Interface and Hardware Component Command Reference for the Cisco NCS 6000 Series Routers

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

Text Part Number: OL-30975-02

Preface

This command reference describes the Cisco IOS XR Interfaces commands. The preface for the *Interface and Hardware Component Command Reference for Cisco NCS 6000 Series Routers* contains the following sections:

Changes to this Document

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

Table 1: Changes to this Document

Revision	Date	Change Summary
OL-30975-02	January 2014	Republished with documentation updates for Cisco IOS XR Release 5.0.1 features.
OL-30975-01	November 2013	Initial Release of this document.

Obtaining Documentation and Submitting a Service Request

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

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

Ethernet Interface Commands

This module provides command line interface (CLI) commands for configuring Ethernet interfaces on the Cisco NCS 6000 Series Router.

carrier-delay

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

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

Syntax Description

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

Command Default

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

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 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 98	Turns on event dampening.

clear mac-accounting (Ethernet)

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

clear mac-accounting {**GigabitEthernet**| **TenGigE**} *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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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, 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 12	Generates accounting information for IP traffic based on the source and destination MAC addresses on LAN interfaces.
show mac-accounting (Ethernet), on page 20	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**}

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

Syntax Description

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

Command Default

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

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

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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.

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

Note The **flow-control** command is supported on Gigabit Ethernet, TenGigE 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 107	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 XR Configmode.

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

no 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

XR config

Command History

Release	Modification
Release 5.0.0	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.

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

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

Task ID

Task ID	Operation
interface	read, write

Examples

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

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

Related Commands

Command	Description
show interfaces, on page 107	Displays statistics for all interfaces configured on the router or for a specific node.

loopback (Ethernet)

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

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

no loopback

Syntax Description

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

Command Default

Loopback mode is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 **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**}

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

Syntax Description

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

Command Default

MAC accounting is disabled

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 **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:router#configure
RP/0/RP0/CPU0:router#interface bundle-ether <bundle-id>
```

```
RP/0/RP0/CPU0:router(config-if)# mac-accounting ingress
```

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 4	Clears MAC accounting statistics for an interface.
show mac-accounting (Ethernet), on page 20	Displays MAC accounting statistics for an interface.

mac-address (Ethernet)

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

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

no mac-address

Syntax Description

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

Command Default

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

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 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

The following example shows how to set the MAC address of a Gigabit Ethernet interface located at 0/1/5/0:

```
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 0/1/5/0
```

```
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

no negotiation auto

Syntax Description

This command has no keywords or arguments.

Command Default

Link autonegotiation is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 **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

no packet-gap non-standard

Syntax Description

This command has no keywords or arguments.

Command Default

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

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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.

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 XR EXEC mode.

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

Syntax Description

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

Command Default

No default behavior or values

Command Modes

XR EXEC

Command History

Release	Modification
Release 5.0.0	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.

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

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

Task ID

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

show mac-accounting (Ethernet)

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

show mac-accounting {**GigabitEthernet| TenGigE| Hundred GigE| bundle-ether**| *bundle-id*} *interface-path-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** , .
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

XR EXEC

Command History

Release	Modification
Release 5.0.1	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.

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


RP/0/RP0/CPU0:router# show mac-accounting hundredGigE 0/1/0/0

HundredGigE0/1/0/0
  Input (51 free)
             Total:  0 packets, 0 bytes
```

Table 2: 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 4	Clears MAC accounting statistics for an interface.
mac-accounting, on page 12	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 NCS 6000 Series Router.

action capabilities-conflict

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

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

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

Syntax Description

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

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 5.0.0	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
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 52	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 49	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 71	Attaches an Ethernet OAM profile to an interface.

action critical-event

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

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

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

Syntax Description

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

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 5.0.0	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
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 52	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 49	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 71	Attaches an Ethernet OAM profile to an interface.

action discovery-timeout

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

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

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

Syntax Description

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

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 5.0.0	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
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 52	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 49	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 71	Attaches an Ethernet OAM profile to an interface.

action dying-gasp

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

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

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

Syntax Description

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

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 5.0.0	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
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 52	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 49	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 71	Attaches an Ethernet OAM profile to an interface.

action high-threshold

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 5.0.0	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
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 52	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 49	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 71	Attaches an Ethernet OAM profile to an interface.

action remote-loopback

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

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

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

Syntax Description

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

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 5.0.0	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
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 52	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 49	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 71	Attaches an Ethernet OAM profile to an interface.

action session-down

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

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

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

Syntax Description

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

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 5.0.0	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
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 52	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 49	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 71	Attaches an Ethernet OAM profile to an interface.

action session-up

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

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

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

Syntax Description

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

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 5.0.0	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
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 52	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 49	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 71	Attaches an Ethernet OAM profile to an interface.

action uni-directional link-fault

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

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

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

Syntax Description

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

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 5.0.0	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.

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 52	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 49	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 71	Attaches an Ethernet OAM profile to an interface.

action wiring-conflict

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 5.0.0	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
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 52	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 49	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 71	Attaches an Ethernet OAM profile to an interface.

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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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
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 86	Displays the local and remote Ethernet OAM statistics for interfaces.
show ethernet oam interfaces, on page 83	

connection timeout

To configure the timeout value for an Ethernet OAM session, use the **connection timeout** command in Ethernet OAM configuration mode.

connection timeout *seconds*

Syntax Description

seconds	Connection timeout period in seconds. The range is 2 to 30.

Command Default

The default value is 5.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 5.0.0	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.

If no packets are received from the OAM peer in the specified time, the OAM session is brought down, and the negotiation phase starts again.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the connection timeout value of an Ethernet OAM session:

```
RP/0/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 29	Configures what action is taken on an interface when a connection timeout occurs.
ethernet oam, on page 49	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
ethernet oam profile, on page 52	Creates an EOAM profile and enters EOAM configuration mode.
show ethernet oam configuration, on page 77	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam discovery, on page 80	Displays the currently configured OAM information of Ethernet OAM sessions on interfaces.
show ethernet oam interfaces, on page 83	

ethernet oam

To enable Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode, use the **ethernet oam** command in interface configuration mode. To disable Ethernet Link OAM, use the **no** form of this command.

ethernet oam

no ethernet oam

Syntax Description

This command has no keywords or arguments.

Command Default

When enabled on an interface, the Ethernet Link OAM default values apply.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 5.0.0	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 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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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.

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
remote-loopback	Enables a remote loopback on the far end of an Ethernet OAM interface.
action remote-loopback, on page 35	Configures what action is taken on an interface when a remote-loopback event occurs.
snmp-server traps ethernet oam events, on page 88	
show ethernet oam configuration, on page 77	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 XR Config mode. To delete an EOAM profile, use the **no** form of this command.

ethernet oam profile *profile-name*

no ethernet oam profile *profile-name*

Syntax Description

profile-name	Text string name of the OAM profile. The maximum length is 32 bytes.

Command Default

No default behavior or values

Command Modes

XR config

Command History

Release	Modification
Release 5.0.0	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.

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)#
```

frame-period threshold

To configure the thresholds that trigger an Ethernet OAM frame-period error event, use the **frame-period threshold** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the threshold to the default value, use the **no** form of this command.

frame-period threshold low *threshold* [**high** *threshold*]

no frame-period threshold low *threshold* [**high** *threshold*]

Syntax Description

low *threshold*	Low threshold, in frames, that triggers a frame-period error event. The range is 0 to 1000000.
high *threshold*	(Optional) High threshold, in frames, that triggers a frame-period error event. The range is 0 to 1000000. The high threshold value can be configured only in conjunction with the low threshold value.

Command Default

The default low threshold is 1.

Command Modes

Ethernet OAM link monitor configuration (config-eoam-lm)

Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

Command History

Release	Modification
Release 5.0.0	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 the low threshold is passed, a frame-period error event notification is generated and transmitted to the OAM peer. Additionally, any registered higher level OAM protocols, such as Connectivity Fault Management (CFM), are also notified. When the high threshold is passed, the configured high threshold action is performed in addition to the low threshold actions. The high threshold is optional and is configurable only in conjunction with the low threshold.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the low and high thresholds that trigger a frame-period error event.

```
RP/0/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 low 100 high 600000
```

frame-period window

To configure the window size for an Ethernet OAM frame-period error event, use the **frame-period window** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the window size to the default value, use the **no** form of this command.

frame-period window *window*

no frame-period window *window*

Syntax Description

window	Size of the window for a frame-period error in milliseconds. The range is 100 to 60000.

Command Default

The default value is 1000.

Command Modes

Ethernet OAM link monitor configuration (config-eoam-lm)

Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

Command History

Release	Modification
Release 5.0.0	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
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 60000
```

frame-seconds threshold

To configure the thresholds that trigger a frame-seconds error event, use the **frame-seconds threshold** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the threshold to the default value, use the **no** form of this command.

frame-seconds threshold low *threshold* [**high** *threshold*]

no frame-seconds threshold low *threshold* [**high** *threshold*]

Syntax Description

low *threshold*	Low threshold, in seconds, that triggers a frame-seconds error event. The range is 0 to 900.
high *threshold*	(Optional) High threshold, in seconds, that triggers a frame-seconds error event. The range is 1 to 900. The high threshold value can be configured only in conjunction with the low threshold value.

Command Default

The default value is 1.

Command Modes

Ethernet OAM link monitor configuration (config-eoam-lm)

Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

Command History

Release	Modification
Release 5.0.0	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 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 52	Creates an EOAM profile and enters EOAM configuration mode.
link-monitor, on page 64	Enters Ethernet OAM link monitor configuration mode.

frame-seconds window

To configure the window size for the OAM frame-seconds error event, use the **frame-seconds window** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the window size to the default value, use the **no** form of this command.

frame-seconds window *window*

no frame-seconds window *window*

Syntax Description

window	Size of the window for a frame-seconds error in milliseconds. The range is 10000 to 900000.

