



Release 3.5.0 Beta Draft—CISCO CONFIDENTIAL



Cisco IOS XR Interface and Hardware Component Command Reference

Cisco IOS XR Software Release 3.5

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

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-12276-01

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco IOS XR Interface and Hardware Component Command Referenc
© 2007 Cisco Systems, Inc. All rights reserved.



Preface

This document describes the commands that support router interface and hardware configuration using Cisco IOS XR software.

The preface contains the following sections:

- [Changes to This Document, page iii](#)
- [Obtaining Documentation, page iii](#)
- [Documentation Feedback, page iv](#)
- [Cisco Product Security Overview, page iv](#)
- [Product Alerts and Field Notices, page v](#)
- [Obtaining Technical Assistance, page vi](#)
- [Obtaining Additional Publications and Information, page vii](#)

Changes to This Document

[Table 1](#) lists the technical changes made to this document since it was first printed.

Table 1 *Changes to This Document*

Revision	Date	Change Summary
OL-12276-01	February 2007	Initial release of this document.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

R3.5.0 Beta Draft—Cisco Confidential Information

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

<http://www.cisco.com/univercd/home/home.htm>

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

If you do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

R3.5.0 Beta Draft—Cisco Confidential Information

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

R3.5.0 Beta Draft—Cisco Confidential Information

<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

To register as a Cisco.com user, go to this URL:

<http://tools.cisco.com/RPF/register/register.do>

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

<http://www.cisco.com/en/US/support/index.html>

Access to all tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.



Tip

Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

R3.5.0 Beta Draft—Cisco Confidential Information

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411

Australia: 1 800 805 227

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

<http://www.cisco.com/offer/subscribe>

R3.5.0 Beta Draft—Cisco Confidential Information

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Internet Protocol Journal* is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:

<http://www.cisco.com/univercd/cc/td/doc/abtnucd/136957.htm>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>



Hardware Redundancy and Node Administration Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

This module describes the commands used to manage the hardware redundancy, power, and administrative status of the nodes on a router running Cisco IOS XR software.

R3.5.0 Beta Draft—Cisco Confidential Information

ce tftp server

To enable Trivial File Transfer Protocol (TFTP) on a specific directory, or to enable files to be written to the TFTP server, use the **ce tftp server** command in global configuration mode.

ce tftp server {**homedir** *name* | **write**}

Syntax Description

homedir <i>name</i>	Specifies the home directory for TFTP server.
write	Enables files to be written to the TFTP server.

Defaults

No default behavior or values

Command Modes

Administration configuration

Command History

Release	Modification
Release 3.0	This command was introduced on the Cisco CRS-1.
Release 3.2	No modification.
Release 3.3.0	The ce tftp server enable EXEC mode command was replaced by the ce tftp server administration configuration mode command.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
root-system	read, write

Examples

The following example shows how to enable files to be written to the TFTP server:

```
RP/0/RP0/CPU0:router(config)# ce tftp server write
```

The following example shows how to enable TFTP on a specific directory. In this example, the directory is called "dir":

```
RP/0/RP0/CPU0:router(config)# ce tftp server homedir dir
```

R3.5.0 Beta Draft—Cisco Confidential Information

clear mbus-statistics location

To clear MBUS firmware statistics on a specific node, use the **clear mbus-statistics location** command in administration EXEC mode.

clear mbus-statistics location {*node-id* | **all**}

Syntax Description

<i>node-id</i>	Identifies the location of the node whose MBUS interface counters you want to clear. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation. Note Enter the show platform command to see the location of all nodes installed in the router.
all	Clears MBUS interface counters for all nodes installed in the router.

Defaults

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
sysmgr	execute

Examples

The following example shows how to clear all MBUS interface counters on a specific node:

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

```
RP/0/0/CPU0:router(admin)# clear mbus-statistics location 0/0/CPU0
```

R3.5.0 Beta Draft—Cisco Confidential Information

diagnostic bootup level

To configure the diagnostic for booting a card, use the **diagnostic bootup level** command in administration configuration mode. To remove the specified command from the configuration file and restore the system to its default condition, use the **no** form of this command.

diagnostic bootup level {bypass | complete | minimal} location node-id

no diagnostic bootup level {bypass | complete | minimal} location node-id

Syntax Description

bypass	Specifies bypassing diagnostics at bootup.
complete	Specifies running full diagnostics at bootup.
minimal	Specifies running minimal diagnostics at bootup.
location node-id	Specifies a card. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults

The default bootup diagnostics level is minimal.

Command Modes

Administration configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

**Note**

There are no bootup diagnostic tests available in Release 3.4. Both the **minimal** and **complete** bootup diagnostic test levels contain no tests.

Use the **diagnostic bootup level** command to specify the level of diagnostics to be run when a card is booted.

The new level takes effect at the next reload or the next time that an online insertion and removal is performed.

You can set the bootup diagnostics level as minimal or complete, or you can bypass the bootup diagnostics entirely. Use the **complete** keyword to run a complete set of bootup diagnostic tests; use the **minimal** keyword to run the minimal set of bootup diagnostic tests. Use the **bypass** keyword to bypass all diagnostic tests.

R3.5.0 Beta Draft—Cisco Confidential Information**Note**

To specify a physical layer interface module (PLIM) node using the *node-id* argument, use the following notation: *rack/PLslot-number/SP*. For example, 0/PL1/SP. PLIM diagnostic tests are supported on the Cisco CRS-1 router.

Task ID**Task ID** **Operations**

diag	read, write

Examples

The following example shows how to configure minimal bootup diagnostics for 0/1/cpu0:

```
RP/0/RP0/CPU0:router(admin-config)# diagnostic bootup level minimal location 0/1/cpu0
```

Related Commands

Command	Description
show diagnostic bootup level	Displays the current bootup level configured for the specified location.
show diagnostic content	Displays test information including test ID, test attributes, and supported coverage test levels for each test and for all components.

R3.5.0 Beta Draft—Cisco Confidential Information

diagnostic load

To load an offline diagnostic image for integrated field diagnostics, use the **diagnostic load** command in administration EXEC mode.

diagnostic load location *node-id* [**autostart** {**basic** | **all**}]

Syntax Description

location <i>node-id</i>	Loads an offline diagnostic image for a specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation. All modules in the specified slot are loaded with the offline diagnostic image.
autostart { basic all }	(Optional) Starts running the diagnostic tests after the image has loaded. The following options are available: • basic—Runs basic tests • all—Runs all tests.

Defaults

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **diagnostic load** command to load an offline diagnostic image used for integrated field diagnostics. Loading a diagnostic image places the specified card out of service.

The time it takes to load a diagnostic image varies depending on the card. Use the **show platform** command to determine if the image has been loaded and if the card has been placed out of service.

For more information about running Cisco IOS XR diagnostics, refer to *Cisco IOS XR Diagnostics*.

Task ID

Task ID	Operations
diag	execute

Examples

The following example shows how to load an offline diagnostic image:

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

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(admin)# diagnostic load location 0/0/CPU0 autostart basic

diagnostic load will bring requested slot out of service. [confirm(y/n)] y
User has confirmed diagnostic load request
Preparing UUT for Diagnostics software.
Downloading IDS diagnostics image /pkg/ucode/hfr-diag-l3sp-fdiags
Downloading IDS diagnostics image /pkg/ucode/hfr-diag-l3-fdiags
Please wait for UUT image downloading ...
diagnostic load in progress.

RP/0/RP0/CPU0:router(admin)#
```

Related Commands

Command	Description
diagnostic unload	Unloads a diagnostic test.
show platform	Displays information and status of each node in the system.

R3.5.0 Beta Draft—Cisco Confidential Information

diagnostic monitor

To configure the health-monitoring diagnostic testing for a specified location, use the **diagnostic monitor** command in administration configuration mode. To remove the specified command from the configuration file and restore the system to its default condition, use the **no** form of this command.

diagnostic monitor location *node-id* **test** {*id* | *test-name*} [**disable**]

no diagnostic monitor location *node-id* **test** {*id* | *test-name*} [**disable**]

Syntax Description

<i>node-id</i>	Location to enable diagnostic monitoring. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
test { <i>id</i> <i>test-name</i> }	Specifies diagnostic test selection. The following test selections are available: <i>id</i>—Test ID, as shown in the show diagnostic content command. <i>test-name</i>—Name of the test.
disable	Disables diagnostic monitoring for a specified location.

Defaults

To view the default value for each test, use the **show diagnostic content** command when the diagnostic image is first installed. The default is different for each test.

Command Modes

Administration configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **diagnostic monitor** command to enable or disable health-monitoring diagnostic testing for a specified test at the specified location.

Use the **disable** keyword to disable a health-monitoring diagnostic test. For example, if test 1 is disabled by default, the **disable** keyword disables the diagnostic test. If the **no** form of the command is used, the test is set to the default condition, which is disabled.

**Note**

To specify a physical layer interface module (PLIM) node using the *node-id* argument, use the following notation: *rack/PLslot-number/SP*. For example, 0/PL1/SP. PLIM diagnostic tests are supported on the Cisco CRS-1 router.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	diag	read, write

Examples

The following example shows how to enable health-monitoring diagnostic testing for 0/1/cpu0:

