An explanation of each component of the interface naming notation (ControlEthernet*rack/slot/module/*[S0 | S1]/*port*) is as follows:

- *rack*: Chassis number of the rack.
- *slot*: Physical slot number of the card.
- *module*: Processor module number is always CPU0.
- [S0 | S1]: S0 indicates an intra-rack switch, and S1 indicates an inter-rack switch.
- *port*: Physical port number of the interface.

Task ID

Task ID	Operations
fabric	read
system	read

Examples

The following example shows how to display statistics for interface ControlEthernet0/RP0/CPU0/S0/1:

```
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet manageability interface
ControlEthernet0/RP0/CPU0/S0/1 statistics

Control Ether Interface Counters
---------------------------------
Interface Name      : ControlEthernet0_RP0_CPU0_S0_1
ifInOctets          : 16168240550
ifInUcastPkts       : 103181424
ifInMulticastPkts   : 5821166
ifInBroadcastPkts   : 1465909
ifInDiscards        : 0
ifInErrors          : 0
ifInUnknownProtos   : 0
ifOutOctets         : 14871704758
ifOutUcastPkts      : 104085365
ifOutMulticastPkts  : 30884564
ifOutBroadcastPkts  : 19
ifOutDiscards       : 0
ifOutErrors         : 0
ifDiscontinuityTime : 0
---------------------------------
```

Table 49: show controllers backplane ethernet manageability interface statistics Field Descriptions

Field	Description
Interface Name	Displays the name of the CE interface in the ControlEthernet*rack_slot_module*_[S0 | S1]_*port* naming notation.
ifInOctets	Displays the total number of octets received on the interface, including framing characters.
ifInUcastPkts	Displays the number of packets that were not addressed to a multicast or broadcast address at this (sub-)layer but were delivered by the sublayer to a higher sublayer.
ifInMulticastPkts	Displays the number of packets that were addressed to a multicast address at this sublayer and were delivered by the sublayer to a higher (sub-)layer.
ifInBroadcastPkts	Displays the number of packets that were addressed to a broadcast address at this sublayer and were delivered by the sublayer to a higher (sub-)layer.
ifInDiscards	Displays the number of inbound packets that were discarded even though no errors that would prevent their delivery to a higher-layer protocol were detected.
ifInErrors	Displays the number of inbound packets or transmission units that contained errors, which prevented them from being delivered to a higher-layer protocol.
ifInUnknownProtos	Displays the number of received packets or transmission units that were discarded because of an unknown or unsupported protocol. If the interface that does not support protocol multiplexing, this field displays 0.
ifOutOctets	Displays the total number of octets, including framing characters, transmitted out of the interface.

Field	Description
ifOutUcastPkts	Displays the total number of packets that were not addressed to a multicast or broadcast address at this sublayer, including packets that were discarded or not sent, and that higher-level protocols requested be transmitted.
ifOutMulticastPkts	Displays the total number of packets that were addressed to a multicast or broadcast address at this sublayer, including packets that were discarded or not sent, and that higher-level protocols requested be transmitted.
ifOutBroadcastPkts	Displays the total number of packets that were addressed to a broadcast address at this sublayer, including packets that were discarded or not sent, and that higher-level protocols requested be transmitted.
ifOutDiscards	Displays the number of outbound packets that were discarded even though no errors that might prevent their transmission was detected.
ifOutErrors	Displays the number of outbound packets or transmission units that were not transmitted because of errors.
ifDiscontinuityTime	Displays the number of times that the interface experienced a discontinuity, which is when an interface is reset and its counter values are retained and not incremented until the interface is up again. If no discontinuities have occurred since the last re-initialization of the local management subsystem, then this field displays 0.

Related Commands

Command	Description
show controllers backplane ethernet manageability interface list, on page 517	Displays a list of CE interfaces for a node.

show controllers backplane ethernet multicast groups

To display information about backplane interfaces that are in multicast groups in a particular location, use the **show controllers backplane ethernet multicast groups** command in administration EXEC mode.

show controllers backplane ethernet multicast groups location *node-id*

Syntax Description

location *node-id*	Displays backplane information for multicast groups for a specified location. **Note** Use the **show platform** command to see a list of all nodes currently in the system.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced. This command replaces the **show controllers backplane ethernet local multicast groups** and **show controllers backplane ethernet location brief multicast groups** commands.

Usage Guidelines

Enter the **location** *node-id* argument in the *rack*/*slot*/*module* notation.

Task ID

Task ID	Operations
fabric	read
system	read

Examples

The following example shows the output from the **show controllers backplane ethernet multicast groups** command, which displays a summary of information for the backplane interfaces.

```
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet multicast groups location
 0/1/cpu0

Intf                    Multicast             Client registered for this address
Name                    address                    Id                 Name
-------------------------------------------------------------------------------
  FastEthernet0_2_CPU0    0100.0000.0064           2                GSP
                          0100.0000.0065           2                GSP
                          0100.0000.0066           2                GSP
                          0100.0000.0068           2                GSP
                          0100.0000.006a           2                GSP
                          0100.0000.006c           2                GSP
                          0100.0000.006e           2                GSP
                          0100.0000.0071           2                GSP
                          0100.0000.2774           2                GSP
                          0100.0000.2775           2                GSP
                          0100.0000.2776           2                GSP
```

```
0100.0000.2778          2               GSP
0100.0000.277a          2               GSP
0100.0000.2782          2               GSP
0100.0000.278a          2               GSP
0100.0000.2796          2               GSP
0100.0000.2798          2               GSP
```

Table 50: show controllers backplane ethernet multicast groups Field Description

Field	Description
Intf Name	Identifies the interface whose multicast addresses are displayed. **Note** A multicast address is a single address that refers to multiple network devices.
Multicast address	Multicast addresses associated with the specified interface. **Note** A multicast address is a single address that refers to multiple network devices.
ID	Client identifier.
Name	Client application name.

Related Commands

Command	Description
show controllers backplane ethernet brief, on page 485	Displays brief information about backplane Ethernet interfaces in a particular location.
show controllers backplane ethernet clients, on page 487	Displays information about client applications in a particular location.
show controllers backplane ethernet detail, on page 492	Displays detailed information about the backplane interfaces in a particular location.

show spantree

To display spanning tree configuration information, enter the **show spantree** command in administration EXEC mode.

show spantree mst 1 brief | **detail** | **port FE** *port-id* | **GE** *port-id* | **mst config location** *node-id*

Syntax Description

mst 1	Shows Multiple Spanning Tree (MST) information for instance 1.
brief	Displays a summary of spanning tree information.
detail	Displays detailed spanning tree information.
port	Displays spanning tree information for a specific Spanning Tree Protocol (STP) port. Replace the *port-id* argument with the number that identifies the port you want to display. Range is 1 through 49.
FE *port-id*	Identifies the FE port for which to display information. Valid values are 0 or 1.
GE *port-id*	Identifies the GE port for which to display information. Valid values are 0 or 1.
mst config	Shows MST configuration information.
location *node-id*	Displays spanning tree information for the specified location. **Note** Use the **show platform** command to see a list of all nodes currently in the system.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Enter the **location** *node-id* argument in the *rack*/*slot*/*module* notation.

Task ID

Task ID	Operations
root-system	read
system	read

Examples

The following example shows how to display MST information for instance 1 at the specified location:

```
RP/0/RP0/CPU0:router(admin)# show spantree mst 1 brief location 0/RP0/CPU0
```

```
##### MST   0 vlans mapped:   2-4094
Bridge        address 0011.93ef.e8e2  priority      36864 (36864 sysid 0)
Root          this switch for the CIST
Operational   hello time  1, forward delay  6, max age  8, txholdcount  6
Configured    hello time  1, forward delay  6, max age  8, max hops     4

Interface        Sts  Role Cost      Prio.Nbr Type
---------------- ---- ---- --------- -------- --------------------------------

##### MST   1 vlans mapped:   1
Bridge        address 0011.93ef.e8e2  priority      36865 (36864 sysid 1)
Root          this switch for MST1

Interface        Sts  Role Cost      Prio.Nbr Type
---------------- ---- ---- --------- -------- --------------------------------
       FE_Port_1  FWD Desg    200000 128.   2 P2p
```

Table 51: show spantree mst 1 brief Field Descriptions

Field	Description
MST *number*	Number of STP MST.
vlans mapped	VLAN numbers mapped to the MST.
Bridge address	MAC address of the bridge.
Bridge priority	STP priority of the bridge.
Root	MAC address of the root bridge.
Operational	Operational values of the following parameters: • hello time • forward delay • max age • txholdcount
Configured	Configured values of the following parameters: • hello time • forward delay • max age • max hops
Interface	Interfaces present in the STP.
Sts	Spanning tree status.
Role	Spanning tree role.

Field	Description
Cost	Spanning tree cost.
Prio. Nbr	Spanning tree priority.
Type	Type of link.

The following example shows how to display MST information for a specified FE port at a specified location:

```
RP/0/RP0/CPU0:router(admin)# show spantree mst 1 port FE 1 location 0/RP0/CPU0

FE_Port_1 of MST1 is designated forwarding
Edge port:             no        (default) port guard :    loop     (default)
Link type: point-to-point           (auto) bpdu filter: disable     (default)
Boundary : internal                        bpdu guard : disable     (default)
Bpdus (MRecords) sent 6122, received 3

Instance Role Sts Cost      Prio.Nbr Vlans mapped
-------- ---- --- --------- -------- -------------------------------
       1 Desg  FWD   200000 128.   2 1
```

Table 52: show spantree mst 1 port Field Descriptions

Field	Description
port-type Port *number* of MST1 is *status*	Spanning tree status of indicated port.
Edge port	Indicates whether or not the port is an edge port.
(default) port guard	Indicates that the loop port guard feature is on.
Link type	Port type, which can be point-to-point or point-to-multipoint.
(auto) bpdu filter	Indicates that the bridge protocol data unit (BPDU) filter is off.
Boundary	Type of boundary.
bpdu guard	Indicates that the BPDU guard feature is off.
Bpdus (MRecords) sent	Number of BPDU records sent.
Bpdus (MRecords) received	Number of BPDU records received.
Instance	Number of instances.
Role	STP role of the port.
Sts	Spanning tree status of the port.
Cost	Spanning tree cost of the port.
Prio. Nbr	Spanning tree priority of the port.
Vlans mapped	VLAN numbers that are mapped to the port.

The following example shows how to display MST configuration information for the specified location:

```
RP/0/RP0/CPU0:router(admin)# show spantree mst config location 0/RP0/CPU0

Name      [STP_1]
Revision      1
Instances configured 2

--------  ------------------------------------------------------------------------
   0      2-4094
   1      1
--------------------------------------------------------------------------------
```

Table 53: show spantree mst config Field Descriptions

Field	Description
Name	Identifies the MST for which information is displayed.
Revision	Revision of the current MST configuration.
Instances configured	Number of configured MST instances.
01	Identifier of the displayed instances.
2-4094q	VLANs that are mapped to the displayed MST.

Inter-rack Switch Control Network Commands on the Cisco IOS XR Software

This module provides command line interface (CLI) commands for configuring inter-rack switch control on the Cisco CRS Router.

clear controller switch

To clear the statistics for the Broadcom switches for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card, use the **clear controller switch** command in administration EXEC mode.

clear controller switch *instance* **statistics all location** *node-id* | **location** *node-id* | **ports** *number* **location** *node-id*

Syntax Description

instance	Switch instance identifier. The switch number is either 0 or 1.
statistics	Clears statistics for packets transmitted/received on switch ports.
all	Clears statistics for all ports.
location *node-id*	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the *node-id* argument as entered in the *rack/slot/module* notation.
ports *number*	Clears statistics for a specific switch port.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.4.1	This command was updated to include inter-rack switches.

Usage Guidelines

The **clear controller switch** command is used to specify intra-rack switches.

Task ID

Task ID	Operations
root-system	execute

Examples

The following example shows how to clear the statistics for the Broadcom switches:

```
RP/0/0/CPU0:router(admin)# clear controller switch 1 statistics all location
f0/sc0/cpu0
```

clear controller switch errdisable

To clear the err-disable state of the switch port for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card, use the **clear controller switch errdisable** command in administration EXEC mode.

clear controller switch errdisable port FE | GE 0 | 1 location *node-id*

Syntax Description

port	Specifies the port.
FE	Specifies the ports for the Fast Ethernet (FE).
GE	Specifies the ports for the Gigabit Ethernet (GE).
0	Specifies port number 0 for the backplane FE.
1	Specifies port number 1 for the backplane FE.
location *node-id*	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the *node-id* argument as entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.4.1	This command was updated to include inter-rack switches.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
root-system	execute

Examples

The following example shows how to clear the error disable state for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card:

```
RP/0/RP0/CPU0:router(admin)## clear controller switch errdisable port GE 1
location f0/sc0/cpu0
```

clear controller switch inter-rack

To clear the ISC switch counters, use the **clear controller switch inter-rack** command in administration EXEC mode.

clear controller switch inter-rack errdisable ports all*number* | **statistics all** | **ports***number* **location** *node-id*

Syntax Description

errdisable	Clears the err-disabled state of the port if the port was brought down by Unidirectional Link Detection (UDLD).
ports	Specifies the port.
number	Number for the port. The range is from 0 to 21.
all	Specifies all ports for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card.
statistics	Clears the statistics for the switch.
all	Specifies all of the ports.
location *node-id*	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the *node-id* argument as entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

The **clear controller switch inter-rack** command is used to specify inter-rack switches.

Task ID

Task ID	Operations
root-system	execute

Examples

The following example shows how to clear statistics for all the ports for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card:

```
RP/0/RP0/CPU0:router(admin)# clear controller switch inter-rack statistics all
 location f0/sc0/cpu0
```

show controllers switch

To display the control Ethernet connection in the route processor (RP), use the **show controllers switch** command in administration EXEC mode.

show controllers switch *instance* **ports** | **statistics location** *node-id*

Syntax Description

instance	Two intra-rack switches are present on the RP/SC. The instance is from 0 to 1 that identifies the specific switch.
ports	Displays the port states as up, down, or err-disabled. The **ports** keyword displays control Ethernet switches, port states, statistics, and Spanning Tree Protocol (STP) information.
statistics	Displays switch port statistics.
location *node-id*	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the *node-id* argument as entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

The **show controllers switch** command is used to specify intra-rack switches.

Task ID

Task ID	Operations
fabric	read
root-system	read

Examples

The following sample output shows how to verify the control Ethernet connection on the RP:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch 0 ports location 0/rp0/Cpu0

 FE Port  0 : Up, STP State : FORWARDING (Connects to - 0/RP0)
 FE Port  1 : Up, STP State : FORWARDING (Connects to - 0/RP1)
 FE Port  2 : Down                       (Connects to - 0/FC0)
 FE Port  3 : Down                       (Connects to - 0/FC1)
 FE Port  4 : Down                       (Connects to - 0/AM0)
 FE Port  5 : Down                       (Connects to - 0/AM1)
 FE Port  6 : Down                       (Connects to - )
 FE Port  7 : Down                       (Connects to - )
 FE Port  8 : Down                       (Connects to - 0/SM0)
 FE Port  9 : Up, STP State : FORWARDING (Connects to - 0/SM1)
 FE Port 10 : Down                       (Connects to - 0/SM2)
```

```
 FE Port 11 : Down                       (Connects to - 0/SM3)
 FE Port 12 : Down                       (Connects to - 0/SM4)
 FE Port 13 : Down                       (Connects to - 0/SM5)
 FE Port 14 : Down                       (Connects to - 0/SM6)
 FE Port 15 : Down                       (Connects to - 0/SM7)
 GE Port  0 : Up, STP State : FORWARDING (Connects to - GE_0)
 GE Port  1 : Up, STP State : FORWARDING (Connects to - Switch 1)
```

The following sample output shows how to verify the control Ethernet connection on intra-rack switches for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch 0 ports location f0/sc0/Cpu0

 FE Port  0 : Up, STP State : FORWARDING (Connects to - F0/SC0)
 FE Port  1 : Up, STP State : FORWARDING (Connects to - F0/SC1)
 FE Port  2 : Down                       (Connects to - F0/FC0)
 FE Port  3 : Down                       (Connects to - F0/FC1)
 FE Port  4 : Down                       (Connects to - F0/AM0)
 FE Port  5 : Down                       (Connects to - F0/AM1)
 FE Port  6 : Down                       (Connects to - F0/LM0)
 FE Port  7 : Down                       (Connects to - F0/LM1)
 FE Port  8 : Down                       (Connects to - F0/SM0)
 FE Port  9 : Down                       (Connects to - F0/SM1)
 FE Port 10 : Down                       (Connects to - F0/SM2)
 FE Port 11 : Down                       (Connects to - F0/SM3)
 FE Port 12 : Down                       (Connects to - F0/SM4)
 FE Port 13 : Down                       (Connects to - F0/SM5)
 FE Port 14 : Down                       (Connects to - F0/SM6)
 FE Port 15 : Down                       (Connects to - F0/SM7)
 GE Port  0 : Up, STP State : FORWARDING (Connects to - GE_0)
 GE Port  1 : Up, STP State : FORWARDING (Connects to - Switch 1)
```

Table 54: show controllers switch Field Descriptions

Field	Description
FE Port	Fast Ethernet (FE) port.
STP State	Spanning Tree Protocol (STP) state of the port.
GE Port	Gigabit Ethernet (GE) port.

show controllers switch inter-rack ports

To display the inter-rack switch port states for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card, use the **show controllers switch inter-rack ports** command in administration EXEC mode.

show controllers switch inter-rack ports all location *node-id*

Syntax Description

all	Displays all the ports for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card.
location *node-id*	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the *node-id* argument as entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The port numbers, which range from 0 to 21, correspond to those on the front panel.

Note The **show controllers switch inter-rack ports** command is applied only to the 22-port SCGE. When you use the **all** and **location** keywords, all other supported cards are displayed including the route processor (RP).

Task ID

Task ID	Operations
fabric	read
root-system	read
admin	read

Examples

The following example shows sample output of the control Ethernet connection for inter-rack switches on the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch inter-rack ports all location f0/sc0/CPU0

 GE_Port_0 : Down
```

```
GE_Port_1 : Down
…
…
GE_Port_13 : Up
GE_Port_14 : Up
…
…
GE_Port_20 : Down
GE_Port_21 : Down
To_5618  :  Up
Stacking : Up
```

show controllers switch inter-rack statistics

To display the statistics on the ports of the inter-rack switches for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card, use the **show controllers switch inter-rack statistics** command in administration EXEC mode.

show controllers switch inter-rack statistics *interface number* | **all brief** | **detail location** *node-id*

Syntax Description

interface number	Number for the Gigabit Ethernet interface. The range is from 0 to 21. The interface number identifies the specific front panel GE port on the 22-port SCGE.
all	Displays statistics of all ports for inter-rack switches.
brief	Displays transmit and receive statistics on the GE ports.
detail	Displays MIB like detailed switch port statistics that include transmit, receive, and error packet counts.
location *node-id*	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the *node-id* argument as entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
fabric	read
root-system	read
admin	read

Examples

The following example shows sample output on the port statistics counters for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch inter-rack statistics all brief location
 f0/sc0/cpu0

Port          Tx Frames   Tx Errors   Rx Frames   Rx Errors
```

```
------------------------------------------------------------
GE_Port_0 :      374423           0     1776848           0
GE_Port_1 :      251232           0      170742           0
GE_Port_2 :      857923           0      414409           0
GE_Port_3 :      239437           0      152772           0
GE_Port_4 :      166166           0       82031           0
GE_Port_5 :           0           0           0           0
GE_Port_6 :           0           0           0           0
…
…
GE_Port_16 :          0           0           0           0
GE_Port_17 :          0           0           0           0
GE_Port_18 :          0           0           0           0
GE_Port_19 :          0           0           0           0
GE_Port_20 :          0           0           0           0
GE_Port_21 :          0           0           0           0
To_5618    :     522072           0      293720           0
Stacking   :       1482           0           0           0
Stacking   :          0           0           0           0
```

The following example shows sample output for the detailed statistics per port for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch inter-rack statistics 0 detail location
 f0/sc0/cpu0

GE_Port_0

 Rx fragment            :          0    Tx fragment           :          0
 Rx unicast             :    1642337    Tx unicast            :     379927
 Rx multicast           :      51619    Tx multicast          :     205950
 Rx broadcast           :      91436    Tx broadcast          :     150357
 Rx FCS error           :          0    Tx FCS error          :          0
 Rx Pause               :          0    Tx Pause              :          0
 Rx Undersize           :          0    Tx Oversize           :          0
 Rx FFP drop            :          0    Tx CFI drop           :          0
 Rx Control frame       :          0    Tx Cell error         :          0
                                        Tx Jabber             :          0
                                        Tx excessive collision:          0
                                        Tx tagged vlan        :          0
                                        Tx abort              :          0
```

Table 55: show controllers switch inter-rack statistics Field Descriptions

Field	Description
Port	Logical port number. The range is from 0 to 21 and corresponds to the ports on the front panel.
Tx Frames	Transmit frame counter.
Tx Errors	Transmit cell error counter.
Rx Frames	Receive frame counter.
Rx Errors	Receive code error counter.
Rx fragment	Receive fragment counter.

Field	Description
Rx unicast	Receive unicast frame counter.
Rx multicast	Receive multicast frame counter.
Rx broadcast	Receive broadcast frame counter.
Rx FCS error	Receive FCS error frame counter.
Rx Pause	Receive pause frame counter.
Rx Undersize	Receive undersize frame counter.
Rx FFP drop	Packets dropped by FFP counter.
Rx Control frame	Receive control frame counter.
Tx fragment	Transmit fragment counter.
Tx unicast	Transmit unicast frame counter.
Tx multicast	Transmit multicast frame counter
Tx broadcast	Transmit broadcast frame counter
Tx FCS error	Transmit FCS error frame counter
Tx Pause	Transmit pause control frame counter.
Tx Oversize	Transmit oversize packet counter.
Tx CFI drop	Number of CFI packets dropped for this port.
Tx Cell error	Transmit cell error counter.
Tx Jabber	Transmit jabber counter.
Tx excessive collision	Transmit excessive collision frame counter.
Tx tagged vlan	Transmit tagged VLAN packet counter.
Tx abort	Transmit aborted packet counter.

show controllers switch inter-rack stp

To display information for the spanning tree protocol (STP) of inter-rack switches for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card, use the **show controllers switch inter-rack stp** command in administration EXEC mode.

show controllers switch inter-rack stp location *node-id* | **ports** *interface number* **location** *node-id* | **region location** *node-id*

Syntax Description

location *node-id*	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the *node-id* argument as entered in the *rack/slot/module* notation.
ports *interface number*	Displays the number for the Gigabit Ethernet interface. The range is from 0 to 21. The interface number that identifies the specific front panel GE port on the 22-port SCGE.
region	Displays MST region configuration information that includes MST revision number, instance to VLAN mapping, and MST region name.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
fabric	read
root-system	read
admin	read

Examples

The following sample output displays information for STP:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch inter-rack stp location f0/sc0/cpu0

##### MST   0 vlans mapped:   2-4094
Bridge        address 5246.48f0.20ff  priority      32768 (32768 sysid 0)
Root          this switch for the CIST
Operational   hello time  1, forward delay  6, max age  8, txholdcount  6
```

```
Configured    hello time  1, forward delay  6, max age  8, max hops     4

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ----------------------------

##### MST   1 vlans mapped:   1
Bridge         address 5246.48f0.20ff  priority      32769 (32768 sysid 1)
Root           this switch for MST1

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ----------------------------
           GE_13 Desg  FWD    20000 128.  14 P2p
           GE_14 Desg  FWD    20000 128.  15 P2p
           GE_15 Desg  FWD    20000 128.  16 P2p
           GE_17 Desg  FWD    20000 128.  18 P2p
           GE_22 Desg  FWD    20000 128.  23 P2p
```

Table 56: show controllers switch inter-rack stp Field Descriptions

Field	Description
MST	Multiple Spanning Tree (MST).
vlans mapped	Number of VLANs mapped.
Bridge	Part of the bridge identifier and is taken as the most significant part of the bridge ID comparisons.
Root	MAC address of Root and Priority.
Operational	Operational STP parameters.
Configured	STP configured parameters.
Interface	Interface running STP.
Role	MSTP role that includes designated, alternate, root, and backup.
Sts	Spanning tree state (STS) that includes forwarding, blocking, and learning.
Cost	Cost associated with the port.
Prio.	Priority associated with the port.

show controllers switch inter-rack udld

To display the inter-rack connection for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card, use the **show controllers switch inter-rack udld** command in administration EXEC mode.

show controllers switch inter-rack udld *interface number* | **all location** *node-id*

Syntax Description

interface number	Number for the Gigabit Ethernet interface. The range is from 0 to 21. The interface number identifies the specific front panel GE port on the 22-port SCGE.
all	Displays statistics of all ports for inter-rack switches.
location *node-id*	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the *node-id* argument as entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
fabric	read
root-system	read
admin	read

Examples

The following sample output shows who is connected to the inter-rack on the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch inter-rack udld all location f0/sc0/cpu0

Interface Gig port# 13
---
…
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
…
…
    Entry 1
    ---
```

```
…
Device name: 0_RP0_CPU0_Switch
Port ID: GE_Port_0
Neighbor echo 1 device: nodeF0_SC0_CPU0
Neighbor echo 1 port: Gig port# 13
```

Table 57: show controllers switch inter-rack udld Field Descriptions

Field	Description
Interface Gig port	Interface number that identifies the specific front panel GE port on the 22-port SCGE.
Current bidirectional state	Current bidirectional state of the port is undetermined, bidirectional, or unidirectional.
Current operational state	Port operational status that includes up or error-disabled.
Device name	Connected device or neighbor.
Port ID	Port ID.
Neighbor echo 1 device	Device ID of neighbor.
Neighbor echo 1 port	Port ID of neighbor.

show controllers switch stp location

To display the STP information for intra-rack switches, use the **show controllers switch stp location** command in administration EXEC mode.

show controllers switch stp location *node-id*

Syntax Description

node-id	The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The spanning tree protocol (STP) runs on links between RPs and SCs.

Task ID

Task ID	Operations
fabric	read
root-system	read

Examples

The following sample output shows how to verify information for the spanning tree for location 0/rp0/CPU0 on the RP:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch stp location 0/rp0/Cpu0

##### MST   0 vlans mapped:   2-4094
Bridge        address 0011.93ef.e392  priority      36864 (36864 sysid 0)
Root          address 5246.48f0.20ff  priority      32768 (32768 sysid 0)
              port       GE_Port_0    path cost           0
Regional Root address 5246.48f0.20ff  priority      32768 (32768 sysid 0)
                                      internal cost     20000 rem hops  3
Operational   hello time  1, forward delay  6, max age  8, txholdcount  6
Configured    hello time  1, forward delay  6, max age  8, max hops     4

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------

##### MST   1 vlans mapped:   1
Bridge        address 0011.93ef.e392  priority      36865 (36864 sysid 1)
Root          address 5246.48f0.20ff  priority      32769 (32768 sysid 1)
              port       GE_Port_0    cost              20000 rem hops  3
```

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ------------------------------
       FE_Port_1 Desg  FWD   200000 128.   2 P2p
       GE_Port_0 Root  FWD    20000 128.  49 P2p
```

The following sample output shows how to verify the connection on intra-rack switches for the 22-port SCGE card:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch stp location f0/sc0/CPU0

##### MST   0 vlans mapped:   2-4094
Bridge        address 0800.453e.469a  priority      36864 (36864 sysid 0)
Root          address 5246.48f0.20ff  priority      32768 (32768 sysid 0)
              port       GE_Port_0    path cost            0
Regional Root address 5246.48f0.20ff  priority      32768 (32768 sysid 0)
                                      internal cost     20000 rem hops  3
Operational   hello time  1, forward delay  6, max age  8, txholdcount  6
Configured    hello time  1, forward delay  6, max age  8, max hops     4

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ----------------------------

##### MST   1 vlans mapped:   1
Bridge        address 0800.453e.469a  priority      36865 (36864 sysid 1)
Root          address 5246.48f0.20ff  priority      32769 (32768 sysid 1)
              port       GE_Port_0    cost              20000 rem hops  3

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ------------------------------
       FE_Port_1 Desg  FWD   200000 128.   2 P2p
       GE_Port_0 Root  FWD    20000 128.  49 P2p
```

Table 58: show controllers switch stp location Field Descriptions

Field	Description
MST	Multiple Spanning Tree Protocol (MST).
vlans mapped	VLANs mapped to MST instance.
Bridge	MAC address of Bridge and Priority.
Root	MAC address of Root and Priority.
Regional Root	Root of the MST region.
Operational	Operational STP parameters.
Configured	STP configured parameters.
Interface	Interface running STP.
Role	MSTP role that includes designated, alternate, root, and backup.
Sts	Spanning tree state (STS) that includes forwarding, blocking, and learning.