Command Default

The default value is 60000.

Command Modes

Ethernet OAM link monitor configuration (config-eoam-lm)

Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

Command History

Release	Modification
Release 5.0.0	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
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)# frame-seconds window 900000
```

Related Commands

Command	Description
ethernet oam profile, on page 52	Creates an EOAM profile and enters EOAM configuration mode.
link-monitor, on page 64	Enters Ethernet OAM link monitor configuration mode.

frame threshold

To configure the thresholds that triggers an Ethernet OAM frame error event, use the **frame threshold** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the threshold to the default value, use the **no** form of this command.

frame threshold low *threshold* [**high** *threshold*]

no frame threshold low *threshold* [**high** *threshold*]

Syntax Description

low *threshold*	Low threshold, in symbols, that triggers a frame error event. The range is 0 to 12000000.
high *threshold*	(Optional) High threshold, in symbols, that triggers a frame error event. The range is 0 range is 0 to 12000000. The high threshold value can be configured only in conjunction with the low threshold value.

Command Default

The default low threshold is 1.

Command Modes

Ethernet OAM link monitor configuration (config-eoam-lm)

Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

Command History

Release	Modification
Release 5.0.0	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 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 52	Creates an EOAM profile and enters EOAM configuration mode.
link-monitor, on page 64	Enters Ethernet OAM link monitor configuration mode.

frame window

To configure the frame window size of an OAM frame error event, use the **frame window** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the window size to the default value, use the **no** form of this command.

frame window *window*

no frame window *window*

Syntax Description

window	Size of the window for a frame error in seconds. The range is 1000 to 60000.

Command Default

The default value is 1000.

Command Modes

Ethernet OAM link monitor configuration (config-eoam-lm)

Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

Command History

Release	Modification
Release 5.0.0	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
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 52	Creates an EOAM profile and enters EOAM configuration mode.
link-monitor, on page 64	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 5.0.0	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
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
```

mib-retrieval

To enable MIB retrieval in an Ethernet OAM profile or on an Ethernet OAM interface, use the **mib-retrieval** command in Ethernet OAM or interface Ethernet OAM configuration mode. To return the interface to the default (disabled), use the **disable** keyword.

mib-retrieval [disable]

Syntax Description

disable	Disables MIB retrieval the Ethernet OAM interface.

Command Default

MIB retrieval is disabled by default.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 5.0.0	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 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 52	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 49	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 71	Attaches an Ethernet OAM profile to an interface.
show ethernet oam configuration, on page 77	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam interfaces, on page 83	

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 5.0.0	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.

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 52	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 49	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 71	Attaches an Ethernet OAM profile to an interface.
show ethernet oam configuration, on page 77	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam interfaces, on page 83	

monitoring

To enable Ethernet OAM link monitoring, use the **monitoring** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return link monitoring to its default state of enabled, use the **no** form of this command.

monitoring [disable]

no monitoring [disable]

Syntax Description

disable	(Optional) Disables Ethernet OAM link monitoring.
	Note When configuring on a profile, only the **monitoring disable** form of the command is supported.

Command Default

Link monitoring is enabled by default.

Command Modes

Ethernet OAM link monitor configuration (config-eoam-lm)

Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

Command History

Release	Modification
Release 5.0.0	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.

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
```

Related Commands

Command	Description
ethernet oam profile, on page 52	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 49	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
link-monitor, on page 64	Enters Ethernet OAM link monitor configuration mode.
profile (EOAM), on page 71	Attaches an Ethernet OAM profile to an interface.
show ethernet oam configuration, on page 77	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam statistics, on page 86	Displays the local and remote Ethernet OAM statistics for interfaces.
show ethernet oam interfaces, on page 83	

profile (EOAM)

To attach an Ethernet OAM profile to an interface, use the **profile** command in interface Ethernet OAM configuration mode. To remove the profile from the interface, use the no form of this command.

profile *name*

no profile *name*

Syntax Description

name	Text name of the Ethernet OAM profile to attach to the interface.

Command Default

No profile is attached.

Command Modes

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 5.0.0	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 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 52	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 49	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
show ethernet oam configuration, on page 77	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam interfaces, on page 83	

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]**}

no 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 behavior or values

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 5.0.0	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 **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 52	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam, on page 49	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM), on page 71	Attaches an Ethernet OAM profile to an interface.
action capabilities-conflict, on page 25	Configures what action is taken on an interface when a capabilities-conflict event occurs.
show ethernet oam configuration, on page 77	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam discovery, on page 80	Displays the currently configured OAM information of Ethernet OAM sessions on interfaces.
show ethernet oam interfaces, on page 83	

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 XR 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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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.

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
```

Related Commands

Command	Description
efd	Enables EFD on all down MEPs in a down MEPs service.
log efd	Enables logging of EFD state changes to an interface (such as when an interface is shut down or brought up via EFD).

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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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.

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 80	Displays the currently configured OAM information of Ethernet OAM sessions on interfaces.
show ethernet oam statistics, on page 86	Displays the local and remote Ethernet OAM statistics for interfaces.
show ethernet oam interfaces, on page 83	

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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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
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 77	Displays the current active Ethernet OAM configuration on an interface.

Command	Description
show ethernet oam statistics, on page 86	Displays the local and remote Ethernet OAM statistics for interfaces.
show ethernet oam interfaces, on page 83	

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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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
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 3: 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.

Field	Description
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 • link-fault • session-down • wiring-conflict

Related Commands

Command	Description
show ethernet oam configuration, on page 77	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam discovery, on page 80	Displays the currently configured OAM information of Ethernet OAM sessions on interfaces.
show ethernet oam statistics, on page 86	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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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
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 77	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam discovery, on page 80	Displays the currently configured OAM information of Ethernet OAM sessions on interfaces.
show ethernet oam interfaces, on page 83	

snmp-server traps ethernet oam events

To enable SNMP traps for Ethernet OAM events, use the **snmp-server traps ethernet oam events** command in XR Config 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

XR config

Command History

Release	Modification
Release 5.0.0	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
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
```

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 t** *hreshold*]

no symbol-period threshold low *threshold* [**high t** *hreshold*]

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.

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 5.0.0	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 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:

```
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 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*

no 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.

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 5.0.0	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
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
```

Global Interface Commands

This module describes the global command line interface (CLI) commands for configuring interfaces on the Cisco NCS 6000 Series Router.

bandwidth (global)

To configure the bandwidth of an interface, use the **bandwidth** command in interface configuration mode.

bandwidth *rate*

Syntax Description

rate	Amount of bandwidth to be allocated on the interface, in Kilobits per second (kbps). Range is from 0 through 4294967295.

Command Default

The default bandwidth depends on the interface type.

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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.

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 Gigabit Ethernet interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router# interface GigabitEthernet 0/4/1/0
```

```
RP/0/RP0/CPU0:router# bandwidth 4000000
```

Related Commands

Command	Description
interface (global)	Configures an interface or creates or configures a virtual interface.
shutdown (global), on page 118	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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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.

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:
- 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
interface (global)	Configures an interface or creates or configures a virtual interface.
shutdown (global), on page 118	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*]]

no dampening [*half-life* [*reuse suppress max-suppress-time*]]

Syntax Description

half-life	(Optional) Time (in minutes) after which a penalty is decreased. Once the interface has been assigned a penalty, the penalty is decreased by half after the half-life period. The process of reducing the penalty happens every 5 seconds. The range of the half-life period is 1 to 45 minutes. The default is 1 minute.
reuse	(Optional) Penalty value below which a stable interface is unsuppressed. Range is from 1 through 20000. Default value is 750.
suppress	(Optional) Limit at which an interface is suppressed when its penalty exceeds that limit. Range is from 1 through 20000, and must be greater than the reuse threshold. The default value is 2000.
max-suppress-time	(Optional) Maximum time (in minutes) that an interface can be suppressed. This value effectively acts as a ceiling that the penalty value cannot exceed. Default value is four times the half-life period.

Command Default

Dampening is turned off by default. When you use the **dampening** command, the following default values are enabled for any optional parameters that you do not enter:

- *half-life*: 1 minute
- *reuse*: 750
- *suppress*: 2000
- *max-suppress-time*: Four times the half-life

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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.