```
RP/0/RP0/CPU0:router(admin-config)# diagnostic monitor location 0/1/cpu0 test 1
```

Related Commands

Command	Description
show diagnostic content	Displays test information including test ID, test attributes, and supported coverage test levels for each test and for all components.

R3.5.0 Beta Draft—Cisco Confidential Information

diagnostic monitor interval

To configure the health-monitoring diagnostic testing for a specified interval for a specified location, use the **diagnostic monitor interval** command in administration configuration mode. To remove the specified command from the configuration file and restore the system to its default condition, use the **no** form of this command.

diagnostic monitor interval location *node-id* **test** {*id* | *test-name*} *number-of-days*
hour:minutes:seconds.milliseconds

no diagnostic monitor interval location *node-id* **test** {*id* | *test-name*} *number-of-days*
hour:minutes:seconds.milliseconds

Syntax Description	location <i>node-id</i>	Schedules interval diagnostic testing for a specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
	test { <i>id</i> <i>test-name</i> }	Specifies diagnostic test selection. The following test selections are available: <i>id</i>—Test ID. <i>test-name</i>—Test name, as shown in the show diagnostic content command.
	<i>number-of-days</i>	Specifies the number of days between testing.
	<i>hour:minutes:seconds.milliseconds</i>	Specifies the interval, where <i>hour</i> is a number in the range from 0 through 23, <i>minutes</i> is a number in the range from 0 through 59, <i>seconds</i> is a number in the range from 0 through 59, and <i>milliseconds</i> is a number in the range from 0 through 999.

Defaults To view the default value for each test, use the **show diagnostic content** command when the diagnostic image is first installed. The default is different for each test.

Command Modes Administration configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **diagnostic monitor interval** command to set the health-monitoring interval of a specified test at the specified location. The **no** version of the command resets the interval to the default setting. The **diagnostic monitor** command is used to enable health-monitoring.

R3.5.0 Beta Draft—Cisco Confidential Information**Note**

To specify a physical layer interface module (PLIM) node using the *node-id* argument, use the following notation: *rack/PLslot-number/SP*. For example, 0/PL1/SP. PLIM diagnostic tests are supported on the Cisco CRS-1 router.

Task ID**Task ID** **Operations**

diag	read, write

Examples

The following example shows how to set the health-monitoring diagnostic testing at an interval of 1 hour, 2 minutes, 3 seconds, and 5 milliseconds for 0/1/cpu0:

```
RP/0/RP0/CPU0:router(admin-config)# diagnostic monitor interval location 0/1/cpu0 test 1 0 1:2:3.4
```

Related Commands

Command	Description
diagnostic monitor	Enables or disables health-monitoring diagnostic testing for a specified test at a specified location.
show diagnostic content	Displays test information including test ID, test attributes, and supported coverage test levels for each test and for all components.

R3.5.0 Beta Draft—Cisco Confidential Information

diagnostic monitor syslog

To enable the generation of a syslog message when any health monitoring test fails, use the **diagnostic monitor syslog** command in administration configuration mode. To remove the specified command from the configuration file and restore the system to its default condition, use the **no** form of this command.

diagnostic monitor syslog

no diagnostic monitor syslog

Syntax Description This command has no arguments or keywords.

Defaults Syslog is disabled.

Command Modes Administration configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **diagnostic monitor syslog** command to enable the generation of a syslog message when a health-monitoring test fails.

Task ID	Task ID	Operations
	diag	read, write

Examples The following example shows how to enable the generation of syslog messages:

```
RP/0/RP0/CPU0:router(admin-config)# diagnostic monitor syslog
```

Related Commands	Command	Description
	show diagnostic content	Displays test information including test ID, test attributes, and supported coverage test levels for each test and for all components.

R3.5.0 Beta Draft—Cisco Confidential Information

diagnostic monitor threshold

To configure the health-monitoring diagnostic testing failure threshold, use the **diagnostic monitor threshold** command in administration configuration mode. To remove the specified command from the configuration file and restore the system to its default condition, use the **no** form of this command.

diagnostic monitor threshold location *node-id* **test** {*id* | *test-name*} **failure count** *failures*

no diagnostic monitor threshold location *node-id* **test** {*id* | *test-name*} **failure count** *failures*

Syntax Description	location <i>node-id</i>	Schedules interval diagnostic testing for a specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
	test { <i>id</i> <i>test-name</i> }	Specifies diagnostic test selection. The following test selections are available: <i>id</i>—Test ID. <i>test-name</i>—Test name, as shown in the show diagnostic content command.
	failure count <i>failures</i>	Specifies the number of allowable test failures. Range is 1 to 99.

Defaults To view the default value for each test, use the **show diagnostic content** command when the diagnostic image is first installed. The default can be different for each test.

Command Modes Administration configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **diagnostic monitor threshold** command to specify health-monitoring diagnostic testing failure threshold.

**Note**

To specify a physical layer interface module (PLIM) node using the *node-id* argument, use the following notation: *rack/PLslot-number/SP*. For example, 0/PL1/SP. PLIM diagnostic tests are supported on the Cisco CRS-1 router.

R3.5.0 Beta Draft—Cisco Confidential Information**Task ID****Task ID****Operations**

diag

read, write

Examples

The following example shows how to set the failure threshold to 35 test failures for all tests for 0/1/cpu0:

```
RP/0/RP0/CPU0:router(admin-config)# diagnostic monitor threshold location 0/1/cpu0 test  
failure count 35
```

Related Commands**Command****Description**

[show diagnostic
content](#)

Displays test information including test ID, test attributes, and supported coverage test levels for each test and for all components.

R3.5.0 Beta Draft—Cisco Confidential Information

diagnostic ondemand action-on-failure

To set when to stop test execution for a **diagnostic start** command, use the **diagnostic ondemand action-on-failure** command in administration EXEC mode. This command is used in conjunction with the **diagnostic ondemand iteration** command.

diagnostic ondemand action-on-failure { **continue** *failure-count* | **stop** }

Syntax Description	continue <i>failure-count</i>	Specifies that test execution continue until the number of failures reaches the specified <i>failure-count</i> . Range is 0 to 65534. A <i>failure-count</i> of 0 indicates to not stop execution until all iterations are complete no matter how many failures are encountered.
	stop	Stops execution immediately when the first test failure occurs.

Defaults	continue <i>failure-count</i> : 0

Command Modes	Administration EXEC

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the Cisco CRS-1.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Use the diagnostic ondemand action-on-failure command to specify whether or when to stop test execution if a test fails. This command is used in conjunction with the diagnostic ondemand iterations command.

Task ID	Task ID	Operations
	diag	read, write

Examples	The following example shows how to set the test failure action to stop:
	RP/0/RP0/CPU0:router(admin)# diagnostic ondemand action-on-failure stop

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	diagnostic ondemand iterations	Specifies the number of times to run the specified tests when diagnostic start command is entered.
	diagnostic start	Runs specified diagnostic tests the number of iterations as set by the diagnostic ondemand iteration command.

R3.5.0 Beta Draft—Cisco Confidential Information

diagnostic ondemand iterations

To set the number of iterations to repeat execution of the tests specified by the **diagnostic start** command, use the **diagnostic ondemand iterations** command in administration EXEC mode.

diagnostic ondemand iterations *count*

Syntax Description	<i>count</i>	Number of times to repeat the specified on-demand tests. Range is 1 to 999.

Defaults	<i>count</i> : 1

Command Modes	Administration EXEC

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the Cisco CRS-1.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the diagnostic ondemand iterations command to specify the number of times the specified on-demand tests run. The on-demand tests are specified using the diagnostic start command.

Task ID	Task ID	Operations
	diag	read, write

Examples	The following example shows how to set the number of iterations to 12: <pre>RP/0/RP0/CPU0:router(admin)# diagnostic ondemand iterations 12</pre>

Related Commands	Command	Description
	diagnostic ondemand action-on-failure	Specifies whether or when to stop execution if there is failure.
	diagnostic start	Runs specified diagnostic tests the number of iterations as set by the diagnostic ondemand iteration command.

R3.5.0 Beta Draft—Cisco Confidential Information

diagnostic schedule

To configure the diagnostic schedule, use the **diagnostic schedule** command in administration configuration mode. To disable the diagnostic schedule, use the **no** form of this command.

diagnostic schedule location *node-id* **test** {*id* | **all** | **basic** | **non-disruptive**} {**daily** | **on** *month day year* | **weekly** *day-of-week*} *hour:minute*

no diagnostic schedule location *node-id* **test** {*id* | **all**} {**daily** | **on** *month day year* | **weekly** *day-of-week*} *hour:minute*

Syntax Description	location <i>node-id</i>	Schedules a diagnostic test for a specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
	test	Specifies a specific diagnostic test, or all diagnostic tests.
	<i>id</i>	Test ID or list of test IDs, as shown in the show diagnostic content command. Multiple tests can be listed if separated by semicolons (;) as follows: x;y-z (for example: 1; 3-4 or 1;3;4)
	all	Specifies all tests.
	basic	Specifies the basic on-demand test suite [Attribute = B].
	non-disruptive	Specifies the nondisruptive test suite [Attribute = N].
	daily	Specifies a daily schedule.
	on <i>month day year</i>	Schedules an exact date.
	weekly <i>day-of-week</i>	Specifies a weekly schedule with a set day of the week. Enter the name of a day of the week or a number that specifies a day of the week in the range from 1 through 6 .
	<i>hour:minute</i>	Scheduled start time, where <i>hour</i> is a number in the range from 0 through 23 , and <i>minute</i> is a number in the range from 0 through 59 .

Defaults No default behavior or values

Command Modes Administration configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.5.0 Beta Draft—Cisco Confidential Information

Use the **diagnostic schedule** command to schedule diagnostic tests for a specific location.

**Note**

To specify a physical layer interface module (PLIM) node using the *node-id* argument, use the following notation: *rack/PLslot-number/SP*. For example, 0/PL1/SP. PLIM diagnostic tests are supported on the Cisco CRS-1 router.

For more information about running Cisco IOS XR diagnostics, refer to *Cisco IOS XR Diagnostics*.

Task ID

Task ID	Operations

diag	read, write

Examples

The following example shows how to load a diagnostic image:

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