Field	Description
Cost	Cost of path to root.
Prio.Nbr Type	Priority of switch port.

show controllers switch stp ports

To display the Spanning Tree Protocol (STP) information for intra-rack switches, use the **show controllers switch stp ports** command in administration EXEC mode.

show controllers switch stp ports FE 0 | 1 | GE 0 | 1 location *node-id*

Syntax Description

FE {**0** | **1**}	Displays information for the Fast Ethernet (FE) port. Choose one of the following values: • 0—FE port number 0. • 1—FE port number 1.
GE {**0** | **1**}	Displays information for the Gigabit Ethernet (GE) port. Choose one of the following values: • 0—GE port number 0. • 1—GE port number 1.
location *node-id*	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the *node-id* argument as entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note The port numbers must match the port numbers that are displayed on the front panel of the 22-port SCGE card.

Task ID

Task ID	Operations
fabric	read
root-system	read

Examples

The following example shows the remote-end point that is connected to the GE link even if the remote endpoint is on a different chassis:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch stp ports FE 1 location 0/rp0/CPU0
```

```
FE_Port_1 of MST1 is designated forwarding
Edge port:             no        (default) port guard :    none     (default)
Link type: point-to-point           (auto) bpdu filter: disable     (default)
Boundary : internal                        bpdu guard : disable     (default)
Bpdus (MRecords) sent 9190, received 3

Instance Role Sts Cost      Prio.Nbr Vlans mapped
-------- ---- --- --------- -------- --------------------------------
       1 Desg  FWD   200000 128.   2 1
```

Table 59: show controllers switch stp ports Field Descriptions

Field	Description
GE Port	Gigabit Ethernet (GE) port.
STP State	Spanning Tree Protocol (STP) state of the port

show controllers switch stp region

To display information for the spanning tree for the Multiple Spanning Tree (MST) region, use the **show controllers switch stp region** command in administration EXEC mode.

show controllers switch stp region location *node-id*

Syntax Description

location *node-id*	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the *node-id* argument as entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
fabric	read
root-system	read

Examples

The following example displays sample output from the **show controllers switch stp region** command:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch stp region location 0/rp0/CPU0

Name      [STP_1]
Revision      1
Instances configured 2

--------  ------------------------------------------------------------------------
   0      2-4094
   1      1
---------------------------------------------------------------------------------
```

show controllers switch udld location

To display the Unidirectional Link Detection (UDLD) information for intra-rack switches, use the **show controllers switch udld location** command in administration EXEC mode.

show controllers switch udld locationn *ode-id*

Syntax Description

node-id	The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

UDLD runs on links between RPs and SCs.

Task ID

Task ID	Operations
fabric	read
root-system	read

Examples

The following sample output shows who is connected on the RP:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch udld location 0/rp0/CPU0

Interface GE_Port_0
…
…
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
…
    Entry 1
    ---
    Device name: nodeF0_SC0_CPU0
    Port ID: Gig port# 13
    Neighbor echo 1 device: 0_RP0_CPU0_Switch
    Neighbor echo 1 port: GE_Port_0
```

The following sample output shows an intra-rack connection for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch udld location f0/sc0/CPU0

Interface GE_Port_0
---
…
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
…

    Entry 1
    ---
    …
    Current neighbor state: Bidirectional
    Device name: nodeF0_SC0_CPU0
    Port ID: Gig port# 22
    Neighbor echo 1 device: F0_SC0_CPU0_Switch
    Neighbor echo 1 port: GE_Port_0
```

Table 60: show controllers switch udld location Field Descriptions

Field	Description
Current bidirectional state	Current bidirectional state of the port is undetermined, bidirectional, or unidirectional.
Current operational state	Port operational status that includes up or error-disabled.
Current neighbor state	Neighbor state states that the link state is observed from the neighbor (undetermined, bidirectional, or unidirectional).
Device name	Connected device or neighbor.
Port ID	Port ID.
Neighbor echo 1 device	Device ID of neighbor.
Neighbor echo 1 port	Port ID of neighbor.

show controllers switch udld ports

To display the information for Unidirectional Link Detection (UDLD) for a specified location, use the **show controllers switch udld ports** command in administration EXEC mode.

show controllers switch udld ports FE 0 | 1 | GE 0 | 1 location *node-id*

Syntax Description

FE {**0** | **1**}	Displays information for the Fast Ethernet (FE) port. Choose one of the following values: • 0—FE port number 0. • 1—FE port number 1.
GE {**0** | **1**}	Displays information for the Gigabit Ethernet (GE) port. Choose one of the following values: • 0—GE port number 0. • 1—GE port number 1.
location *node-id*	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the *node-id* argument as entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.4.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

UDLD runs on links between RPs and SCs.

Task ID

Task ID	Operations
fabric	read
root-system	read

Examples

The following example displays sample output from the **show controllers switch udld ports** command:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch udld ports FE 1 location 0/rp0/CPU0

Interface FE_PORT_1
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
```

```
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 7
Time out interval: 5

    Entry 1
    ---
    Expiration time: 16
    Device ID: 1
    Current neighbor state: Bidirectional
    Device name: 0_RP1_CPU0_Switch
    Port ID: FE_PORT_0
    Neighbor echo 1 device: 0_RP0_CPU0_Switch
    Neighbor echo 1 port: FE_PORT_1

    Message interval: 7
    Time out interval: 5
    CDP Device name: BCM_SWITCH
```

Link Bundling Commands

This module provides command line interface (CLI) commands for configuring Link Bundle interfaces on the Cisco CRS Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

backbone interface

To configure interchassis group ICCP backbone interface, use the **backbone interface** command in the redundancy group ICCP configuration mode. To return to the default behavior, use the **no** form of this command.

backbone 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

None

Command Modes

Redundancy group ICCP configuration

Command History

Release	Modification
Release 4.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
config-services	read, write

Examples

This example shows how to configure interchassis group ICCP backbone interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# redundancy iccp group 10
RP/0/RP0/CPU0:router(config-redundancy-iccp-group)# backbone interface GigabitEthernet
0/2/1/0
RP/0/RP0/CPU0:router(config-redundancy-iccp-group)#
```

Related Commands

Command	Description
redundancy iccp group, on page 606	Configures Inter Chassis Communication Protocol (ICCP) parameters.

bundle lacp delay

To apply delay of a specified duration in adding a member to a specific bundle, use the **bundle lacp-delay** command in the interface configuration mode.

bundle lacp-delay

Syntax Description

lacp-delay	Duration of delay before a member is added to the bundle. The range is from 1 sec to 15 sec.

Command Default

No default behavior or values. If not configured, there is no delay that is imposed on bundle members.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
bundle	read, write

Examples

The following example shows how to set the delay for a newly added member on a bundle interface. In this example, the delay defined is for 6 secs:

```
RP/0/RP0/CPU0:router(config)# int bundle-ether 1
RP/0/RP0/CPU0:router(config-if)#bundle lacp-delay ?
<1000-15000>  Lacp-delay timeout in milliseconds
RP/0/RP0/CPU0:router(config-if)#bundle lacp-delay 6000
RP/0/RP0/CPU0:router(config-if)#commit
```

Related Commands

Command	Description
bundle maximum-active links, on page 577	
show bundle, on page 607	Displays information about configured bundles.

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** | **TenGigabitEthernet** | **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.
TenGigE	Specifies the 10 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.
location	Location of source interface.

Command Default

No default behavior or values

Command Modes

EXEC mode

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 or L4/7-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 or L4/7-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.

Table 61: bundle-hash Command Options, on page 570 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 61: bundle-hash Command Options, on page 570.

Table 61: 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
L4/7-tuple	L3 information: • Source IP address • Destination IP address • Protocol L4 information: • Source port • Destination port Platform-related information: • Router ID • Ingress interface
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
IPv6	IPv6 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/RP0/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 28) using the 3-tuple hash algorithm, a single source and destination, and IPv4 addresses:

```
RP/0/RP0/CPU0:router# bundle-hash bundle-ether 28

Specify load-balance configuration (L3/3-tuple or L4/7-tuple) (L3,L4): l3
Single SA/DA pair (IPv4,IPv6) or range (IPv4 only): S/R [S]: s

Enter bundle type IP V4 (1) or IP V6 (2): 1
Enter source IP V4 address: 10.12.28.2
Enter destination IP V4 address: 10.12.28.1
Compute destination address set for all members? [y/n]: y
Enter subnet prefix for destination address set: 8
Enter bundle IP V4 address [10.12.28.2]: 10.12.28.2

Link hashed to is GigabitEthernet0/6/5/7

Destination address set for subnet 10.0.0.0:
  10.0.0.6 hashes to link GigabitEthernet0/1/5/6
  10.0.0.8 hashes to link GigabitEthernet0/6/5/5
  10.0.0.12 hashes to link GigabitEthernet0/6/5/6
  10.0.0.2 hashes to link GigabitEthernet0/6/5/7
  10.0.0.1 hashes to link GigabitEthernet0/1/5/7
```

The following example shows how to calculate load balancing across the members of a link bundle (bundle-ether 28) using the 3-tuple hash algorithm, a range of source and destinations, and IPv4 addresses:

```
RP/0/RP0/CPU0:router# bundle-hash bundle-ether 28

Specify load-balance configuration (L3/3-tuple or L4/7-tuple) (L3,L4): l3
Single SA/DA pair (IPv4,IPv6) or range (IPv4 only): S/R [S]: r


Maximum number of flows (num src addr * num dst addr): 65536

Enter first source IP address: 10.12.28.2
Enter subnet prefix for source address set: 8
Enter number of source addresses (1-245): 20
Enter source address modifier (1-12) [def:1]: 5

  Enter destination IP address: 10.12.28.1
  Enter subnet prefix for destination address set: 8
```

```
  Enter number of destination addresses (1-245): 20
Enter destination address modifier (1-12) [1]: 5
Many to many (M) or simple pairs (S)? [M]: s

Calculating simple pairs...

Total number of hits 20
Member GigabitEthernet0/1/5/6 has 6 hits
Member GigabitEthernet0/6/5/5 has 2 hits
Member GigabitEthernet0/6/5/6 has 2 hits
Member GigabitEthernet0/6/5/7 has 9 hits
Member GigabitEthernet0/1/5/7 has 1 hits
```

The following example shows how to calculate load balancing across the members of a link bundle (bundle-ether 202) using the 7-tuple hash algorithm, a single source and destination, and IPv4 addresses:

```
RP/0/RP0/CPU0:router# bundle-hash bundle-ether 202

Specify load-balance configuration (L3/3-tuple or L4/7-tuple) (L3,L4): l4
Single SA:SP/DA:SP pair (IPv4,IPv6) or range (IPv4 only): S/R [S]: s

Enter bundle type IP V4 (1) or IP V6 (2): 1
Enter source IP V4 address: 172.20.180.167
Enter destination IP V4 address: 172.30.15.42

  Ingress interface --
  - physical interface format: [ POS | GigabitEthernet | TenGigE ]R/S/I/P
  - bundle interface format:   [ Bundle-Ether | Bundle-POS ]bundle-id
  Enter ingress interface: GigabitEthernet0/2/0/3

  Enter L4 protocol (TCP,UDP,SCTP,L2TPV3,NONE): UDP
  Enter src port: 1000
  Enter destination port: 2000
Compute destination address set for all members? [y/n]: n

S/D pair 172.20.180.167:1000/172.30.15.42:2000 -- Link hashed to is GigabitEthernet0/3/3/6

Another? [y]: y

Enter bundle type IP V4 (1) or IP V6 (2): 1
Enter source IP V4 address [172.20.180.167]: 172.20.180.167
Enter destination IP V4 address [172.30.15.42]: 172.30.15.42

  Ingress interface --
  - physical interface format: [ POS | GigabitEthernet | TenGigE ]R/S/I/P
  - bundle interface format:   [ Bundle-Ether | Bundle-POS ]bundle-id
  Enter ingress interface [GigabitEthernet0/2/0/3]: GigabitEthernet0/2/0/3

  Enter L4 protocol (TCP,UDP,SCTP,L2TPV3,NONE) [udp]: UDP
  Enter src port [1000]: 1000
  Enter destination port [2000]: 2000
Compute destination address set for all members? [y/n]: y
Enter subnet prefix for destination address set: 24
Enter bundle IP V4 address [172.20.180.167]: 209.165.200.225

S/D pair 172.20.180.167:1000/172.30.15.42:2000 -- Link hashed to is GigabitEthernet0/3/3/6

Destination address set for subnet 172.30.15.0:
  S/D pair 172.20.180.167:1000/172.30.15.1:2000 hashes to link GigabitEthernet0/3/3/6
  S/D pair 172.20.180.167:1000/172.30.15.6:2000 hashes to link GigabitEthernet0/2/0/1
```

```
  S/D pair 172.20.180.167:1000/172.30.15.3:2000 hashes to link GigabitEthernet0/2/0/2
  S/D pair 172.20.180.167:1000/172.30.15.5:2000 hashes to link GigabitEthernet0/0/3/0

Another? [y]: n
```

The following example shows how to calculate load balancing across the members of a link bundle (bundle-ether 28) using the 7-tuple hash algorithm, a range of source and destinations, and IPv4 addresses:

```
RP/0/RP0/CPU0:HUCRS1#bundle-hash bundle-ether 33509
Thu May 18 00:07:56.222 EDT
Specify load-balance configuration (L3/3-tuple or L4/7-tuple) (L3,L4): L4
Single SA:SP/DA:SP pair (IPv4,IPv6) or range (IPv4 only) or Entropy Label (MPLS only): S/R/E
 [S]: S
Enter bundle type IP V4 (1) or IP V6 (2): 1
Enter source IP V4 address: 45.227.0.25
Enter destination IP V4 address: 35.227.0.25
  Ingress interface handler --
  Note: interface handler can be gotten by 'sh im data interface'
  Enter ingress interface handler (hex format): 0x000841b0
    Ingress interface Bundle-Ether218
  Enter L4 protocol (TCP,UDP,SCTP,L2TPV3,NONE): NONE
  Enter L4 protocol field [0]: 253
Compute destination address set for all members? [y/n]: n
S/D pair 45.227.0.25/35.227.0.25 -- Link hashed to is TenGigE0/5/0/1
```

Note To ensure that the hashing is done correctly, do not set the L4 protocol field value to 0.

Related Commands

Command	Description
show bundle, on page 607	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. To remove a port from the bundle, use the **no** form of the command.

bundle id *bundle-id* [**mode** **active** | **on** | **passive**]

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 3.2	This command was introduced.
Release 3.3.0	The **bundle id** command syntax was changed from **bundle-id**.

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/RP0/CPU0:router(config)# interface GigabitEthernet 0/1/5/0
RP/0/RP0/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/RP0/CPU0:router(config)# interface GigabitEthernet 0/6/5/7
RP/0/RP0/CPU0:router(config-if)# bundle id 5 mode active
```

Related Commands

Command	Description
show bundle, on page 607	Displays information about configured bundles.
show interfaces, on page 469	Displays statistics for all interfaces configured on the router or for a specific node.
show lacp bundle, on page 625	Displays detailed information about LACP ports and their peers.
show lacp port, on page 635	

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**]

Syntax Description

links	Number of active links you want to bring up in the specified bundle, up to the maximum supported on the platform. The range is 1 to 64.
hot-standby	Modifies some default timeouts, such as wait-while timer and suppress-flaps, to avoid bundle-level flaps when the highest priority link fails or recovers.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.8.0	The **hot-standby** keyword was added.

Usage Guidelines

Misconfiguration or inconsistent configuration with a remote side can be causing traffic loss even though the bundle is up. We recommend that you use LACP protocol to better protect against the misconfiguration.

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:

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.)

When you configure the **hot-standby** keyword, if the partner device is not XR, you may have to further modify the timeouts. Use the commands that are used for refining the timeouts on the partner device as well. For best performance, do not configure with **bundle-maximum-active links** command on the partner device.

The **bundle maximum-active links hot-standby** command can be configured at both ends. However, this will impact the switchover times.

Task ID

Task ID	Operations
bundle	read, write

Examples

The following example shows how to display information about Ethernet bundle 5:

```
RP/0/RP0/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/RP0/CPU0:router(config)# interface bundle-ether 5
RP/0/RP0/CPU0:router(config-if)# bundle maximum-active links 1
```

The following example shows how to set default values for timeouts, to avoid bundle-level flaps when the highest priority link fails or recovers:

```
RP/0/RP0/CPU0:router(config)# interface bundle-ether 5
RP/0/RP0/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/RP0/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/RP0/CPU0:router(config)# interface bundle-ether 5
RP/0/RP0/CPU0:router(config-if)#bundle maximum-active links 1
```

The following example shows how to display information about Ethernet bundle 5:

```
RP/0/RP0/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 582	Sets the number of active links required to bring up a specific bundle.
show bundle, on page 607	Displays information about configured bundles.
show lacp bundle, on page 625	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 3.3.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router(config)# interface Bundle-Ether 1
RP/0/RP0/CPU0:router(config-if)# bundle minimum-active bandwidth 620000
```

Related Commands

Command	Description
show bundle, on page 607	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 64.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.9.0	The command range maximum was changed from 32 to 64.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router(config)# interface Bundle-Ether 5
RP/0/RP0/CPU0:router(config-if)# bundle minimum-active links 2
```

Related Commands

Command	Description
bundle maximum-active links, on page 577	
show bundle, on page 607	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*

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 3.2	This command was introduced.
Release 3.3.0	The command name was changed from **lacp port-priority** to **bundle port-priority**.

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/RP0/CPU0:router# config
```

```
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# bundle port-priority 1
```

Related Commands

Command	Description
bundle id, on page 575	Adds a port to an aggregated interface or bundle.
show lacp bundle, on page 625	Displays detailed information about LACP ports and their peers.
show lacp port, on page 635	
show lacp system-id, on page 638	Displays the local system ID used by the LACP.

bundle wait-while

To specify the duration of the wait-while timer for a bundle, use the **bundle wait-while** command in the bundle interface configuration mode. To disable waiting, use the **no** form of the command.

bundle wait-while *wait-while-time*

Syntax Description

wait-while-time	Wait-while time, in milliseconds. The range is between 0 to 2000.

Command Default

The default wait-while time is 2000 milliseconds.

Command Modes

Bundle interface configuration (config-if)

Command History

Release	Modification
Release 5.1.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
bundle	read, write
interface	read, write

The following example shows how to configure the wait-while time.

```
RP/0/RP0/CPU0:router(config)# interface Bundle-Ether 100
RP/0/RP0/CPU0:router(config-if)#  bundle wait-while 20
```

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 mode

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
bundle	execute
basic-services	read, write

Examples

The following example shows how to clear LACP counters:

```
RP/0/RP0/CPU0:router# clear lacp counters
```

Related Commands

Command	Description
show lacp counters, on page 627	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*

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 mode

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
bundle	read, write

This example shows how to create an Ethernet bundle and enter interface configuration mode:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface Bundle-Ether 3
RP/0/RP0/CPU0:router(config-if)#
```

This example shows how to create a new POS bundle and enter interface configuration mode:

```
RP/0/RP0/CPU0:router(config)# interface Bundle-POS 10
RP/0/RP0/CPU0:router(config-if)#
```

Related Commands

Command	Description
show bundle, on page 607	Displays information about configured bundles.

isolation recovery-delay

To specify a delay before clearing the isolation condition after recovery from failure, use the **isolation recovery-delay** command in the redundancy group ICCP configuration mode. To return to the default value, use the **no** form of this command.

isolation recovery-delay *seconds*

Syntax Description

seconds	Recovery delay in seconds.

Command Default

By default, the delay is set to 180 seconds.

Command Modes

Redundancy group ICCP configuration

Command History

Release	Modification
Release 4.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Examples

This example shows how to configure ICCP parameters:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# redundancy iccp group 10
RP/0/RP0/CPU0:router(config-redundancy-iccp-group)# isolation recovery-delay 35
RP/0/RP0/CPU0:router(config-redundancy-iccp-group)#
```

Task ID

Task ID	Operations
config-services	read, write

Related Commands

Command	Description
redundancy iccp group, on page 606	Configures Inter Chassis Communication Protocol (ICCP) parameters.

lacp fast-switchover

To disable the wait-while timer in the LACP state machine, use the **lacp fast-switchover** command in interface configuration mode. To re-enable the wait-while timer, use the **no** form of this command.

lacp fast-switchover

Syntax Description

This command has no keywords or arguments.

Command Default

The wait-while timer in the LACP state machine is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

If you have 1:1 link protection enabled (you set the value of the **bundle maximum-active links** command to 1) on a bundle with member links running LACP, you can optionally disable the wait-while timer in the LACP state machine. Disabling this timer causes a bundle member link in standby mode to expedite its normal state negotiations, thereby enabling a faster switchover from a failed active link to the standby link.

Regardless of the type of switchover you are using, the default IEEE standard-based or the faster proprietary optimized switchover, the state negotiations of the standby link is expedited. (For more information about the switchover types, refer to the bundle maximum-active links, on page 577 command.) However, enabling the **lacp fast-switchover** command provides a greater benefit if used with the IEEE standard-based switchover.

Examples

The following example shows how to disable the wait-while timer for LACP-enabled member links of Bundle-Ether 28:

```
RP/0/RP0/CPU0:router(config)# interface Bundle-Ether 28
RP/0/RP0/CPU0:router(config-if)# lacp fast-switchover
```

The following example shows how to re-enable the wait-while timer for LACP-enabled member links of Bundle-Ether 28:

```
RP/0/RP0/CPU0:router(config)# interface Bundle-Ether 28
RP/0/RP0/CPU0:router(config-if)# no lacp fast-switchover
```

Related Commands

Command	Description
bundle maximum-active links, on page 577	

lacp non-revertive

To configure the currently active but lower priority port to remain active port even after a higher priority port is capable of being operational, use the **lacp non-revertive** command in the bundle interface configuration mode. To revert to the default configuration, use the **no** form of this command.

lacp non-revertive

This command has no keywords or arguments.

Command Default

A higher priority port would become the active port after it becomes operational again.

Command Modes

Bundle interface configuration mode

Command History

Release	Modification
Release 5.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
	read, write

Example

The following example shows how to configure the non-revertive behaviour on an LACP bundle interface.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface bundle-ether 1
RP/0/RP0/CPU0:router(config-if)# lacp non-revertive
```

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 mode

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/RP0/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/RP0/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/RP0/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/RP0/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/RP0/CPU0:router# lacp packet-capture gigabitethernet 0/2/0/0 stop
```

Related Commands

Command	Description
show lacp io, on page 629	Displays the LACP transmission information that used by the transmitting device for sending packets on an interface.
show lacp packet-capture, on page 632	Displays the contents of LACP packets that are sent and received on an interface.
lacp period short, on page 595	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*]

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 3.2	This command was introduced.
Release 3.9.0	The keywords **transmit** and **receive** were added.

Usage Guidelines

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.

Note Starting with Cisco IOS XR Software Release 7.1.1, the `lacp period short receive` and `lacp period short transmit` commands are deprecated. Use the `lacp period <time in milliseconds>` command to configure LACP receive and transmit time. Before using this command, you must first execute `lacp cisco enable` command in the bundle interface mode. Without `lacp cisco enable` command, the members may still transmit at the standard interval of 1 second.

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/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# lacp period short
RP/0/RP0/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:

Router A

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# lacp period short
RP/0/RP0/CPU0:router(config-if)# commit
```

Router B

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# lacp period short
RP/0/RP0/CPU0:router(config-if)# commit
```

Router A

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# lacp period short transmit 500
RP/0/RP0/CPU0:router(config-if)# commit
```

Router B

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# lacp period short transmit 500
RP/0/RP0/CPU0:router(config-if)# commit
```

Router A

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# lacp period short receive 500
RP/0/RP0/CPU0:router(config-if)# commit
```

Router B

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# lacp period short receive 500
RP/0/RP0/CPU0:router(config-if)# commit
```

Related Commands

Command	Description
show lacp io, on page 629	Displays the LACP transmission information that used by the transmitting device for sending packets on an interface.
show lacp packet-capture, on page 632	Displays the contents of LACP packets that are sent and received on an interface.
lacp packet-capture, on page 592	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 mode. To return to the default LACP system priority value, use the **no** form of this command.

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 mode

Command History

Release	Modification
Release 3.2	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/RP0/CPU0:router(config)# lacp system priority 100
```

The following example shows how to configure an LACP priority of 10 and MAC address on the Bundle-Ether interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface Bundle-Ether 1
RP/0/RP0/CPU0:router(config-if)# lacp system priority 10
RP/0/RP0/CPU0:router(config-if)# lacp system mac 00c1.4c00.bd15
RP/0/RP0/CPU0:router(config-if)# commit
```

Related Commands

Command	Description
show lacp system-id, on page 638	Displays the local system ID used by the LACP.

Command	Description
show lacp bundle, on page 625	Displays detailed information about LACP ports and their peers.
show lacp port, on page 635	

mlacp connect

To specify configuration options for connecting to mLACP peers, use the **mlacp connect** command in the redundancy ICCP group configuration mode. To disable this feature, use the **no** form of this command.

mlacp connect timeout *seconds*

Syntax Description

timeout	Specifies the time to wait before assuming mLACP peer is down.
seconds	Number of seconds to wait before assuming the mLACP peer is down.

Command Default

No default behavior or values

Command Modes

Redundancy ICCP group configuration

Command History

Release	Modification
Release 4.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
bundle	read, write

Examples

This example shows how to specify configuration options for connecting to mLACP peers:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# redundancy iccp group 10
RP/0/RP0/CPU0:router(config-redundancy-iccp-group)# mlacp connect timeout 100
RP/0/RP0/CPU0:router(config-redundancy-iccp-group)#
```

Related Commands

redundancy iccp group	Configures ICCP parameters.

mlacp iccp-group

To configure ICCP redundancy group for a bundle, use the **mlacp iccp-group** command in bundle interface configuration mode. To return to the default value, use the **no** form of this command.

mlacp iccp-group *group-id*

Syntax Description

group-id	Specifies the ICCP redundancy group in which the bundle should operate. The group-id value ranges between 1-4294967295.