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 POS 0/4/0/0
RP/0/RP0/CPU0:router(config-if))# dampening
```

Related Commands

Command	Description
show im dampening, on page 103	Displays the state of all interfaces on which dampening has been configured.

mtu

To adjust the maximum transmission unit (MTU) value for packets on the interface, use the **mtu** command in interface configuration mode. To return the interface to the default MTU for the interface type, use the **no** form of this command.

mtu *bytes*

no mtu

Syntax Description

bytes	Maximum number of bytes in a Layer 2 frame. Range is from 64 through 65535.

Command Default

The default MTU for each interface is as follows:

- Ethernet—1514 bytes
- POS—4474 bytes
- Tunnel—1500 bytes
- Loopback—1514 bytes
- ATM—4470 bytes

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 **mtu** command to set a specific MTU value for an interface, or use the **no mtu** command to return the interface to the default MTU value for that interface type. The MTU value can be increased or decreased using the **mtu** command, subject to minimum and maximum MTU limits for the interface type.

If the MTU value is not configured, then each interface will have a default MTU value that is specific to the interface type. The default MTU value is generally the largest Layer 2 frame size possible for the interface type.

The default/configured MTU value on an atm interface includes the L2 header.

The MTU size consists of L2 header that includes either SNAP(8bytes)/MUX(0)/NLPID(2) header or the AAL5 SDU. The AAL5 SDU includes the L3 datagram and the optional Logical Link Control/Subnetwork Access Protocol (LLC/SNAP) header.

The Ethernet interface is the Layer 3 datagram plus 14 bytes. For ATM main interface, the MTU is L3 datagram + 0 bytes.

For ATM L3 sub interface, mtu is as follows:

- SNAP - L3 datagram + 8 bytes
- NLPID - L3 datagram + 2 bytes
- MUX - L3datagram + 0 bytes
- When no pvc is configured under sub interface - L3datagram + 0 bytes

Note All serial links in a Multilink Point-to-Point Protocol (MLPPP) bundle or a Multilink Frame Relay (MFR) bundle inherit the default MTU value from the multilink bundle. If a serial interface has a nondefault MTU value, the Cisco IOS XR software blocks that serial interface from being added to an MLPPP or MFR bundle. Therefore, you must not configure the MTU value on a serial interface until you have added that serial interface to an MLPPP or MFR bundle.

You can use the **show interfaces** command to determine if the MTU value has been changed. The **show interfaces** command output displays the MTU size for each interface in the MTU (byte) field.

Note You can use the **show interfaces** command to determine if the MTU value has been changed. The **show interfaces** command output displays the MTU size for each interface in the MTU (byte) field. Note that the MTU size that is displayed includes the Layer 2 header bytes used for each encapsulation type.

Note Changing the MTU on an interface triggers a change on the protocols and capsulations configured on that interface, although some protocol-specific configurations can override the interface MTU. For example, specifically changing the interface MTU configuration does not affect the IP MTU configuration, but may affect the resulting MTU on that node.

Task ID

Task ID	Operations
interface	read, write

Examples

In the following example, the MTU value for all interfaces is verified. The MTU value is shown in the next-to-last column:

```
RP/0/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  4474   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//CPU0/0           up           up               ARPA  1514    100000

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 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//CPU0/0             up           up               ARPA  1514    100000
```

Related Commands

Command	Description
shutdown (global), on page 118	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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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.

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

The following example shows the output from the **show im dampening** command issued with default values:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/4/0/3
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

---------               -----              ----               ----------------
POS0/4/0/3              0                  0                  0       NO

RP/0/RP0/CPU0:router# show im dampening interface POS 0/4/0/3

POS0/4/0/3 (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 POS 0/4/0/3

POS0/4/0/3 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 Packet-over-SONET
  Description: ensoft-gsr5 POS 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 as shown for the POS interface in the previous example.

Table 4: 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 98	Turns on event dampening.
shutdown (global), on page 118	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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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.

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:
- 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.

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.
```

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

          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 5: show interfaces Field Descriptions

Field	Description
Interface name	Displays the name of the current interface. For example, POS0/1/0/1.
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.

Field	Description
line protocol state	Displays the state of the Layer 2 line protocol. This field may be different from the interface state if, for example, a keepalive failure has brought down the Layer 2. **Note** The line protocol state is not the same as the protocol state displayed in the **show ip interfaces** command, because it is the state of Layer 2 (media) rather than Layer 3 (IP protocol).
Hardware	Displays the current hardware type.
Internet address is *n.n.n.n/n*	Displays the Layer 2 address (MAC address for Ethernet interfaces). **Note** Enter the **mac-address** command to configure the hardware address.
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.
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.

Field	Description
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.

Field	Description
ARP type	Address Resolution Protocol (ARP) type used on the interface. This value is not displayed on interface types that do not use ARP.
ARP timeout	ARP timeout in *hours*:*mins*:*secs*. This value is configurable using the **arp timeout** command.
Last clearing of counters	Time since the following counters were last cleared using the **clear counters** exec command in *hours*:*mins*:*secs*.
5 minute input rate	Average number of bits and packets received per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic that it sends and receives (rather than all network traffic). **Note** The 5-minute period referenced in the command output is a load interval that is configurable under the interface. The default value is 5 minutes. **Note** The 5-minute input should be used only as an approximation of traffic per second during a given 5-minute period. This rate is exponentially weighted average with a time constant of 5 minutes. A period of four time constants must pass before the average is within two percent of the instantaneous rate of a uniform stream of traffic over that period.
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.

Field	Description
bytes input	Total number of bytes successfully received on the interface
total input drops	Total number of packets that were dropped after they were received. This includes packets that were dropped due to configured quality of service (QoS) or access control list (ACL) policies. QoS drops include policer drops, WRED drops, and tail drops. This does not include drops due to unknown Layer 3 protocol.
drops for unrecognized upper-level protocol	Total number of packets that could not be delivered because the necessary protocol was not configured on the interface.
Received broadcast packets	Total number of Layer 2 broadcast packets received on the interface. This is a subset of the total input packet count.
Received multicast packets	Total number of Layer 2 multicast packets received on the interface. This is a subset of the total input packet count.
runts	Number of received packets that were too small to be handled. This is a subset of the input errors count.
giants	Number of received packets that were too large to be handled. This is a subset of the input errors count.
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.

Field	Description
ignored	Total number of ignored packet errors. Ignored packets are those that are discarded because the interface hardware does not have enough internal buffers. Broadcast storms and bursts of noise can result in an increased number of ignored packets.
abort	Total number of abort errors on the interface.
packets output	Number of packets received on the interface that were successfully delivered to higher layers.
bytes output	Total number of bytes successfully received on the interface.
total output drops	Number of packets that were dropped before being transmitted. This includes packets that were dropped due to configured quality of service (QoS), (policer drops, WRED drops, and tail drops).
Received broadcast packets	Number of Layer 2 broadcast packets transmitted on the interface. This is a subset of the total input packet count.
Received multicast packets	Total number of Layer 2 multicast packets transmitted on the interface. This is a subset of the total input packet count.
output errors	Number of times that the receiver hardware was unable to handle received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
underruns	Number of underrun errors experienced by the interface. Underruns represent the number of times that the hardware is unable to transmit data to a hardware buffer because the output rate exceeds the transmitter’s ability to handle the data.
applique	Number of applique errors.
resets	Number of times that the hardware has been reset. The triggers and effects of this event are hardware-specifc.
output buffer failures	Number of times that a packet was not output from the output hold queue because of a shortage of MEMD shared memory.

Field	Description
output buffers swapped out	Number of packets stored in main memory when the output queue is full; swapping buffers to main memory prevents packets from being dropped when output is congested. The number is high when traffic is bursty.
carrier transitions	Number of times the carrier detect (CD) signal of a serial interface has changed state.

Related Commands

Command	Description
show controller interface	Displays information that is specific to the interface hardware statistics for all interfaces configured on the networking device.

shutdown (global)

To disable an interface (to force an interface to be administratively down), use the **shutdown** command in interface configuration mode. To enable an interface that has been shut down, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no keywords or arguments.

Command Default

The interface is enabled by default and is disabled only when shutdown is configured.

Note When you add an interface to the system, or when all the configuration for an interface is lost or deleted, the interface is put in the shutdown state by the system adding the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 **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 the following example, POS interface 0/4/0/2 is turned off:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/4/0/2
RP/0/RP0/CPU0:router(config-if)# shutdown
```

Related Commands

Command	Description
show interfaces, on page 107	Displays statistics for all interfaces configured on the router or on a specific node.
show ip interface	Displays IPv4 interface status and configuration.

Link Bundling Commands

This module provides command line interface (CLI) commands for configuring Link Bundle interfaces on the Cisco NCS 6000 Series Router.

bundle-hash

To display the source and destination IP addresses for the member links, distributed by the load balancing feature, in a multilink interface bundle, use the **bundle-hash** command in EXEC mode.

bundle-hash {**Bundle-Ether** *bundle-id*| **members** {**GigabitEthernet**| **TenGigabitEthernet**| **HundredGigabitEthernet**} *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.
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.
HundredGigE	Specified the 100 Gigabit Ethernet interface for which you want to calculate load balancing.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values

Command Modes

XR EXEC

Command History

Release	Modification
Release 5.0.0	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.

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 6: bundle-hash Command Options, on page 123 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 6: bundle-hash Command Options, on page 123.

Table 6: 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
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 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: [ GigabitEthernet | TenGigE ]R/S/I/P
  - bundle interface format:   [ Bundle-Ether]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: [GigabitEthernet | TenGigE ]R/S/I/P
  - bundle interface format:   [ Bundle-Ether ]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
```

Related Commands

Command	Description
show bundle, on page 150	Displays information about configured bundles.

bundle id

To add a port to an aggregated interface (or bundle), enter the **bundle id** command in interface configuration mode.

bundle id *bundle-id* [**mode** {**active**| **on**| **passive**}]

no bundle id *bundle-id*

Syntax Description

bundle-id	Number of the bundle (from 1 to 65535) on which you want to add a port.
mode	(Optional) Specifies the mode of operation, as follows: • **active—**Use the **mode active** keywords to run Link Aggregation Control Protocol (LACP) in active mode over the port. When you specify **active**, the port joins the bundle and is activated if LACP determines that it is compatible. • **on—**Use the **mode on** keywords to configure an Etherchannel link over the port (no LACP running over the port). • **passive—**Use the **mode passive** keywords to run LACP in passive mode over the port. When you specify **passive**, LACP packets are sent only if the other end of the link is using active LACP. The link joins the bundle and is activated if LACP packets are exchanged and the port is compatible.

Command Default

The default setting is **mode on**.

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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.