```
RP/0/RP0/CPU0:router(admin)# configure
```

```
RP/0/RP0/CPU0:router(admin-config)# diagnostic schedule location 0/0/CPU0 test all daily 12:30
```

Related Commands

Command	Description
show diagnostic schedule	Displays the diagnostic schedule for a specified location.

R3.5.0 Beta Draft—Cisco Confidential Information

diagnostic start

To run a specified diagnostic test, use the **diagnostic start** command in administration EXEC mode.

diagnostic start location *node-id* **test** {*id* | **all** | **basic** | **non-disruptive**}

Syntax Description	location <i>node-id</i>	Runs diagnostic testing for a specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
	test	Specifies a specific diagnostic test, or all diagnostic tests.
	<i>id</i>	Test ID or list of test IDs, as shown in the show diagnostic content command. Multiple tests can be listed if separated by semicolons (;) as follows: x;y-z (for example: 1; 3-4 or 1;3;4)
	all	Specifies all tests.
	basic	Specifies the basic on-demand test suite [Attribute = B].
	non-disruptive	Specifies the nondisruptive test suite [Attribute = N].

Defaults No default behavior or values

Command Modes Administration EXEC

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **diagnostic start** command to run a diagnostic test on a specified card.

**Note**

To specify a physical layer interface module (PLIM) node using the *node-id* argument, use the following notation: *rack/PLslot-number/SP*. For example, 0/PL1/SP. PLIM diagnostic tests are supported on the Cisco CRS-1 router.

For more information about running Cisco IOS XR diagnostics, refer to *Cisco IOS XR Diagnostics*.

Task ID	Task ID	Operations
	diag	execute

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to run a specified diagnostic test for a specified location:

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

```
RP/0/RP0/CPU0:router(admin)# diagnostic start location 0/0/CPU0 test basic
```

Related Commands

Command	Description
diagnostic stop	Stops a diagnostic test.

R3.5.0 Beta Draft—Cisco Confidential Information

diagnostic stop

To stop the diagnostic testing process on a node, use the **diagnostic stop** command in administration EXEC mode.

diagnostic stop location *node-id*

Syntax Description

location <i>node-id</i>	Stops diagnostic testing for a specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **diagnostic stop** command to stop a diagnostic test on a specified node. The command is used for scheduled tests, a test that is causing errors, or a test that does not finish.

**Note**

To specify a physical layer interface module (PLIM) node using the *node-id* argument, use the following notation: *rack/PLslot-number/SP*. For example, 0/PL1/SP. PLIM diagnostic tests are supported on the Cisco CRS-1 router.

For more information about running Cisco IOS XR diagnostics, refer to *Cisco IOS XR Diagnostics*.

Task ID

Task ID	Operations
diag	execute

Examples

The following example shows how to stop the diagnostic test process:

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

```
RP/0/RP0/CPU0:router(admin)# diagnostic stop location 0/0/CPU0
```

R3.5.0 Beta Draft—Cisco Confidential Information**Related Commands**

Command	Description
diagnostic start	Starts a diagnostic test.

R3.5.0 Beta Draft—Cisco Confidential Information

diagnostic unload

To unload an offline diagnostic image, use the **diagnostic unload** command in administration EXEC mode.

diagnostic unload location *node-id*

Syntax Description

location <i>node-id</i>	Unloads an offline diagnostic image for a specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation. The diagnostic image is unloaded for all modules in the specified slot.

Defaults

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **diagnostic unload** command to unload an offline diagnostic image used for integrated field diagnostics. Unloading the image returns the specified card to service.

Use the **show platform** command to determine if the card has been placed back into service.

For more information about running Cisco IOS XR diagnostics, refer to *Cisco IOS XR Diagnostics*.

Task ID

Task ID	Operations
diag	execute

Examples

The following example shows how to unload a diagnostic image:

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

```
RP/0/RP0/CPU0:router(admin)# diagnostic unload location 0/0/CPU0
```

Related Commands

R3.5.0 Beta Draft—Cisco Confidential Information

Command	Description
diagnostic load	Loads a diagnostic test.
show platform	Displays information and status of each node in the system.

R3.5.0 Beta Draft—Cisco Confidential Information

dsc serial

To define serial ID for a rack, use the **dsc serial** command in administration configuration mode. To remove a serial ID entry from the designated shelf controller (DSC) table, use the **no** form of this command.

dsc serial *serial_Id* **rack** *rack_num*

no dsc serial *serial_Id* **rack** *rack_num*

Syntax Description	<i>serial_Id</i>	Defines a serial ID for a rack. The serial ID is included as an entry in the DSC table. Range is from 0 through 16 characters.
	rack <i>rack_num</i>	Identifies the rack whose ID you are configuring to be the <i>serialId</i> .
	Note	For systems that include two line card chassis and one fabric chassis, the line card chassis IDs are 0 and 1, and the fabric chassis ID is F0.

Defaults No default behavior or values

Command Modes Administration configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	The Task-ID was updated to system.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.
		No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

For more information about identifying and selecting a DSC on a Cisco CRS-1 router, Cisco XR 12000 Series Router, or Cisco CRS-1 Multishelf System, refer to *Cisco IOS XR Getting Started Guide*.

**Note**

The serial ID is the hardware serial number that identifies the chassis.

Use the **show running-config** command to display and verify the defined serial ID for a rack.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	system	read, write

Examples

The following example shows how to define the serial ID for a rack:

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

```
RP/0/RP0/CPU0:router(admin)# configure
```

```
RP/0/RP0/CPU0:router(admin-config)# dsc serial TBC0610991700000 rack 1
```

Related Commands

Command	Description
show dsc	Displays the current DSC configuration for the shelf or for the system.
show running-config	Displays the contents of the currently running configuration or a subset of that configuration.

R3.5.0 Beta Draft—Cisco Confidential Information

env disable

To disable environment monitoring on the chassis, use the **env disable** command in administration configuration mode. To reenable environment monitoring after it has been disabled, use the **no** form of this command.

env disable

no env disable

Syntax Description This command has no arguments or keywords.

Defaults Environment monitoring is enabled.

Command Modes administration configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	No modification.
Release 3.3.0	This command was first supported on the Cisco XR 12000 Series Router. The env disable command was moved from the root-system task ID to the system task ID.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

By default, environment monitoring related to temperature and voltage is enabled on a router running Cisco IOS XR software. If environmental monitoring is disabled, you are not alerted if the router overheats.

Task ID

Task ID	Operations
system	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to disable environment monitoring with the **env disable** command:

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

```
RP/0/RP0/CPU0:router(admin)# configure
```

```
RP/0/RP0/CPU0:router(admin-config)# env disable
```

Related Commands

Command	Description
env power-supply	Enables power supply monitoring on the chassis.

R3.5.0 Beta Draft—Cisco Confidential Information

env power-supply

To enable power supply monitoring on the chassis and set the voltage thresholds for system shutdown and restart, use the **env power-supply** command in administrative configuration mode. To disable the power supply, use the **no** form of this command.

env power-supply [**threshold** {**restart** *voltage* | **shutdown** *voltage*}]

no env power-supply [**threshold** {**restart** *voltage* | **shutdown** *voltage*}]

Syntax Description

threshold	(Optional) Sets the voltage threshold for system shutdown or restart.
restart <i>voltage</i>	Sets the minimum voltage required before the system can be restarted after a shutdown. Replace <i>voltage</i> with the minimum voltage. Range is from 36000 through 44000.
shutdown <i>voltage</i>	Sets the maximum voltage allowed on the system before it automatically shuts down. Replace <i>voltage</i> with the minimum voltage. Range is from 36000 through 44000.

Defaults

Power supply monitoring is disabled.

restart *voltage* = 43500

shutdown *voltage* = 38500

Command Modes

Administrative configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	No modification.
Release 3.3.0	The env power-supply command was moved from the root-system task ID to the system task ID. The threshold { restart <i>voltage</i> shutdown <i>voltage</i> } keyword argument was added to the env power-supply command.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

**Note**

Do not enable power supply monitoring unless the system uses B0 (or greater) power supplies.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	system	read, write

Examples

The following example shows how to disable power supply monitoring with the **no env power-supply** command:

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

```
RP/0/RP0/CPU0:router(admin)# configure
```

```
RP/0/RP0/CPU0:router(admin-config)# no env power-supply
```

The following example shows how to set the maximum voltage allowed on the system before it automatically shuts down to be 43,000 volts:

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

```
RP/0/RP0/CPU0:router(admin)# configure
```

```
RP/0/RP0/CPU0:router(admin-config)# env power-supply threshold shutdown 43000
```

Related Commands	Command	Description
	env disable	Enables environment monitoring on the chassis.

R3.5.0 Beta Draft—Cisco Confidential Information

facility-alarm contacts

To set or unset facilities for processing alarms related to temperature and power supply conditions, use the **facility-alarm contacts** command in administration EXEC mode.

facility-alarm contacts {**all** | **critical** | **major** | **minor**} {**audio** | **both** | **visual**} {**on** | **off**}

Syntax Description

all	Sets the facility alarm contacts so that an audio and visual alarm alerts the user to a facility alarm of any severity.
critical	Sets the facility alarm contacts so that an audio and visual alarm alerts the user to critical facility alarms.
major	Sets the facility alarm contacts so that an audio and visual alarm alerts the user to major facility alarms.
minor	Sets the facility alarm contacts so that an audio and visual alarm alerts the user to minor facility alarms.
audio	Sets the facility alarm contacts so that an audio alarm alerts the user to alarms of the specified severity.
both	Sets the facility alarm contacts so that an audio and visual alarm alerts the user to alarms of the specified severity.
visual	Sets the facility alarm contacts so that a visual alarm alerts the user to alarms of the specified severity.
on	Enables facility alarm contacts configuration.
off	Disables facility alarm contacts configuration.

Defaults

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	root-system	read

Examples

The following example shows how to enable an audio alarm to alert the user when a critical facility-alarm occurs:

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