Command Default

The bundle behaves as a single chassis LAG.

Command Modes

Bundle interface configuration

Command History

Release	Modification
Release 4.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
Bundle	read, write

Examples

The following example shows how to configure an ICCP redundancy group for a bundle:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface Bundle-Ether 30
RP/0/RP0/CPU0:router(config-if)# mlacp iccp-group 200
RP/0/RP0/CPU0:router(config-if)#
```

mlacp node

To configure the mLACP node ID to be used in the ICCP group, use the **mlacp node** command in the redundancy ICCP group configuration mode. To return to the default value, use the **no** form of this command.

mlacp node *node-id*

Syntax Description

node-id	Specifies the unique node ID in the ICCP group for this system. The node-id value ranges between 0 to 7.

Command Default

No default behavior or values

Command Modes

Redundancy ICCP group configuration

Command History

Release	Modification
Release 4.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
bundle	read, write

Examples

This example shows how to configure the mLACP node ID to be used in the ICCP group:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# redundancy iccp group 10
RP/0/RP0/CPU0:router(config-redundancy-iccp-group)# mlacp node 3
```

Related Commands

redundancy iccp group	Configures ICCP parameters.

mlacp port-priority

To set the priority for all member links, use the **mlacp port-priority** command in bundle interface configuration mode. To return to the default value, use the **no** form of this command.

mlacp port-priority *priority*

Syntax Description

priority	Specifies the priority for member ports. The priority value ranges between 1-65535. A lower value indicates higher priority.

Command Default

No default behavior or values

Command Modes

Bundle interface configuration

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
Bundle	read, write

Examples

This example shows how to set the priority for all member links:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface Bundle-Ether 30
RP/0/RP0/CPU0:router(config-if)# mlacp port-priority 20
```

mlacp system mac

To configure the LACP system ID to be used in an ICCP group, use the **mlacp system mac** command in the redundancy ICCP group configuration mode. To return to the default value, use the **no** form of this command.

mlacp system mac *mac-id*

Syntax Description

mac-id	Specifies the unique ID for the system.

Note A non-zero value is permitted.

Command Default

No default behavior or values

Command Modes

Redundancy ICCP group configuration

Command History

Release	Modification
Release 4.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
bundle	read, write

Examples

The following example shows how to configure the LACP system ID to be used in an ICCP group:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# redundancy iccp group 10
RP/0/RP0/CPU0:router(config-redundancy-iccp-group)# mlacp system mac 1.1.1
```

Related Commands

redundancy iccp group	Configures ICCP parameters.

mlacp system priority

To configure the LACP system priority to be used in the ICCP group, use the **mlacp system priority** command in the redundancy ICCP group configuration mode. To return to the default value, use the **no** form of this command.

mlacp system priority *priority*

Syntax Description

priority	Specifies the priority for the system. **Note** Lower value indicates higher priority.

Command Default

No default behavior or values

Command Modes

Redundancy ICCP group configuration

Command History

Release	Modification
Release 4.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
bundle	read, write

Examples

This example shows how to configure the LACP system priority to be used in the ICCP Group:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# redundancy iccp group 10
RP/0/RP0/CPU0:router(config-redundancy-iccp-group)# mlacp system priority 10
```

Related Commands

redundancy iccp group	Configures ICCP parameters.

redundancy iccp group

To configure Inter Chassis Communication Protocol (ICCP) parameters, use the **redundancy iccp group** command in the Global Configuration mode. To return to the default, use the **no** form of this command.

redundancy iccp group *group-id*

Syntax Description

group-id	Specifies ICCP group ID.

Command Default

ICCP redundancy is disabled.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
config-services	read, write

Examples

The following example shows how to configure ICCP parameters:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# redundancy iccp group 10
RP/0/RP0/CPU0:router(config-redundancy-iccp-group)#
```

show bundle

To display information about all bundles or a specific bundle of a particular type, use the **show bundle** command in EXEC 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 mode

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	• The output for this command was modified. • The **reasons** keyword was added.
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
Release 5.3.2	The "Non-revertive" output field was added.

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

The following example shows output for all bundle interfaces that are configured on the router:

```
RP/0/RP0/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
 Non-revertive:                           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 62: 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.
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.

Field	Description
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.
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.)

Field	Description
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.
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.

Field	Description
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" and "Disabled".
Non-revertive:	Displays whether non-revertive behavior for the bundle interface is enabled or not. The possible values are "Enabled" and "Disabled".
mLACP:	mLACP is not supported on the platform.
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.

Field	Description
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.
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.

Field	Description
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.
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.

Field	Description
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 63: 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.

Reason	Description
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.
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.

Reason	Description
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.
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.

Reason	Description
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.
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.

Reason	Description
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 588	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 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 mode

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
bundle	read

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/RP0/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 64: show bundle brief Field Descriptions, on page 619 describes the fields shown in the display.

Table 64: 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.

Field	Description
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.
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.

Field	Description
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 607	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 mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
bundle	read

Examples

```
RP/0/RP0/CPU0:router# show bundle replication bundle-ether 1 all
```

show iccp group

To display information for the ICCP parameters, use the **show iccp** command in EXEC mode.

show iccp group *group-id* | **location** *node-id*

Syntax Description

group-id	ICCP group ID.
location	Specifies the location.
node-id	Node ID. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 4.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
mpls-ldp	read

Examples

The following example shows the output of the **show iccp group** command:

```
RP/0/RP0/CPU0:router#show iccp group

Redundancy Group 1
  member ip:2.2.2.2 (router2), up (connected)
    monitor: route-watch (up)
  backbone interface Gi0/2/0/3: up
  enabled applications: mLACP
  isolation recovery delay timer: 180 s, not running
Redundancy Group 2
  member ip:2.2.2.2 (router2), up (disconnected)
    monitor: route-watch (up)
  backbone interface Gi0/2/0/3: up
  enabled applications: mLACP
  isolation recovery delay timer: 180 s, not running


RP/0/RP0/CPU0:router#show iccp group 1
Redundancy Group 1
  member ip:2.2.2.2 (router2), up (connected)
    monitor: route-watch (up)
  backbone interface Gi0/2/0/3: up
```

```
enabled applications: mLACP
isolation recovery delay timer: 180 s, not running
```

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 mode

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
bundle	read

Examples

The following example shows how to display LACP information for a specific Ethernet Bundle:

```
RP/0/RP0/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 65: 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.
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 575	Adds a port to an aggregated interface or bundle.
show bundle, on page 607	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 mode

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
bundle	read

Examples

The following example shows how to display LACP counters on an Ethernet bundle:

```
RP/0/RP0/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 66: 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 586	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 mode

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/RP0/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/RP0/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 632	Displays the contents of LACP packets that are sent and received on an interface.
lacp period short, on page 595	Enables a short period time interval for the transmission and reception of LACP packets.
lacp packet-capture, on page 592	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 mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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/RP0/CPU0:router# lacp packet-capture gigabitethernet 0/1/0/0 100
RP/0/RP0/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/RP0/CPU0:router# lacp packet-capture gigabitethernet 0/1/0/0 100
RP/0/RP0/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 629	Displays the LACP transmission information that used by the transmitting device for sending packets on an interface.
lacp period short, on page 595	Enables a short period time interval for the transmission and reception of LACP packets.
lacp packet-capture, on page 592	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 mode

Command History

Release	Modification
Release 3.2	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/RP0/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 67: 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.
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.

Field	Description
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 575	Adds a port to an aggregated interface or bundle.
show bundle, on page 607	Displays information about configured bundles.
show lacp bundle, on page 625	Displays detailed information about LACP ports and their peers.

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 mode

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

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/RP0/CPU0:router# show lacp system-id

Priority  MAC Address
--------  -----------------
  0x8000  08-00-45-3a-65-01
```

Table 68: show lacp system-id Field Descriptions

Field	Description
Priority	Priority for this system. A lower value is higher priority.
MAC Address	MAC address associated with the LACP system ID.

Related Commands

Command	Description
bundle id, on page 575	Adds a port to an aggregated interface or bundle.
show bundle, on page 607	Displays information about configured bundles.

Command	Description
show lacp bundle, on page 625	Displays detailed information about LACP ports and their peers.
show lacp port, on page 635	

show mlacp

To display the MC-LAG information configured locally and for any connected mLACP peer devices, use the **show mlacp** command in the EXEC mode.

show mlacp [**Bundle-Ether** *interface-path-id* | **iccp-group** *group-id*] [**brief** | **verbose**]

Syntax Description

Bundle-Ether *interface-path-id*	Displays the information for the ICCP group of the bundle and only the specified bundle.
iccp-group *group-id*	Displays information related to the ICCP group.
brief	Displays only the ICCP group information without any bundle information.
verbose	Displays the ICCP group, the bundle and member information.

Command Default

No default behavior or values

Command Modes

Exec

Command History

Release	Modification
Release 4.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
bundle	Read

Examples

These examples display the MC-LAG information:

```
RP/0/RP0/CPU0:router# show mlacp brief

ICCP Group 1
  Connect timer:  Off

  Node  LDP ID           State         System ID                 Sync   Vers
  ----  ---------------  ------------  ------------------------  -----  ----
     1  5.4.3.1          Up            0x0001,00-0d-00-0e-00-0f  Done   1
     2  Local            Up            0x0001,00-0d-00-0e-00-0f  Done   -

RP/0/RP0/CPU0:poa2#show mlacp

ICCP Group 1
  Connect timer:  Off

  Node  LDP ID           State         System ID                 Sync   Vers
  ----  ---------------  ------------  ------------------------  -----  ----
```

```
     1  5.4.3.1          Up            0x0001,00-0d-00-0e-00-0f  Done   1
     2  Local            Up            0x0001,00-0d-00-0e-00-0f  Done   -


  Bundle-Ether1 (ROID: 0000.0001.0000.0000)
    Node  Aggregator Name       State       Agg ID  MAC Address
    ----  --------------------  ----------  ------  --------------
       1  BE1                   Up          0x0001  0000.deaf.0000
       2  Bundle-Ether1         Up          0x0001  0000.deaf.0000

RP/0/RP0/CPU0:router#show mlacp verbose

ICCP Group 1
  Connect timer:  Off

  Node  LDP ID           State         System ID                 Sync   Vers
  ----  ---------------  ------------  ------------------------  -----  ----
     1  5.4.3.1          Up            0x0001,00-0d-00-0e-00-0f  Done   1
     2  Local            Up            0x0001,00-0d-00-0e-00-0f  Done   -


  Bundle-Ether1 (ROID: 0000.0001.0000.0000)
    Node  Aggregator Name       State       Agg ID  MAC Address
    ----  --------------------  ----------  ------  --------------
       1  BE1                   Up          0x0001  0000.deaf.0000
       2  Bundle-Ether1         Up          0x0001  0000.deaf.0000

                                                      Priority
    Node  Port Name             State       Port    Oper   (Cfgd)
    ----  --------------------  ----------  ------  --------------
       1  Gi0/1/0/3             Up          0x9001  0x03e8 (0x03e8)
       2  Gi0/0/0/1             Up          0xa001  0x07d0 (0x07d0)
```

show mlacp counters

To display counters relating to mLACP information transferred to and from the local device, use the **show mlacp counters** command in the EXEC mode.

show mlacp counters [**bdl-info** | **ig-info** | **mbr-info** [**bundle interface** | **member interface** | **iccp-group** *group-id* | **mlacp-device** *device-id* | **mlacp-interface** *foreign-member-interface*]]

Syntax Description

Bundle-Ether	Displays the requested information associated with the bundle interface.
member interface	Displays the requested information associated with the member interface.
counters	Displays information on the mLACP counters.
bdl-info	Displays the bundles counters.
ig-info	Displays the ICCP group counters.
mbr-info	Displays the member counters.
mlacp-device	Displays the requested information associated with the mLACP device. **Note** The **mlacp-device** and **mlacp-interface** keywords are available only when mLACP devices and mLACP interfaces are configured.
mlacp-interface	Displays the requested information associated with the mLACP interface.

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 4.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
bundle	Read

Examples

These examples display MC-LAG counter information:

Note The GigabitEthernet 0/0/0/1 is configured to Bundle-Ether 1 which is within ICCP Group1. Hence, the **show mlacp counters bdl-info GigabitEthernet 0/0/0/1** command displays the counters of the bundle that GigabitEthernet 0/0/0/1 is associated with (i.e. Bundle-Ether1). The **show mlacp counters mbr-info Bundle-Ether 1** displays the counters of the members that Bundle-Ether1 is associated with (locally: GigabitEthernet 0/0/0/1, and on the foreign device: GigabitEthernet 0/1/0/3).

```
RP/0/RP0/CPU0:router# show mlacp counters bdl-info GigabitEthernet 0/0/0/1

ICCP Group 1
                                      TLVs Sent                TLVs Received
Bundle                Config     State      Priority    NAKs        Priority
--------------------  ---------------------------------  ----------------------
Local Device
Bundle-Ether1 ????????????3          4          0           0          0
mLACP Peer 5.4.3.1
Bundle-Ether1 ????????????3          4          0           0          0

                                Sync Requests
Bundle                TLVs       (config)   (state)     Last Cleared
--------------------  ---------------------------------  ------------
Local Device
Bundle-Ether1 ???????????0          0          0        18m12s
mLACP Peer 5.4.3.1
Bundle-Ether1 ???????????0          0          0        17m57s


RP/0/0/CPU0:router#show mlacp counters mbr-info Bundle-Ether 1

Bundle-Ether1 (ICCP Group 1)
                                      TLVs Sent                TLVs Received
Port                  Config     State      Priority    NAKs        Priority
--------------------  ---------------------------------  ----------------------
Local Device
Gi0/0/0/1 ???????????????7          0          0           0          0
mLACP Peer 5.4.3.1
Gi0/1/0/3 ???????????????7          5          3           0          0

                                Sync Requests
Port                  TLVs       (config)   (state)     Last Cleared
--------------------  ---------------------------------  ------------
Local Device
All ports ????????????????0          0          0         19m3s
Gi0/0/0/1 ????????????????0          0          0         19m3s
mLACP Peer 5.4.3.1
All ports ????????????????1          1          1        18m49s
Gi0/1/0/3 ????????????????0          0          0        18m49s
```

Management Ethernet Interface Commands

This module provides command line interface (CLI) commands for configuring Management Ethernet interfaces on the Cisco CRS Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

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

Syntax Description

full	Configures the Management Ethernet interface to operate in full duplex mode.

Note The system does not support half duplex on Management Ethernet interface.

Command Default

Autonegotiates duplex operation

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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

The following example shows how to return a Management Ethernet interface to autonegotiated duplex mode:

```
RP/0/RP0/CPU0:router(config)# interface MgmtEth 0/RP0/CPU0/0
RP/0/RP0/CPU0:router(config-if)# no duplex
```

Related Commands

Command	Description
interface MgmtEth, on page 648	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*

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 mode

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router(config)# interface MgmtEth 0/RP0/CPU0/0
RP/0/RP0/CPU0:router(config-if)#
```

Related Commands

Command	Description
duplex (Management Ethernet), on page 646	Configures duplex mode operation on a Management Ethernet interface.
mac-address (Management Ethernet), on page 651	Sets the MAC layer address of a Management Ethernet interface.
speed (Management Ethernet), on page 652	Configures the speed for a Management Ethernet interface.

ipv6 address autoconfig

The **ipv6 address** command is used to configure IPv6 addresses or prefix on the interface. This command enables IPv6 processing on the interface. To remove all manually configured IPv6 addresses from an interface, use the **no ipv6 address** command without arguments.

ipv6 address { *[ipv6addr]* | *[ipv6-prefix/prefix length]* | [autoconfig] }

Syntax Description

ipv6addr	(Optional) Specify the IPv6 address.
ipv6-prefix/prefix length	(Optional) Specify the IPv6 prefix and the prefix length preceded by a slash [/].
autoconfig	(Optional) Enalbe IPv6 Stateless Address Auto Configuration (SLAAC) on Management interface. **Note** The **autoconfig** option is only available for Management Interfaces.

Command Default

No default behavior or values

Command Modes

Management Interface Configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

In the **ipv6 address** interface configuration command, you can enter the *ipv6addr* or *ipv6-prefix/prefix length* variables with the address specified in hexadecimal using 16-bit values between colons. The *prefix length* variable (preceded by a slash [/]) is a decimal value that shows how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

The IPv6 Stateless Address Auto Configuration (SLAAC) is used to automatically assign IPv6 addresses to the host interfaces. This functionality can be used when the exact addresses used by the host need not be specific, as long as they are unique and can be properly routed. SLAAC helps in automating provisioning of the router. IPv6 auto configuration is disabled by default. To enable IPv6 SLAAC on Management interface, use the **ipv6 address autoconfig** command on the Management interface configuration mode.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure the IPv6 address based on the IPv6 prefix 2001:0DB8:c18:1::/64:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitEthernet 0/2/0/0
```

```
RP/0/RP0/CPU0:router(config-if)# ipv6 address 2001:0DB8:c18:1::/64
```

The following example shows how to enable IPv6 auto configuration on router:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface mgmtEth 0/RSP0/CPU0/0
RP/0/RP0/CPU0:router(config-if)# ipv6 address autoconfig
```

Related Commands

Command	Description
interface MgmtEth, on page 648	Enters interface configuration mode for the 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*

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 2.0	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).

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/RP0/CPU0:router(config)# interface MgmtEth 0/RP0/CPU0/0
RP/0/RP0/CPU0:router(config-if)# mac-address 0001.2468.ABCD
```

Related Commands

Command	Description
interface MgmtEth, on page 648	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

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 2.0	This command was introduced.

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 69: Relationship Between duplex and speed Commands, on page 652 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 69: 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.
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 Command	speed Command	Resulting System Action
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/RP0/CPU0:router(config)# interface MgmtEth 0/RP0/CPU0/0
RP/0/RP0/CPU0:router(config-if)# speed 1000
```

Related Commands

Command	Description
interface MgmtEth, on page 648	Enters interface configuration mode for the Management Ethernet interface.

Null Interface Commands

This module provides command line interface (CLI) commands for configuring null interfaces on the Cisco CRS 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 2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router(config)# interface null 0
RP/0/RP0/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/RP0/CPU0:router(config)# interface null 0
RP/0/RP0/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 3.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router# show controllers null interface

Null interface:
name     : Null0
handle   : 0x00080010
rx_count : 0
tx_count : 0
drops    : 0
```

Table 70: show controllers null interface Field Descriptions

Field	Description
name	Interface whose controller information is displayed.
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.

Field	Description
drops	Total number of packets dropped by the interface.

Related Commands

Command	Description
show interfaces null0, on page 659	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

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/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

This module provides command line interface (CLI) commands for configuring Packet-over-SONET/SDH (POS) on the Cisco CRS Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

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**

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 2.0	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
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 674	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**

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 2.0	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/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
```

Related Commands

Command	Description
show interfaces pos, on page 671	Displays information about a POS interface.

Command	Description
show ppp interfaces (BNG), on page 714	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* [**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.
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 mode

Command History

Release	Modification
Release 2.0	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, write

Examples

The following example shows how to enter interface configuration mode for a POS interface:

```
RP/0/RP0/CPU0:router(config)# interface pos 0/1/0/0
RP/0/RP0/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/RP0/CPU0:router(config)# interface pos 0/1/1/2.1
RP/0/RP0/CPU0:router(config-subif)#
```

Related Commands

Command	Description
show interfaces pos, on page 671	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**

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 2.0	This command was introduced.
Release 3.9.0	The *retry* argument was added.

Usage Guidelines

HDLC 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/RP0/CPU0:router(config)# interface POS 0/7/0/1
RP/0/RP0/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 2.0	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/RP0/CPU0:router(config)# interface POS 0/1/0/2
RP/0/RP0/CPU0:router(config-if)# POS
RP/0/RP0/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/RP0/CPU0:router(config)# interface POS 0/1/0/2
RP/0/RP0/CPU0:router(config-if)# POS
RP/0/RP0/CPU0:router(config-if-pos)#
```

Related Commands

Command	Description
crc (POS), on page 662	Sets the length of the CRC on a Packet-over-SONET/SDH (POS) interface.
transmit-delay, on page 674	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 mode

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 4.0.0	The **summary** keyword was removed.

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/RP0/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 71: 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/RP0/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 72: 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.

Field	Description
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 782	Displays information on the POS controllers.
show controllers sonet, on page 788	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*

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

No specific guidelines impact the use of this command.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/1/0/2
RP/0/RP0/CPU0:router(config-if)# pos
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/1/0/2
RP/0/RP0/CPU0:router(config-if)# pos
RP/0/RP0/CPU0:router(config-if-pos)# no transmit-delay
```

Related Commands

Command	Description
show interfaces	

PPP Commands

This module provides command line interface (CLI) commands for configuring Point-to-Point Protocol (PPP) on the Cisco CRS Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

Point-to-Point Protocol (PPP) is an encapsulation scheme that can be used on Packet-over-SONET (POS) and serial 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

clear ppp sso state

To clear the replicated Inter-Chassis Stateful Switchover (ICSSO) states for the specified standby interface or for all interfaces on the specified node, use the **clear ppp sso state** command in EXEC mode.

clear ppp sso state interface *interface-path-id* | **all location** *node-id*

Syntax Description

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.
all location *node-id*	Specifies the full qualified path of a specific node in the format *rack*/*slot*/*module*.

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

This command sets the PPP sessions in the Standby-Up state to the Standby-Down state. All replicated data received from the peer is purged, and SSRP Request messages are re-sent to the peer.

Task ID

Task ID	Operations
ppp	execute

Examples

The following example shows how to clear the replicated ICSSO states for the specified standby interface:

```
RP/0/RP0/CPU0:router# clear ppp sso state interface 0/1/0/1
```

The following example shows how to clear the replicated Inter-Chassis Stateful Switchover (ICSSO) states for all interfaces on the specified node:

```
RP/0/RP0/CPU0:router# clear ppp sso state all location 1/0/1
```

clear ppp statistics

To clear all Point-to-Point Protocol (PPP) statistics for a PPP interface, use the **clear ppp statistics** command in EXEC mode.

clear ppp statistics interface *interface-path-id*

Syntax Description

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

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ppp	execute

Examples

The following example shows how to clear PPP statistics for a PPP interface:

```
RP/0/RP0/CPU0:router# clear ppp statistics interface 0/1/0/1
```

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

Syntax Description

This command has no keywords or arguments.

Command Default

PPP encapsulation is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
```

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router# interface serial 0/0/1/2/4:3
RP/0/RP0/CPU0:router# encapsulation ppp
```

Related Commands

Command	Description
show ppp interfaces (BNG), on page 714	Displays PPP state information for an interface.

group

To create a Session State Redundancy Protocol (SSRP) group and associate it with a profile, use the **group** command in Global Configuration mode. To remove this group, use the no form of this command.

group *group-id* **profile** *profile_name* [**default**]

Syntax Description

group-id	SSRP group identifier. The range is 1 to 65535.
profile *profile_name*	Profile to associate with this group.
default	Associates the group to the default profile.

Command Default

No default behavior or values

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

Any interfaces on this card can be configured to use this group. The group number must be unique across the router.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to create an SSRP group:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# ssrp location 0/1/cpu0
RP/0/RP0/CPU0:router(config-ssrp-node)# group 1 profile default
```

Related Commands

Command	Description
ssrp location, on page 726	specify the node on which to create a SSRP group and enter the SSRP node configuration mode.

multi-router aps

To configure Multi-Router Automatic Protection Switching (MR-APS) and enter APS redundancy configuration mode, use the **multi-router aps** command in redundancy configuration mode. To deactivate Multi-Router Automatic Protection Switching (MR-APS), use the no form of this command.

multi-router aps

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Redundancy configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ppp	read

Examples

The following example shows how to

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# redundancy
RP/0/RP0/CPU0:router(config-redundancy)# multi-router aps
RP/0/RP0/CPU0:router(config-redundancy-aps)
```

Related Commands

Command	Description
redundancy, on page 712	Enters the redundancy configuration mode to configure MR-APS.

peer ipv4 address

To configure the IPv4 address for a Session State Redundancy Protocol (SSRP) peer, use the **peer ipv4 address** command in SSRP configuration mode. To remove the address, use the no form of this command.

peer ipv4 address *ip-address*

Syntax Description

ip-address	IP address of the peer interface whose states will be replicated by SSRP.

Command Default

No default behavior or values

Command Modes

SSRP configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to configure the IPv4 address for a Session State Redundancy Protocol (SSRP) peer:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# ssrp profile Profile_1
RP/0/RP0/CPU0:router(config-ssrp)# peer ipv4 address 10.10.10.10
```

Related Commands

Command	Description
ssrp profile, on page 727	Configures a SSRP profile and enters the SSRP configuration mode.

ppp authentication (BNG)

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 in an appropriate configuration mode. To disable PPP authentication, use the **no** form of this command.

ppp authentication *protocol* [*protocol* [*protocol*]] *list-name* | **default**

Syntax Description

protocol	Name of the authentication protocol used for PPP authentication. See Table 73: PPP Authentication Protocols for Negotiation, on page 684 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

Dynamic template configuration

Command History

Release	Modification
Release 2.0	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.

To enter the dynamic template configuration mode, run **dynamic-template** command in the Global Configuration mode.