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 150	Displays information about configured bundles.
show interfaces, on page 107	Displays statistics for all interfaces configured on the router or for a specific node.
show lacp bundle, on page 166	Displays detailed information about LACP ports and their peers.
show lacp port, on page 177	

bundle maximum-active links

To designate one active link and one link in standby mode that can take over immediately for a bundle if the active link fails, use the **bundle maximum-active links** command in interface configuration mode. To return to the default maximum active links value, use the **no** form of this command.

bundle maximum-active links *links* **[hot-standby]**

no bundle maximum-active links *links*

Syntax Description

links	Number of active links you want to bring up in the specified bundle, up to the maximum supported on the platform.
hot-standby	(Optional) Determines how a switchover between active and standby links is implemented. This option is available only on links with LACP enabled. By default, a switchover is implemented per an IEEE standard approach. If you optionally specify the **hot-standby** keyword, a switchover is implemented per a faster proprietary optimization.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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.

By default, multiple links can actively carry traffic for a bundle. However, if one of the links fails, there is no dedicated standby link to take its place. The **bundle maximum-active links** command enables you to implement the optional 1:1 link protection, which means for the specified bundle, you designate one active link and one or more standby links that can take over immediately if the active link fails.

By setting the **bundle maximum-active links** command to 1, the highest-priority link within the bundle becomes active (distributing state) and the remaining links are in standby mode. If a standby link meets one of the following criteria, it is in the collecting state:

- Running Link Aggregation Control Protocol (LACP), and the **hot-standby** option is implemented.
- Not running LACP.

If a standby link does not meet either of these criteria, it is in the waiting state.

The second highest-priority link within the bundle becomes the standby link that takes over immediately if the active link fails. The priority is based on the value from the **bundle port-priority** command, where a lower value is a higher priority. Therefore, you must configure the highest priority (lowest value) for the link that you want to be active and the second-highest priority for the link that you want to act as a backup to the active link.

Note We recommend designating only one backup link to the active link. Although you can designate an additional backup link, maintaining two backup links consumes more bandwidth and offsets any benefits that may be gained.

Note If a link is not running LACP, the configuration of the **bundle maximum-active links** and **bundle port-priority** commands or equivalent commands must be the same on both ends of the link. If a link is running LACP, the configuration of the **bundle maximum-active links** command only must be the same on both ends of the link.

The **hot-standby** option of using an IEEE standard-based switchover (the default) or a faster proprietary optimized switchover is available only for active and standby links running LACP. For links not running LACP, the proprietary optimized switchover option is used.

When using one of the **hot-standby** options on a Cisco IOS XR device, the peer device must have a standby link configured and be one of the following:

- Another Cisco IOS XR device using the same option.
- Another device using an IEEE standard-based switchover. (Cisco does not recommend using this option because unexpected behavior, such as the peer sending traffic on the standby link, can occur.)

Task ID

Task ID	Operations
bundle	read, write

Examples

In the following example, the user implements 1:1 link protection for Ethernet bundle 5 and specifies that the proprietary optimization is used for the LACP-enabled active and standby links:

```
RP/0/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      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 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)#
```

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 134	Sets the number of active links required to bring up a specific bundle.
show bundle, on page 150	Displays information about configured bundles.

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 5.0.0	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
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 150	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 5.0.0	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
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 129	

Command	Description
show bundle, on page 150	Displays information about configured bundles.

bundle port-priority

To configure a port priority for a bundle member link, enter the **bundle port-priority** command in interface configuration mode. To return to the default priority value, use the **no** form of this command.

bundle port-priority *priority*

no bundle port-priority *priority*

Syntax Description

priority	Priority for this port, where a lower value equals a higher priority. Replace the *priority* argument with a number. Range is from 1 through 65535.

Command Default

priority: 32768

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 **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 127	Adds a port to an aggregated interface or bundle.
show lacp bundle, on page 166	Displays detailed information about LACP ports and their peers.
show lacp port, on page 177	
show lacp system-id, on page 180	Displays the local system ID used by the LACP.

clear lacp counters

To clear Link Aggregation Control Protocol (LACP) counters for all members of all bundles, all members of a specific bundle, or for a specific port, enter the **clear lacp counters** command in EXEC mode.

clear lacp counters [**bundle** {**Bundle-Ether** *bundle-id*| **Bundle-POS** *bundle-id*}| **port** {**GigabitEthernet** *interface-path-id*| **TenGigE** *interface-path-id*| **POS** *interface-path-id*}]

Syntax Description

bundle	(Optional) Clears LACP counters for all members of a bundle.
Bundle-Ether *node-id*	(Optional) Ethernet bundle. Use the *node-id* argument to specify the node ID number of the LACP counters you want to clear. Range is 1 through 65535.
Bundle-POS *bundle-id*	(Optional) POS bundle. Use the *bundle-id* argument to specify the bundle ID number of the LACP counters you want to clear. Range is from 1 through 65535.
port	(Optional) Clears all LACP counters on the specified bundle or interface.
GigabitEthernet	(Optional) Gigabit Ethernet interface. Use the *interface-path-id* argument to specify the Gigabit Ethernet interface whose LACP counters you want to clear.
TenGigE	(Optional) Ten Gigabit Ethernet interface. Use the *interface-path-id* argument to specify the Ten Gigabit Ethernet interface whose LACP counters you want to clear.
POS	(Optional) Packet-over-SONET/SDH (POS) interface. Use the *interface-path-id* argument to specify the POS interface whose LACP counters you want to clear.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values

Command Modes

XR EXEC

Command History

Release	Modification
Release 5.0.0	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.

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:
- 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 169	Displays LACP statistics.

interface (bundle)

To create a new bundle and enter interface configuration mode for that bundle, use the **interface (bundle)** command in XR Config mode. To delete a bundle, use the **no** form of this command.

interface {**Bundle-Ether | Bundle-POS** }*bundle-id*

no interface {**Bundle-Ether | Bundle-POS** }*bundle-id*

Syntax Description

Bundle-Ether	Specifies or creates an Ethernet bundle interface.
Bundle-POS	Specifies or creates a POS bundle interface.
bundle-id	Number from 1 to 65535 that identifies a particular bundle.

Command Default

No bundle interface is configured.

Command Modes

XR config

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
bundle	read, write

Examples

This example shows how to create an Ethernet bundle and enter interface configuration mode:

```
RP/0/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 150	Displays information about configured bundles.

lacp packet-capture

To capture LACP packets so that their information can be displayed by the **show lacp packet-capture** command, use the **lacp packet-capture** command in EXEC mode.

{**lacp packet-capture gigabitethernet** *interface-path-id*| **pos interface-path-id** | **tengige** *interface-path-id number-of-packets*}

To stop capturing LACP packets or to clear captured LACP packets, use the **lacp packet-capture stop** or **lacp packet-capture clear** command in EXEC mode.

{**lacp packet-capture** [**bundle-ether** *bundle-id*] [**bundle-pos bundle-id**] [**gigabitethernet** *interface-path-id*] [**pos interface-path-id**] [**tengige** *interface-path-id*] **clear**| **stop**}

Syntax Description

bundle-ether	Ethernet bundle interface specified by *bundle-id*.
bundle-pos	Packet-over-SONET (POS) bundle interface specified by *bundle-id*.
GigabitEthernet	Gigabit Ethernet interface specified by *interface-path-id*.
POS	Packet-over-SONET (POS) interface specified by *interface-path-id*.
TenGigE	Ten Gigabit Ethernet interface specified by *interface-path-id*.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
bundle-id	Number specifying the bundle interface. The range is 1 to 65535.
number-of-packets	Number of packets to capture.
clear	Clears all currently captured packets.
stop	Stops capturing packets.

Command Default

The default (no parameters) executes globally for all interfaces on the line card.

Command Modes

XR EXEC

Command History

Release	Modification
Release 5.0.0	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 **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 171	Displays the LACP transmission information that used by the transmitting device for sending packets on an interface.
show lacp packet-capture, on page 174	Displays the contents of LACP packets that are sent and received on an interface.
lacp period short, on page 145	Enables a short period time interval for the transmission and reception of LACP packets.

lacp period short

To enable a short period time interval for the transmission and reception of Link Aggregation Control Protocol (LACP) packets, use the **lacp period short** command in interface configuration mode. To return to the default short period, use the **no** form of this command.

lacp period short [**receive** *interval*] [**transmit** *interval*]

no lacp period short [**receive** *interval*] [**transmit** *interval*]

Syntax Description

receive *interval*	Time interval (in milliseconds) for receiving LACP packets when LACP short period is enabled. The range is 100 to 1000 and must be multiples of 100, such as 100, 200, 300, and so on.
transmit *interval*	Time interval (in milliseconds) for transmitting LACP packets when LACP short period is enabled. The range is 100 to 1000 and must be multiples of 100, such as 100, 200, 300, and so on.

Command Default

The default is 1000.

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 configure a custom LACP short period *transmit* interval at one end of a link, you must configure the same time period for the *receive* interval at the other end of the link.

Note You must always configure the *transmit* interval at both ends of the connection before you configure the *receive* interval at either end of the connection. Failure to configure the *transmit* interval at both ends first results in route flapping (a route going up and down continuously). When you remove a custom LACP short period, you must do it in reverse order. You must remove the *receive* intervals first and then the *transmit* intervals.

Task ID

Task ID	Operations
bundle	read, write

Examples

The following example shows how to enable a default Link Aggregation Control Protocol (LACP) short period on a Gigabit Ethernet interface:

```
RP/0/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:

```
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
```

```
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
```

```
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
```

```
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
```

```
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
```

```
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 171	Displays the LACP transmission information that used by the transmitting device for sending packets on an interface.

Command	Description
show lacp packet-capture, on page 174	Displays the contents of LACP packets that are sent and received on an interface.
lacp packet-capture, on page 142	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 XR Config mode. To return to the default LACP system priority value, use the **no** form of this command.

lacp system priority *priority*

no lacp system priority *priority*

Syntax Description

s	Priority for this system. Replace *priority* with a number. Range is from 1 through 65535. A lower value is higher priority.

Command Default

priority: 32768

Command Modes

XR config

Command History

Release	Modification
Release 5.0.0	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 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
```

Related Commands

Command	Description
show lacp system-id, on page 180	Displays the local system ID used by the LACP.
show lacp bundle, on page 166	Displays detailed information about LACP ports and their peers.
show lacp port, on page 177	

show bundle

To display information about all bundles or a specific bundle of a particular type, use the **show bundle** command in EXEC configuration mode.

show bundle [{**Bundle-Ether | Bundle-POS** }*bundle-id*]

Syntax Description

Bundle-Ether	Displays information for the specified Ethernet bundle.
Bundle-POS	Displays information for the specified POS bundle.
bundle-id	Number from 1 to 65535 that identifies a particular bundle.