```
RP/0/RP0/CPU0:router(admin)# configure
```

```
RP/0/RP0/CPU0:router(admin-config)# facility-alarm contacts critical audio on
```

Related Commands	Command	Description
	show facility-alarm contacts	Displays audio and visual facility alarm information for the router.

R3.5.0 Beta Draft—Cisco Confidential Information

hw-module boot override

To place the standby RP into ROM Monitor mode so that you can update the ROMMON software in a single chassis system to Cisco IOS XR Software Release 1.32, use the **hw-module boot override** command in administration configuration mode. To remove an RP from ROM Monitor mode, use the **no** form of this command.

hw-module boot override

no hw-module boot override

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Administration configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Before you can upgrade a single-chassis system to Cisco IOS XR Software Release 3.3.0, you need to first upgrade the ROMMON to Cisco IOS XR Software Release 1.32. If you do not perform this upgrade in a single-chassis system, the standby RP fails to boot and an error message appears. To avoid boot failure, you need to use the **hw-module boot override** command to place the standby RP into ROM Monitor mode, and update the ROMMON software as required.

Use the [show platform](#) command to view a summary of the nodes in the router, including status information.

Task ID

Task ID	Operations
root-system	read, write
root-lr	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to boot the standby RP to upgrade its ROMMON software to Cisco IOS XR Software Release 1.32:

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

```
RP/0/RP0/CPU0:router(admin)# configure
```

```
RP/0/RP0/CPU0:router(admin-config)# hw-module boot override
```

Related Commands

Command	Description
show platform	Displays information and status for each node in the system.

R3.5.0 Beta Draft—Cisco Confidential Information

hw-module location

To configure various hardware attributes for a specific node, or for all nodes installed in the router, use the **hw-module location** command. The syntax and tasks performed by the **hw-module location** command differ, depending on the command mode you are running when you enter the **hw-module location** command.

To reset a specific node or all nodes, or to put a node into maintenance mode, use the **hw-module location** command in EXEC mode as follows:

```
hw-module location node-id {reload {path | warm} | maintenance-mode}
```

To reset a specific node or all nodes, use the **hw-module location** command in administration EXEC mode as follows:

```
hw-module location node-id reload {path | warm}
```

To disable the power, monitor, or shutdown states of the hardware on a specific node, or on all nodes installed in the router, use the **hw-module location** command in administration configuration mode, as follows (on the Cisco XR 12000 Series Router only):

```
hw-module location {node-id {power disable | reset auto disable | shutdown} | all reset auto disable}
```

Syntax Description	<i>node-id</i>	Identifies the node whose hardware attributes you want to configure. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.
	Note	Enter the show platform command to see the location of all nodes installed in the router.
	all	Indicates that you want to configure the hardware attributes for all nodes installed in the router.
	reload	Resets power-cycle, reload hardware, or both on a specific node.
	<i>path</i>	Specifies a specific image you want to download onto the specific node or nodes. Replace <i>path</i> with the TFTP or disk path to the image you want to download.
	warm	Specifies a warm reload of the node.
	maintenance-mode	Bring the node down and puts the node into maintenance mode.
	power disable	Disables the power state on the specified node.
	reset auto disable	Disables the auto monitor state on the specified node.
	shutdown	Disables the shutdown state on the specified node.
	all reset auto disable	Disables the auto monitor state on all nodes installed in the router.

Defaults No default behavior or values

Command Modes EXEC
Administration EXEC

R3.5.0 Beta Draft—Cisco Confidential Information

Administration configuration (Cisco XR 12000 Series Router only)

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.3.0	This command was introduced in EXEC and administration EXEC mode on the Cisco CRS-1.
Release 3.4.0	The maintenance-mode keyword was added in EXEC mode.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

**Note**

By default, the node remains powered until you specify that you want it powered down with the **hw-module location node-id power disable** command.

**Note**

Before reloading nodes on a Cisco CRS-1, we recommend using the **cfs check** command to check the sanity of the configuration file system and attempt to recover from internal inconsistencies. You need to enter the **cfs check** command on each SDR that has nodes impacted by the reload.

Task ID

Task ID	Operations
root-lr	execute (on the Cisco CRS-1 router in EXEC mode) read (on the Cisco XR 12000 Series Router in EXEC mode, administration EXEC mode, and administration configuration mode) write (on the Cisco XR 12000 Series Router in administration configuration mode)
root-system	execute (on the Cisco CRS-1 router in EXEC mode and administration EXEC mode)
sysmgr	execute (on the Cisco XR 12000 Series Router in EXEC mode and administration EXEC mode) read (on the Cisco XR 12000 Series Router in administration configuration mode) write (on the Cisco XR 12000 Series Router in administration configuration mode)

Examples

The following example shows how to reset the hardware on all nodes in the router:

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

```
RP/0/RP0/CPU0:router(admin)# hw-module location all reload
```

R3.5.0 Beta Draft—Cisco Confidential Information

The following example shows how to reset the hardware on a specific node:

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

```
RP/0/RP0/CPU0:router(admin)# hw-module location 0/3/CPU0 reload
```

R3.5.0 Beta Draft—Cisco Confidential Information

hw-module port

To enable a SONET/SDH port to be used for Spatial Reuse Protocol (SRP), use the **hw-module port** command in global configuration mode. To disable SRP and enable the port for POS, use the **no** form of this command.

hw-module port *port-id* **srp** **location** [**preconfigure**] *node-id*

no hw-module port *port-id* **srp** **location** [**preconfigure**] *node-id*

Syntax Description

port-id	Number that identifies the physical port on a line card. Range is from 1 through 3.
srp	Sets the port in Spatial Reuse Protocol (SRP) mode
location	Indicates a specific node location.
preconfigure	(Optional) Specifies the preconfigure option.
	Note Use the preconfigure option only a node has not yet been inserted into the specified location.
node-id	Identifies the location of the node on which you want to enable an SRP port, in the <i>rack/slot/module</i> notation.

Defaults

SRP is disabled on all SONET/SDH ports.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the [show platform](#) command to view a summary of the nodes in the router, including status information.

Task ID

Task ID	Operations
root-lr	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to enable a SONET/SDH port to be used for SRP:

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

```
RP/0/RP0/CPU0:router(config)# hw-module port 1 srp location 0/1/CPU0
```

Related Commands

Command	Description
show platform	Displays information and status for each node in the system.

R3.5.0 Beta Draft—Cisco Confidential Information

hw-module power

To power on a specified line card or disable the node power on feature, use the **hw-module power** command in administration configuration mode. To power off a line card, use the **no** form of this command.

hw-module power [**disable**] **location** *node-id*

no hw-module power [**disable**] **location** *node-id*

Syntax Description

disable	(Optional) Disables the power state
location <i>node-id</i>	Identifies the node you want to power on, or whose node power on feature you want to disable. The <i>node-id</i> argument is expressed in the <i>rack/slot/module</i> notation.

Defaults

Power is on for all nodes.

Command Modes

Administration configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **hw-module power** command is available for line cards only; it is not available for RP cards.

Use the [show platform](#) command to view a summary of the nodes in the router, including status information.

Task ID

Task ID	Operations
root-system	read, write
root-lr	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to power on a line card:

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

```
RP/0/RP0/CPU0:router(admin)# configure
```

```
RP/0/RP0/CPU0:router(admin-config)# hw-module power location 0/1/0
```

The following example shows how to disable the power on feature for a line card:

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

```
RP/0/RP0/CPU0:router(admin)# configure
```

```
RP/0/RP0/CPU0:router(admin-config)# hw-module power disable location 0/SM3/SP
```

Related Commands

Command	Description
show platform	Displays information and status for each node in the system.

R3.5.0 Beta Draft—Cisco Confidential Information

hw-module power disable

To disable the node power on feature on a specific line card, use the **hw-module power disable** command in administration configuration mode. To reenable the node power on feature on a line card, use the **no** form of this command.

hw-module power disable location *node-id*

no hw-module disable location *node-id*

Syntax Description	location <i>node-id</i> Identifies the node you whose power on feature you want to disable. The <i>node-id</i> argument is expressed in the <i>rack/slot/module</i> notation.	
Defaults	Power is on for all nodes.	
Command Modes	Administration configuration	
Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .	
	Use the show platform command to view a summary of the nodes in the router, including status information.	
	The hw-module power disable command is available for line cards only; it is not available for RP cards.	
Task ID	Task ID	Operations
	sysmgr	read, write
	root-lr	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to disable the node power on feature on a line card:

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