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 73: PPP Authentication Protocols for Negotiation, on page 684 lists the protocols used to negotiate PPP authentication.

Table 73: 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/4/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp authentication chap MIS-access
```

This is an example of configuring the **ppp authentication** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ppp authentication chap ms-chap pap
```

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*

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 2.0	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/RP0/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/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 1/0/1/0
RP/0/RP0/CPU0:router(config-if)# ppp chap password xxxx
RP/0/RP0/CPU0:router(config-if)# ppp chap password clear xxxx
RP/0/RP0/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 (BNG), on page 683	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 688	Refuses CHAP authentication from peers requesting it.
ppp max-bad-auth (BNG), on page 693	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

Syntax Description

This command has no keywords or arguments.

Command Default

CHAP authentication is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/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.

Command	Description
ppp authentication (BNG), on page 683	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 (BNG), on page 693	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 707	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 ipcp dns

To configure the primary and secondary Domain Name System (DNS) IP addresses for the Internet Protocol Control Protocol (IPCP), use the **ppp ipcp dns** command in interface configuration mode. To remove the addresses, use the no form of this command.

ppp ipcp dns *primary-ip-address* [*sec-ip-address*]

Syntax Description

primary-ip-address	Primary DNS IP address, in the format A.B.C.D.
sec-ip-address	Secondary DNS IP address, in the format W.X.Y.Z.

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

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to configure the primary and secondary DNS IP addresses for Internet Protocol Control Protocol (IPCP):

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ppp ipcp dns 10.10.10.10 10.10.10.11
```

ppp ipcp neighbor-route disable

To disable installation of a route to the peer address negotiated by Internet Protocol Control Protocol (IPCP), use the **ppp ipcp neighbor-route disable** command in interface configuration mode. To re-enable installation of a route to the peer address negotiated by IPCP, use the no form of this command.

ppp ipcp neighbor-route disable

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 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to disable installation of a route to the peer address negotiated by IPCP:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ppp ipcp neighbor-route disable
```

ppp ipcp peer-address default

To specify the default IPv4 address that is assigned to the peer by the Internet Protocol Control Protocol (IPCP), use the **ppp ipcp peer-address default** command in interface configuration mode. To remove the address, use the no form of this command.

ppp ipcp peer-address default *ip-address*

Syntax Description

ip-address	Specifies the IP address for the peer node.

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

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to specify the default IPv4 address that is assigned to the peer by IPCP.

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ppp ipcp peer-address default 10.10.10.10
```

ppp max-bad-auth (BNG)

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*

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

Dynamic template configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

The **ppp max-bad-auth** command applies to any interface on which PPP encapsulation is enabled.

To enter the dynamic template configuration mode, run **dynamic-template** command in the Global Configuration mode.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp authentication chap
RP/0/RP0/CPU0:router(config-if)# ppp max-bad-auth 3
```

This example shows how to allow two additional retries after an initial authentication failure in the dynamic template configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ppp max-configure 5
```

ppp max-configure (BNG)

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*

Syntax Description

retries	Maximum number of retries. Range is 4 through 20. Default is 10.

Command Default

retries: 10

Command Modes

Interface configuration

Dynamic template configuration

Command History

Release	Modification
Release 2.0	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.

To enter the dynamic template configuration mode, run **dynamic-template** command in the Global Configuration mode.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

This example shows a limit of four configure requests:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp max-configure 4
```

This example shows how a limit of four configure requests is specified in the dynamic template configuration mode:

```
RP/0/RP0/CPU0:router# configure
```

```
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ppp ipcp
```

Related Commands

Command	Description
ppp max-failure (BNG), on page 696	Configures the maximum number of consecutive CONFNAKs to permit before terminating a negotiation.

ppp max-failure (BNG)

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*

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

Dynamic template configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

To enter the dynamic template configuration mode, run **dynamic-template** command in the

Global Configuration mode.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp max-failure 3
```

This example shows how no more than three CONFNAKs are permitted before terminating the negotiation in the dynamic template configuration mode:

```
RP/0/RP0/CPU0:router# configure
```

```
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ppp max-failure 4
```

Related Commands

Command	Description
ppp max-configure (BNG), on page 694	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*

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 2.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp max-terminate 5
```

Related Commands

Command	Description
ppp max-configure (BNG), on page 694	Specifies the maximum number of configure requests to attempt (without response) before stopping the requests.
ppp max-failure (BNG), on page 696	Configures the maximum number of consecutive CONFNAKs to permit before terminating a negotiation.

ppp ms-chap hostname

To configure the hostname for MS-CHAP authentication on an interface, use the **ppp ms-chap hostname** command in interface configuration mode. To remove the hostname, use the no form of this command.

ppp ms-chap hostname *hostname*

Syntax Description

hostname	Specifies the hostname for MS-CHAP authentication.

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

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

The following example shows how to configure the hostname for MS-CHAP authentication on an interface:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ppp ms-chap hostname Host_1
```

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*

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/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

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp ms-chap refuse
```

Related Commands

Command	Description
ppp authentication (BNG), on page 683	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

To enable multiclass multilink PPP, use the **ppp multilink multiclass** command in interface configuration mode. To disable multiclass multilink PPP, use the no form of this command.

ppp multilink multiclass

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 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to enable multiclass multilink PPP:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface Multilink 0/1/0/0/1
RP/0/RP0/CPU0:router(config-if)# ppp multilink multiclass
```

ppp multilink multiclass local

To configure the initial number and maximum number of Multiclass Multilink PPP (MCMP) receive classes in a Conf-Request sent from a local host to its peer, use the **ppp multilink multiclass local** command in interface configuration mode. To remove these settings, use the no form of this command.

ppp multilink multiclass local initial *init-number* **maximum** *max-number*

Syntax Description

initial *init-number*	Specifies the initial number of receive classes in the Conf-Request. The range is 1 to 16.
maximum *max-number*	Specifies the maximum number of receive classes in the Conf-Request. The range is 1 to 16.

Command Default

When MCMP is enabled, the default **initial** value is 2 and the default **maximum** value is 4.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

The maximum number of receive classes configures the number of transmission classes on the local host.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to configure the initial number and maximum number of Multiclass Multilink PPP (MCMP) receive classes in a Conf-Request sent from a local host to its peer:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface Multilink 0/1/0/0/1
RP/0/RP0/CPU0:router(config-if)# ppp multilink multiclass local initial 1 maximum 16
```

ppp multilink multiclass remote apply

To configure the minimum number of Multiclass Multilink PPP (MCMP) receive classes that a local host will accept from its peer in a Conf-Request, use the **ppp multilink multiclass** command in interface configuration mode. To remove this setting, use the no form of this command.

ppp multilink multiclass remote apply *min-number*

Syntax Description

min-number	Specifies the minimum number of receive classes in the Conf-Request. The range is 1 to 16.

Command Default

The default is 2 if MCMP is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

This command is used to coerce the peer to accept a minimum number of MCMP classes. If the peer does not accept the minimum number of MCMP classes specified by this command, the local router will not bring up the PPP link.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to use the **ppp multilink multicast remove** apply command.

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface Multilink 0/1/0/0/1
RP/0/RP0/CPU0:router(config-if)# ppp multilink multiclass remote apply 16
```

Related Commands

Command	Description
ppp ipcp dns, on page 690	Configures the primary and secondary DNS IP addresses for the IPCP.
ppp ipcp neighbor-route disable, on page 691	Disables installation of a route to the peer address negotiated by IPCP.
ppp ipcp peer-address default, on page 692	Specifies the default IPv4 address that is assigned to the peer by the IPCP.
ppp ms-chap hostname, on page 699	Configures the hostname for MS-CHAP authentication on an 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

Syntax Description

This command has no keywords or arguments.

Command Default

PAP authentication is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/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.

Command	Description
ppp authentication (BNG), on page 683	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 (BNG), on page 693	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 707	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*

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 2.0	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/RP0/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/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ppp pap sent-username xxxx password notified
RP/0/RP0/CPU0:router(config-if)# ppp pap sent-username xxxx password clear notified
RP/0/RP0/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 (BNG), on page 683	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, on page 702	Refuses PAP authentication from peers requesting it
ppp timeout authentication, on page 709	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*

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 2.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/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 (BNG), on page 683	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*

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 2.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp timeout retry 8
```

redundancy

To enter the redundancy configuration mode to configure Multi-Router Automatic Protection Switching (MR-APS), use the **redundancy** command in Global Configuration mode.

redundancy

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ppp	read

Examples

The following example shows how to enter the redundancy configuration mode:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# redundancy
RP/0/RP0/CPU0:router(config-redundancy)#
```

security ttl

To specify that the time-to-live (TTL) value in the IP header of the packet is used to validate that a packet is from the expected source, use the **security ttl** command in SSRP configuration mode. To remove the TTL requirement, use the no form of this command.

security ttl max-hops *number*

Syntax Description

max-hops *number*	Maximum number of hops between the peer routers.

Command Default

The **max-hops** default is 255.

Command Modes

SSRP configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

If **max-hops** is not specified, the TTL value must be 255 for a packet to be accepted.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to specify that the time-to-live (TTL) value in the IP header of a packet is used to validate that the packet is from the expected source:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# ssrp profile Profile_1
RP/0/RP0/CPU0:router(config-ssrp)# peer ipv4 address 10.10.10.10
RP/0/RP0/CPU0:router(config-ssrp)# security ttl max-hops number 50
```

show ppp interfaces (BNG)

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 mode

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.9.0	For ICSSO, when SSRP is configured, the **show ppp interfaces** command displays the SSO-State for LCP, IPCP, and authentication layers.
Release 4.2.0	This command was supported in the dynamic template configuration mode for BNG.
Release 5.3.2	The command was modified to include a new output display field, **SRG-state**, as part of geo redundancy support for PPPoE sessions in BNG router.

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/RP0/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/RP0/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/RP0/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 74: 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.
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.
Keepalive	Keepalive setting and interval in seconds for echo request packets.

Field	Description
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.
Open	Connection open.

Field	Description
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.
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.

show ppp sso alerts

To display all Inter-Chassis Stateful Switchover (ICSSO) alerts that have occurred, use the **show ppp sso alerts** command in EXEC mode.

show ppp sso alerts location *node-id*

Syntax Description

location *node-id*	Specifies the full qualified path of a specific node in the format *rack*/*slot*/*module.*

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

This command displays the following information for alerts that have prevented a standby session from being brought to the Standby-Up state using replicated data.

- The interfaces on which the alerts have occurred
- The layer in which the error has occurred
- A short description of the error

Note Only one error is reported for each layer for each interface. The error displayed is the most recent error that has occurred.

Task ID

Task ID	Operations
ppp	read

Examples

The following example shows how to display all ICSSO alerts that have occurred:

```
RP/0/RP0/CPU0:router# show ppp sso errors location 0/3/cpu0

 Intf              Layer          SSO
 Name              with error     Error
 ------------------------------------------------------------------------------
 Mu0/3/0/0/100     IPCP           Unsupported IPCP option 0x07
 Se0/3/1/3/1:0     LCP            Unacceptable value for LCP MRU option
 Se0/3/1/3/2:0     of-us-auth     Incorrect Authentication protocol, CHAP
 Se0/3/1/3/3:0     of-peer-auth   Invalid CHAP Authentication options
 Se0/3/1/3/4:0     LCP            Inconsistent LCP MRRU options
```

show ppp sso state

To display the Inter-Chassis Stateful Switchover (ICSSO) states of a Point-to-Point Protocol (PPP) session running under a particular Multi-Router Automatic Protection Switching (MR-APS) group, use the **show ppp sso state** command in EXEC mode.

show ppp sso state group *group-id* **location** *node-id*

Syntax Description

group *group-id*	Specifies the redundancy group number. The range is 1 to 32.
location *node-id*	Specifies the full qualified path of a specific node in the format *rack*/*slot*/*module.*

Command Default

If group is not specified, states are displayed for all redundancy groups.

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

This command shows the states of these session layers:

- LCP
- of-us authentication
- of-peer authentication
- IPCP

Note When an interface is in Standby mode, it is ready to forward traffic immediately after a switchover, if all the session layers, including IPCP, are in the S-Negd state.

Task ID

Task ID	Operations
ppp	read

Examples

The following example shows how to display the ICSSO states for PPP running under a redundancy group:

```
RP/0/RP0/CPU0:router# show ppp sso state location 0/3/cpu0

 Not-Ready : The session is not yet ready to run as Active or Standby
 S-UnNegd  : In Standby mode, no replication state received yet
 A-Down    : In Active mode, lower layer not yet up
 Deact'ing : Session was Active, now going Standby
 A-UnNegd  : In Active mode, not fully negotiated yet
```

```
S-Negd    : In Standby mode, replication state received and pre-programmed
Act'ing   : Session was Standby and pre-programmed, now going Active
A-Negd    : In Active mode, fully negotiated and up
-         : This layer not running

SSO-Group 1                     |            of-us     of-peer
Sess-ID    Ifname               |  LCP       auth      auth      IPCP
--------------------------------+-------------------------------------------
1          Multilink0/3/0/0/100 :  S-Negd    S-Negd    S-Negd    S-Negd

2          Multilink0/3/0/0/101 :  S-UnNegd  S-UnNegd  S-UnNegd  Not-Ready
3          Serial0/3/1/3/1      :  S-Negd    S-Negd    S-Negd    -
4          Serial0/3/1/3/2      :  A-Negd    A-Negd    A-Negd    A-UnNegd
5          Serial0/3/1/3/3      :  A-Down    Not-Ready Not-Ready -
6          Serial0/3/1/3/4      :  A-Up      A-Up      A-Up      A-Up

SSO-Group 1                     |            of-us     of-peer
Sess-ID    Ifname               |  LCP       auth      auth      IPCP
--------------------------------+-------------------------------------------
1          Multilink0/3/0/0/102 :  S-Negd    S-Negd    S-Negd    S-Negd

2          Serial0/3/1/3/5      :  S-Negd    S-Negd    S-Negd    -
3          Serial0/3/1/3/6      :  A-Negd    A-Negd    A-Negd    A-UnNegd
```

show ppp sso summary

To display the number of sessions in each Inter-Chassis Stateful Switchover (ICSSO) state for each session layer, use the **show ppp sso summary** command in EXEC mode.

show ppp sso summary location *node-id*

Syntax Description

location *node-id*	Specifies the full qualified path of a specific node in the format *rack*/*slot*/*module.*

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

This command displays information for these session layers:

- LCP
- of-us
- of-peer authentication
- IPCP

Note Only sessions with Session State Redundancy Protocol (SSRP) configured are displayed.

Task ID

Task ID	Operations
ppp	read

Examples

This example shows how to display the number of sessions in each ICSSO state for each session layer.

```
RP/0/RP0/CPU0:router# show ppp sso summary location 0/3/cpu0

Not-Ready    : The session is not yet ready to run as Active or Standby
Stby-UnNegd  : In Standby mode, no replication state received yet
Act-Down     : In Active mode, lower layer not yet up
Deactivating : Session was Active, now going Standby
Act-UnNegd   : In Active mode, not fully negotiated yet
Stby-Negd    : In Standby mode, replication state received and pre-programmed
Activating   : Session was Standby and pre-programmed, now going Active
Act-Negd     : In Active mode, fully negotiated and up
-            : This layer not running
```

```
                      Not-   Stby-  Act- Deactiv- Act-   Stby-  Activ- Act
Layer         | Total  Ready  UnNegd Down   ating  UnNegd Negd   ating  Negd
--------------+------- ------ ------ ------ ------ ------ ------ ------ -----
LCP           |     20      2      5      0      0      3      6      0     4
of-us-auth    |     20     10      2      0      0      1      4      0     3
of-peer-auth  |     20     10      3      0      0      2      3      0     2
IPCP          |     10      1      2      1      0      3      2      0     1
```

ssrp group

To attach an Session State Redundancy Protocol (SSRP) group on an interface, use the **ssrp group** command in interface configuration mode. To remove the SSRP group from the interface, use the **no** form of this command.

ssrp group *group-number* **id** *id-number* **ppp**

Syntax Description

group-number	SSRP group number. The range is 1 to 65535.
id *id-number*	SSRP identifier number. The range is 1 to 4294967295.
ppp	Specifies point-to-point protocol.

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

The group must be configured first on a specific location (linecard) and then assigned to the interface. The redundancy ID must be unique within the group. This command specifies a list the protocols that the group can replicate. Currently only PPP is supported.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface Multilink 0/1/0/0/1
RP/0/RP0/CPU0:router(config-if)# ssrp group 1 id 1 ppp
```

ssrp location

To specify the node on which to create a Session State Redundancy Protocol (SSRP) group and enter the SSRP node configuration mode, use the **ssrp location** command in Global Configuration mode.

ssrp location *node_id*

Syntax Description

node_id	Specifies the full qualified path of a specific node in the format *rack*/*slot*/*module*.

Command Default

No default behavior or values

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

The location specifies the card on which an SSRP group is created.

Task ID

Task ID	Operations
ppp	read, write

Examples

This example shows how to create an SSRP group on a specified node for use by any interface on the card:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# ssrp location 0/1/cpu0
RP/0/RP0/CPU0:router(config-ssrp-node)#
```

ssrp profile

To configure a Session State Redundancy Protocol (SSRP) profile and enter the SSRP configuration mode, use the **ssrp profile** command in Global Configuration mode. To remove the profile, use the **no** form of this command.

ssrp profile *profile-name*

Syntax Description

profile-name	Name of this SSRP profile.

Command Default

No default behavior or values

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

A Session State Redundancy Protocol (SSRP) profile allows the same SSRP configuration to be shared across multiple groups. The same profile can be attached to multiple groups across the router. The group must be configured before the interface that uses the group can be configured. The group number is used in the TCP port number so, the group number must be unique across the router.

Task ID

Task ID	Operations
ppp	read, write

Examples

This example shows how to configure an SSRP profile:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# ssrp profile Profile_1
RP/0/RP0/CPU0:router(config-ssrp)#
```

SONET Controller Commands

This module provides command line interface (CLI) commands for configuring SONET operation, using Layer 1 SONET transport technology, on the Cisco CRS Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

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

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 2.0	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/RP0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/RP0/CPU0:router(config-sonet)# ais-shut
```

Related Commands

Command	Description
show controllers sonet, on page 788	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

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 2.0	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/RP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RP0/CPU0:router(config-sonet)# path
RP/0/RP0/CPU0:router(config-sonet-path)# ais-shut
```

Related Commands

Command	Description
show controllers sonet, on page 788	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 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 2.0	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:

Forced Switchover Request From Working to Protect Channel

```
RP/0/RP0/CPU0:router# aps group 1 force 1 enable
RP/0/RP0/CPU0:router# aps group 1 force 1 disable
```

Manual Switchover Request From Working to Protect Channel

```
RP/0/RP0/CPU0:router# aps group 1 manual 1 enable
RP/0/RP0/CPU0:router# aps group 1 manual 1 disable
```

Forced Switchover Request from Protect to Working Channel

```
RP/0/RP0/CPU0:router# aps group 1 force 0 enable
RP/0/RP0/CPU0:router# aps group 1 force 0 disable
```

Manual Switchover Request From Protect to Working Channel

```
RP/0/RP0/CPU0:router# aps group 1 manual 0 enable
RP/0/RP0/CPU0:router# aps group 1 manual 0 disable
```

Related Commands

Command	Description
aps group (global), on page 736	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
lockout, on page 758	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 773	Enables automatic switchover from the protect interface to the working interface after the working interface becomes available.
signalling, on page 796	Configures the K1K2 overhead byte signaling protocol used for APS.

Command	Description
show aps, on page 776	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*

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 2.0	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/RP0/CPU0:router(config)# aps group 1
RP/0/RP0/CPU0:router(config-aps)#
```

Related Commands

Command	Description
aps group, on page 733	Manually switches an APS channel.
authenticate (PGP), on page 738	Configures the authentication string for the PGP message exchange between the protect and working routers.
channel local, on page 741	Assigns local SONET physical ports as SONET APS channels in the current APS group.
channel remote, on page 743	Assigns a port and interface that is physically located in a remote router as a SONET working or protect APS channel.

Command	Description
lockout, on page 758	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 773	Enables automatic switchover from the protect interface to the working interface after the working interface becomes available.
signalling, on page 796	Configures the K1K2 overhead byte signaling protocol used for APS.
timers (APS), on page 798	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 804	Configures a protect interface for unidirectional mode.
show aps, on page 776	Displays the operational status for all configured SONET APS groups.

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*

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 2.0	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/RP0/CPU0:router(config)# aps group 1
RP/0/RP0/CPU0:router(config-aps)# authenticate abctown
```

Related Commands

Command	Description
aps group (global), on page 736	Adds an automatic protection switching (APS) group and enter APS group configuration mode.

Command	Description
channel local, on page 741	Assigns local SONET physical ports as SONET APS channels in the current APS group.
channel remote, on page 743	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 776	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

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

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows a PRDI enabled on all paths:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RP0/CPU0:router(config-sonet)# path
RP/0/RP0/CPU0:router(config-sonet-path)# b3-ber-prdi
```

Related Commands

Command	Description
path (SONET), on page 767	Enters SONET/SDH path configuration mode.
show controllers sonet, on page 788	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 2.0	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.

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/RP0/CPU0:router(config)# aps group 1
RP/0/RP0/CPU0:router(config-aps)# channel 0 local SONET 0/2/0/2
```

Related Commands

Command	Description
aps group (global), on page 736	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
channel remote, on page 743	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 776	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*

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 2.0	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/RP0/CPU0:router(config)# aps group 1
RP/0/RP0/CPU0:router(config-aps)# channel 1 remote 192.168.1.1
```

Related Commands

Command	Description
aps group (global), on page 736	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
channel local, on page 741	Assigns local SONET physical ports as SONET APS channels in the current APS group.
show aps, on page 776	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 2.0	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.

Use the **clear counters sonet** command to clear SONET counters for a specific SONET controller.

Task ID

Task ID	Operations
sonet-sdh	read, write
basic-services	read, write

Examples

The following example shows the SONET counters being cleared on the SONET interface:

```
RP/0/RP0/CPU0:router# clear counters sonet 0/1/0/0
```

Related Commands

Command	Description
show controllers sonet, on page 788	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

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 2.0	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/RP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RP0/CPU0:router(config-sonet)# clock source internal
```

Related Commands

Command	Description
show controllers sonet, on page 788	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*

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 2.0	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.

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/RP0/CPU0:router(config)# controller SONET 0/2/0/1
RP/0/RP0/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/RP0/CPU0:router(config)# controller SONET 0/2/0/1 path b3-ber-prdi
RP/0/RP0/CPU0:router(config-sonet)#
```

Related Commands

Command	Description
path (SONET), on page 767	Enters SONET/SDH path configuration mode.
show controllers sonet, on page 788	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*

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

No specific guidelines impact the use of this command.

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/RP0/CPU0:router(config)# controller sonet 0/2/0/3
RP/0/RP0/CPU0:router(config-sonet)# sts 1
RP/0/RP0/CPU0:router(config-stsPath)# delay clear 7000
```

Related Commands

Command	Description
delay trigger, on page 751	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*

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/RP0/CPU0:router(config)# controller sonet 0/2/0/3
RP/0/RP0/CPU0:router(config-sonet)# sts 1
RP/0/RP0/CPU0:router(config-stsPath)# delay trigger 6000
```

Related Commands

Command	Description
delay clear, on page 750	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/RP0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/RP0/CPU0:router(config-sonet)# down-when-looped

down-when-looped is a traffic-affecting operation
```

Related Commands

Command	Description
loopback (SONET), on page 759	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 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 733 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 2.0	This command was introduced.
Release 3.8.0	This command was replaced by the **aps group** command.

Usage Guidelines

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/RP0/CPU0:router(config)# aps group 1
RP/0/RP0/CPU0:router(config-aps)# force 1
```

Related Commands

Command	Description
lockout, on page 758	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 760	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**

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 2.0	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/RP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RP0/CPU0:router(config-sonet)# framing sdh
```

In the following example, the SONET controller is configured for SONET framing:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RP0/CPU0:router(config-sonet)# framing sonet
```

Related Commands

Command	Description
show controllers sonet, on page 788	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*

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/RP0/CPU0:router(config)# controller SONET 0/0/0/2
RP/0/RP0/CPU0:router(config-sonet)# line delay clear 4000
```

Related Commands

Command	Description
line delay trigger, on page 757	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*

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/RP0/CPU0:router(config)# controller SONET 0/0/0/2
RP/0/RP0/CPU0:router(config-sonet)# line delay trigger 3000
```

Related Commands

Command	Description
line delay clear, on page 756	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**]

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 2.0	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/RP0/CPU0:router(config)# aps group 1
RP/0/RP0/CPU0:router(config-aps)# lockout 0
```

Related Commands

Command	Description
aps group (global), on page 736	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
aps group, on page 733	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**

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 2.0	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.

Examples

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

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RP0/CPU0:router(config-sonet)# loopback internal
```

Related Commands

Command	Description
show controllers sonet, on page 788	Displays information about the operational status of SONET layers.

manual

manual *channel-number* **0** | **1**

Command History

Release 2.0	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/RP0/CPU0:router(config)# aps group 1
RP/0/RP0/CPU0:router(config-aps)# manual 1
```

Related Commands

Command	Description
force, on page 753	Initiates a forced APS request at the local end of the SONET link.
lockout, on page 758	Overrides a manual or forced APS request at the local end of the SONET link and block the protect channel from receiving traffic.

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*

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 2.0	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/RP0/CPU0:router(config)# controller sonet 0/1/0/1
RP/0/RP0/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/RP0/CPU0:router(config)# controller sonet 0/1/0/1
RP/0/RP0/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*

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 2.0	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/RP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RP0/CPU0:router(config-sonet)# path
RP/0/RP0/CPU0:router(config-sonet-path)# overhead c2 0x13
```

Related Commands

Command	Description
scrambling disable (SONET path), on page 775	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*

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

No specific guidelines impact the use of this command.