Command Default

Information is displayed for all configured bundles.

Command Modes

XR EXEC

Command History

Release	Modification
Release 5.0.0	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.

To see information for all bundles configured on the router, use the **show bundle**form of the command.

To see information for a specific bundle, use the **show bundle Bundle-Ether***bundle-id*or **show bundle Bundle-POS***bundle-id* form of the command with the number of the configured bundle.

Task ID

Task ID	Operation
bundle	read

Examples

The following example shows output for all bundle interfaces that are configured on the router:

```
RP/0/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
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 7: show bundle Field Descriptions

Field	Description
Bundle-*typenumber*	Full name of the bundle interface, where *type* is Ether (Ethernet) , 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 or Disabled.
mLACP:	
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 8: 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.

Reason	Description
BFD state of this link is Down	The link is in BFD Running state because LACP is negotiated but the BFD session between the local system and the remote device is Down.
Bundle has been shut down	The link is in Configured state because the bundle it is configured as a member of is administratively down.
Bundle interface is not present in configuration	The link is in Configured state because the bundle it is configured as a member of has not itself been configured.
Bundle is in the process of being created	The link is in Configured state because the bundle it is configured as a member of is still being created.
Bundle is in the process of being deleted	The link is in Configured state because the bundle it is configured as a member of is being deleted.
Bundle is in the process of being replicated to this location	The link is in Configured state because the bundle it is configured as a member of is still being replicated to the linecard where the link is located.
Forced switchover to the mLACP peer	The link is in Configured state because it has been brought down as part of a forced switchover to the mLACP peer PoA. This happens only when brute force switchovers are configured.
ICCP group is isolated from the core network	The link is in Configured state because there is no connectivity through the network core for the ICCP group that the link and its bundle are part of. Therefore, the link has been brought down to prevent any traffic being sent by the LACP partner device.
Incompatible with other links in the bundle (bandwidth out of range)	The link is in Configured state because its bandwidth is incompatible with other links configured to be in the same bundle. The bandwidth may be too high or too low.
LACP shutdown is configured for the bundle	The link is in Standby state because the bundle is configured with LACP shutdown.
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.

Reason	Description
Link is Attached and has not gone Collecting (reason unknown)	The link is in Negotiating state because the mLACP peer PoA has not indicated that the link has gone Collecting in the Mux machine. This could be because of an issue between the mLACP peer and its LACP partner or because this state has not been communicated to the local system.
Link is Collecting and has not gone Distributing (reason unknown)	The link is in Negotiating state because the mLACP peer PoA has not indicated that the link has gone Distributing in the Mux machine. This could be because of an issue between the mLACP peer and its LACP partner or because this state has not been communicated to the local system.
Link is being removed from the bundle	The link is being removed from the bundle and remains in Configured state while this happens.
Link is Defaulted; LACPDUs are not being received from the partner	The link is in Configured state because no LACPDUs are being received from the LACP partner device. Either the partner is not transmitting or the packets are getting lost.
Link is down	The link is in Configured state because it is operationally or administratively down.
Link is Expired; LACPDUs are not being received from the partner	The link is in Negotiating state because no LACPDUs have been received from the LACP Partner device in the Current-While period and the link is now marked as Expired in the Receive machine.
Link is in the process of being created	The link is in Configured state because the member configuration is still being processed.
Link is marked as Standby by mLACP peer	The link is in Standby state because this has been indicated by the mLACP peer PoA.
Link is Not Aggregatable (reason unknown)	The link is in Configured state because it is marked as an Individual link by the mLACP peer PoA.
Link is not operational as a result of mLACP negotiations	mLACP negotiations with the peer have led to this link being kept in Configured state. This is likely to indicate a misconfiguration between the two peer devices.
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.

Reason	Description
Link is Standby due to maximum-active links configuration	The link is in Standby state because the number of links in Selected state has already reached the configured maximum active links threshold.
Link is waiting for BFD session to start	The link is in BFD Running state because LACP is negotiated but the BFD session has not started from the remote device.
Loopback: Actor and Partner have the same System ID and Key	The link is in Configured state because a loopback condition has been detected on the link—two links configured to be members of the bundle are actually connected to each other.
Not enough links available to meet minimum-active threshold	The link is in Standby state because there are not enough selectable links (i.e. links which meet the criteria to be marked Selected within the bundle) to meet the minimum active links/bandwidth threshold.
Partner has marked the link as Not Aggregatable	The link is in Configured state because it is marked as an Individual link by the LACP partner device.
Partner has not advertised that it is Collecting	The link is in Negotiating state because the LACP partner device has not advertised that the link is in Collecting state in its LACPDUs.
Partner has not echoed the correct parameters for this link	The link is in Negotiating state because the LACP partner device has not correctly echoed the local system's port information in the LACPDUs it is sending.
Partner is not Synchronized (Waiting, not Selected, or out-of-date)	The link is in Negotiating state because the mLACP peer PoA has not indicated that its LACP partner device is Synchronized. This could be because the devices are genuinely not Synchronized or because this state has not been communicated to the local system.
Partner is not Synchronized (Waiting, Standby, or LAG ID mismatch)	The link is in Negotiating state because the LACP partner device has not indicated that it is Synchronized in the LACPDUs it is sending. On the partner device the link could still be waiting for the Wait-While timer to expire, it could be held in Standby state, or there could be a misconfiguration leading to a LAG ID mismatch between links configured to be within the same bundle.

Reason	Description
Partner System ID/Key do not match that of the Selected links	The link is in Configured state because the System ID or Operational Key specified by the LACP partner device does not match that seen on other Selected links within the same bundle. This probably indicates a misconfiguration.
Wait-while timer is running	The link is in Configured state because the Wait-While timer is still running and the new state has not yet been determined.

Related Commands

Command	Description
interface (bundle), on page 140	Specifies or creates a new bundle and enters interface configuration mode for that bundle.

show bundle brief

To display summary information about all configured bundles, use the **show bundle brief** command in EXEC configuration mode.

show bundle brief

Syntax Description

This command has no keywords or arguments.

Command Default

Information for all configured bundles is displayed.

Command Modes

XR EXEC

Command History

Release	Modification
Release 5.0.0	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	Operation
bundle	read

Examples

These examples shows the status of two bundles, BE16 and BE100, that are configured on the router. Both are Ethernet bundles and only bundle 16 is Up:

```
RP/0/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 9: show bundle brief Field Descriptions, on page 163 describes the fields shown in the display.

Table 9: show bundle brief Field Descriptions

Field	Description
Name	Abbreviated name of the bundle interface, with the following possible formats: • BE*x*—Ethernet bundle with ID number *x*. • BP*y*—POS bundle with ID number *y*.
IG	Interchassis group ID (if configured) of which the bundle is a member.
State	State of the bundle on the local device, with the following possible values: • Admin down—The bundle has been configured to be shut down. • Bundle shut—The bundle is holding all links in Standby state and will not support any traffic. • Down—The bundle is operationally down. It has no Active members on the local device. • • • Nak—The local and peer devices cannot resolve a configuration error. • Partner down—The partner system indicates that the bundle is unable to forward traffic at its end. • PE isolated—The bundle is isolated from the core. • Up—The bundle has Active members on this device.
LACP	Status of the Link Aggregation Control Protocol (LACP) on the bundle, with the following possible values: • On—LACP is in use on the bundle. • Off—LACP is not active.

Field	Description
BFD	When BFD is enabled, displays the state of BFD sessions on the bundle from the sessions running on bundle members that is communicated to interested protocols, with the following possible values: • Down—The configured minimim threshold for active links or bandwidth for BFD bundle members is not available so BFD sessions are down. • Off—BFD is not configured on bundle members. • Up—BFD sessions on bundle members are up because the minimum threshold for the number of active links or bandwidth is met.
Links act/stby/cfgd	Number of links on the bundle with a particular status in the format *x/y/z*, with the following values: • *x*—Number of links in Active state on the bundle for the local device (from 1 to the maximum number of links supported on the bundle). • *y*—Number of links in Standby state on the bundle for the local device (from 1 to the maximum number of links supported on the bundle). • *z*—Total number of links configured on the bundle for the local device (from 1 to the maximum number of links supported on the bundle).
Local b/w, kbps	Current bandwidth of the bundle on the local device (this effective bandwidth might be limited by configuration).