```
RP/0/0/CPU0:router(admin)# configure
```

```
RP/0/0/CPU0:router(admin-config)# hw-module power disable location 0/0/CPU0
```

Related Commands

Command	Description
show platform	Displays information and status for each node in the system.

R3.5.0 Beta Draft—Cisco Confidential Information

hw-module reset auto

To reset a specific node, use the **hw-module reset auto** command in administration configuration mode. To disable the reset feature on a specific node, use the **no** form of this command.

hw-module reset auto [**disable**] **location** *node-id*

no hw-module reset auto [**disable**] **location** *node-id*

Syntax Description	disable	(Optional) Disables the node reset feature on the specified node.
	location <i>node-id</i>	Identifies the node you want to reload. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults	The node reset feature is enabled for all nodes.

Command Modes	Administration configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	The hw-module reset auto command is used to reload Cisco IOS XR software on a specific node. The node reloads with the current running configuration and active software set for that node.

Task ID	Task ID	Operations
	root-system	read, write
	root-lr	read, write

Examples	The following example shows how to reload a node:
	RP/0/RP0/CPU0:router # admin
	RP/0/RP0/CPU0:router(admin)# configure
	RP/0/RP0/CPU0:router(admin-config)# hw-module reset auto location 0/2/CPU0
	RP/0/RP0/CPU0:router# RP/0/RP0/CPU0:Apr 2 22:04:43.659 : shelfmgr[294]: %S

R3.5.0 Beta Draft—Cisco Confidential Information

HELFMGR-3-USER_RESET : Node 0/2/CPU0 is reset due to user reload request

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	hw-module power	Powers on a specified node.
	hw-module shutdown	Administratively shuts down a specified node.

R3.5.0 Beta Draft—Cisco Confidential Information

hw-module reset auto disable

To disable the node reset feature on a specific node, use the **hw-module reset auto disable** command in administration configuration mode. To reenable the reset feature on a specific node, use the **no** form of this command.

hw-module reset auto disable location *node-id*

no hw-module reset auto disable location *node-id*

Syntax Description	disable	(Optional) Disables the node reset feature on the specified node.
	location <i>node-id</i>	Identifies the node you want to reload. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults The node reset feature is enabled for all nodes.

Command Modes Administration configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	sysmgr	read, write
	root-lr	read, write

Examples The following example shows how to disable the reload feature on a node:

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

```
RP/0/0/CPU0:router(admin)# configure
```

```
RP/0/0/CPU0:router(admin-config)# hw-module reset auto disable location 0/0/CPU0
```


R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	hw-module power	Powers on a specified node.
	hw-module shutdown	Administratively shuts down a specified node.

R3.5.0 Beta Draft—Cisco Confidential Information

hw-module shutdown

To administratively shut down a specific node, use the **hw-module shutdown** command in administration configuration mode. To return a node to the up state, use the **no** form of this command.

hw-module shutdown location *node-id*

no hw-module shutdown location *node-id*

Syntax Description	location <i>node-id</i>	Identifies the node you want to shut down. The <i>node-id</i> argument is expressed in the <i>rack/slot/module</i> notation.

Defaults	Nodes are in the up state.

Command Modes	Administration configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1 router.
	Release 3.0	No modification.
	Release 3.2	No modification.
	Release 3.3.0	This command was supported on the Cisco XR 12000 Series Router. This command was modified from the hw-module node shutdown command. The node keyword was replaced by the location keyword, which was moved to the end of the command string.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Nodes that are shut down still have power, but cannot load or operate Cisco IOS XR software.

**Note**

Route processors (RPs) cannot be administratively shut down.

Enter the **show platform** command in EXEC mode to display the results of the **hw-module shutdown** command.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	root-system	read, write (on the Cisco CRS-1)
	sysmgr	read, write (on the Cisco XR 12000 Series Router)
	root-lr	read, write

Examples

The following example shows how to administratively shut down the node 0/2/CPU0:

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

```
RP/0/RP0/CPU0:router(admin)# configure
```

```
RP/0/RP0/CPU0:router(admin-config)# hw-module shutdown location 0/2/CPU0
```

The following example shows how to bring up a node using the **no** form of the **hw-module shutdown** command:

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

```
RP/0/RP0/CPU0:router(admin)# configure
```

```
RP/0/RP0/CPU0:router(admin-config)# no hw-module shutdown location 0/2/CPU0
```

Related Commands	Command	Description
	hw-module power	Powers on a specified node. (Cisco CRS-1 only)
	hw-module power disable	Disables the node power on feature on a specific node. (Cisco XR 12000 Series Router only)
	hw-module reset auto	Reloads a specified node. (Cisco CRS-1 only)
	hw-module reset auto disable	Disables the node reset feature on a specific node. (Cisco XR 12000 Series Router only)

R3.5.0 Beta Draft—Cisco Confidential Information

hw-module subslot reload

To reload Cisco IOS XR software on a specific subslot, use the **hw-module subslot reload** command in EXEC mode.

hw-module subslot *subslot-id* **reload**

Syntax Description

<i>subslot-id</i>	Specifies the subslot to be restarted. The <i>subslot-id</i> argument is entered in the <i>rack/slot/subslot</i> notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

This command reloads Cisco IOS XR software on the specified shared port adapter (SPA) and restarts the SPA interfaces. The SPA reloads with the current running configuration and active software set for the SPA.

Task ID

Task ID	Operations
root-lr	read, write

Examples

The following example shows how to restart the SPA in slot 2, subslot 1:

```
RP/0/RP1/CPU0:router# hw-module subslot 0/2/1 reload
```

Related Commands

Command	Description
hw-module subslot power-cycle	Power-cycles a SPA module.

R3.5.0 Beta Draft—Cisco Confidential Information

hw-module subslot shutdown

To administratively shut down a specific shared port adapter (SPA), use the **hw-module subslot shutdown** command in global configuration mode. To return a SPA to the up state, use the **no** form of this command.

hw-module subslot *subslot-id* **shutdown** [**powered** | **unpowered**]

no hw-module subslot *subslot-id* **shutdown**

Syntax Description

subslot-id	Specifies the subslot to be shut down. The <i>subslot-id</i> argument is entered in the <i>rack/slot/subslot</i> notation.
powered	(Optional) Retains power to the specified subslot.
unpowered	(Optional) Powers down completely the specified subslot.

Defaults

Shutdown is powered if no option is specified.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

This command administratively shuts down the SPA in the specified subslot. Subslots that are shut down still have power, but cannot load or operate Cisco IOS XR software.

Task ID

Task ID	Operations
root-lr	read, write

Examples

The following example shows how to shut down the SPA in subslot 1 of the SIP in slot 2:

```
RP/0/RP1/CPU0:router# configure
```

```
RP/0/RP1/CPU0:router(config)# hw-module subslot 0/2/1 shutdown powered
```

R3.5.0 Beta Draft—Cisco Confidential Information**Related Commands**

Command	Description
shutdown	Disables an interface (forces an interface to be administratively down).

R3.5.0 Beta Draft—Cisco Confidential Information

led mode

To specify LED mode parameters, use the **led mode** command in administration configuration mode. To return the LED mode to the default settings, use the **no** form of this command.

led mode {**default** | **blink** | **scroll**} {**lock** | **unlock**} *led-display-text* **location** *node-id*

no led mode {**default** | **blink** | **scroll**} {**lock** | **unlock**} *led-display-text* **location** *node-id*

Syntax Description

default	Sets the LED mode to the default fixed display.
blink	Sets the LED mode to blink alpha display.
scroll	Sets the LED mode to scroll alpha display.
lock	Locks LED so the display message cannot be changed.
unlock	Unlocks the LED and allows the display message to be changed.
<i>led-display-text</i>	Specifies the message shown on the card in the LED display.
location <i>node-id</i>	Specifies the LED mode parameters for the designated node. The <i>node-id</i> argument is expressed in the <i>rack/slot/module</i> notation.

Defaults

led-display-text: IOX-RUN (except for active and standby route processors (RPs), which display “ACTV RP” and “STBY RP”)

Command Modes

Administration configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	No modification.
Release 3.3.0	This command was first supported on the Cisco XR 12000 Series Router. The led mode command was moved from the root-system task ID to the system task ID.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **led mode** command to specify the message to be displayed on the LED display on the card.

Use the **no** form of the **led mode** command to reset the message to the default setting. The default message is “IOX-RUN,” except for the RP, which has “ACTV RP” for the active RP, and “STBY RP” for the standby RP.

R3.5.0 Beta Draft—Cisco Confidential Information**Task ID**

Task ID	Operations
system	read, write

Examples

The following example shows the LED display message being set to “SW-RUN”:

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

```
RP/0/RP0/CPU0:router(admin)# configure
```

```
RP/0/RP0/CPU0:router(admin-config)# led mode default unlock SW-RUN location 0/0/SP
```

Related Commands

Command	Description
show led	Lists the LED locations on the router.

R3.5.0 Beta Draft—Cisco Confidential Information

ping (administration EXEC)

To send internal echo messages from one node to another, use the **ping** command in administration EXEC mode.

ping { **control-eth** | **fabric** } **location** *node-id* [**count** *pings* | **interval** *milliseconds* | **pattern** **random** | **retries** *number* | **size** *payload_size* | **timeout** *seconds*]

Syntax Description	
control-eth	Specifies a control ethernet ping test.
fabric	Specifies a fabric ping test.
count <i>pings</i>	(Optional) Number of pings to send each time the command is run. The test reports results and statistics after all pings have been sent and received (or timed out). Range is from 0 through 4294967295.
interval <i>milliseconds</i>	(Optional) Hold-off time between each ping in milliseconds. Range is from 0 through 4294967295. The total test time will be as follows: $(\text{count}-1) * (\text{RTT} + \text{interval}) + \text{RTT}$ RTT = Round Trip Time for the ping.
pattern random	(Optional) Specifies a data pattern for the ping packet payload.
retries <i>number</i>	(Optional) Maximum number of times a failed ping transmission is sent before the packet transmission is considered a failure. Range is from 0 through 4294967295. Note Packet transmission failure is usually an indication of a server software transient. In this case, Cisco recommends that you run the ping command again.
size <i>payload_size</i>	(Optional) Specifies the payload size for each ping packet size. Range is from 0 through 4294967295 bytes. The maximum payload size allowed may be limited, depending on the transport type that is used (fabric or control-ethernet).
timeout <i>seconds</i>	(Optional) Specifies the maximum time to wait for response to a ping. Range is from 0 through 4294967295 seconds. If a ping does not receive a response before the configured timeout expires, the ping statistics reflect it as a discrepancy between the “Sent:” and “Rec'd:” packet count, and the test is considered failed. Because of this, Cisco recommends that you do not set the timeout to 0.

Defaults No default behavior or values

Command Modes Administration EXEC

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1.

R3.5.0 Beta Draft—Cisco Confidential Information

Release	Modification
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When you enter the **ping** command, a ping is sent to the node at the specified location. The received response is compared byte-by-byte to the sent packet. If a ping response is not received before the specified time-out, or if the ping response does not match the transmitted ping, the ping is considered failed.

A node that is unreachable or intermittently working impacts the total run time for the test as follows:

$$(\text{received\_packet\_count} * \text{RTT} + \text{lost\_packet\_count} * \text{timeout} + (\text{count}-1) * \text{interval})$$
Task ID

Task ID	Operations
diag	execute

Examples

The following example shows sample output from a control-ethernet ping to an SP node in slot 0/0:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# ping control-eth location 0/0/SP count 5

Src node:          529 : 0/RP0/CPU0
Dest node:          0 : 0/0/SP
Local node:         529 : 0/RP0/CPU0
Packet cnt:         5  Packet size: 128  Payload ptn type: default (0)
Hold-off (ms):     300  Time-out(s):    2  Max retries: 5
Destination node has MAC addr 5246.4800.0000

Running CE node ping.
Please wait...
Src: 529:, Dest: 0, Sent: 5, Rec'd: 5, Mismatched: 0
Min/Avg/Max RTT: 0/200/1000
CE node ping succeeded for node: 0
```