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/RP0/CPU0:router(config)# controller SONET 0/0/0/1
RP/0/RP0/CPU0:router(config-sonet)# path delay clear 7000
```

Related Commands

Command	Description
path delay trigger, on page 766	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*

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/RP0/CPU0:router(config)# controller SONET 0/0/0/1
RP/0/RP0/CPU0:router(config-sonet)# path delay trigger 6000
```

Related Commands

Command	Description
path delay clear, on page 765	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 2.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/RP0/CPU0:router(config-sonet)# path
```

Related Commands

Command	Description
ais-shut (SONET path), on page 732	Enables automatic insertion of PAIS in the sent SONET signal whenever the SONET path enters the administratively down state.
b3-ber-prdi, on page 740	Enables sending of a PRDI when the BER bit interleaved parity (BIP) B3 threshold is exceeded.
delay clear, on page 750	Configures the amount of time before a STS path delay trigger alarm is cleared.
delay trigger, on page 751	Configures a time value for the STS path delay trigger.
overhead (SONET path), on page 763	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 771	Configures whether or not selected SONET alarms are logged to the console for a SONET path controller.

Command	Description
scrambling disable (SONET path), on page 775	Disables payload scrambling on a SONET path.
threshold (SONET path), on page 802	Sets the bit error rate (BER) threshold values of the specified alarms for a SONET path.
uneq-shut (SONET path), on page 803	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**]

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 2.0	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/RP0/CPU0:router(config)# controller sonet 0/1/0/1
RP/0/RP0/CPU0:router(config-sonet)# report lais
```

Related Commands

Command	Description
show controllers sonet, on page 788	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**]

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 2.0	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/RP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RP0/CPU0:router(config-sonet)# path
RP/0/RP0/CPU0:router(config-sonet-path)# report pais
```

Related Commands

Command	Description
show controllers sonet, on page 788	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*

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 2.0	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/RP0/CPU0:router(config)# aps group 1
RP/0/RP0/CPU0:router(config-aps)# revert 5
```

Related Commands

Command	Description
aps group (global), on page 736	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
show aps, on page 776	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

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 2.0	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/RP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RP0/CPU0:router(config-sonet)# path
RP/0/RP0/CPU0:router(config-sonet-path)# scrambling disable
```

Related Commands

Command	Description
show controllers sonet, on page 788	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 2.0	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/RP0/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 75: 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 778	Displays the status of the APS WP distributed communication subsystem.
show aps group, on page 780	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 2.0	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/RP0/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 76: 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 776	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 2.0	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/RP0/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 77: 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 776	Displays the operational status for all configured SONET APS groups.
show aps agents, on page 778	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 mode

Command History

Release	Modification
Release 2.0	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 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/RP0/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/RP0/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 78: 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.
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 terminated
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 terminated.
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 mode

Command History

Release	Modification
Release 2.0	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.

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/RP0/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 79: 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.
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.

Field	Description
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.
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.

Field	Description
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).
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.

Field	Description
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/RP0/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/RP0/CPU0:router# show controllers sonet 0/1/2/1 internal-state

Interface(layer)      admin_up if_state
```

[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]

```
---------------------- -------- --------

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 80: show controllers sonet Field Descriptions

Field	Description
Interface (layer)	Slot number of the POS interface.
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.

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

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 2.0	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/RP0/CPU0:router(config)# controller sonet 0/1/0/2
RP/0/RP0/CPU0:router(config-sonet)# shutdown
```

Related Commands

Command	Description
show controllers sonet, on page 788	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**

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 2.0	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/RP0/CPU0:router(config)# aps group 1


RP/0/RP0/CPU0:router(config-aps)# signalling sdh
```

The following example sets the signaling to SONET:

```
RP/0/RP0/CPU0:router(config)# aps group 1
RP/0/RP0/CPU0:router(config-aps)# signalling sonet
```

Related Commands

Command	Description
aps group (global), on page 736	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
show aps group, on page 780	Displays information about the APS groups.

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*

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 2.0	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 maximum interval starting with the first failed periodic message after which, if no successful exchange takes place, the PGP link is declared dead. If the Hello timer is X seconds and Hold Timer is configured as Y seconds (where, X < Y), then the PGP link down announcement happens in a minimum of Y-X seconds and maximum of Y seconds.

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/RP0/CPU0:router(config)# aps group 3
RP/0/RP0/CPU0:router(config-aps)# timers 2 6
```

Related Commands

Command	Description
aps group (global), on page 736	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
show aps group, on page 780	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*

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 2.0	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/RP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RP0/CPU0:router(config-sonet)# threshold sd-ber 8
RP/0/RP0/CPU0:router(config-sonet)# threshold sf-ber 4
RP/0/RP0/CPU0:router(config-sonet)# threshold b1-tca 4
```

Related Commands

Command	Description
report (SONET), on page 769	Permits selected SONET alarms to be logged to the console for a SONET controller.
show controllers sonet, on page 788	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*

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 2.0	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/RP0/CPU0:router(config)# controller sonet 0/1/0/1
RP/0/RP0/CPU0:router(config-sonet)# path
RP/0/RP0/CPU0:router(config-sonet-path)# threshold b3-tca 4
```

Related Commands

Command	Description
report (SONET), on page 769	Permits selected SONET alarms to be logged to the console for a SONET controller.
show controllers sonet, on page 788	Displays information about the operational status of SONET layers.

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

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 2.0	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/RP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RP0/CPU0:router(config-sonet)# path
RP/0/RP0/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

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 2.0	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/RP0/CPU0:router(config)# aps group 1
RP/0/RP0/CPU0:router(config-aps)# unidirectional
```

Related Commands

Command	Description
aps group (global), on page 736	Adds an automatic protection switching (APS) group and enter APS group configuration mode.

Command	Description
show aps, on page 776	Displays the operational status for all configured SONET APS groups.

SRP Commands on the Cisco IOS XR Software

This module provides command line interface (CLI) commands for configuring Spatial Reuse Protocol (SRP) on supported Cisco Dynamic Packet Transport (DPT) interfaces.

SRP is a MAC-layer protocol developed by Cisco and is used in conjunction with Cisco DPT products. DPT products deliver scalable Internet service, reliable IP-aware optical transport, and simplified network operations. These solutions allow you to scale and distribute your IP services across a reliable optical packet ring infrastructure.

Note Throughout the remainder of this publication, the term SRP is used to describe features related to the DPT product family.

clear srp counters

To clear the SRP counters, use the **clear srp counters** command in EXEC mode.

clear srp counters interface srp *interface-path-id* | **location** *node-id*

Syntax Description

interface srp	Specifies the SRP 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

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2.2	This command was introduced and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
Release 3.4.0	This command was introduced on the 16-port OC-48c/STM-16c POS/DPT PLIM.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 **clear srp counters** command clears the counters displayed in the following commands:

- show controllers srp rac-error
- show srp counters
- show srp counters source
- show srp transit

Task ID

Task ID	Operations
pos-dpt	read, write

Examples

The following example shows how to use the **clear srp counters** command to make the counts displayed from the **show srp source-counters** command return to zero:

```
RP/0/RP0/CPU0:router# show srp counters interface srp 0/7/0/0

Data Traffic Counters for Interface SRP0/7/0/0
 Side A:
 Transit                                  Packets                 Bytes
     Total Low Priority:                        0                     0
     Total High Priority:                     183                768543
     Total Multicast:                         174                767913
     Total Unicast:                             9                   630
 Host Receive                             Packets                 Bytes
     Unicast Low Priority:                      6                   648
     Unicast High Priority:                     0                     0
     Multicast Low Priority:                    0                     0
     Multicast High Priority:                   1                    41
 Total Receive                            Packets                 Bytes
     Unicast Low Priority:                      6                   648
     Unicast High Priority:                     9                   630
     Multicast Low Priority:                    3                   144
     Multicast High Priority:                 174                767913
 Host Transmit                            Packets                 Bytes
     Unicast Low Priority:                      4                   480
     Unicast High Priority:                     0                     0
     Multicast Low Priority:                    0                     0
     Multicast High Priority:                   0                     0
 Total Transmit                           Packets                 Bytes
     Unicast Low Priority:                      4                   480
     Unicast High Priority:                     0                     0
     Multicast Low Priority:                    0                     0
     Multicast High Priority:                 772               1575090
 Traffic Rate (5 Minutes)              packets/sec               bits/sec
     Transit Low Priority                       0                     0
     Transit High Priority                      0                     0
     Transit Multicast                          0                     0
     Transit Unicast                            0                     0
     Host Receive                               0                     0
     Total Receive                              0                     0
     Host Transmit                              0                     0
     Total Transmit                             0                     0
 Received Errors:
     0 input errors, 0 CRC, 0 ignored,
     0 framer runts, 0 framer giants, 0 framer aborts,
     0 mac runts, 0 mac giants, 0 mac ttl strips

 Side B:
 Transit                                  Packets                 Bytes
     Total Low Priority:                        0                     0
     Total High Priority:                     772               1575090
     Total Multicast:                         772               1575090
     Total Unicast:                             0                     0
 Host Receive                             Packets                 Bytes
     Unicast Low Priority:                      6                   648
```

```
    Unicast High Priority:                      0                   0
    Multicast Low Priority:                     0                   0
    Multicast High Priority:                    1                  41
Total Receive                               Packets               Bytes
    Unicast Low Priority:                       6                 648
    Unicast High Priority:                      0                   0
    Multicast Low Priority:                     0                   0
    Multicast High Priority:                  772             1575090
Host Transmit                               Packets               Bytes
    Unicast Low Priority:                       6                 720
    Unicast High Priority:                      0                   0
    Multicast Low Priority:                     3                 144
    Multicast High Priority:                    0                   0
Total Transmit                              Packets               Bytes
    Unicast Low Priority:                       6                 720
    Unicast High Priority:                      9                 630
    Multicast Low Priority:                     3                 144
    Multicast High Priority:                  174              767913
Traffic Rate (5 Minutes)                packets/sec             bits/sec
    Transit Low Priority                        0                   0
    Transit High Priority                       0                   0
    Transit Multicast                           0                   0
    Transit Unicast                             0                   0
    Host Receive                                0                   0
    Total Receive                               0                   0
    Host Transmit                               0                   0
    Total Transmit                              0                   0
Received Errors:
    0 input errors, 0 CRC, 0 ignored,
    0 framer runts, 0 framer giants, 0 framer aborts,
    0 mac runts, 0 mac giants, 0 mac ttl strips

RP/0/RP0/CPU0:router# clear srp counters interface srp 0/7/0/0
RP/0/RP0/CPU0:router# show srp counters interface srp 0/7/0/0

Data Traffic Counters for Interface SRP0/7/0/0
Side A:
Transit                                     Packets               Bytes
    Total Low Priority:                         0                   0
    Total High Priority:                        0                   0
    Total Multicast:                            0                   0
    Total Unicast:                              0                   0
Host Receive                                Packets               Bytes
    Unicast Low Priority:                       0                   0
    Unicast High Priority:                      0                   0
    Multicast Low Priority:                     0                   0
    Multicast High Priority:                    0                   0
Total Receive                               Packets               Bytes
    Unicast Low Priority:                       0                   0
    Unicast High Priority:                      0                   0
    Multicast Low Priority:                     0                   0
    Multicast High Priority:                    0                   0
Host Transmit                               Packets               Bytes
    Unicast Low Priority:                       0                   0
    Unicast High Priority:                      0                   0
    Multicast Low Priority:                     0                   0
    Multicast High Priority:                    0                   0
Total Transmit                              Packets               Bytes
    Unicast Low Priority:                       0                   0
    Unicast High Priority:                      0                   0
    Multicast Low Priority:                     0                   0
    Multicast High Priority:                    0                   0
Traffic Rate (5 Minutes)                packets/sec             bits/sec
    Transit Low Priority                        0                   0
```

```
    Transit High Priority                       0                   0
    Transit Multicast                           0                   0
    Transit Unicast                             0                   0
    Host Receive                                0                   0
    Total Receive                               0                   0
    Host Transmit                               0                   0
    Total Transmit                              0                   0
Received Errors:
    0 input errors, 0 CRC, 0 ignored,
    0 framer runts, 0 framer giants, 0 framer aborts,
    0 mac runts, 0 mac giants, 0 mac ttl strips

Side B:
Transit                                     Packets               Bytes
    Total Low Priority:                           0                   0
    Total High Priority:                          0                   0
    Total Multicast:                              0                   0
    Total Unicast:                                0                   0
Host Receive                                Packets               Bytes
    Unicast Low Priority:                         0                   0
    Unicast High Priority:                        0                   0
    Multicast Low Priority:                       0                   0
    Multicast High Priority:                      0                   0
Total Receive                               Packets               Bytes
    Unicast Low Priority:                         0                   0
    Unicast High Priority:                        0                   0
    Multicast Low Priority:                       0                   0
    Multicast High Priority:                      0                   0
Host Transmit                               Packets               Bytes
    Unicast Low Priority:                         0                   0
    Unicast High Priority:                        0                   0
    Multicast Low Priority:                       0                   0
    Multicast High Priority:                      0                   0
Total Transmit                              Packets               Bytes
    Unicast Low Priority:                         0                   0
    Unicast High Priority:                        0                   0
    Multicast Low Priority:                       0                   0
    Multicast High Priority:                      0                   0
Traffic Rate (5 Minutes)              packets/sec            bits/sec
    Transit Low Priority                          0                   0
    Transit High Priority                         0                   0
    Transit Multicast                             0                   0
    Transit Unicast                               0                   0
    Host Receive                                  0                   0
    Total Receive                                 0                   0
    Host Transmit                                 0                   0
    Total Transmit                                0                   0
Received Errors:
    0 input errors, 0 CRC, 0 ignored,
    0 framer runts, 0 framer giants, 0 framer aborts,
    0 mac runts, 0 mac giants, 0 mac ttl strips
```

hw-module port

To enable a port to be used for SRP, use the **hw-module port** command in global configuration mode. To disable SRP and enable the port for Packet over SONET (POS), use the **no** form of this command.

hw-module port *port-number* **srp location** *node-id* **spa-bay** *number*
no hw-module port *port-number* **srp location** *node-id* **spa-bay** *number*

Syntax Description

port-number	Number of the physical interface on the PLIM or SPA.
srp	Specifies an SRP interface.
location	Specifies the location of the module.
node-id	Location of the PLIM or SPA, in the *rack*/*slot*/*module* notation.
spa-bay	Bay number of one of the following: • 16-port OC-48c/STM-16c POS/DPT PLIM • 4-port OC-192c/STM-64c POS/DPT PLIM • 1-port OC-192/STM-64 POS/RPR SPA XFP optics • 4-port OC-48/STM-16 POS/RPR SPA • 2-port OC-48/STM-16 POS/RPR SPA **Note** After this command is executed, the SPA must be reloaded to apply the configuration and create the SRP ports. On the OC-192 SPAs, both SPAs at each end of the SRP interface must be reloaded.
number	Number of the SPA bay.

Command Default

When there is no **hw-module port** configuration, ports are enabled for POS by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2.2	This command was introduced and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.
Release 3.8.0	This command was first supported on the following SPAs: • 1-port OC-192/STM-64 POS/RPR SPA XFP optics • 4-port OC-48/STM-16 POS/RPR SPA • 2-port OC-48/STM-16 POS/RPR SPA The **spa-bay** keyword was added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

POS is the default port mode on POS/DPT PLIMs and SPAs. Use the **hw-module port** command to allow the ports to be configured for SRP use.

SRP requires two consecutive physical ports for use as a single SRP interface. The first port must be even numbered and the second port must be odd numbered. No other combinations are allowed. You must use this command on both of the ports to be used as an SRP interface. SRP interfaces take the number of the lower, even-numbered port. For example, if ports 0/1/0/2 and 0/1/0/3 are enabled as an SRP interface, the interface would be referred to as SRP0/1/0/2.

On the 16-port OC-48c/STM-16c POS/DPT PLIM, groups of four consecutive ports must be configured the same. Ports 0 through 3 must all be configured as either SRP or POS. The same is true for ports 4 through 7, 8 through 11, and 12 through 15. All four ports must be on the same SPA bay.

On the 4-port OC-192c/STM-64c POS/DPT PLIM, groups of two ports must be configured the same; either as SRP or POS. The two ports must be on different SPA bays; either 0, 1, or 2 or 3, 4, or 5.

After using the **hw-module port** command, you must save the configuration and reload the PLIM or SPA to enable this configuration change and create the SRP or POS interface. For the PLIMs, use the **hw-module location reload** command in EXEC mode. For all SPAs except for the 1-port OC-192/STM-64 POS/RPR SPA XFP optics, use the **hw-module subslot reload** command in EXEC mode. For the OC-192/STM-64 POS/RPR SPA, use the **hw-module subslot shutdown** command in global configuration mode to shut down the SPA, then the **no hw-module subslot shutdown** command in the same mode to return the SPA to the up state. We do not recommend using the **hw-module subslot reload** command to reload the OC-192/STM-64 POS/RPR SPA, because doing so can cause synchronization problems with the two SPAs and processes that comprise a SRP interface.

To disable SRP and reenable POS on the port, use the **no** form of the command.

Note Internal clocking is required for SRP interfaces. Use the clock source internal command in SONET configuration mode to configure the clock source.

Task ID

Task ID	Operations
root-lr	read, write

Examples

In the following example, ports 0 through 3 are enbled for SRP on the PLIM:

```
RP/0/RP0/CPU0:Router(config)# hw-module port 0 srp location 0/1/cpu0
RP/0/RP0/CPU0:Router(config)# hw-module port 1 srp location 0/1/cpu0
RP/0/RP0/CPU0:Router(config)# hw-module port 2 srp location 0/1/cpu0
RP/0/RP0/CPU0:Router(config)# hw-module port 3 srp location 0/1/cpu0
RP/0/RP0/CPU0:Router(config)# exit
RP/0/RP0/CPU0:Router# hw-module location 0/1/CPU0 reload
```

In the following example, ports 0 and 1 are enbled for SRP on the PLIM:

```
RP/0/RP0/CPU0:Router(config)# hw-module port 0 srp location 0/1/cpu0
RP/0/RP0/CPU0:Router(config)# hw-module port 1 srp location 0/1/cpu0
RP/0/RP0/CPU0:Router(config)# exit
RP/0/RP0/CPU0:Router# hw-module location 0/1/CPU0 reload
```

In the following example, ports 0, 1, 2, and 3 are enbled for SRP on the SPA:

```
RP/0/RP0/CPU0:router(config)# hw-module port 0 srp location 0/3/CPU0 spa-bay 2
RP/0/RP0/CPU0:router(config)# hw-module port 1 srp location 0/3/CPU0 spa-bay 2
RP/0/RP0/CPU0:router(config)# hw-module port 2 srp location 0/3/CPU0 spa-bay 2
RP/0/RP0/CPU0:router(config)# hw-module port 3 srp location 0/3/CPU0 spa-bay 2
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router(config)# end
RP/0/RP0/CPU0:router# hw-module subslot 0/3/CPU0 reload
```

```
RP/0/RP0/CPU0:router(config)# hw-module port 0 srp location 0/3/CPU0 spa-bay 0
RP/0/RP0/CPU0:router(config)# hw-module port 0 srp location 0/3/CPU0 spa-bay 1
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router(config)# hw-module subslot 0/3/0 shutdown
RP/0/RP0/CPU0:router(config)# hw-module subslot 0/3/1 shutdown
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router(config)# no hw-module subslot 0/3/0 shutdown
RP/0/RP0/CPU0:router(config)# no hw-module subslot 0/3/1 shutdown
RP/0/RP0/CPU0:router(config)# commit
```

Related Commands

Command	Description
clock source internal	Configures SONET clocking as internal.
hw-module location reload	Reloads all PLIMs.
hw-module subslot reload	Reloads all SPAs except the for the 1-port OC-192/STM-64 POS/RPR SPA XFP optics.
hw-module subslot shutdown	Administratively shuts down a SPA.
no hw-module subslot shutdown	Returns a SPA to the up state.

interface srp

To configure the SRP protocol on a DPT interface and enter interface configuration mode, use the **interface srp** command in global configuration mode.

interface srp *interface-path-id* [**arp** | **bandwidth** | **cdp** | **dampening** | **description** | **flow** | **ipv4** | **ipv6** | **load-interval** | **mac-address** | **mpls** | **mtu** | **ppp** | **proxy-arp** | **service-policy** | **shutdown** | **srp** | **vrf**]

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.
arp	Configures Address Resolution Protocol (ARP) on the interface.
bandwidth	Sets the bandwidth for the interface.
cdp	Enables Cisco Discovery Protocol (CDP) on the interface.
dampening	Configures state dampening on the interface.
description	Sets the description for this interface.
flow	Enables NetFlow configuration on the interface.
ipv4	Enables IPv4 address subcommands on the interface.
ipv6	Enables IPv6 address subcommands on the interface.
load-interval	Configures the interval for load calculation on the interface.
mac-address	Sets the Mac address (*xxxx.xxxx.xxxx*) on the interface.
mpls	Enables MPLS subcommands on the interface.
mtu	Sets the maximum transmission unit (MTU) for the interface.
ppp	Enables Point-to-Point Protocol (PPP) on the interface.
proxy-arp	Enables proxy Address Resolution Protocol (ARP) on the interface.
service-policy	Configures a QoS policy on the interface.
shutdown	Shuts down the interface.
srp	Enables SRP parameters on the interface.
vrf	Sets the VRF in which the interface operates.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2.2	This command was introduced and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.
Release 3.8.0	The following new keywords were added, arp, bandwidth, cdp, dampening, description, flow, ipv4, ipv6, load-interval, mac-address, mpls, mtu, ppp, proxy-arp, service-policy, shutdown, srp, vrf.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 srp interface mode:

```
RP/0/RP0/CPU0:router(config)# interface srp 0/1/0/0
RP/0/RP0/CPU0:router(config-if)#
```

show controllers srp

To display information on the SRP controllers, use the **show controllers srp** command in EXEC mode.

show controllers srp *interface-path-id* **side a** | **b rac-error** | **rac-reg** | **ucode-inst** | **ucode-reg**

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.
side	Specify the side of the node.
a	The side of a node that has outer ring receive fiber is identified as side A.
b	The side of a node that has inner ring receive fiber is identified as side B.
rac-error	Displays the error reported by the Ring Access Controller (RAC) device.
rac-reg	Displays the value of the RAC device register set.
ucode-inst	Displays the RAC micro-controller binary code instruction set (currently loaded or executing) in hexidecimal format. **Note** This is an intrusive command that will cause adjacent nodes to detect a MAC keepalive failure and then wrap.
ucode-reg	Displays the RAC micro-controller register set.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2.2	This command was introduced and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

This example shows how to display the RAC registers for a specified SRP interface:

```
RP/0/RP0/CPU0:router# show controllers srp 0/5/0/0 side a rac-reg
```

Related Commands

Command	Description
show srp, on page 819	Displays information about an SRP interface.

show srp

To display information about an SRP interface, use the **show srp** command in EXEC mode.

show srp [**counters** [**source**] | **failures** | **ips** | **platform** | **srr** | **topology** | **transit**] [**interface srp** *interface-path-id* | **location** *node-id*]

Syntax Description

counters	(Optional) Displays counters for the packets received, transmitted, and transited on both sides of an SRP node.
source	(Optional) Displays the counters for the SRP source address.
failures	(Optional) Displays all SRP failures that were detected by the router.
ips	(Optional) Displays the Intelligent Protection Switching (IPS) status.
platform	(Optional) Displays platform-specific SRP interface details.
srr	(Optional) Displays single ring recovery (SRR) information.
topology	(Optional) Identifies the nodes on the ring.
transit	(Optional) Displays transit delays (in nanoseconds) between the time that a packet enters the transit buffer and the time it comes back on the ring.
interface	(Optional) Specifies the interface for which to display the counters.
srp	(Optional) Specifies an SRP 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	(Optional) Specifies the location of the module.
node-id	Location of the module in the *rack*/*slot*/*module* notation.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2.2	This command was introduced and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

To clear the SRP counters, use the clear srp counters, on page 808 command. The **show srp** command with the **counters** keyword reports the per-side counters and rates for various packet paths.

The **show srp** command with the **failures** keyword reports the SRP failures that were detected by the router. Use the **failures** keyword when an SRP interface is wrapped and you want to display information about the cause of the failure.

Use the **transit** keyword to determine the approximate latency when transmitting a packet, which due to higher latency, gives the approximation of congestion at this interface. If there is no latency, there is no congestion. Latency indicates that traffic transiting the ring and transmitted from the host are competing, meaning there is congestion.

Regarding the **topology** keyword, Address Resolution Protocol (ARP) is independent of the Layer 2 topology mapping. In other words, the absence of a MAC address in the topology map does not prevent ARP or any Layer 3 protocol from reaching the node. Alternatively, the presence of a MAC address in the topology map does not mean that it is possible to resolve the Layer 3 address. The topology map is used to determine the most efficient side (in hops) to use to reach any given MAC address.

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
pos-dpt	read

Examples

In the following example, output from the **show srp** command with the **counters** keyword is displayed:

```
RP/0/RP0/CPU0:router# show srp counters interface srp 0/7/0/0

Data Traffic Counters for Interface SRP0/7/0/0
 Side A:
 Transit                                 Packets                 Bytes
     Total Low Priority:                       0                     0
     Total High Priority:                    183                768543
     Total Multicast:                        174                767913
     Total Unicast:                            9                   630
 Host Receive                            Packets                 Bytes
     Unicast Low Priority:                     6                   648
     Unicast High Priority:                    0                     0
     Multicast Low Priority:                   0                     0
```

```
    Multicast High Priority:                  1                   41
Total Receive                            Packets               Bytes
    Unicast Low Priority:                     6                 648
    Unicast High Priority:                    9                 630
    Multicast Low Priority:                   3                 144
    Multicast High Priority:                174              767913
Host Transmit                            Packets               Bytes
    Unicast Low Priority:                     4                 480
    Unicast High Priority:                    0                   0
    Multicast Low Priority:                   0                   0
    Multicast High Priority:                  0                   0
Total Transmit                           Packets               Bytes
    Unicast Low Priority:                     4                 480
    Unicast High Priority:                    0                   0
    Multicast Low Priority:                   0                   0
    Multicast High Priority:                772             1575090
Traffic Rate (5 Minutes)              packets/sec             bits/sec
    Transit Low Priority                      0                   0
    Transit High Priority                     0                   0
    Transit Multicast                         0                   0
    Transit Unicast                           0                   0
    Host Receive                              0                   0
    Total Receive                             0                   0
    Host Transmit                             0                   0
    Total Transmit                            0                   0
Received Errors:
    0 input errors, 0 CRC, 0 ignored,
    0 framer runts, 0 framer giants, 0 framer aborts,
    0 mac runts, 0 mac giants, 0 mac ttl strips

Side B:
Transit                                  Packets               Bytes
    Total Low Priority:                       0                   0
    Total High Priority:                    772             1575090
    Total Multicast:                        772             1575090
    Total Unicast:                            0                   0
Host Receive                             Packets               Bytes
    Unicast Low Priority:                     6                 648
    Unicast High Priority:                    0                   0
    Multicast Low Priority:                   0                   0
    Multicast High Priority:                  1                  41
Total Receive                            Packets               Bytes
    Unicast Low Priority:                     6                 648
    Unicast High Priority:                    0                   0
    Multicast Low Priority:                   0                   0
    Multicast High Priority:                772             1575090
Host Transmit                            Packets               Bytes
    Unicast Low Priority:                     6                 720
    Unicast High Priority:                    0                   0
    Multicast Low Priority:                   3                 144
    Multicast High Priority:                  0                   0
Total Transmit                           Packets               Bytes
    Unicast Low Priority:                     6                 720
    Unicast High Priority:                    9                 630
    Multicast Low Priority:                   3                 144
    Multicast High Priority:                174              767913
Traffic Rate (5 Minutes)              packets/sec             bits/sec
    Transit Low Priority                      0                   0
    Transit High Priority                     0                   0
    Transit Multicast                         0                   0
    Transit Unicast                           0                   0
    Host Receive                              0                   0
    Total Receive                             0                   0
    Host Transmit                             0                   0
```