Related Commands

Command	Description
show bundle, on page 150	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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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
bundle	read

Examples

The following example shows how to

```
RP/0/RP0/CPU0:router# show bundle replication bundle-ether 1 all
```

show lacp bundle

To display detailed information about Link Aggregation Control Protocol (LACP) ports and their peers, enter the **show lacp bundle** command in EXEC mode.

show lacp bundle {**Bundle-Ether| bundle-POS**} *bundle-id*

Syntax Description

Bundle-Ether *bundle-id*	(Optional) Specifies the number of the Ethernet bundle whose information you want to display. Range is 1 through 65535.

Command Default

No default behavior or values

Command Modes

XR EXEC

Command History

Release	Modification
Release 5.0.0	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
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 10: show lacp bundle Field Descriptions

Field	Description
Flags	Describes the possible flags that may apply to a device or port, under the “Flags” field.
State	Describes the possible flags that may apply the port state, under the “State” field.
Port	Port identifier, in the *rack/slot/module/port* notation.
State	Provides information about the state of the specified port. Possible flags are: • 0—Port is not aggregatable. • 1—Port is out of sync with peer. • 2—Port is in sync with peer. • 3—Port is collecting. • 4—Port is collecting and distributing.
Flags	Provides information about the state of the specified device or port. Possible flags are: • A—Device is in Active mode. • P—Device is in Passive mode. • S—Device requests peer to send PDUs at a slow rate. • F—Device requests peer to send PDUs at a fast rate. • D—Port is using default values for partner information. • E—Information about partner has expired.
Port ID	Port identifier, expressed in the format *N*x*nnnn*. *N* is the port priority, and *nnnn* is the port number assigned by the sending router.

Field	Description
Key	Two-byte number associated with the specified link and aggregator. Each port is assigned an operational key. The ability of one port to aggregate with another is summarized by this key. Ports which have the same key select the same bundled interface. The system ID, port ID and key combine to uniquely define a port within a LACP system.
System-ID	System identifier. The system ID is a LACP property of the system which is transmitted within each LACP packet together with the details of the link.

Related Commands

Command	Description
bundle id, on page 127	Adds a port to an aggregated interface or bundle.
show bundle, on page 150	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.

Command Default

No default behavior or values

Command Modes

XR EXEC

Command History

Release	Modification
Release 5.0.0	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
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 11: 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 138	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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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.

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 174	Displays the contents of LACP packets that are sent and received on an interface.
lacp period short, on page 145	Enables a short period time interval for the transmission and reception of LACP packets.
lacp packet-capture, on page 142	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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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.

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 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

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 171	Displays the LACP transmission information that used by the transmitting device for sending packets on an interface.
lacp period short, on page 145	Enables a short period time interval for the transmission and reception of LACP packets.
lacp packet-capture, on page 142	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.
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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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.

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 12: show lacp port Field Descriptions

Field	Description
Port	Identifies the LACP port whose information is displayed. The port number is expressed in the *rack/slot/module/port* notation.
State	Provides information about the state of the specified device or port. Possible flags are: • 0—Port is not aggregatable. • 1—Port is out of sync with peer. • 2—Port is in sync with peer. • 3—Port is collecting. • 4—Port is collecting and distributing.

Field	Description
Flags	Provides information about the state of the specified port. Possible flags are: • A—Device is in Active mode. • P—Device is in Passive mode. • S—Device requests peer to send PDUs at a slow rate. • F—Device requests peer to send PDUs at a fast rate. • D—Port is using default values for partner information. • E—Information about partner has expired.
Port ID	Port identifier, expressed in the following format: *Nxnnnn*. *N* is the port priority, and *nnnn* is the port number assigned by the sending router.
Key	Two-byte number associated with the specified link and aggregator. Each port is assigned an operational key. The ability of one port to aggregate with another is summarized by this key. Ports which have the same key select the same bundled interface. The system ID, port ID and key combine to uniquely define a port within a LACP system.
System-ID	System identifier. The System ID is an LACP property of the system which is transmitted within each LACP packet together with the details of the link.

Related Commands

Command	Description
bundle id, on page 127	Adds a port to an aggregated interface or bundle.
show bundle, on page 150	Displays information about configured bundles.

show lacp system-id

To display the local system ID used by the Link Aggregation Control Protocol (LACP), enter the **show lacp system-id** command in EXEC mode.

show lacp system-id

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

XR EXEC

Command History

Release	Modification
Release 5.0.0	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.

Note The System ID and details about the specific link are transmitted within each LACP packet.

Task ID

Task ID	Operations
bundle	read

Examples

The following example shows how to display the system ID used by the LACP:

```
RP/0/RP0/CPU0:router# show lacp system-id

Priority  MAC Address
--------  -----------------
  0x8000  08-00-45-3a-65-01
```

Table 13: 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 127	Adds a port to an aggregated interface or bundle.
show bundle, on page 150	Displays information about configured bundles.

Management Ethernet Interface Commands

This module provides command line interface (CLI) commands for configuring Management Ethernet interfaces on the Cisco NCS 6000 Series Router.

duplex (Management Ethernet)

To configure duplex mode operation on a Management Ethernet interface, use the **duplex** command in interface configuration mode. To return the interface to autonegotiated duplex mode, use the **no** form of the **duplex** command.

duplex {**full**| **half**}

no duplex

Syntax Description

full	Configures the Management Ethernet interface to operate in full duplex mode.
half	Configures the Management Ethernet interface to operate in half duplex mode.

Command Default

Autonegotiates duplex operation

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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, 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//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//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//CPU0/0
RP/0/RP0/CPU0:router(config-if)# no duplex
```

Related Commands

Command	Description
interface MgmtEth, on page 186	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 XR configmode. To delete a Management Ethernet interface configuration, use the **no** form of this command.

interface MgmtEth *interface-path-id*

no interface MgmtEth *interface-path-id*

Syntax Description

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

Command Default

No default behavior or values

Command Modes

XR config

Command History

Release	Modification
Release 5.0.0	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, 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//CPU0/0
RP/0/RP0/CPU0:router(config-if)#
```

Related Commands

Command	Description
duplex (Management Ethernet), on page 184	Configures duplex mode operation on a Management Ethernet interface.
mac-address (Management Ethernet), on page 188	Sets the MAC layer address of a Management Ethernet interface.
speed (Management Ethernet), on page 190	Configures the speed for a Management Ethernet interface.

mac-address (Management Ethernet)

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

mac-address *value1.value2.value3*

no mac-address

Syntax Description

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

Command Default

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

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 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

The following example shows how to set the MAC address of the Management Ethernet interface located at 0/ /CPU0/0:

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

Related Commands

Command	Description
interface MgmtEth, on page 186	Enters interface configuration mode for the Management Ethernet interface.

speed (Management Ethernet)

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

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

no speed

Syntax Description

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

Command Default

Interface speed is autonegotiated.

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 14: Relationship Between duplex and speed Commands, on page 190 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 14: Relationship Between duplex and speed Commands

duplex Command	speed Command	Resulting System Action
no duplex	no speed	Autonegotiates both speed and duplex modes.
no duplex	speed 1000	Forces 1000 Mbps (1 Gbps) and full duplex.

duplex Command	speed Command	Resulting System Action
no duplex	speed 100	Autonegotiates for duplex mode and forces 100 Mbps.
no duplex	speed 10	Autonegotiates for duplex mode and forces 10 Mbps.
duplex full	no speed	Forces full duplex and autonegotiates for speed.
duplex full	speed 1000	Forces 1000 Mbps (1 Gbps) and full duplex.
duplex full	speed 100	Forces 100 Mbps and full duplex.
duplex full	speed 10	Forces 10 Mbps and full duplex.
duplex half	no speed	Forces half duplex and autonegotiates for speed (10 or 100 Mbps.)
duplex half	speed 100	Forces 100 Mbps and half duplex.
duplex half	speed 10	Forces 10 Mbps and half duplex.

Task ID

Task ID	Operations
interface	read, write

Examples

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

```
RP/0/RP0/CPU0:router(config)# interface MgmtEth 0//CPU0/0
RP/0/RP0/CPU0:router(config-if)# speed 1000
```

Related Commands

Command	Description
interface MgmtEth, on page 186	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 NCS 6000 Series Router.

interface null 0

To enter null0 interface configuration mode, use the **interface null 0** command in XR config mode.

interface null 0

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

XR config

Command History

Release	Modification
Release 5.0.0	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 XR config 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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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 15: 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.
drops	Total number of packets dropped by the interface.

Related Commands

Command	Description
show interfaces null0, on page 198	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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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 **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 NCS 6000 Series Router.

This module describes the Cisco IOS XR commands used to configure, monitor, and troubleshoot Packet-over-SONET/SDH (POS).

POS provides a method for efficiently carrying data packets in SONET or Synchronous Digital Hierarchy (SDH) frames. High-bandwidth capacity and efficient link utilization are characteristics that make POS largely preferred for building the core of data networks. POS uses PPP in High-Level Data Link Control (HDLC)-like framing for data encapsulation at Layer 2 (data link) of the Open System Interconnection (OSI) stack. This method provides efficient packet delineation and error control.

In addition to high-bandwidth efficiency, POS offers secure and reliable transmission for data. Reliable data transfer depends on timing integrity.

The real-time POS functionality is performed in hardware, according to the hardware configuration setup. Configured hardware events are detected by the framer application-specific integrated circuits (ASICs) and the control is passed to the software. The generic POS driver is responsible for providing a mechanism to configure the hardware on a per-interface basis, to handle interface state transitions, and to collect POS-related statistics.

crc (POS)

To set the length of the cyclic redundancy check (CRC) on a Packet-over-SONET/SDH (POS) interface, use the **crc** command in POS configuration mode. To return the CRC setting on a POS interface to the 32-bit default setting, use the **no** form of this command.

crc {**16**| **32**}

no crc [**16**| **32**]

Syntax Description

16	Sets 16-bit CRC mode.
32	Sets 32-bit CRC mode. The default is 32 bits.

Command Default

The default CRC mode is 32 bits.