The following example shows a fabric ping from the active RP to the active RP. In this example, the ping contains 72 packets of 1 kilobyte each. This command performs a good coverage test of the entire switch fabric:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# ping fabric location 0/RP0/CPU0 count 72 size 1024

Src node:          529 : 0/RP0/CPU0
Dest node:          529 : 0/RP0/CPU0
Local node:         529 : 0/RP0/CPU0
Packet cnt:         72  Packet size: 1024  Payload ptn type: default (0)
Hold-off (ms):     300  Time-out(s):    2  Max retries: 5

Running Fabric node ping.
Please wait...
Src: 529:, Dest: 529, Sent: 72, Rec'd: 72, Mismatched: 0
Min/Avg/Max RTT: 3000/3013/4000
```

R3.5.0 Beta Draft—Cisco Confidential Information

Fabric node ping succeeded for node: 529

The following example shows a ping to a control Ethernet node that has a problem or does not exist:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# ping control-eth location 0/1/CPU0 count 3
```

```
Src node:          529   : 0/RP0/CPU0
Dest node:          17   : 0/1/CPU0
Local node:         529   : 0/RP0/CPU0
Packet cnt:         3    Packet size: 128 Payload ptn type: default (0)
Hold-off (ms):     300   Time-out(s): 2   Max retries: 5
Destination node has MAC addr 5246.4800.0011
```

Running CE node ping.

Please wait...

Src: 529:, Dest: 17, Sent: 3, Rec'd: 0, Mismatched: 0

Requested ping failed for node: 17

R3.5.0 Beta Draft—Cisco Confidential Information

redundancy reddrv

To enable and configure route processor (RP) and system controller (SC) redundancy, use the **redundancy reddrv** command in global configuration mode.

redundancy reddrv *rackID* [**prefer-slot** {32 | 33}]

Syntax Description

rackID Identifies the rack on which you want to enable RP or SC redundancy. Range is from 1 through 127.

prefer-slot {32 | 33} (Optional) Sets a slot number as the preferred active RP or SC. Possible slot numbers are 32 or 33.

**Note**

Although the Cisco CRS-1 chassis has only 16 slots, keep in mind that the internal slot numbers for RP0 and RP1 are 32 and 33, as specified by the **prefer-slot** keyword.

Defaults

RP redundancy is enabled, and the lower-numbered slot is the default primary RP.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	No modification.
Release 3.3.0	The disable keyword was removed from the redundancy reddrv command.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
root-lr	read, write
system	read, write

Examples

The following example shows how to enable redundancy on a rack that is identified by the number 1:

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

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(config)# redundancy reddrv 1
```

Related Commands

Command	Description
show screddrv	Displays SC redundancy information.

R3.5.0 Beta Draft—Cisco Confidential Information

redundancy switchover

To cause the primary (active) route processor (RP) to fail over to the redundant standby RP, use the **redundancy switchover** command in EXEC mode. To disable the forced failover, use the **no** form of this command.

redundancy switchover [**location** *node-id*]

no redundancy switchover [**location** *node-id*]

Syntax Description	location <i>node-id</i> (Optional) Specifies the primary RP on which to force a failover. The <i>node-id</i> argument is expressed in the <i>rack/slot/module</i> notation.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	No modification.
	Release 3.3.0	This command was first supported on the Cisco XR 12000 Series Router. The redundancy switchover command was moved from the system task ID to the root-lr task ID.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **redundancy switchover** command to trigger a failover from the primary RP to the standby RP. When the **redundancy switchover** command is issued, the running (committed) configuration is automatically saved and loaded during failover, and the standby RP becomes the active primary RP, while the original primary RP becomes the standby RP.

**Note**

The **redundancy switchover** command can be issued only if the standby RP is in the ready state. Enter the **show redundancy** command to view the status of the RPs.

Task ID

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Operations
root-lr	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows partial output for a successful redundancy switchover operation:

```
RP/0/RP0/CPU0:router# show redundancy

Redundancy information for node 0/RP0/CPU0:
=====
Node 0/RP0/CPU0 is in ACTIVE role
Partner node (0/RP1/CPU0) is in STANDBY role
Standby node in 0/RP1/CPU0 is ready

Reload and boot info
-----
RP reloaded Tue Mar 28 09:02:26 2006: 5 hours, 41 minutes ago
Active node booted Tue Mar 28 09:02:56 2006: 5 hours, 41 minutes ago
Last switch-over Tue Mar 28 09:09:26 2006: 5 hours, 34 minutes ago
Standby node boot Tue Mar 28 09:10:37 2006: 5 hours, 33 minutes ago
Standby node last went not ready Tue Mar 28 09:25:49 2006: 5 hours, 18 minutes
go
Standby node last went ready Tue Mar 28 09:25:51 2006: 5 hours, 18 minutes ago
There has been 1 switch-over since reload
....
RP/0/RP0/CPU0:router# redundancy switchover

Initializing DDR SDRAM...found 2048 MB
Initializing ECC on bank 0
...
Turning off data cache, using DDR for first time

Initializing NVRAM...
Testing a portion of DDR SDRAM ...done
Reading ID EEPROMs ...
Initializing SQUID ...
Initializing PCI ...

PCI0 device[1]: Vendor ID 0x10ee

Configuring MPPs ...
Configuring PCMCIA slots ...
--More--
```

If the standby RP is not in ready state, the failover operation is not allowed. The following example shows output for a failed redundancy switchover attempt:

```
RP/0/RP0/CPU0:router# show redundancy

This node (0/RP0/CPU0) is in ACTIVE role
Partner node (0/RP1/CPU0) is in UNKNOWN role

RP/0/RP0/CPU0:router# redundancy switchover

Standby card not running; failover disallowed.
```

Related Commands

Command	Description
show redundancy	Displays the redundancy status of the route processor (RP) nodes.

R3.5.0 Beta Draft—Cisco Confidential Information

show diag

To display details about the hardware and software on each node in a router, use the **show diag** command in the appropriate mode.

In EXEC mode.

```
show diag [node-id] [details | eeprom-info | power-regs | summary]
```

In administrative EXEC mode:

```
show diag [node-id] [[chassis | fans | power-supply] [eeprom-info] | details | summary]
```

Syntax Description	
<i>node-id</i>	(Optional) Identifies the node whose information you want to display. The <i>node-id</i> argument is expressed in the <i>rack/slot/module</i> notation. Follow the <i>node-id</i> argument with one of the following optional keywords to specify specific test results: details eeprom-info power-regs summary
details	(Optional) Displays detailed diagnostics information for the current node.
eeprom-info	(Optional) Displays field diagnostics results from the EEPROM.
power-regs	(Optional) Displays field diagnostics results from the power registers.
summary	(Optional) Displays summarized diagnostics results for all nodes in the system.
chassis-info	(Optional) Displays information about the chassis.
fans	(Optional) Displays information about the fans tray.
power-supply	(Optional) Displays information about the power supply.

Defaults Diagnostics for all nodes installed in the router are displayed.

Command Modes EXEC
Administrative EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	The show diag command was modified to display the last diagnostic result for a card.
	Release 3.3.0	The chassis and details keywords were removed from the show diag command.

R3.5.0 Beta Draft—Cisco Confidential Information

Release	Modification
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **show diag** command displays detailed information on the hardware components for each node, and on the status of the software running on each node.

Task ID

Task ID	Operations
sysmgr	read

Examples

The following example shows partial sample output from the **show diag details** command on a Cisco CRS-1 router:

```
RP/0/RP1/CPU0:router# show diag details

NODE 0/0/SP : MSC(SP)
  MAIN:  board type 500060
         0-0-00 rev 00
         dev N/A
         S/N SAD072102RS
  PCA:   73-7648-04 rev 08
  PID:   rev 00
  VID:   V00
  CLEI:
  ECI:   0
Board State : IOS-XR RUN
PLD:   Motherboard: 0x0025, Processor: 0xda13, Power: N/A
MONLIB: QNXFFS Monlib Version 3.0
ROMMON: Version 1.19(20040603:013227) [CRS-1 ROMMON]
SPEED: OSC Speed: 100 Mhz, CPU Speed: 800 Mhz
        BUS Speed: 100 Mhz, MEM Speed: 100 Mhz
MEM Size: 2048 Mbytes
RMA:   Test Hist: ab, RMA#: 00-00-00, RMA Hist: 00
DIAGNOSTICS RESULTS:
  ENTRY 1: 0
    TIMESTAMP: 00/00/0000 00:00:00
    VERSION: v0.0
    PARAM1: 0      PARAM2: n/a
    TESTNUM: 0
    RESULT: 0 (PASS)
    ERRCODE: 0
  ENTRY 2: 0
    TIMESTAMP: 00/00/0000 00:00:00
    VERSION: v0.0
    PARAM1: 0      PARAM2: n/a
    TESTNUM: 0
    RESULT: 0 (PASS)
    ERRCODE: 0
  ENTRY 3: 0
    TIMESTAMP: 00/00/0000 00:00:00
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