```
    Total Transmit                              0                   0
Received Errors:
    0 input errors, 0 CRC, 0 ignored,
    0 framer runts, 0 framer giants, 0 framer aborts,
    0 mac runts, 0 mac giants, 0 mac ttl strips
```

Table 81: show srp counters Command Output Fields

Field	Description
Side A	Header for packets received, transmitted, and transited by the Resource Availability Confirmation (RAC) device on side A.
Side B	Header for packets received, transmitted, and transited by the RAC device on side B.
TransitTotal Low Priority	Total number of unicast and multicast packets marked as SRP low priority (based on the SRP priority mapping) that transit the router and are counted in the transmit low-priority counters.
TransitTotal High Priority	Total number of unicast and multicast packets marked as SRP high priority (based on the SRP priority mapping) that transit the router and are counted in the transmit high-priority counters.
TransitTotal Multicast	Total number of low- and high-priority multicast packets that transit the router and are counted in the transmit multicast counters.
TransitTotal Unicast	Total number of low- and high-priority unicast packets that transit the router and are counted in the transmit unicast counters.
Host ReceiveUnicast Low/High priority	Total number of low- and high-priority unicast packets received by the router.
Host ReceiveMulticast Low/High priority	Total number of low- and high-priority multicast packets received by the router.
Total ReceiveUnicast Low/High priority	Total number of low- and high-priority unicast packets that transit or are received by the router.
Total ReceiveMulticast Low/High priority	Total number of low- and high-priority multicast packets that transit or are received by the router.
Host TransmitUnicast Low/High priority	Total number of low- and high-priority unicast packets sourced onto the ring by the router.
Host TransmitMulticast Low/High priority	Total number of low- and high-priority multicast packets sourced onto the ring by the router.
Total TransmitUnicast Low/High priority	Total number of low- and high-priority unicast packets transmitted by this side and transited out of the other side of the node.
Total TransmitMulticast Low/High priority	Total number of low- and high-priority multicast packets transmitted by this side and transited out of the other side of the node.

Field	Description
Traffic Rate (5 Minutes)	Average number of packets and bits transmitted per second during the last 5 minutes. The 5-minute traffic 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. The 5-minute value is the load interval, and it is configurable using the **load-interval** command.
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 LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of a station transmitting bad data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be increased.
framer runts	Number of packets dropped by the framer as runts, that are smaller than 16 bytes.
framer giants	Number of packets dropped by the framer as giants, whose size is greater than the MTU.
framer aborts	Number of packets dropped by the framer due to an error in packet insertion from the SONET frame. Normally a framer abort is caused by a delimiter inserted at the transmit framer that forces the receive framer to drop the packet on reception because it is bad. The delimiter is inserted by the transmit framer when it cannot transmit a packet due to a transmission error. A runt or CRC error may also result. A framer abort can be caused by any of the following: • A bad transmit framer at the neighbor node (upstream) • BIP errors in the SONET frame that cause a false abort delimiter (often due to intermediate equipment failure or clocking issues) • A bad receive framer at this node
mac runts	Packets dropped by the MAC controller as runts, that are smaller than 24 bytes.
mac giants	Packets dropped by the MAC controller as giants, whose size is greater than the MTU.

Field	Description
mac ttl strips	Packets stripped by the MAC controller when the SRP Time to Live value expires. (TTL value is 1 when a packet arrives.) These packets are removed from the ring because the TTL value cannot be decreased. As a result, the packet is dropped if it is not destined for the node that strips it.

In the following example, self-detected failures in the SRP interface configured on slot 7, subslot 0, and port 0 are displayed:

```
RP/0/RP0/CPU0:router# show srp failures

 Self Detected Failures Information for Interface SRP0/7/0/0
 Side A:
                 Reported  Debounced  Current  Stable    Debounce
                 state     state      state    for(sec)  delay(sec)
HW missing       IDLE      IDLE       IDLE     778       0
L1 Admin State   IDLE      IDLE       IDLE     777       0
Layer 1          IDLE      IDLE       IDLE     778       0
MAC Keepalive    IDLE      IDLE       IDLE     477       5
Link quality     IDLE      IDLE       IDLE     778       0
Mate interface   IDLE      IDLE       IDLE     778       10
Side mismatch    IDLE      IDLE       IDLE     477       5
Result Self Detect = IDLE

 Side B:
                 Reported  Debounced  Current  Stable    Debounce
                 state     state      state    for(sec)  delay(sec)
HW missing       IDLE      IDLE       IDLE     778       0
L1 Admin State   IDLE      IDLE       IDLE     775       0
Layer 1          IDLE      IDLE       IDLE     778       0
MAC Keepalive    IDLE      IDLE       IDLE     477       5
Link quality     IDLE      IDLE       IDLE     778       0
Mate interface   IDLE      IDLE       IDLE     778       10
Side mismatch    IDLE      IDLE       IDLE     477       5
Result Self Detect = IDLE
```

Table 82: show srp failures Command Output Fields

Field	Description
HW missing	Presence of this side's hardware port. Possible states: IDLE—No error or failureSF—Port is not installed or is still booting
L1 Admin State	Layer 1 administrative state. Possible states:IDLE—SONET controller is configured as upFS—SONET controller is configured as administratively down **Note** This is the only field in which the status is related to a user-configurable state.
Layer 1	Operating state of the SONET controller. Possible states:IDLE—No alarms, etc.SF—Some alarms, such as section loss of signal (SLOS), section loss of frame (SLOF), or line alarm indicator signal (LAIS) **Note** For detailed information about a Layer 1 failure, use the **show controllers sonet** command.

Field	Description
MAC keepalive	The MAC keepalive timer has expired.
Link quality	The SONET B3 bit error rate (BER) threshold has been crossed. To configure SRP signal degrade detection and signal fail detection, use the srp priority-threshold, on page 841 command.
Mate interface	The external mate cable on a line card interface is missing or malfunctioning. **Note** This is only applicable to one-port PLIMs or SPAs that would require a second PLIM or SPA to create an SRP interface.
Side mismatch	Side A of the node is connected to side A of the neighbor node, or side B of the node is connected to side B of the neighbor node.
Result Self Detect	IPS state requested for this side. The state is the highest IPS request listed under "Reported state."
Reported state	State that is reported to the IPS engine.
Debounced state	Current SF/FS state or the current IDLE state if IDLE has been stable for the amount of time of the debounce delay.
Current state	Current state as reported by the source.
Stable for (sec)	Amount of time the current state has been stable.
Debounce delay (sec)	Amount of time to wait when transitioning from SF to IDLE. The IDLE state must be stable for this amount of time before getting debounced or reported. This is to prevent flapping and is similar to higher-level WTR values.

In the following example, the display from the **show srp** command with the **interface** keyword is shown:

```
RP/0/RP0/CPU0:router# show srp interface srp 0/5/0/0

IPS Information for Interface SRP0/5/0/0
 MAC Addresses
   Side A (Outer ring RX) neighbor 0009.11d8.3c66
   Side B (Inner ring RX) neighbor 0012.da6a.f664
   Node MAC address 0800.453d.8644
 IPS State
   Side A not wrapped
   Side B not wrapped
   Side A (Inner ring TX) IPS pkt. sent every 1 sec. (next pkt. after 1 sec.)
   Side B (Outer ring TX) IPS pkt. sent every 1 sec. (next pkt. after 1 sec.)
   inter card bus disabled
   IPS WTR period is 60 sec. (timer is inactive)
   Node IPS State: idle
 IPS Self Detected Requests           IPS Remote Requests
   Side A IDLE                          Side A IDLE
   Side B IDLE                          Side B IDLE
   Side A Failures: none
   Side B Failures: none
 IPS messages received
   Side A (Outer ring RX) { 0009.11d8.3c66,IDLE,SHORT}, TTL 255
```

```
  Side B (Inner ring RX) { 0012.da6a.f664,IDLE,SHORT}, TTL 255
IPS messages transmitted
  Side A (Inner ring TX) { 0800.453d.8644,IDLE,SHORT}, TTL 255
  Side B (Outer ring TX) { 0800.453d.8644,IDLE,SHORT}, TTL 255
IPS delay trigger keepalive
  Side A: 0 milliseconds
  Side B: 0 milliseconds

Topology Map for Interface: SRP0/5/0/0
 Topology pkt. sent every 5 sec.  (next pkt. after 1 sec.)
 Last received topology pkt. 00:00:05
 Last topology change was 00:01:59 ago.
 Nodes on the ring: 3
 Hops (outer ring)      MAC       IP Address      Wrapped SRR   Name
        0          0800.453d.8644 0.0.0.0           No      -   ios
        1          0012.da6a.f664 0.0.0.0           No      -   gsrd
        2          0009.11d8.3c66 0.0.0.0           No      -   gsre

SRR not enabled for Interface SRP0/5/0/0

Rate Limit Information for Interface SRP0/5/0/0
  Minimum SRP priority value of high priority outgoing/transit traffic: 2
```

Fields from the **show srp** command output with the **interface** keyword are described in Table 83: show srp ips Command Output Fields, on page 827 and Table 84: show srp topology Command Output Fields, on page 828. The minimum SRP priority value for high-priority traffic is set to 2 by default.

The following example shows the display from the **show srp** command with the **ips** keyword:

```
RP/0/RP0/CPU0:router# show srp ips

 IPS Information for Interface SRP0/7/0/0
 MAC Addresses
   Side A (Outer ring RX) neighbor 000e.3900.4800
   Side B (Inner ring RX) neighbor 000a.8b08.9600
   Node MAC address 0800.453c.f882
 IPS State
   Side A not wrapped
   Side B not wrapped
   Side A (Inner ring TX) IPS pkt. sent every 1 sec. (next pkt. after 1 sec.)
   Side B (Outer ring TX) IPS pkt. sent every 1 sec. (next pkt. after 1 sec.)
   inter card bus disabled
   IPS WTR period is 60 sec. (timer is inactive)
   Node IPS State: idle
 IPS Self Detected Requests           IPS Remote Requests
   Side A IDLE                          Side A IDLE
   Side B IDLE                          Side B IDLE
   Side A Failures: none
   Side B Failures: none
 IPS messages received
   Side A (Outer ring RX) { 000e.3900.4800,IDLE,SHORT}, TTL 255
   Side B (Inner ring RX) { 000a.8b08.9600,IDLE,SHORT}, TTL 255
 IPS messages transmitted
   Side A (Inner ring TX) { 0800.453c.f882,IDLE,SHORT}, TTL 255
   Side B (Outer ring TX) { 0800.453c.f882,IDLE,SHORT}, TTL 255
 IPS delay trigger keepalive
   Side A: 0 milliseconds
   Side B: 0 milliseconds
```

Table 83: show srp ips Command Output Fields

Field	Description
IPS Information for Interface	IPS (Intelligent Protection Switching) identifies the status of an SRP interface on the SRP ring.
MAC AddressesSide A (Outer ring RX) neighbor	MAC address of the next SRP node on the outer ring.
MAC AddressesSide B (Inner ring RX) neighbor	MAC address of the next SRP node on the inner ring.
Node MAC address	MAC address of this SRP node.
IPS State	Reports whether or not a wrap exists on side A or side B of the SRP ring.
IPS WTR period is 60 seconds (timer is inactive)	Displays the current WTR (Wait to Restore) timer value. If a timer is active, the time remaining before the timer expires also is given.
Node IPS State IDLE	Displays the current IPS state of the node. IDLE is the normal state. Other states are WRAPPED and UNKNOWN. Unknown means that the node is in pass-through mode.
IPS self-detected requests	Indicates any locally generated requests. Displays local IPS requests, as well as IDLE status. Possible requests include the following:FS — Forced SwitchSF — Signal FailSD — Signal DegradeMS — Manual SwitchWTR — Wait to Restore
IPS remote requests	Indicates any remotely generated requests. Displays remote IPS requests, as well as IDLE status. Possible requests include the following:FS — Forced SwitchSF — Signal FailSD — Signal DegradeMS — Manual SwitchWTR — Wait to Restore
IPS messages received	Provides details of the last IPS messages received. Fields within the braces ({}) are the MAC addresses of the sending node and the IPS state (IDLE, FS, and so on). It also indicates either a short or long path.
IPS messages transmitted	Provides details of the last IPS messages transmitted, in the format used for received messages.
IPS delay trigger keepalive	Configured value of the **srp ips delay trigger-keepalive** command. The default value is 0.

The following example shows the display from the **show srp** command with the **topology** keyword:

```
RP/0/RP0/CPU0:router# show srp topology

 Topology Map for Interface SRP0/7/0/0
  Topology pkt. sent every 5 sec.  (next pkt. after 5 sec.)
  Last received topology pkt. 00:00:01
  Last topology change was 00:09:44 ago.
  Nodes on the ring: 3
  Hops (outer ring)      MAC       IP Address      Wrapped SRR   Name
```

```
0          0800.453c.f882 30.30.30.2        No      -   crs1
1          000a.8b08.9600 30.30.30.1        No      -   gsra
2          000e.3900.4800 30.30.30.3        No      -   gsrb
```

Table 84: show srp topology Command Output Fields, on page 828 describes the significant fields shown in the display.

Table 84: show srp topology Command Output Fields

Field	Description
Topology map for interface	Displays SRP topology information that identifies the SRP interface.
Topology packet sent every 10 seconds (next packet after 5 seconds)	Displays the interval between successive topology packets sent from this node and the time until the next one is to be sent (rounded down to the nearest second).
Last received topology packet 00:00:04	Displays the time since the last topology packet was received at this node.
Nodes on the ring: 4	Displays the number of nodes in the current ring topology.
Hops	Displays the number of hops to the destination node along the outer ring (from side B). The local node is at hop count zero.
MAC	Displays the MAC address of the node.
IP Address	Displays the IP address of the SRP interface on the node. If the address is not known, the text string “unknown” is displayed. The IP address information is gathered by the ARP table. When a ring is first established, it is normal for the IP address of a node to remain unknown until some time after the MAC address is known.
Wrapped	Uses Yes or No to indicates whether the SRP ring is wrapped at that node.
SRR	Indicates whether SRR is enabled on the node.
Name	Displays the hostname of the router. If the name is not known, this field is left blank. The hostname is obtained from information that is broadcast on the ring at a slower rate than other topology information. When a ring is first established, it is normal for the hostname of a remote node to remain unknown until some time after the MAC address is known.

The following example shows the display from the **show srp** command with the **transit** keyword:

```
RP/0/RP0/CPU0:router# show srp transit interface srp 0/7/0/0

 Transit Buffer Delay Counters for Interface SRP0/7/0/0
   Side A:
   Transit Delay (5 Minutes)             Nanoseconds
     Low TB Min Delay:                             0
     Low TB Avg Delay:                             0
     Low TB Max Delay:                             0
     High TB Min Delay:                          569
```

```
  High TB Avg Delay:                          569
  High TB Max Delay:                          570

Side B:
Transit Delay (5 Minutes)              Nanoseconds
  Low TB Min Delay:                             0
  Low TB Avg Delay:                             0
  Low TB Max Delay:                             0
  High TB Min Delay:                           15
  High TB Avg Delay:                          261
  High TB Max Delay:                          574
```

Table 85: show srp transit Command Output Fields

Field	Description
Low TB Min Delay	Minimum value for the low transit buffer as calculated over the last load interval.
Low TB Avg Delay	Average value for the low transit buffer as calculated over the last load interval.
Low TB Max Delay	Maximum value for the low transit buffer as calculated over the last load interval.
High TB Min Delay	Minimum value for the high transit buffer as calculated over the last load interval.
High TB Avg Delay	Average value for the high transit buffer as calculated over the last load interval.
High TB Max Delay	Maximum value for the high transit buffer as calculated over the last load interval.

Related Commands

Command	Description
clear srp counters, on page 808	Clears the various SRP packet counters.
load-interval	Sets the time (in seconds) used to gather data for computing load statistics.
show controllers sonet	Displays the SONET controller information for the interface.
show controllers srp, on page 817	Displays the current controller configuration on an SRP interface.
show interfaces srp	Displays current IPS wrap state, along with other SRP interface information.

srp ips delay trigger-keepalive

To specify a delay for the IPS keepalive value, use the **srp ips delay keep-alive** command in interface configuration mode. To restore the default value, use the **no** form of this command.

srp ips delay trigger-keepalive *value* **a** | **b**
no srp ips delay trigger-keepalive *value* **a** | **b**

Syntax Description

value	Time in milliseconds of the trigger keepalive. Values can range from 51 to 200.
a	The side of a node that has outer ring receive fiber is identified as side A.
b	The side of a node that has inner ring receive fiber is identified as side B.

Command Default

The default IPS keepalive delay value is 0.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2.2	This command was introduced and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The default keepalive value is 1 ms. Use the **srp ips delay trigger-keepalive** command to delay this 1 ms up to the configured delay value. You should use this command only if the Layer 1 (SONET) is already protected (for example, with SONET APS). This delay gives the first protection mechanism time to protect, before the Layer 2 protection is enabled. For example, if an SRP side is connected to an Add-Drop Multiplexer (ADM) that utilizes dual SONET ring and APS, you should delay the Layer 2 keepalive value using this command.

Task ID

Task ID	Operations
pos-dpt	read, write

Examples

The following example indicates how to set the trigger keepalive timer to 60 milliseconds:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface srp 0/5/0/0
RP/0/RP0/CPU0:router(config-if)# srp ips delay trigger-keepalive 60 a
```

Related Commands

Command	Description
show srp, on page 819	Displays information about an SRP interface.

srp ips request forced-switch

To initiate a forced-switch wrap on a ring, use the **srp ips request forced-switch** command in interface configuration mode. To remove the wrap, use the **no** form of this command.

srp ips request forced-switch a | b
no srp ips request forced-switch a | b

Syntax Description

a	The side of a node that has outer ring receive fiber is identified as side A.
b	The side of a node that has inner ring receive fiber is identified as side B.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2.2	This command was introduced and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
pos-dpt	read, write

Examples

The following example shows how to insert a forced-switch wrap on side A of the interface by entering the **srp ips request forced-switch** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface srp 0/5/0/0
RP/0/RP0/CPU0:router(config-if)# srp ips request forced-switch a
```

Related Commands

Command	Description
show interfaces srp	Displays current IPS wrap state, along with other SRP interface information.

Command	Description
show srp, on page 819	Displays information about SRP interfaces on the ring, including MAC addresses of neighboring nodes, IPS status, source-counters, and topology map.
srp ips wtr-timer, on page 836	Determines how long a wrap remains on the fiber after the original cause of the wrap is removed.
srp manual-switch, on page 839	Inserts a manual-switch wrap on the ring.
srp shutdown, on page 843	Provides an alternative form of the **srp ips request forced-switch** command.

srp ips timer

To control the frequency of the transmission of Intelligent Protection Switching (IPS) requests, use the **srp ips timer** command in interface configuration mode. To restore the default value, use the **no** form of this command.

srp ips timer *value*
no srp ips timer *value*

Syntax Description

value	Amount of time in seconds between transmission of IPS requests. Values can range from 1 to 60.

Command Default

The default IPS timer value is 1 second.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2.2	This command was introduced and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

In general, you should not need to adjust the IPS timer value.

We recommend that you configure the same IPS timer value on all nodes on an SRP ring. This means that if you modify the IPS timer setting on one node, you must reconfigure all other nodes on the ring with the same IPS timer value.

Task ID

Task ID	Operations
pos-dpt	read, write

Examples

The following example indicates how to change the IPS timer to 30 seconds:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface srp 0/5/0/0
RP/0/RP0/CPU0:router(config-if)# srp ips timer 30
```

Related Commands

Command	Description
show srp, on page 819	Displays information about an SRP interface.

Command	Description
srp ips wtr-timer, on page 836	Controls the amount of time to wait before a wrap is removed after there is no more reason for the wrap.

srp ips wtr-timer

To control the amount of time to wait before a wrap is removed after there is no more reason for the wrap, use the **srp ips wtr-timer** command in interface configuration mode. To restore the default value, use the **no** form of this command.

srp ips wtr-timer *value*
no srp ips wtr-timer *value*

Syntax Description

value	Amount of time in seconds for the wait-to-restore (WTR) timer. Values can range from 10 to 600.

Command Default

The default WTR timer value is 60 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2.2	This command was introduced and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

In general, you should not need to adjust the Intelligent Protection Switching (IPS) wait-to-restore (WTR) timer value.

Task ID

Task ID	Operations
pos-dpt	read, write

Examples

The following example indicates how to change the IPS wait-to-restore timer to 120 seconds:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface srp 0/5/0/0
RP/0/RP0/CPU0:router(config-if)# srp ips wtr-timer 120
```

Related Commands

Command	Description
show srp, on page 819	Displays information about an SRP interface.
srp ips timer, on page 834	Controls the frequency of the transmission of IPS requests.

srp mac-count

To keep track of the number of SRP packets from a specific source MAC address, use the **srp mac-count** command in interface configuration mode. To disable counting by MAC address, use the **no** form of this command.

srp mac-count *mac-address*
no srp mac-count *mac-address*

Syntax Description

mac-address	48-bit source MAC address from which to count SRP packets.

Command Default

The **srp mac-count** command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2.2	This command was introduced and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
pos-dpt	read, write

Examples

The following example shows how to count SRP packets from the source with MAC address 2.2.2:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface srp 0/5/0/0
RP/0/RP0/CPU0:router(config-if)# srp mac-count 2.2.2
```

Related Commands

Command	Description
clear srp counters, on page 808	Clears the SRP counters.
show srp, on page 819	Displays information about an SRP interface.

srp mac-reject

To reject SRP packets from a specific source MAC address, use the **srp mac-reject** command in interface configuration mode. To disable rejection by MAC address, use the **no** form of this command.

srp mac-reject *mac-address*
no srp mac-reject *mac-address*

Syntax Description

mac-address	48-bit source MAC address from which to reject SRP packets.

Command Default

The **srp mac-reject** command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2.2	This command was introduced and is supported on the 4-port OC-192c/STM-64c POS/DPT PLIM.
Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use **srp mac-reject** command to control a node that cannot be fixed because it is owned or administered by someone else. For example, if such a node is flooding your node with packets, you can use this command to limit the amount of traffic that is processed.

Task ID

Task ID	Operations
pos-dpt	read, write

Examples

The following example shows how to reject SRP packets from the source with MAC address 2.2.2:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface srp 0/5/0/0
RP/0/RP0/CPU0:router(config-if)# srp mac-reject 2.2.2
```

Related Commands

Command	Description
clear srp counters, on page 808	Clears the SRP counters.
show srp, on page 819	Displays information about an SRP interface.

srp manual-switch

To initiate or remove a manual switch wrap on a ring, use the **srp manual-switch** command in EXEC mode.

srp request | **remove manual-switch a** | **b interface srp** *interface-path-id*

Syntax Description

request	Initiate a manual switch wrap on the interface.
remove	Remove a manual switch wrap on the interface.
a	The side of a node that has outer ring receive fiber is identified as side A.
b	The side of a node that has inner ring receive fiber is identified as side B.
interface	Specifies the interface for which to display the counters.
srp	Specifies an SRP 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

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2.2	This command was introduced and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
pos-dpt	read, write

Examples

The following example shows how to insert a manual switch wrap on side A of the interface:

```
RP/0/RP0/CPU0:router# srp request manual-switch a interface srp 0/5/0/0
```

Related Commands

Command	Description
show interfaces srp	Displays current IPS wrap state, along with other SRP interface information.
show srp, on page 819	Displays information about SRP interfaces on the ring, including MAC addresses of neighboring nodes, IPS status, source-counters, and topology map.
srp ips request forced-switch, on page 832	Inserts a forced switch wrap on the ring; this command is an alternate form of the **srp shutdown** command.
srp ips wtr-timer, on page 836	Determines how long a wrap remains on the fiber after the original cause of the wrap is removed.
srp shutdown, on page 843	Provides an alternative form of the **srp ips request forced-switch** command.

srp priority-threshold

To specify the RAC threshold for placing packets in the high-priority queue, use the **srp priority-threshold** command in Interface configuration mode. To return the priority threshold to its default value, use the **no** form of this command.

srp priority-threshold [*RAC-threshold* | **non-high**]
no srp priority-threshold [*RAC-threshold* | **non-high**]

Syntax Description

RAC-threshold	RAC priority slicing point threshold ranging from 1 to 7.
non-high	Specifies not to place any packets into the RAC high priority transmit queue.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
3.2.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Examples

The following example shows how to qualify traffic with a RAC of 5 or greater into the high-priority transmit queue:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface srp 0/5/0/0
RP/0/RP0/CPU0:router(config-if)# srp priority-threshold 5
```

Related Commands

Command	Description
show srp, on page 819	Displays information about an SRP interface.

srp rate-limit

To configure the amount of high- and low-priority traffic being transmitted from the router onto the SRP ring, use the **srp rate-limit** command in Interface configuration mode. To disable rate limiting, use the **no** form of this command.

rate-limit [**high** | **low**] *limit*
no rate-limit [**high** | **low**] *limit*

Syntax Description

high	Specifies the SRP high priority transmit queue rate limit.
low	Specifies the SRP low priority transmit queue rate limit.
limit	Rate limit in Mbps. The value can range from 0 to 4,294,967,295.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
3.2.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Examples

The following example shows how to limit the traffic in the high and low priority traffic to the SRP ring:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface srp 0/5/0/0
RP/0/RP0/CPU0:router(config-if)# srp rate-limit high 622
RP/0/RP0/CPU0:router(config-if)# srp rate-limit low 1866
```

Related Commands

Command	Description
show srp, on page 819	Displays information about an SRP interface.

srp shutdown

To shut down an interface by entering a forced switch, use the **srp shutdown** command in interface configuration mode. To remove the forced switch wrap near the interface, use the **no** form of this command.

srp shutdown
no srp shutdown

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 3.2.2	This command was introduced and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
pos-dpt	read, write

Examples

The following example shows how to enter a forced switch on the interface:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface srp 0/5/0/0
RP/0/RP0/CPU0:router(config-if)# srp shutdown
```

Related Commands

Command	Description
show interfaces srp	Displays current IPS wrap state along with other SRP interface information.
show srp, on page 819	Displays information about SRP interfaces on the ring, including MAC addresses of neighboring nodes, IPS status, source-counters, and topology map.