Command Modes

POS configuration

Command History

Release	Modification
Release 5.0.0	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.

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(config)# interface POS 0/1/0/2
rack/slot(config-if)# POS
rack/slot(config-if-pos)# crc 32
```

Related Commands

Command	Description
transmit-delay, on page 215	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**}

no 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 5.0.0	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 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 212	Displays information about a POS interface.
show ppp interfaces (BNG), on page 263	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 XR config mode. To delete a POS configuration, use the **no** form of this command.

interface pos *interface-path-id*[**.***subinterface* **[point-to-point]**]

no 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

XR config

Command History

Release	Modification
Release 5.0.0	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.

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.
- f 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 212	Displays information about a POS interface.

keepalive (POS)

To set the keepalive timer for a specific interface, use the **keepalive** command in interface configuration mode. To reset the keepalive timer to the default of 10 seconds, use the **no** form of this command.

keepalive {*interval* [*retry*]| **disable**}

no keepalive

Syntax Description

interval	Number of seconds (from 1 to 30) between keepalive messages. The default is 10.
retry	(Optional) Number of keepalive messages (from 1 to 255) that can be sent to a peer without a response before transitioning the link to the down state. The default is 5 for interfaces with PPP encapsulation, and 3 for interfaces with HDLC encapsulation.
disable	Turns off the keepalive timer.

Command Default

The default interval is 10 seconds between keepalive messages. The default number of retry keepalive messages that can be sent without a response is 5 for interfaces with PPP encapsulation, and 3 for interfaces with HDLC encapsulation. However, when more than 5 (or 3) keepalive messages are sent to a peer without a response, the link transitions to the down state.

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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.

cHDLC keepalives require that the **keepalive** command is configured the same way on both routers. The two connected routers have no way of negotiating the keepalive value, because there is no way for the routers to tell each other what their configured values are. The keepalive value configured on each router (local and partner) sets the rate at which the Cisco IOS XR software sends packets. It also sets the rate at which the local end expects to receive incoming packets.

To set the keepalive value to the default value, use the **keepalive** command without specifying a value for the *seconds* argument.

If three keepalives are sent to the peer and no response is received from the peer, then the link makes the transition to the down state.

Task ID

Task ID	Operations
hdlc	read, write
ppp	read,write

Examples

This example shows how to configure keepalives for 3 seconds on POS interface 0/7/0/1:

```
RP/0/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 5.0.0	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 **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 202	Sets the length of the CRC on a Packet-over-SONET/SDH (POS) interface.
transmit-delay, on page 215	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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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.

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 16: 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.

Field	Description
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 17: show interfaces pos Field Descriptions

Field	Description
Intf Name	Interface identifier, in the *type***rack*/*slot*/*module*/*port* notation.
Intf State	Indicates whether the interface is in the admin-up or admin down state.
LineP State	Line protocol state.
Encap Type	Encapsulation type for the specified interface. Can be HDLC or PPP.
MTU (byte)	Maximum transmission unit (MTU) value configured for the specified interface, in bytes.
BW (Kbps)	Bandwidth of the interface, in kbps.

Related Commands

Command	Description
show controllers pos	Displays information on the POS controllers.
show controllers sonet	Displays information about the operational status of SONET layers.

transmit-delay

To specify a number of flag sequences to be inserted between the packets, use the **transmit-delay** command in POS configuration mode. To restore the default, use the **no** form of this command.

transmit-delay *microseconds*

no transmit-delay *microseconds*

Syntax Description

microseconds	Number of microseconds of minimum delay after sending a packet. Range is from 0 to 1023. Default is 0 (disabled).

Command Default

microseconds = 0 (disabled)

Command Modes

POS configuration

Command History

Releases	Modifications
Release 5.0.0	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
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 NCS 6000 Series Router.

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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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.

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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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
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

no encapsulation ppp

Syntax Description

This command has no keywords or arguments.

Command Default

PPP encapsulation is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 **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 263	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 XR config mode. To remove this group, use the no form of this command.

group *group-id* **profile** *profile_name* **[default]**

no 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

XR config

Command History

Release 5.0.0	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.

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 279	specify the node on which to create a SSRP group and enter the SSRP node configuration mode.

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*

no 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 5.0.0	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
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 280	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 an appropriate configuration mode. To disable PPP authentication, use the **no** form of this command.

ppp authentication *protocol* [*protocol* [*protocol*]] {*list-name*| **default**}

no ppp authentication

Syntax Description

protocol	Name of the authentication protocol used for PPP authentication. See Table 18: PPP Authentication Protocols for Negotiation, on page 228 for the appropriate keyword. You may select one, two, or all three protocols, in any order.
list-name	(Optional) Used with authentication, authorization, and accounting (AAA). Name of a list of methods of authentication to use. If no list name is specified, the system uses the default. The list is created with the **aaa authentication ppp** command.
default	(Optional) Specifies the name of the list of methods created with the **aaa authentication ppp** command.

Command Default

PPP authentication is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 enable CHAP or PAP authentication (or both), the local router requires the remote device to prove its identity before allowing data traffic to flow. PAP authentication requires the remote device to send a name and a password, which is checked against a matching entry in the local username database or in the remote security server database. CHAP authentication sends a challenge message to the remote device. The remote device encrypts the challenge value with a shared secret and returns the encrypted value and its name to the local router in a response message. The local router attempts to match the remote device's name with an associated secret stored in the local username or remote security server database; it uses the stored secret to encrypt the original challenge and verify that the encrypted values match.

You can enable CHAP, MS-CHAP, or PAP in any order. If you enable all three methods, the first method specified is requested during link negotiation. If the peer suggests using the second method, or refuses the first method, the second method is tried. Some remote devices support only one method. Base the order in which you specify methods on the remote device's ability to correctly negotiate the appropriate method, and on the level of data line security you require. PAP usernames and passwords are sent as clear text strings, which can be intercepted and reused.

Note If you use a *list-name* value that was not configured with the **aaa authentication ppp** command, then authentication does not complete successfully and the line does not come up.

Table 18: PPP Authentication Protocols for Negotiation, on page 228 lists the protocols used to negotiate PPP authentication.

Table 18: 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
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
encapsulation	Sets the encapsulation method used by the interface.
username	Configures a new user with a username, establishes a password, and grants permissions for the user.

ppp chap password

To enable a router calling a collection of routers to configure a common Challenge Handshake Authentication Protocol (CHAP) secret password, use the **ppp chap password** command in interface configuration mode. To disable the password, use the **no** form of this command.

ppp chap password [**clear**| **encrypted**] *password*

no ppp chap password [**clear**| **encrypted**] *password*

Syntax Description

clear	(Optional) Specifies the cleartext encryption parameter for the password.
encrypted	(Optional) Indicates that the password is already encrypted.
password	Cleartext or already-encrypted password.

Command Default

The password is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 **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 227	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 232	Refuses CHAP authentication from peers requesting it.
ppp max-bad-auth (BNG), on page 237	Configures a PPP interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.

ppp chap refuse

To refuse Challenge Handshake Authentication Protocol (CHAP) authentication from peers requesting it, use the **ppp chap refuse** command in interface configuration mode. To allow CHAP authentication, use the **no** form of this command.

ppp chap refuse

no ppp chap refuse

Syntax Description

This command has no keywords or arguments.

Command Default

CHAP authentication is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 **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.
ppp authentication (BNG), on page 227	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 237	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 257	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*]

no 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 5.0.0	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
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

no 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 5.0.0	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
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*

no 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 5.0.0	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
ppp	read, write

Examples

The following example shows how to specifies 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*

no ppp max-bad-auth

Syntax Description

retries	Number of retries after which the interface is to reset itself. Range is from 0 to 10. Default is 0 retries.

Command Default

retries: 0

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 **ppp max-bad-auth** command applies to any interface on which PPP encapsulation is enabled.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

In this example, POS interface 0/3/0/1 is set to allow two additional retries after an initial authentication failure (for a total of three failed authentication attempts):

```
RP/0/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
```

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*

no ppp max-configure

Syntax Description

retries	Maximum number of retries. Range is 4 through 20. Default is 10.

Command Default

retries: 10

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 **ppp max-configure** command to specify how many times an attempt is made to establish a Link Control Protocol (LCP) session between two peers for a particular interface. If a configure request message receives a reply before the maximum number of configure requests are sent, further configure requests are abandoned.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

This example shows a limit of four configure requests:

```
RP/0/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
```

Related Commands

Command	Description
ppp max-failure (BNG), on page 241	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*

no ppp max-failure

Syntax Description

retries	Maximum number of CONFNAKs to permit before terminating a negotiation. Range is from 2 to 10. Default is 5.

Command Default

retries: 5

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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
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
```

Related Commands

Command	Description
ppp max-configure (BNG), on page 239	Specifies the maximum number of configure requests to attempt (without response) before stopping the requests.

ppp max-terminate

To configure the maximum number of terminate requests (TermReqs) to send without reply before closing down the Link Control Protocol (LCP) or Network Control Protocol (NCP), use the **ppp max-terminate** command in interface configuration mode. To disable the maximum number of TermReqs and return to the default, use the **no** form of this command.

ppp max-terminate *number*

no ppp max-terminate

Syntax Description

number	Maximum number of TermReqs to send without reply before closing down the LCP or NCP. Range is from 2 to 10. Default is 2.

Command Default

number: 2

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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
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 239	Specifies the maximum number of configure requests to attempt (without response) before stopping the requests.
ppp max-failure (BNG), on page 241	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*

no 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 5.0.0	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
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*

no ppp ms-chap password [**clear**| **encrypted**] *password*

Syntax Description

clear	(Optional) Specifies the cleartext encryption parameter for the password.
encrypted	(Optional) Indicates that the password is already encrypted.
password	Cleartext or already-encrypted password.

Command Default

The password is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 **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

no ppp ms-chap refuse

Syntax Description

This command has no keywords or arguments.

Command Default

MS-CHAP authentication is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 **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 227	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

no 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 5.0.0	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
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*

no 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 5.0.0	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 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*

no 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 5.0.0	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.

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 234	Configures the primary and secondary DNS IP addresses for the IPCP.
ppp ipcp neighbor-route disable, on page 235	Disables installation of a route to the peer address negotiated by IPCP.
ppp ipcp peer-address default, on page 236	Specifies the default IPv4 address that is assigned to the peer by the IPCP.
ppp ms-chap hostname, on page 245	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

no ppp pap refuse

Syntax Description

This command has no keywords or arguments.

Command Default

PAP authentication is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 **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.
ppp authentication (BNG), on page 227	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 237	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 257	Enables remote PAP support for an interface, and includes the **sent-username** and **password** commands in the PAP authentication request packet to the peer.

ppp pap sent-username password

To enable remote Password Authentication Protocol (PAP) support for an interface, and to use the values specified for username and password in the PAP authentication request, use the **ppp pap sent-username password** command in interface configuration mode. To disable remote PAP support, use the **no** form of this command.

ppp pap sent-username *username* **password** [**clear**| **encrypted**] *password*

no ppp pap sent-username *username* **password** [**clear**| **encrypted**] *password*

Syntax Description

username	Username sent in the PAP authentication request.
clear	(Optional) Specifies the cleartext encryption parameter for the password.
encrypted	(Optional) Indicates that the password is already encrypted.
password	Cleartext or already-encrypted password.

Command Default

Remote PAP support is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 **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 227	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 250	Refuses PAP authentication from peers requesting it
ppp timeout authentication, on page 259	Sets PPP authentication timeout parameters.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.

ppp timeout authentication

To set PPP authentication timeout parameters, use the **ppp timeout authentication** command in interface configuration mode. To reset the default value, use the **no** form of this command.

ppp timeout authentication *seconds*

no ppp timeout authentication

Syntax Description

seconds	Maximum time, in seconds, to wait for a response to an authentication packet. Range is from 3 to 30 seconds. Default is 10 seconds.

Command Default

seconds: 10

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 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 227	Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.

ppp timeout retry

To set PPP timeout retry parameters, use the **ppp timeout retry** command in interface configuration mode. To reset the time value, use the **no** form of this command.

ppp timeout retry *seconds*

no ppp timeout retry

Syntax Description

seconds	Maximum time, in seconds, to wait for a response during PPP negotiation. Range is from 1 to 10 seconds. Default is 3 seconds.

Command Default

seconds: 3

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	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 **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
```

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*

no 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 5.0.0	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.

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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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.

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 19: 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.

Field	Description
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.

Field	Description
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

XR EXEC

Command History

Release 5.0.0	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.

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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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.

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 XR 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

XR EXEC

Command History

Release	Modification
Release 5.0.0	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.

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 5.0.0	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 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 XR config 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

XR config

Command History

Release	Modification
Release 5.0.0	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 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 XR config mode. To remove the profile, use the no form of this command.

ssrp profile *profile-name*

no ssrp profile *profile-name*

Syntax Description

profile-name	Name of this SSRP profile.

Command Default

No default behavior or values

Command Modes

XR config

Command History

Release	Modification
Release 5.0.0	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.

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)#
```

VLAN Subinterface Commands

This module provides command line interface (CLI) commands for configuring 802.1Q VLANs on the Cisco NCS 6000 Series Router.

dot1q vlan

To assign a VLAN ID to a subinterface (or to modify the VLAN ID that is currently assigned to a subinterface), use the **dot1q vlan** command in subinterface configuration mode. To remove the VLAN ID assigned to a subinterface, use the **no** form of this command.

dot1q vlan *vlan-id* [*vlan-id2*| **any**]

no dot1q vlan *vlan-id*

Syntax Description

vlan-id	ID of the subinterface. Range is from 1 to 4094 (0 and 4095 are reserved).
vlan-id2	(Optional) Identifies the host VLAN of a Q-in-Q VLAN pair. Replace *vlan-id2* with a number that specifies the host VLAN. Range is from 1 to 4094.
any	(Optional) Identifies the host VLAN of a Q-in any VLAN pair.

Command Default

No default behavior or values

Command Modes

Subinterface configuration

Command History

Release	Modification
Release 5.0.0	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 VLAN ID specifies where 802.1Q tagged packets are sent and received on a specified subinterface. An 802.1Q VLAN subinterface must have a configured VLAN ID to send and receive traffic; without a VLAN ID, the subinterface remains in the down state. All VLAN IDs must be unique among all subinterfaces configured on the same physical interface. To change a VLAN ID, the new VLAN must not already be in use on the same physical interface. To exchange VLAN IDs, you must remove the configuration information and reconfigure the ID for each device.

Note The subinterface does not pass traffic without an assigned VLAN ID.

Task ID

Task ID	Operations
vlan	read, write

Examples

The following 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
```

The following 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
```

The following 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
dot1q native vlan	Assigns the native VLAN ID of a physical interface trunking 802.1Q VLAN traffic.
show interfaces, on page 107	Displays statistics for all interfaces configured on the router or for a specific node.

interface (VLAN)

To create a VLAN subinterface, use the **interface** command in XR config mode. To delete a subinterface, use the **no** form of this command.

interface *type interface-path-id.subinterface* **[l2transport]**

no interface *type interface-path-id.subinterface* **[l2transport]**

Syntax Description

type	Type of Ethernet interface on which you want to create a VLAN. Enter **GigabitEthernet**, **TenGigE**,, 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

XR config

Command History

Release	Modification
Release 5.0.0	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.

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 native vlan	Assigns the native VLAN ID of a physical interface trunking 802.1Q VLAN traffic.
dot1q vlan, on page 282	Assigns a VLAN ID to a subinterface (or modifies the VLAN ID that is currently assigned to a 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 NCS 6000 Series Router.

For information on 10-Gigabit Ethernet (GE) interface commands see the *Ethernet Interface Commands* 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 XR EXECmode.

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

XR EXEC

Command History

Release	Modification
Release 5.0.1	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
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 295	Displays alarms, registers, and module information for a 10-Gigabit Ethernet WAN PHY controller.
clear counters wanphy	Clears the alarms counters for a specific 10-Gigabit Ethernet WAN PHY interface.

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 XR config 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

no 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

XR config

Command History

Release	Modification
Release 5.0.1	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 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)#
```

Related Commands

Command	Description
show controllers wanphy, on page 295	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

no 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 5.0.1	This command was introduced.

Usage Guidelines

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 293	Disables SF BER reporting.
show controllers wanphy, on page 295	Displays alarms, registers, and module information for a 10-Gigabit Ethernet WAN PHY controller.
threshold sf-ber, on page 307	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 disable Signal Failure (SF) Bit Error Rate (BER) reporting, use the no form of this command.

report sf-ber disable

no 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 5.0.1	This command was introduced.

Usage Guidelines

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 292	Enables Signal Degrade (SD) Bit Error Rate (BER) reporting.
show controllers wanphy, on page 295	Displays alarms, registers, and module information for a 10-Gigabit Ethernet WAN PHY controller.
threshold sf-ber, on page 307	Configures the threshold of the SF BER that is used to trigger a link state change.

signal sf-ber remote-fault

To configure the remote fault signaling of the Signal Failure (SF) Bit Error Rate (BER) that is used to trigger a signal failure, use the **signal sf-ber remote-fault**command in wanphy configuration mode.

signal sf-ber remote-fault *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 3, meaning (10-3).

Command Modes

Wanphy configuration

Command History

Release	Modification
Release 5.0.1	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
interface	read, write

Examples

This example shows how to configure remote fault signaling 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)# signal sf-ber remote-fault
RP/0/RP0/CPU0:router(config-wanphy)#
```

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

XR EXEC

Command History

Release	Modification
Release 5.0.1	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
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, FELCDP = 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 20: 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.
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.

Field	Description
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.

Field	Description
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. • 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 Seconds (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.

Field	Description
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.

Field	Description
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. • 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 20: show controllers wanphy Command Output Fields, on page 297.

The following 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 20: show controllers wanphy Command Output Fields, on page 297.

Related Commands

Command	Description
clear controller wanphy, on page 288	Clears the alarms counters for a specific 10-Gigabit Ethernet WAN PHY controller.

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*

no 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 5.0.1	This command was introduced.

Usage Guidelines

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 292	Enables Signal Degrade (SD) Bit Error Rate (BER) reporting.

Command	Description
report sf-ber disable, on page 293	Disables SF BER reporting.
threshold sf-ber, on page 307	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*

no 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 5.0.1	This command was introduced.

Usage Guidelines

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 292	Enables Signal Degrade (SD) Bit Error Rate (BER) reporting.

Command	Description
report sf-ber disable, on page 293	Disables SF BER reporting.
show controllers wanphy, on page 295	Displays alarms, registers, and module information for a 10-Gigabit Ethernet WAN PHY controller.

INDEX

K

L

M

N

P

R

S

T