Command	Description
srp ips request forced-switch, on page 832	Inserts a forced switch wrap on the ring; this command is an alternate form of the **srp shutdown** command.

srp topology-timer

To specify the frequency of the topology timer, use the **srp topology-timer** command in interface configuration mode. To restore the default value, use the **no** form of this command.

srp topology-timer *value*
no srp topology-timer *value*

Syntax Description

value	Value of topology timer in seconds, ranging from 1 to 600.

Command Default

The default topology timer value is 10 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2.2	This command was introduced and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **srp topology-timer** interface configuration command determines how frequently topology discovery messages are sent around the ring to identify the current nodes on the SRP ring.

In general, you should not need to adjust the topology timer value.

Task ID

Task ID	Operations
pos-dpt	read, write

Examples

The following example indicates how to change the topology timer to 300 seconds:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface srp 0/5/0/0
RP/0/RP0/CPU0:router(config-if)# srp topology-timer 1
```

Related Commands

Command	Description
show srp, on page 819	Displays information about an SRP interface.

T3 and E3 Controller Commands on the Cisco IOS XR Software

This module provides command line interface (CLI) commands for configuring T3/E3 controllers on the Cisco CRS Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

- shutdown (T3/E3), on page 896

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 3.5.0	This command was introduced for T3/E3 lines.

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/RP0/CPU0:router# bert e3 0/3/0/0/0 start
RP/0/RP0/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/RP0/CPU0:router# bert e3 0/3/0/0 error
```

Related Commands

Command	Description
bert interval, on page 852	Specifies the duration of a bit error rate test (BERT) pattern on a T3/E3 line.
bert pattern, on page 853	Enables a BERT pattern on a T3/E3 line or an individual channel group.
show controllers e3, on page 885	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 line, use the **bert error** command in T3 configuration mode. To disable a BERT pattern, use the **no** form of this command.

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

Command History

Release	Modification
Release 3.5.0	This command was introduced for T3/E3 lines.

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/RP0/CPU0:router(config)# controller t3 0/0/3/1/10
RP/0/RP0/CPU0:router(config-t3e3)# bert error 10
```

Related Commands

Command	Description
bert interval, on page 852	Specifies the duration of a bit error rate test (BERT) pattern on a T3/E3 line.
bert pattern, on page 853	Enables a BERT pattern on a T3/E3 line or an individual channel group.
show controllers e3, on page 885	Displays information about the E3 links and hardware and software drivers for the E3 controller.
show controllers t3, on page 889	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 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*

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

Command History

Release	Modification
Release 3.5.0	This command was introduced for T3/E3 lines.

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/RP0/CPU0:router(config)# controller t3 0/0/3/1/10
RP/0/RP0/CPU0:router(config-t3e3)# bert interval 10
```

Related Commands

Command	Description
bert error, on page 851	Insert errors into a BERT stream on a T3/E3 line.
bert pattern, on page 853	Enables a BERT pattern on a T3/E3 line or an individual channel group.
show controllers e3, on page 885	Displays information about the E3 links and hardware and software drivers for the E3 controller.
show controllers t3, on page 889	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 line or an individual channel group, use the **bert pattern** command in T3 or E3 configuration mode. To disable a BERT pattern, use the **no** form of this command.

bert pattern **0s** | **1s** | **2^11** | **2^15** | **2^20** | **2^20-QRSS** | **2^23** | **2^9**

Syntax Description

0s	Invokes a repeating pattern of zeros (...000...).
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.
alt-0-1	Invokes a repeating pattern of alternating zeros and ones (...01010...).

Command Default

BERT pattern test is disabled

Command Modes

T3 configuration

E3 configuration

Command History

Release	Modification
Release 3.5.0	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 links. It is done only over an unframed T3/E3 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 t3** or **bert e3** command in EXEC 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 enable the running of a BERT pattern of all zeros on the T3 controller in slot 0, subslot 3:

```
RP/0/RP0/CPU0:router(config)# controller t3 0/0/3/1/10
RP/0/RP0/CPU0:router(config-t3e3)# bert pattern 0s
```

Related Commands

Command	Description
bert error, on page 851	Insert errors into a BERT stream on a T3/E3 line.
bert interval, on page 852	Specifies the duration of a bit error rate test (BERT) pattern on a T3/E3 line.
show controllers e3, on page 885	Displays information about the E3 links and hardware and software drivers for the E3 controller.
show controllers t3, on page 889	Displays information about the T3 links and hardware and software drivers for the T3 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 3.5.0	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/RP0/CPU0:router# bert t3 0/3/0/0 start
RP/0/RP0/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/RP0/CPU0:router# bert t3 0/3/0/0 error
```

Related Commands

Command	Description
bert interval, on page 852	Specifies the duration of a bit error rate test (BERT) pattern on a T3/E3 line.
bert pattern, on page 853	Enables a BERT pattern on a T3/E3 line or an individual channel group.
show controllers t3, on page 889	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*

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 3.5.0	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/RP0/CPU0:router(config)# controller t3 0/6/0/0
RP/0/RP0/CPU0:router(config-t3)# cablelength 300
```

clear controller t3

To clear T3 controller data, use the **clear controller t3** command in EXEC 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 3.5.0	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
interface	read, write

Task ID	Operations
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/RP0/CPU0:router(config)# controller t3 0/6/2/0/1
```

Related Commands

Command	Description
controller t3, on page 864	Configures a T3 controller and enters T3 configuration mode.
show controllers t3, on page 889	Displays information about the T3 links and hardware and software drivers for the T3 controller.

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**

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 3.5.0	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 reference clock of the T3 or E3 connection.

Configure the **clock source internal** command if your router provides the reference 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/RP0/CPU0:router(config)# controller t3 0/6/0/0/1
RP/0/RP0/CPU0:router(config-t3)# clock source line
```

Related Commands

Command	Description
controller e3, on page 862	Configures an E3 controller and enters E3 configuration mode.
controller t3, on page 864	Configures a T3 controller and enters T3 configuration mode.

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*

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 3.5.0	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/RP0/CPU0:router(config)# controller e3 0/6/2/0
RP/0/RP0/CPU0:router(config-e3)#
```

Related Commands

Command	Description
hw-module subslot cardtype, on page 877	Sets the ports on a SPA in T3 or E3 mode.
show controllers e3, on page 885	Displays information about the E3 links and hardware and software drivers for the E3 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*

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 3.5.0	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/RP0/CPU0:router(config)# controller t3 0/6/2/0/1
RP/0/RP0/CPU0:router(config-t3)#
```

Related Commands

Command	Description
hw-module subslot cardtype, on page 877	Sets the ports on a SPA in T3 or E3 mode.
show controllers t3, on page 889	Displays information about the T3 links and hardware and software drivers for the T3 controller.

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*

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

No specific guidelines impact the use of this command.

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/RP0/CPU0:router(config)# controller t3 0/4/2/0/1
RP/0/RP0/CPU0:router(config-t3)# delay clear 9000
```

Related Commands

Command	Description
delay trigger (T3/E3), on page 867	Configures a time value for the T3 or E3 path delay trigger.

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*

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/RP0/CPU0:router(config)# controller t3 0/4/2/0/1
RP/0/RP0/CPU0:router(config-t3)# delay trigger 8000
```

Related Commands

Command	Description
delay clear (T3/E3), on page 866	Configures the amount of time before a T3 or E3 path delay trigger alarm is cleared.

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*

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

No specific guidelines impact the use of this command.

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/RP0/CPU0:router(config)# controller t3 0/6/2/0
RP/0/RP0/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 885	Displays information about the E3 links and hardware and software drivers for the E3 controller.
show controllers t3, on page 889	Displays information about the T3 links and hardware and software drivers for the 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/RP0/CPU0:router(config)# controller t3 0/4/2/0
RP/0/RP0/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 879	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

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 3.5.0	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 86: 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

Mode	Bandwidth (in kbps)	Bandwidth Multiples (in kbps)
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/RP0/CPU0:router(config)# controller t3 0/6/2/0/1
RP/0/RP0/CPU0:router(config-t3)# dsu bandwidth 16000
```

Related Commands

Command	Description
show controllers e3, on page 885	Displays information about the E3 links and hardware and software drivers for the E3 controller.
show controllers t3, on page 889	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

Syntax Description

mode DSU mode. Valid values are as follows:

- (T3 only) **adtran**
- (E3 only) cisco
- digital-link
- kentrox
- (T3 only) **larscom**
- (T3 only) **verilink**

For T3, digital-link is default and for E3 cisco is default.

Command Default

For T3, digital-link is default and for E3 cisco is default.

Command Modes

T3 configuration

E3 configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

The default DSU mode Cisco is equivalent to Digilink Mode with Scrambling Enabled. This mode was added to enable scrambling along with Digilink mode on E3 Controllers.

Digilink Mode, by definition does not support scrambling for E3 Controllers though it supports the same for T3 Controllers. For T3 controllers, there is no functional default DSU mode. The DSU Mode Cisco is not applicable for T3 Controller.

For interoperability, it is recommended to always configure the DSU mode command under T3/E3 Controller by matching the DSU type of the remote port.

To enable Scrambling, configure Scramble under the respective Serial Interface for the T3/E3 Controller.

Refer to Table 86: DSU Modes and Vendor-supported Bandwidths, on page 870 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/RP0/CPU0:router(config)# controller t3 0/6/2/0/1
RP/0/RP0/CPU0:router(config-t3)# dsu mode digital-link
```

Related Commands

Command	Description
show controllers e3, on page 885	Displays information about the E3 links and hardware and software drivers for the E3 controller.
show controllers t3, on page 889	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**

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 3.5.0	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/RP0/CPU0:router(config)# controller t3 0/6/2/0
RP/0/RP0/CPU0:router(config-t3)# dsu remote fullrate
```

Related Commands

Command	Description
show controllers e3, on page 885	Displays information about the E3 links and hardware and software drivers for the E3 controller.
show controllers t3, on page 889	Displays information about the T3 links and hardware and software drivers for the T3 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

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 3.5.0	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.

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/RP0/CPU0:router(config)# controller e3 0/6/0/0
RP/0/RP0/CPU0:router(config-e3)# framing g751
```

Related Commands

Command	Description
show controllers e3, on page 885	Displays information about the E3 links and hardware and software drivers for the E3 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

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 3.5.0	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.

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/RP0/CPU0:router(config)# controller t3 0/6/0/0/1
RP/0/RP0/CPU0:router(config-t3)# framing m23
```

Related Commands

Command	Description
show controllers t3, on page 889	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 or E3 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 e3 | t3

Syntax Description

subslot-id	Subslot to be power cycled. The *subslot-id* argument is entered in the *rack/slot/subslot* notation.
e3	Clear-channel E3 with integrated DSUs.
t3	Clear-channel T3 with integrated data service units (DSUs). The default for the 2-Port and 4-Port Clear Channel T3/E3 SPAs is T3 .

Command Default

The default for the 2-Port and 4-Port Clear Channel T3/E3 SPAs is T3.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced for T3 and E3 modes.

Usage Guidelines

The **hw-module subslot cardtype** command applies only to the following SPAs:

- 2-Port and 4-Port Clear Channel T3/E3 SPAs

By default, the 2-Port and 4-Port Clear Channel T3/E3 SPAs boot in T3 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 .

If there are nondefault configurations on the card interfaces, you must delete them before you can change the card type. Use the **no controller** { **e3** | **t3**}and **no interface serial** commands to delete any T3, E3, 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/RP0/CPU0:router(config)# hw-module subslot 0/5/2 cardtype e3
```

Related Commands

Command	Description
controller e3, on page 862	Configures an E3 controller and enters E3 configuration mode.

Command	Description
controller t1	
controller t3, on page 864	Configures a T3 controller and enters T3 configuration mode.

loopback (T3/E3)

To loop the entire T3 or E3 line 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

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	Modification
Release 3.5.0	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.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

This example shows how to configure the T3 for a local loopback:

```
RP/0/RP0/CPU0:router(config)# controller t3 0/3/0/0
RP/0/RP0/CPU0:router(config-t3)# loopback local
```

Related Commands

Command	Description
show controllers e3, on page 885	Displays information about the E3 links and hardware and software drivers for the E3 controller.

Command	Description
show controllers t3, on page 889	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**

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 3.5.0	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/RP0/CPU0:router(config)# controller t3 0/1/2/0
RP/0/RP0/CPU0:router(config-t3)# clock source line
RP/0/RP0/CPU0:router(config-t3)# mdl string eic ID
RP/0/RP0/CPU0:router(config-t3)# mdl string fic Building B
RP/0/RP0/CPU0:router(config-t3)# mdl string unit ABC
RP/0/RP0/CPU0:router(config-t3)# mdl string fi Facility Z
RP/0/RP0/CPU0:router(config-t3)# mdl string port-number Port 7
RP/0/RP0/CPU0:router(config-t3)# mdl transmit path enable
RP/0/RP0/CPU0:router(config-t3)# mdl transmit idle-signal enable
```

Related Commands

Command	Description
show controllers t3, on page 889	Displays information about the T3 links and hardware and software drivers for the T3 controller.

mode

To set the mode of the T3/E3 controller, use the **mode** command in T3 or E3 configuration mode. To disable the controller mode, use the **no** form of this command.

mode atm | serial

Syntax Description

atm	Specifies the mode of the port to be a clear channel transporting ATM.
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.

Command Modes

T3 configuration

E3 configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced for T3/E3 controllers.

Usage Guidelines

You can change the mode of a controller only when there are no subinterfaces defined for the controller.

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 atm:

```
RP/0/RP0/CPU0:router(config)# controller t3 0/6/0/0
RP/0/RP0/CPU0:router(config-t3)# mode atm
```

Related Commands

Command	Description
show controllers e3, on page 885	Displays information about the E3 links and hardware and software drivers for the E3 controller.
show controllers t3, on page 889	Displays information about the T3 links and hardware and software drivers for the T3 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

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 3.5.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0/CPU0:router(config)# controller e3 0/6/2/0
RP/0/RP0/CPU0:router(config-e3)# national bits enable
```

Related Commands

Command	Description
show controllers e3, on page 885	Displays information about the E3 links and hardware and software drivers for the E3 controller.

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 3.5.0	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/RP0/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/RP0/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 87: 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.
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.

Field	Description
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 862	Configures an E3 controller and enters E3 configuration mode.

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 3.5.0	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.

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/RP0/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 88: 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).
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.

Field	Description
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 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/RP0/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/RP0/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 89: 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 .
MDL transmission	Status of the Maintenance Data Link (either enabled or disabled) and the values of the MDL message fields.
EIC	Equipment Identification code.

Field	Description
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.
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.

Field	Description
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.
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 864	Configures a T3 controller and enters T3 configuration mode.

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

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 3.5.0	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/RP0/CPU0:router(config)# controller t3 0/6/0/0
RP/0/RP0/CPU0:router(config-t3)# no shutdown
```

Related Commands

Command	Description
show controllers e3, on page 885	Displays information about the E3 links and hardware and software drivers for the E3 controller.
show controllers t3, on page 889	Displays information about the T3 links and hardware and software drivers for the T3 controller.

Traffic Mirroring Commands

This module describes the commands used to configure and monitor traffic mirroring.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

acl

To configure ACL-based traffic mirroring, use the **acl** command in monitor session configuration mode. To stop ACL-based traffic mirroring, use the **no** form of this command.

acl

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Monitor session configuration

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

If you use the **acl** command, traffic is mirrored according to the definition of the global interface access list (ACL) defined in one of the following commands: **ipv4 access-list**, **ipv6 access-list**, **ethernet-services access-list**.

Even when the **acl** command is configured on the source mirroring port, if the ACL configuration command does not use the **capture** keyword, no traffic gets mirrored.

If the ACL configuration uses the **capture** keyword, but the **acl** command is not configured on the source port, although traffic is mirrored, no access list configuration is applied.

Examples

This example shows how to configure ACL-based traffic mirroring on the interface:

```
RP/0/RP0/CPU0:router(config)# monitor-session tm_example
RP/0/RP0/CPU0:router(config)# ethernet-services access-list tm_filter
RP/0/RP0/CPU0:router(config-es-acl)# 10 deny 0000.1234.5678 0000.abcd.abcd any capture
RP/0/RP0/CPU0:router(config-es-acl)# exit
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet0/2/0/0
RP/0/RP0/CPU0:router(config-if)# monitor-session tm_example direction rx-only
RP/0/RP0/CPU0:router(config-if)# acl
RP/0/RP0/CPU0:router(config-if)# l2transport
RP/0/RP0/CPU0:router(config-if-l2)# exit
RP/0/RP0/CPU0:router(config-if)# ethernet-services access-group tm_filter ingress
RP/0/RP0/CPU0:router(config-if)# end
```

Related Commands

Command	Description
ethernet-services access-list	Defines an Ethernet services (Layer 2) access list by name.
ipv4 access-list	Defines an IPv4 access list by name.

clear monitor-session counters

To clear the traffic mirroring session statistics, use the **clear monitor-session counters** command in EXEC mode .

clear monitor-session counters [*session-name*]**ipv4** | **ipv6**

Syntax Description

interface	Identifies the interface for which the counters are to be cleared.
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.
session-name	Name of the monitor session to clear.
ipv6	Specifies an ipv6 address.

Command Default

All stored statistics for all interfaces are cleared.

Command Modes

EXEC mode

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
interface	read

Examples

This example shows how to clear the traffic mirroring statistic counters:

```
RP/0/RP0/CPU0:routerclear monitor-session  counters
```

destination next-hop

To configure the destination address for the monitor-session, use the **destination next-hop** command in the monitor session configuration mode.

destination next-hop *ip address*

Syntax Description

ip address	Specifies a valid IPv4 or IPv6 address and configures the destination for the current monitor-session to be a next-hop IP address (whose type matches that of the monitor-session).

Command Default

No default behavior or values

Command Modes

Monitor session configuration

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

This may only be specified for ipv4 and ipv6 monitor-sessions. A monitor session can be either for IPv4 or for IPv6. It cannot support both together.

Task ID

Task ID	Operation
ethernet-services	read, write

Example

This example shows how to execute the **destination next-hop** command:

```
RP/0/RP0/CPU0:router(config)#
RP/0/RP0/CPU0:router(config-mon-sess)#destination next-hop ipv4 254.23.24.5
```

mirror first

To configure partial traffic mirroring, use the **mirror first** command in monitor session configuration mode. To stop mirroring a portion of the packet, use the **no** form of this command.

mirror first *bytes*

Syntax Description

bytes	Number of bytes mirrored. The mirrored packet length value can range from 65 to 128.

Command Default

The entire packet is mirrored.

Command Modes

Monitor session configuration

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

Use the **mirror first** command to mirror the first 64 to 128 bytes of the packet. The actual mirrored packet is the configured partial packet monitoring size plus the 4-byte trailing CRC.

Examples

This example shows how to mirror the first 100 bytes of the packet:

```
RP/0/RP0/CPU0:router(config)# interface gigabitethernet0/0/0/11
RP/0/RP0/CPU0:router(config-if)# monitor-session mon1
RP/0/RP0/CPU0:router(config-if-mon)# mirror first 100
```

Related Commands

Command	Description
monitor-session, on page 903	Defines a traffic mirroring session and enter monitor session configuration mode.

mirror interval

To configure mirror interval for a specified number of packets in traffic mirroring, use the **mirror interval** command in monitor session configuration mode. To stop mirroring the packet in the interval, use the **no** form of this command.

mirror interval 512 | 1k | 2k | 4k | 8k | 16k

Syntax Description

interval Number of packets per mirror interval. The interval can be configured for every 512, 1k, 2k, 4k, 8k, or 16k packets.

Note
- port-level mirroring is only supported in the ingress direction.
- port-level mirroring is only supported in sampling mode with a minimal sampling rate of 1:512

Command Default

The mirror interval is set as per the specified packet count.

Command Modes

Monitor session configuration

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Examples

This example shows how to set the mirror interval for every 512 packets:

```
RP/0/RP0/CPU0:router(config)# interface gigabitethernet0/0/0/11
RP/0/RP0/CPU0:router(config-if)# monitor-session mon1
RP/0/RP0/CPU0:router(config-if-mon)# mirror first 100
RP/0/RP0/CPU0:router(config-if-mon)# mirror interval 512
```

Related Commands

Command	Description
monitor-session, on page 903	Defines a traffic mirroring session and enter monitor session configuration mode.

monitor-session

To define a traffic mirroring session and enter monitor session configuration mode, use the **monitor-session** command in global configuration mode. To remove the traffic mirroring session, use the **no** form of this command.

monitor-session *session-name***[ethernet|ipv4|ipv6] destination(interface** *<Interface> slot/port***)**

Syntax Description

session-name	Name of the monitor session to configure.
ethernet	Specifies ethernet interface as destination.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

Before you can assign a monitor session to a specific interface, you must configure it using the **monitor-session** command. The *session-name* should not be the same as any interface name.

In monitor session configuration mode, you should define the destination interface to be used in the traffic mirroring session using the **destination** command.

This commands triggers entry in to the monitor-session sub-mode and creates the session. The session will be non-operable until a destination is configured for the session. The destination can be either IPv4 or IPv6.

Examples

This example shows how to enter monitor session configuration mode:

```
RP/0/RP0/CPU0:router(config)# monitor-session mon1
RP/0/RP0/CPU0:router(config-mon)#
```

Related Commands

Command	Description
destination next-hop, on page 900	Configures the destination for the current monitor-session.

monitor-session (interface)

To associate a traffic mirroring session with a specific interface, use the **monitor-session** command in interface configuration mode. To remove the association between a traffic mirroring session and an interface, use the **no** form of this command.

monitor-session *session-name* **[ethernet|ipv4|ipv6]**[**direction rx-only**] **[port-level]**

Syntax Description

session-name	Name of the monitor session to configure.
direction	Specifies that traffic replication is in only one direction.
rx-only	Specifies that only ingress traffic is replicated.
ethernet	Specifies ethernet interface as destination.
ipv4	Indicates that Ipv4 traffic needs to be monitored.
ipv6	Indicates that Ipv6 traffic needs to be monitored.
port-level	Specifies the configuration at port level. **Note** • port-level mirroring is only supported in the ingress direction. • port-level mirroring is only supported in sampling mode with a minimal sampling rate of 1:512.

Command Default

Replicates both ingress and egress traffic.

Command Modes

Interface configuration

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

Before you can associate a traffic mirroring session to a specific interface, you must define it using the **monitor-session** global configuration command. After the traffic mirroring session is defined, use the **monitor-session** interface configuration command or dynamic template configuration command to associate this session with a specific source interface. For BNG sessions, the subscriber is attached to the monitor session, only when the dynamic template is applied to the subscriber. When the session is associated, all specified traffic on the interface is then replicated to the destination location defined in the monitor session configuration.

The **monitor-session** interface configuration command also enters monitor session configuration mode for you to configure additional features of the mirroring session.

If a physical interface is configured for Layer 3, then the traffic mirroring session can be associated on physical interfaces. Example:

```
interface TenGigE0/1/0/0
ipv4 address 10.0.0.1 255.255.255.0
```

If a physical interface has sub-interfaces configured for Layer 3, then the traffic mirroring session must be associated on each sub-interface. Example:

```
interface TenGigE0/1/0/1.601
ipv4 address 10.0.1.1 255.255.255.0
encapsulation dot1q 601
```

Task ID

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

Examples

This example shows a sample configuration of the **monitor-session** command in the interface configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface gigabitethernet0/2/0/0
RP/0/RP0/CPU0:router(config-if)# monitor-session test  ipv4 rx-only
RP/0/RP0/CPU0:router(config-if)# acl
```

show monitor-session status

To display status information about configured traffic mirroring sessions, use the **show monitor-session status** command in EXEC mode .

show monitor-session [*session-name*] **status** [**detail**] [**errors**]

Syntax Description

session-name	Name of the monitor session to configure.
detail	Displays the full error string for any errors.
errors	Displays all sessions, but only source interfaces with errors are displayed (if no source interfaces have errors, then 'No errors' is displayed).

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

The **show monitor-sessions status** command displays the following information:

- Destination information for the session (including the name of the interface).
- Destination status (interface state).
- List of source interfaces.
- Any other status information that may be pertinent, such as a software or hardware error that would stop sessions operating correctly. If an error is returned from interactions with another component, then the full error string is only displayed in detail output; standard tabular output reports that there has been an error but refers the user to the detailed output.

Examples

This example shows the sample output for the **show monitor-session status detail** command:

```
RP/0/RP0/CPU0:router show monitor-session status detail

Monitor-session foo
  Destination interface GigabitEthernet 0/0/0/0
  Source Interfaces
  -----------------
  GigabitEthernet 0/1/0/0.100:
    Direction: Both
    Status:    Operating
  GigabitEthernet 0/2/0/0.200:
    Direction: Rx
    Status:    Error: <blah>

Monitor session bar
  No destination configured
  Source Interfaces
```

```
-----------------
GigabitEthernet 0/3/0/0.100:
  Direction: Rx
  Status:    Not operational(no destination interface)
```

show monitor-session counters

To display statistics regarding traffic mirroring sessions, use the **show monitor-session counters** command in EXEC mode .

show monitor-session [*session-name*] **ipv4** | **ipv6counters**

Syntax Description

session-name	Name of the monitor session to configure.
ipv4	Specifies the counters of next-hop ipv4 address associated with a monitor-session.
ipv6	Specifies the counters of next-hop ipv6 address associated with a monitor-session.

Command Default

If you do not specify an address, the IPv4 counters are displayed.

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

The **show monitor-sessions counters** command displays a list of all source interfaces, and the replicated packet statistics for each interface. The full set of statistics displayed for each interface is:

- Ingress replicated packets and octets
- Egress replicated packets and octets
- Non-replicated packets and octets

Examples

This example shows sample output from the **show monitor-session counters** command:

```
RP/0/RP0/CPU0:router show monitor-session 2 counters

Global Non Replicated : 100 Packets 8000 Bytes
Monitor session test1 ipv4
      Next Hop : 20.1.1.1
      Rx Replicated: 100 Packets 8000 Bytes
Monitor session test2
      Next Hop : 30.1.1.1
      Rx Replicated: 200 Packets 16000 Bytes
```

VLAN Subinterface Commands

This module provides command line interface (CLI) commands for configuring 802.1Q VLANs on the Cisco CRS Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

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*

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 3.0	This command was introduced.

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/RP0/CPU0:router(config)# interface TenGigE 0/2/0/4
RP/0/RP0/CPU0:router(config-if)# dot1q native vlan 1
```

Related Commands

Command	Description
dot1q vlan, on page 911	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.

Note Effective with Cisco IOS XR Release 3.7.2, the **dot1q vlan** command is replaced by the **encapsulation dot1q** command. See the **encapsulation dot1q** command for more information.

dot1q vlan *vlan-id* [*vlan-id2* | **any**]

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 3.0	This command was introduced.
Release 5.1.1	This command was introduced and was also replaced by the **encapsulation dot1q** command.

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.

Note The **dot1q vlan** command is is replaced by the **encapsulation dot1q** command. It is still available for backward-compatibility, but only for Layer 3 interfaces. The **encapsulation dot1q** command must be used going forward.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface TenGigE 0/2/0/4.1
RP/0/RP0/CPU0:router(config-subif)# dot1q vlan 10
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface TenGigE 0/2/0/4.1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface TenGigE 0/2/0/4.1 l2transport
RP/0/RP0/CPU0:router(config-subif)# dot1q vlan 10 any
```

Related Commands

Command	Description
show interfaces, on page 469	Displays statistics for all interfaces configured on the router or for a specific node.
show vlan interface, on page 915	Displays summarized information about VLAN subinterfaces.
show vlan tags, on page 917	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**]

Syntax Description

type	Type of Ethernet interface on which you want to create a VLAN. Enter **GigabitEthernet**, **TenGigE**,, 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 3.0	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 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/RP0/CPU0:router(config)# interface TenGigE 0/0/0/1.2
RP/0/RP0/CPU0:router(config-subif)# dot1q vlan 1
RP/0/RP0/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/RP0/CPU0:router(config)# interface GigabitEthernet 0/4/0/1.1
RP/0/RP0/CPU0:router(config-if-l2)#
```

Related Commands

Command	Description
dot1q vlan, on page 911	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 .

Note Effective with Cisco IOS XR Release 5.1.1, the**show vlan interface** command is replaced by the **show ethernet tags** command.

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**, 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 3.0	This command was introduced.
Release 5.1.1	This command was replaced with **show ethernet tags** command.

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 90: 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 469	Displays statistics for all interfaces configured on the router or for a specific node.
show vlan trunks, on page 919	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**, **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 3.0	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 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/RP0/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 91: 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 911	Assigns a VLAN ID to a subinterface (or modifies the VLAN ID that is currently assigned to a subinterface).
show vlan interface, on page 915	Displays summarized information about VLAN subinterfaces.
show vlan trunks, on page 919	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** , 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 3.0	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 **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/RP0/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 92: 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.
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.

Field	Description
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 469	Displays statistics for all interfaces configured on the router or for a specific node.
interface (VLAN), on page 913	Creates a VLAN subinterface.

10-Gigabit Ethernet WAN PHY Controller Commands

This module describes the commands to configure a 10-Gigabit Ethernet WAN PHY physical controller on the Cisco CRS Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

For information on 10-Gigabit Ethernet (GE) interface commands see the *Ethernet Interface Commandson* module.

clear controller wanphy

To clear the alarms counters for a specific 10-Gigabit Ethernet WAN PHY controller, use the **clear controller wanphy** command in EXEC mode.

clear controller wanphy interface-id stats

Syntax Description

interface-id	Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. • *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. Shared port adapters (SPAs) are referenced by their subslot number. • *port*: Physical port number of the interface. For more information about the syntax for the router, use the question mark (?) online help function.
stats	Clears alarm counters for the specified 10-Gigabit Ethernet WAN PHY controller.

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
interface	read, write, execute

Examples

This example shows how to configure a 10-Gigabit Ethernet WAN PHY controller in Slot 6:

```
RP/0/RP0/CPU0:router # clear controller wanphy 0/6/0/0 stats
```

Related Commands

Command	Description
show controllers wanphy, on page 932	Displays alarms, registers, and module information for a 10-Gigabit Ethernet WAN PHY controller.

clear counters wanphy

To clear the alarms counters for a specific 10-Gigabit Ethernet WAN PHY interface, use the **clear counters wanphy** command in EXEC mode.

clear counters wanphy interface-id stats

Syntax Description

interface-id	Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. • *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. Shared port adapters (SPAs) are referenced by their subslot number. • *port*: Physical port number of the interface. For more information about the syntax for the router, use the question mark (?) online help function.
stats	Clears alarm counters for the specified 10-Gigabit Ethernet WAN interface.

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
interface	read, write, execute

Examples

This example shows how to clear the alarms counters for a 10-Gigabit Ethernet WAN interface:

```
RP/0/RP0/CPU0:router # clear counters wanphy 0/6/0/0 stats
```

Related Commands

Command	Description
show controllers wanphy, on page 932	Displays alarms, registers, and module information for a 10-Gigabit Ethernet WAN PHY controller.
clear controller wanphy, on page 924	Clears the alarms counters for a specific 10-Gigabit Ethernet WAN PHY controller.

controller wanphy

To enter WAN physical controller configuration mode in which you can configure a 10-Gigabit Ethernet WAN PHY controller, use the **controller wanphy** command in Global Configuration mode . To return the 10-Gigabit Ethernet WAN PHY controller to its default WAN mode configuration, use the **no** form of this command.

controller wanphy interface-id

Syntax Description

interface-id Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation.

- *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. Shared port adapters (SPAs) are referenced by their subslot number.
- *port*: Physical port number of the interface.

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 3.5.0	This command was introduced.

Usage Guidelines

Note After you use the **no controller wanphy** command to return a 10-Gigabit Ethernet WAN PHY controller to its default configuration, you need to cycle the power to the 10-Gigabit Ethernet SPA for the mode configuration changes to take effect.

Task ID

Task ID	Operations
interface	read, write

Examples

This example shows how to enter WAN PHY controller configuration mode:

```
RP/0/RP0/CPU0:router # configure
RP/0/RP0/CPU0:router(config)# controller wanphy 0/6/0/0
RP/0/RP0/CPU0:router(config-wanphy)#
```

The following example shows how to configure a 10-Gigabit Ethernet WAN PHY controller in slot 6 to run in LAN mode:

```
RP/0/RP0/CPU0:router # configure
RP/0/RP0/CPU0:router(config)# controller wanphy 0/6/0/0
RP/0/RP0/CPU0:router(config-wanphy)# lanmode on
RP/0/RP0/CPU0:router(config-wanphy)# commit
RP/0/RP0/CPU0:router(config-wanphy)# exit
RP/0/RP0/CPU0:router(config)# exit
RP/0/RP0/CPU0:router(config)# hw-module subslot 0/6/0 shutdown unpowered
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router(config)# no hw-module subslot 0/6/0 shutdown unpowered
```

The following example shows how to return a 10-Gigabit Ethernet WAN PHY controller in slot 6 to run in its default WAN mode:

```
RP/0/RP0/CPU0:Router # configure
RP/0/RP0/CPU0:Router(config)# no controller wanphy 0/6/0/0
RP/0/RP0/CPU0:Router(config)# commit
RP/0/RP0/CPU0:Router(config)# exit
RP/0/RP0/CPU0:router(config)# hw-module subslot 0/6/0 shutdown unpowered
RP/0/RP0/CPU0:Router(config)# commit
RP/0/RP0/CPU0:router(config)# no hw-module subslot 0/6/0 shutdown unpowered
```

Related Commands

Command	Description
lanmode on, on page 928	Configures a 10-Gigabit Ethernet WAN PHY controller to run in LAN mode for a 1-Port 10-Gigabit Ethernet LAN/WAN-PHY SPA.
show controllers wanphy, on page 932	Displays alarms, registers, and module information for a 10-Gigabit Ethernet WAN PHY controller.

lanmode on

To configure a 10-Gigabit Ethernet WAN PHY controller to run in LAN mode for a 1-Port 10-Gigabit Ethernet LAN/WAN-PHY SPA, use the **lanmode on** command in WAN physical controller configuration mode. To return the controller to the default, use the **no** form of this command.

Note This command is not supported on 10-Gigabit Ethernet Line Cards and MPAs. It is supported with WAN PHY SPA.

lanmode on

Syntax Description

This command has no keywords or arguments.

Command Default

The 10-Gigabit Ethernet WAN PHY controller default varies depending on the installed line card:

- For the 1-Port 10-Gigabit Ethernet LAN/WAN-PHY SPA, the default mode is WAN mode.
- For the 4-Port, 8-Port, 14-Port, and 20-Port 10-Gigabit Ethernet LAN/WAN-PHY PLIMs, the default mode is LAN mode.
- For the 1-Port, 2-Port 100-Gigabit Ethernet LAN/WAN-PHY SPA, the default mode is LAN mode.

Command Modes

WAN physical controller configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
interface	read, write

Examples

This example shows how to enable LAN mode on a 10-Gigabit Ethernet WAN PHY controller:

```
RP/0/RP0/CPU0:router:Router # configure
RP/0/RP0/CPU0:router:Router(config)# controller wanphy 0/6/0/0
RP/0/RP0/CPU0:router:Router(config-wanphy)# lanmode on

To complete the mode change the SPA must be power-cycled.
```

This example shows how to disable LAN mode on a 10-Gigabit Ethernet WAN PHY controller and return that controller to the default WAN mode:

```
RP/0/RP0/CPU0:router:Router # configure
RP/0/RP0/CPU0:router:Router(config)# controller wanphy 0/6/0/0
```

```
RP/0/RP0/CPU0:router:srt-crs1(config-wanphy)# no lanmode on

To complete the mode change the SPA must be power-cycled.
```

Related Commands

Command	Description
show controllers wanphy, on page 932	Displays alarms, registers, and module information for a 10-Gigabit Ethernet WAN PHY controller.

report sd-ber

To enable Signal Degrade (SD) Bit Error Rate (BER) reporting, use the **report sd-ber** command in wanphy configuration mode. To disable Signal Degrade (SD) Bit Error Rate (BER) reporting, use the **no** form of this command.

report sd-ber

Syntax Description

This command has no keywords or arguments.

Command Default

Signal Degrade (SD) Bit Error Rate (BER) reporting is disabled by default.

Command Modes

Wanphy configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
interface	read, write

Examples

This example shows how to enable Signal Degrade (SD) Bit Error Rate (BER) reporting.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# controller wanphy 0/6/1/0
RP/0/RP0/CPU0:router(config-wanphy)# report sd-ber
RP/0/RP0/CPU0:router(config-wanphy)#
```

Related Commands

Command	Description
report sf-ber disable, on page 931	Disables SF BER reporting.
show controllers wanphy, on page 932	Displays alarms, registers, and module information for a 10-Gigabit Ethernet WAN PHY controller.
threshold sf-ber, on page 939	Configures the threshold of the SF BER that is used to trigger a link state change.

report sf-ber disable

To disable Signal Failure (SF) Bit Error Rate (BER) reporting, use the **report sf-ber disable** command in wanphy configuration mode. To enable Signal Failure (SF) Bit Error Rate (BER) reporting, use the no form of this command. In the case of A9K-8X100GE-SE line cards, the commands **report sf-ber** and **no report sf-ber** are used to enable and disable SF BER respectively.

report sf-ber disable

Syntax Description

This command has no keywords or arguments.

Command Default

Signal Failure (SF) Bit Error Rate (BER) reporting is enabled by default.

Command Modes

Wanphy configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
interface	read, write

Examples

This example shows how to disable Signal Failure (SF) Bit Error Rate (BER) reporting.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# controller wanphy 0/6/1/0
RP/0/RP0/CPU0:router(config-wanphy)# report sf-ber disable
RP/0/RP0/CPU0:router(config-wanphy)#
```

Related Commands

Command	Description
report sd-ber, on page 930	Enables Signal Degrade (SD) Bit Error Rate (BER) reporting.
show controllers wanphy, on page 932	Displays alarms, registers, and module information for a 10-Gigabit Ethernet WAN PHY controller.
threshold sf-ber, on page 939	Configures the threshold of the SF BER that is used to trigger a link state change.

show controllers wanphy

To display alarms, registers, and module information for a 10-Gigabit Ethernet WAN PHY controller, use the **show controllers wanphy** command in EXEC mode.

show controller wanphy *interface-id* [**alarms** | **all** | **registers**]

Syntax Description

interface-id	Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. • *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. Shared port adapters (SPAs) are referenced by their subslot number. • *port*: Physical port number of the interface. For more information about the syntax for the router, use the question mark (?) online help function.
alarms	Displays information about any alarms that are detected by the specified 10-Gigabit Ethernet WAN PHY controller.
all	Displays registers, alarms, and module information for the specified 10-Gigabit Ethernet WAN PHY controller.
registers	Displays registers for the specified 10-Gigabit Ethernet WAN PHY controller.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
interface	read

Examples

This example shows sample output from the **show controllers wanphy** command with the **all** keyword:

```
RP/0/RP0/CPU0:router# show controllers wanphy 0/3/4/0 all

Interface: wanphy0_3_4_0
Configuration Mode: WAN Mode
SECTION
```

```
  LOF = 1, LOS = 1, BIP(B1) = 2912
LINE
  AIS = 1, RDI = 0, FEBE = 949, BIP(B2) = 48562
PATH
  AIS = 1, RDI = 0, FEBE = 0, BIP(B2) = 0
  LOP = 0, NEWPTR = 0, PSE = 0, NSE = 0
WIS ALARMS
  SER = 9, FEPLMP = 0, FEAISP = 0
  WLOS = 1, PLCD = 0
  LFEBIP = 47260, PBEC = 949

Active Alarms[All defects]: lof,
Active Alarms[Highest Alarms]: lof
  Rx(K1/K2): N/A, Tx(K1/K2): N/A
  S1S0 = N/A, C2 = N/A
PATH TRACE BUFFER
Remote IP addr: 000.000.000.000
BER thresholds: N/A
TCA thresholds: N/A

REGISTERS
P_FEBE  : 949
L_FE_BIP: 47260
L_BIP   : 48562
P_BEC   : 949
S_BIP   : 2912
J1-Rx0  : 0x3136
J1-Rx1  : 0x352e
J1-Rx2  : 0x3234
J1-Rx3  : 0x332e
J1-Rx4  : 0x3132
J1-Rx5  : 0x3900
J1-Rx6  : 0x3138
J1-Rx7  : 0x372e
Internal Information
Operational Mode  : WAN Mode
Curent Alarms: 0x8
```

Table 93: show controllers wanphy Command Output Fields

Field	Description
Interface	Identifies the WAN physical interface, in the format *rack/slot/module/port*. • *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. Shared port adapters (SPAs) are referenced by their subslot number. • *port*: Physical port number of the interface.
Configuration Mode	Current configuration mode running on this controller. Can be WAN mode or LAN mode.

Field	Description
SECTION	Displays the following section alarms: • LOF—Number of Loss of Framing (LOF) errors on this connection section. LOF alarms are critical because they indicate that the link associated with this section is down. • LOS—Number of loss of signal (LOS) errors on this connection section. LOS alarms are critical because they indicate that the link associated with this section is down. • BIP(B1)—Number of bit interleaved parity (BIP) B1 errors on this section that exceeded the specified threshold.

LINE	Displays the following line alarms:
	• AIS—Number of AIS errors on this line. AIS alarms are critical because they indicate that the line is down.
	• 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—Number of far-end block errors (FEBE) on this line. Line FEBE errors are accumulated from the M0 or M1 byte, and are reported when the downstream LTE detects BIP7 (B2) errors.
	• BIP(B2)—Number of bit interleaved parity (BIP) B2 errors on this line that exceeded the specified threshold.

PATH	Displays the following path alarms: • AIS—Number of AIS errors on this path. AIS alarms are critical because they indicate that the line associated with this path is down. • RDI—Number of RDI errors on this path. Path RDI is a legacy alarm and is not supported. • FEBE—Number of FEBE errors on this path. Path FEBEs are accumulated from the G1 byte, and are reported when the downstream PTE detects BIP (B3) errors. • BIP(B2)—Number of bit interleaved parity (BIP) errors on this path that exceeded the specified threshold. • LOP—Number of loss of pointer (LOP) errors on this path. Path LOPs are reported as a result of an invalid pointer (H1, H2) or an excess number of new data flag 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 (PSE) 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). **Note** For Cisco IOS XR software release 3.5.0, the following fields display no errors:RDIFEBEBIP(B2)NEWPTRPSENSE

Field	Description
WIS ALARMS	Displays the following WAN Interconnect Sublayer (WIS) layer alarms: • SER—Number of Severely Errored Frames (SER) errors • FELCDP—Number of Far End - Loss of Code-group Delineation - Path (FELCDP) errors • FEAISP—Number of Far End - AIS - Path (FEAISP) errors • WLOS—Number of WIS LOS (WLOS) errors. • PLCD—Number of Path Loss of Code-group Delineation (PLCD) errors • LFEBIP—Number of Line - Far End - BIP (LFEBI) errors • PBEC—Number of Path - Block Error Counter (PBEC) errors **Note** Alarms are applicable only when the controller is configured in WAN-PHY mode.
Active Alarms[All defects]	Total number of currently active alarms on this interface. **Note** Alarms are applicable only when the controller is configured in WAN-PHY mode.
Active Alarms[Highest Alarms]	Total number of the most significant active alarms on this interface. These alarms are likely causing all other alarms on the interface. **Note** Alarms are applicable only when the controller is configured in WAN-PHY mode.
Rx(K1/K2)	Total number of errored K1/K2 bytes from the Line OverHead (LOH) of the SONET frame that were received by this interface.
Tx(K1/K2)	Total number of errored K1/K2 bytes from the Line OverHead (LOH) of the SONET frame that were transmitted by this interface.
S1S0	Number of errored payload pointer bytes on this interface.
C2	Number of errored STS identifier (C1) bytes on this interface.
PATH TRACE BUFFER	Rx J1 trace buffer received from the far end. If the received data is valid it will be shown below the PATH TRACE BUFFER field.
Remote IP addr	Byte string containing the IP address of the remote end of this connection. If the received data is invalid, this field displays no IP address.
BER thresholds	BER threshold values of the specified alarms for a the 10-Gigabit Ethernet controller.
TCA thresholds	TCA threshold values of the specified alarms for a the 10-Gigabit Ethernet controller.

Field	Description
REGISTERS	Displays output from the following registers in hexadecimal format: • P_FEBE—Total number of Far End Block Errors (FEBEs) that occurred on the path that is associated with this interface. • L_FE_BIP—Total number of far end BIP errors that occurred on this interface. • L_BIP—Total number of local BIP errors that occurred on this interface. • P_BEC—Total BIP error count (BEC) that occurred on the path that is associated with this interface. • S_BIP—Total number of far end BIP errors that occurred on the current section. • J1-Rx0—Characters from far end IPV4 address string. • J1-Rx1—Characters from far end IPV4 address string. • J1-Rx2—Characters from far end IPV4 address string. • J1-Rx3—Characters from far end IPV4 address string. • J1-Rx4—Characters from far end IPV4 address string. • J1-Rx5—Characters from far end IPV4 address string. • J1-Rx6—Characters from far end IPV4 address string. • J1-Rx7—Characters from far end IPV4 address string. **Note** The following Serdes-WIS HW registers are used to debug counters and can be cleared only by power cycling the hardware:P_FEBEL_FE_BIPL_BIPP_BECS_BIPThe J1-Rx registers (J1-Rx0 through J1-Rx7) comprise the raw 16 bytes of data received from the Rx J1 Path Trace Buffer, and are used to debug IPV4 address sent from far end.
Internal Information	Displays the following internal information for the interface: • Operational Mode—Current operation mode for this controller. Can be WAN mode or LAN mode. Use the Operational Mode field to detect whether the hardware was power cycled after a mode configuration change. If the Operational Mode field shows output that is different from the Configuration Mode field, then the hardware was not power cycled properly after a mode configuration change. • Current Alarms—Bit map of all currently active alarms on this controller. Use this information for debugging purposes. **Note** Alarms are applicable only when the controller is configured in WAN-PHY mode.

The following example shows sample output from the **show controllers wanphy** command with the **alarms** keyword:

```
RP/0/RP0/CPU0:router# show controllers wanphy 0/3/4/0 alarms

Interface: wanphy0_3_4_0
Configuration Mode: WAN Mode
SECTION
  LOF = 1, LOS = 1, BIP(B1) = 2912
LINE
  AIS = 1, RDI = 0, FEBE = 949, BIP(B2) = 48562
```

```
PATH
  AIS = 1, RDI = 0, FEBE = 0, BIP(B2) = 0
  LOP = 0, NEWPTR = 0, PSE = 0, NSE = 0
WIS ALARMS
  SER = 9, FELCDP = 0, FEAISP = 0
  WLOS = 1, PLCD = 0
  LFEBIP = 47260, PBEC = 949

Active Alarms[All defects]:
Active Alarms[Highest Alarms]:
  Rx(K1/K2): N/A, Tx(K1/K2): N/A
  S1S0 = N/A, C2 = N/A
PATH TRACE BUFFER
Remote IP addr: 981.761.542.321
BER thresholds: N/A
TCA thresholds: N/A
```

The alarm information displayed in the **show controllers wanphy** *interface-id* **alarms** command output are described in Table 93: show controllers wanphy Command Output Fields, on page 933.

This example shows sample output from the **show controllers wanphy** command with the **registers** keyword:

```
RP/0/RP0/CPU0:router# show controllers wanphy 0/3/4/0 registers
Interface: wanphy0_3_4_0

Configuration Mode: WAN Mode
REGISTERS
P_FEBE  : 949
L_FE_BIP: 47260
L_BIP   : 48562
P_BEC   : 949
S_BIP   : 2912
J1-Rx0  : 0x3136
J1-Rx1  : 0x352e
J1-Rx2  : 0x3234
J1-Rx3  : 0x332e
J1-Rx4  : 0x3132
J1-Rx5  : 0x3900
J1-Rx6  : 0x3138
J1-Rx7  : 0x372e
Internal Information
Operational Mode  : WAN Mode
Curent Alarms: 0x0
```

The registers displayed in the **show controllers wanphy** *interface-id* **registers** command output are described in Table 93: show controllers wanphy Command Output Fields, on page 933.

Related Commands

Command	Description
clear controller wanphy, on page 924	Clears the alarms counters for a specific 10-Gigabit Ethernet WAN PHY controller.
lanmode on, on page 928	Configures a 10-Gigabit Ethernet WAN PHY controller to run in LAN mode for a 1-Port 10-Gigabit Ethernet LAN/WAN-PHY SPA.

threshold sd-ber

To configure the threshold of the Signal Degrade (SD) Bit Error Rate (BER) that is used to trigger a signal degrade alarm, use the **threshold sd-ber** command in wanphy configuration mode. To return the Signal Degrade (SD) Bit Error Rate (BER) to the default value, use the **no** form of this command.

threshold sd-ber *exponent*

Syntax Description

exponent	Value of 10 raised to the *n* power, where *n* is the exponent of 10, as in10-n. Valid values are 3 to 9, meaning 10-3 to 10-9.

Command Default

The default is 6, meaning (10-6).

Command Modes

Wanphy configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
interface	read, write

Examples

This example shows how to configure sd-ber threshold:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# controller wanphy 0/6/1/0
RP/0/RP0/CPU0:router(config-wanphy)# threshold sd-ber 9
RP/0/RP0/CPU0:router(config-wanphy)#
```

Related Commands

Command	Description
report sd-ber, on page 930	Enables Signal Degrade (SD) Bit Error Rate (BER) reporting.
report sf-ber disable, on page 931	Disables SF BER reporting.
threshold sf-ber, on page 939	Configures the threshold of the SF BER that is used to trigger a link state change.

threshold sf-ber

To configure the threshold of the Signal Failure (SF) Bit Error Rate (BER) that is used to trigger a link state change, use the **threshold sf-ber** command in wanphy configuration mode. To return the Signal Failure (SF) Bit Error Rate (BER) to the default value, use the **no** form of this command.

threshold sf-ber *exponenet*

Syntax Description

exponent	Value of 10 raised to the *n* power, where *n* is the exponent of 10, as in10-n. Valid values are 3 to 9, meaning 10-3 to 10-9.

Command Default

The default is 3, meaning (10-3).

Command Modes

Wanphy configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
interface	read, write

Examples

This example shows how to configure the threshold of the Signal Failure (SF) Bit Error Rate (BER):

```
RP/0/RP0/CPU0:router # configure
RP/0/RP0/CPU0:router(config)# controller wanphy 0/6/1/0
RP/0/RP0/CPU0:router(config-wanphy)# threshold sf-ber 9
RP/0/RP0/CPU0:router(config-wanphy)#
```

Related Commands

Command	Description
report sd-ber, on page 930	Enables Signal Degrade (SD) Bit Error Rate (BER) reporting.
report sf-ber disable, on page 931	Disables SF BER reporting.
show controllers wanphy, on page 932	Displays alarms, registers, and module information for a 10-Gigabit Ethernet WAN PHY controller.

wanmode on

To configure a 10-Gigabit Ethernet WAN PHY controller to run in WAN mode for the 10-Gigabit Ethernet LAN/WAN-PHY physical layer interface modules (PLIMs), use the **wanmode on** command in WAN physical controller configuration mode. To return the controller to the default, use the **no** form of this command.

wanmode on

Syntax Description

This command has no keywords or arguments.

Command Default

The 10-Gigabit Ethernet WAN PHY controller default varies depending on the installed line card:

- For the 1-Port 10-Gigabit Ethernet LAN/WAN-PHY SPA, the default mode is WAN mode. This command does not apply.
- For the 4-Port, 8-Port, 14-Port, and 20-Port 10-Gigabit Ethernet LAN/WAN-PHY PLIMs, the default mode is LAN mode.

Command Modes

WAN physical controller configuration

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

Use the **wanmode on** command to change from the default LAN mode state for all 10-Gigabit Ethernet LAN/WAN-PHY physical layer interface modules (PLIMs).

Note This command does not apply to the 1-Port 10-Gigabit Ethernet LAN/WAN-PHY SPA because the default state is WAN mode. Use the **lanmode on** and **no lanmode on** commands to change modes for that SPA.

Task ID

Task ID	Operations
interface	read, write

Examples

This example shows how to enable WAN mode on a 10-Gigabit Ethernet WAN PHY controller for a 10-Gigabit Ethernet LAN/WAN-PHY PLIM:

```
RP/0/RP0/CPU0:Router # configure
RP/0/RP0/CPU0:Router(config)# controller wanphy 0/6/0/0
RP/0/RP0/CPU0:Router(config-wanphy)# wanmode on
```

This example shows how to disable WAN mode on a 10-Gigabit Ethernet WAN PHY controller and return that controller to the default WAN mode for 10-Gigabit Ethernet LAN/WAN-PHY PLIMs:

```
RP/0/RP0/CPU0:Router # configure
```

```
RP/0/RP0/CPU0:Router(config)# controller wanphy 0/6/0/0
RP/0/RP0/CPU0:srt-crs1(config-wanphy)# no wanmode on
```

Related Commands

Command	Description
show controllers wanphy, on page 932	Displays alarms, registers, and module information for a 10-Gigabit Ethernet WAN PHY controller.