VERSION: v0.0
PARAM1: 0      PARAM2: n/a
TESTNUM: 0
RESULT: 0 (PASS)
ERRCODE: 0
--More--

```

Table 1 describes the significant fields shown in the display.

Table 1 *show diag Field Descriptions*

Field	Description
MAIN	Provides the following general information about the hardware: - Board type - Revision - Device identifier - S/N
PCA	Cisco PCA ¹ hardware and revision number.
PID	Displays the PID ² revision for the specified node.
VID	Displays the VID ³ for the specified node.
CLEI	Displays the CLEI ⁴ for the specified node.
ECI	Displays the ECI ⁵ for the specified node.
Board State	Displays the current software on the board (in this case, Cisco IOS XR software) and whether or not the board is running.
PLD	Displays the information about the following PLD ⁶ components on the current module: - Processor - Power - MONLIB
SPEED	Displays speed information for the various components of the specified node, in Mhz.
MEM Size	Displays the memory size of the specified node, in megabytes.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 1** *show diag Field Descriptions (continued)*

Field	Description
RMA	Displays RMA ⁷ information for the specified node.
DIAGNOSTICS RESULTS	Provides the following information about the last diagnostics test that was run on the specified node: - ENTRY 1 - TIMESTAMP—Time stamp for the last diagnostic test that was run on the node. - VERSION - PARAM1 - PARAM2 - TESTNUM—Identifies the test that was run on the node. - RESULT—Displays whether the last diagnostic test passed or failed. - ERRCODE

1. printed circuit assembly
2. product identifier
3. version identifier
4. common language equipment identifier
5. equipment catalog item
6. programmable logic device
7. returned material adjustment

Related Commands

Command	Description
show platform	Displays information and status for each node in the system.
show version	Displays details on the hardware and software status of the system.

R3.5.0 Beta Draft—Cisco Confidential Information

show diags

To display details about the hardware and software on each node in a router, use the **show diags** command in EXEC mode or Administration EXEC mode.

show diags [*slot* [**details** | **summary**] | **chassis-info** | **details** | **summary**]

Syntax Description

<i>slot</i>	Identifies the slot that hosts the node on which you want to run diagnostics. Replace <i>slot-number</i> with a slot number. Range is from 0 through 22. To display detailed diagnostics information for the slot, follow the <i>slot</i> argument with the details keyword. To display summarized diagnostics results for the slot, follow the <i>slot</i> argument with the summary keyword.
details	(Optional) Displays detailed diagnostics information for the current node.
summary	(Optional) Displays summarized diagnostics results for all nodes in the system.
chassis-info	(Optional) Displays information about the chassis.

Defaults

Diagnostics for all nodes installed in the router are displayed.

Command Modes

EXEC
Administration EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.0	No modification.
Release 3.2	No modification.
Release 3.3.0	The chassis-info keyword was added to the show diags command syntax on the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **show diags** command displays detailed information on the hardware components for each node, and on the status of the software running on each node.

Task ID

Task ID	Operations
sysmgr	read

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows sample output from the **show diags** command on a Cisco XR 12000 Series Router. In this example, the **show diags** command is entered without any of the optional parameters. Diagnostic test results are displayed for all nodes in the router:

```
RP/0/0/CPU0:router# show diags

SLOT 0 (RP/LC 0 ): Route Processor
  MAIN: type 19, 800-2427-01 rev J0
        Deviation: 0
        HW config: 0xFF SW key: FF-FF-FF
  PCA: 73-2170-03 rev G0 ver 3
        Design Release 1.4 S/N CAB040879NN
  MBUS: MBUS Agent (1) 73-2146-07 rev B0 dev 0
        HW version 1.2 S/N CAB040877IM
        Test hist: 0xFF RMA#: FF-FF-FF RMA hist: 0xFF
  DIAG: Test count: 0xFFFFFFFF Test results: 0xFFFFFFFF
  FRU: Linecard/Module: GRP=
        Route Memory: MEM-GRP-512=
  MBUS Agent Software version 1.100 (RAM) (ROM version is 2.9)
  ROM Monitor version 181 (old numbering scheme)
  Primary clock is CSC 1
  Board State is IOS Running ACTIVE (ACTV RP )
  Insertion time: 00:00:04 (5d01h ago)
  DRAM size: 536870912 bytes
```

Table 2 describes the significant fields shown in the display.

Table 2 *show diags* Field Descriptions

Field	Description
SLOT	Physical slot number of the line card.
MAIN	General information about the hardware.
PCA	Cisco PCA ¹ hardware and revision number.
MBUS	Provides version information for the Mbus agent.
DIAG	Results of the last diagnostics test, in hexadecimal format.
FRU	Information about the FRUs ² associated with the nodes that are installed in the router.
MBUS Agent Software version	Mbus agent software version currently running on the router.
ROM monitor version	Version of monitor library used by ROMMON.
Primary clock	Primary clock source configured on the router.
Board State	Current software on the board (in this case, Cisco IOS XR software), and whether or not the board is running.
Insertion time	Time at which the last diagnostics test was executed.
DRAM size	DRAM ³ size in bytes.

1. protection channel access

2. Field-replaceable units

3. dynamic random-access memory

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show platform	Displays information and status for each node in the system.
	show version	Displays details on the hardware and software status of the system.

R3.5.0 Beta Draft—Cisco Confidential Information

show diagnostic bootup level

To display the current diagnostic bootup level, use the **show diagnostic bootup level** command in EXEC mode.

show diagnostic bootup level location *node-id*

Syntax Description

location <i>node-id</i>	Specifies a card. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

**Note**

There are no bootup diagnostic tests available in Release 3.4. Both the **minimal** and **complete** bootup diagnostic test levels contain no tests.

Use the **show diagnostic bootup level** command to display the current diagnostic bootup level for a specified card.

Task ID

Task ID	Operations
diag	read

Examples

The following example shows how to display the current diagnostic bootup level for 0/1/cpu0:

```
RP/0/RP0/CPU0:router(admin)# show diagnostic bootup level location 0/1/cpu0
```

```
Current bootup diagnostic level for LC 0/1/CPU0: minimal
```

Related Commands

R3.5.0 Beta Draft—Cisco Confidential Information

Command	Description
diagnostic bootup level	Specifies the diagnostic bootup level.

R3.5.0 Beta Draft—Cisco Confidential Information

show diagnostic content

To display test information including test ID, test attributes, and supported coverage test levels for each test and for all components, use the **show diagnostic content** command in administration EXEC mode.

show diagnostic content location *node-id*

Syntax Description

location <i>node-id</i>	Displays the diagnostic content for a specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	The command output has been modified.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show diagnostic content** command to display diagnostic test information for a specific location. The test information includes the supported tests and attributes.

For more information about running Cisco IOS XR diagnostics, refer to *Cisco IOS XR Diagnostics*.

Task ID

Task ID	Operations
diag	read

Examples

The following example shows how to display the test information for a specified location:

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

```
RP/0/RP0/CPU0:router(admin)# show diagnostic content location 0/0/CPU0
```

```
LC 0/0/CPU0:
```

```
Diagnostics test suite attributes:
```

```
  M/C/* - Minimal bootup level test / Complete bootup level test / NA
```

```
  B/* - Basic ondemand test / NA
```

```
  P/V/* - Per port test / Per device test / NA
```

```
  D/N/* - Disruptive test / Non-disruptive test / NA
```

R3.5.0 Beta Draft—Cisco Confidential Information

S/* - Only applicable to standby unit / NA
 X/* - Not a health monitoring test / NA
 F/* - Fixed monitoring interval test / NA
 E/* - Always enabled monitoring test / NA
 A/I - Monitoring is active / Monitoring is inactive

ID	Test Name	Attributes	Test Interval (day hh:mm:ss.ms)	Thre- shold
1)	ControlEthernetPingTest	-----> *B*N****I	001 00:00:00.000	1
2)	SelfPingOverFabric	-----> *B*N****I	001 00:00:00.000	1

Table 3 describes the significant fields shown in the display.

Table 3 *show diagnostic content Field Descriptions*

Field	Description
M/C/* - Minimal bootup level test / Complete bootup level test / NA	Minimal bootup test or complete bootup test.
B/* - Basic ondemand test / NA	Basic on-demand test.
P/V/* - Per port test / Per device test / NA	Test is per port or device.
D/N/* - Disruptive test / Non-disruptive test / NA	Test is disruptive or nondisruptive.
S/* - Only applicable to standby unit / NA	Test is available for standby node only.
X/* - Not a health monitoring test / NA	Test is not a health-monitoring test.
F/* - Fixed monitoring interval test / NA	Test is a fixed monitoring interval test.
E/* - Always enabled monitoring test / NA	Test is an always enabled monitoring test.
A/I - Monitoring is active / Monitoring is inactive	Test is active or inactive.
ID	ID of the test.
Test Name	Name of the test.
Attributes	Attributes for the test.
Test Interval	Interval of the test.
Threshold	Failure threshold of the text.

Related Commands

Command	Description
diagnostic bootup level	Specifies the diagnostic bootup level.
diagnostic load	Loads a diagnostic test.
diagnostic monitor interval	Specifies the diagnostic test interval.
diagnostic unload	Specifies the test failure threshold.

R3.5.0 Beta Draft—Cisco Confidential Information

Command	Description
diagnostic schedule	Schedules a diagnostic test.
diagnostic start	Starts a diagnostic test.

R3.5.0 Beta Draft—Cisco Confidential Information

show diagnostic result

To display diagnostic test results, use the **show diagnostic result** command in administration EXEC mode.

show diagnostic result location *node-id* [**test** {*id* | **all**}] [**detail**]

Syntax Description	location <i>node-id</i>	Displays the diagnostic test results for a specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
	test { <i>id</i> all }	(Optional) Specifies diagnostic test selection. The following test selections are available: <i>id</i>—Test ID or list of test IDs, as shown in the show diagnostic content command. Multiple tests can be listed if separated by semicolons (;) as follows: - x;y-z (for example: 1; 3-4 or 1;3;4) all—Specifies all tests.
	detail	(Optional) Specifies detailed results.

Defaults	No default behavior or values

Command Modes	Administration EXEC

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1.
	Release 3.4.0	Current bootup diagnostic level display output was added.
	Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show diagnostic result** command to display diagnostic results for a specific location.

For more information about running Cisco IOS XR diagnostics, refer to *Cisco IOS XR Diagnostics*.

Task ID	Task ID	Operations
	diag	read

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to display detailed diagnostic test results:

```
RP/0/RP0/CPU0:router(admin)# show diagnostic result location 0/3/CPU0 test 1 detail
```

Test results: (. = Pass, F = Fail, U = Untested)

```
1 ) Control Ethernet Ping Test -----> .
   Error code -----> 0 (DIAG_SUCCESS)
   Total run count -----> 1
   Last test execution time -----> Thu Aug 11 18:13:38.918 2005
   First test failure time -----> n/a
   Last test failure time -----> n/a
   Last test pass time -----> Thu Aug 11 18:13:38.918 2005
   Total failure count -----> 0
   Consecutive failure count -----> 0
```

Table 4 describes the significant fields shown in the display.

Table 4 *show diagnostic result Field Descriptions*

Field	Description
Test results:	Test result options: • P—Pass • F—Fail • U—Untested
Error code	Code for the error. DIAG_SUCCESS is indicated if there were no code errors. DIAG_FAILURE is indicated for any failure. DIAG_SKIPPED is indicated if the test was stopped.
Total run count	Number of times the test has run.
Last test execution time	Last time the test was run.
First test failure time	First time the test failed to run.
Last test failure time	Last time the test failed to run.
Last test pass time	Last time the test passed.
Total failure count	Number of times the test has failed.
Consecutive failure count	Number of consecutive times the test has failed.

Related Commands

Command	Description
diagnostic load	Loads a diagnostic test.
diagnostic schedule	Schedules a diagnostic test.
diagnostic start	Starts a diagnostic test.

R3.5.0 Beta Draft—Cisco Confidential Information

show diagnostic schedule

To display the current scheduled diagnostic tasks, use the **show diagnostic schedule** command in administration EXEC mode.

show diagnostic schedule location *node-id*

Syntax Description	location <i>node-id</i>	Displays the diagnostic schedule for a specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults	No default behavior or values

Command Modes	Administration EXEC

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the show diagnostic schedule command to display schedule diagnostic tasks for a specific location. For more information about running Cisco IOS XR diagnostics, refer to <i>Cisco IOS XR Diagnostics</i>.

Task ID	Task ID	Operations
	diag	read

Examples	The following example shows how to display scheduled diagnostic tasks: <pre>RP/0/RP0/CPU0:router# admin RP/0/RP0/CPU0:router(admin)# show diagnostic schedule location 0/3/CPU0</pre> Current Time = Tue Sep 27 12:41:24 2005 Diagnostic for LC 0/3/CPU0: Schedule #1: To be run daily 14:40 Test ID(s) to be executed: 1 .

R3.5.0 Beta Draft—Cisco Confidential Information

Table 5 describes the significant fields shown in the display.

Table 5 *show diagnostic schedule Field Descriptions*

Field	Description
Current Time	Current system time.
Diagnostic for	Card for which the diagnostic is scheduled.
Schedule	Schedule number.
To be run	Time at which the diagnostics are scheduled to run.
Test ID(s) to be executed	Tests to be run at scheduled time.

Related Commands

Command	Description
diagnostic schedule	Schedules a diagnostic test.

R3.5.0 Beta Draft—Cisco Confidential Information

show dsc

To display the current designated shelf controller (DSC) configuration for the shelf or for the system, enter the **show dsc** command in administration EXEC mode.

```
show dsc [all | mine | location {node-id}]
```

Syntax Description	all	(Optional) Displays DSC information from all available nodes in the system.
	mine	(Optional) Displays information about the current DSC.
	location <i>node-id</i>	(Optional) Displays DSC information for a specific node. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.

Defaults	No default behavior or values

Command Modes	Administration EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	The node keyword was replaced by the location keyword. The show dsc command was moved from the root-system task ID to the system task ID.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. For more information about identifying and selecting a DSC on a Cisco CRS-1, Cisco XR 12000 Series Router, or Cisco CRS-1 Multishelf System, refer to <i>Cisco IOS XR Getting Started Guide</i>.

Task ID	Task ID	Operations
	system	read

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following is sample output from the **show dsc mine** command on a Cisco CRS-1:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# show dsc mine
```

NODE	ROLE	PRIORITY	TBEACON	PRESENT
0/0/CPU0	DSC	3	2000	YES

[Table 6](#) describes the significant fields shown in the display.

Table 6 *show dsc Field Descriptions*

Field	Description
NODE	Location of the node, in the <i>rack/slot/module</i> notation.
ROLE	Role this node is performing. Because the show dsc command shows the DSC node, the ROLE is always DSC.
PRIORITY	DSC priority assigned to this node.
TBEACON	Current DSC beacon timeout value.
PRESENT	Indicates whether the node is present in the slot.
SERIAL ID	Serial ID assigned to this node.

The following is sample output from the **show dsc all** command on a Cisco XR 12000 Series Router:

```
RP/0/0/CPU0:router(admin)# show dsc all
```

NODE	ROLE	PRIORITY	TBEACON	PRESENT
0/RP1/CPU0	DSC	DEFAULT	500	YES

[Table 6](#) describes the significant fields shown in the display.

Related Commands

Command	Description
dsc serial	Defines a serial ID for a rack.

R3.5.0 Beta Draft—Cisco Confidential Information

show environment

To display environmental monitor parameters for the system, use the **show environment** command in EXEC mode or administration EXEC mode.

On the Cisco CRS-1 router, in EXEC mode:

```
show environment [all | last | leds | table | temperatures | voltages] [node-id]
```

On the Cisco CRS-1 router, in administration EXEC mode:

```
show environment [all | fans | last | leds | power-supply | table | temperatures | voltages]  
[node-id]
```

On the Cisco XR 12000 Series Router, in EXEC mode:

```
show environment [all | table | temperatures | voltages] [last] [node-id]
```

On the Cisco XR 12000 Series Router, in administration EXEC mode:

```
show environment [all | fans | last | leds | power-supply | table | temperatures | voltages]  
[node-id]
```

Syntax Description		
all	(Optional)	Displays information for all environmental monitor parameters.
last	(Optional)	Displays information for prior environmental monitor parameters.
fans	(Optional)	Displays information about the fans.
leds	(Optional)	Displays monitor parameters for LEDs on all cards in the node.
table	(Optional)	Displays environmental parameter ranges.
temperatures	(Optional)	Displays system temperature information.
power-supply	(Optional)	Displays power supply voltage and current information.
voltages	(Optional)	Displays system voltage information.
<i>node-id</i>	(Optional)	Identifies the node whose information you want to display. The <i>node-id</i> argument is expressed in the <i>rack/slot/module</i> notation.

Defaults All environmental monitor parameters are displayed.

Command Modes EXEC
Administration EXEC

R3.5.0 Beta Draft—Cisco Confidential Information**Command History**

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The optional <i>node-id</i> argument was supported on the Cisco CRS-1. The show environment command was moved from the root-system task ID to the system task ID.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **show environment** command displays information on the hardware that is installed in the system, including fans, LEDs, power supply voltage, and current information and temperatures.

Task ID

Task ID	Operations
system	read

Examples

The following is sample output from the **show environment** command with the **temperatures** keyword:

```
RP/0/RP0/CPU0:router# show environment temperatures
```

R/S/I	Modules	Inlet Temperature (deg C)	Exhaust Temperature (deg C)	Hotspot Temperature (deg C)
0/2/*	host	31, 27	43, 45	48
	cpu			31
	fabricq0			46
	fabricq1			44
	ingressq			34
	egressq		41	43
	ingresspse			35
	egresspse			42
	plimasic	30, 31	42	
0/RP1/*	host	38		44
	cpu			36
	ingressq			42
	fabricq0			43
0/SM0/*	host	29, 29		41, 33

R3.5.0 Beta Draft—Cisco Confidential Information

Table 7 describes the significant fields shown in the display.

Table 7 *show environment temperatures Field Descriptions*

Field	Description
R/S/I	Rack number, slot number, and interface for which information is displayed, in the format <i>rack_num/slot_num/*</i> .
Modules	Module for which temperature information is displayed.
Inlet Temperature (deg C)	Current temperature of the inlet sensor in degrees Celsius. Note The inlet temperature corresponds to the room air temperature entering the router.
Exhaust Temperature (deg C)	Current temperature of the exhaust sensor in degrees Celsius. Note The exhaust temperature corresponds to the air being exhausted from the router.
Hotspot Temperature (deg C)	Displays the current temperature of the hotspot in degrees Celsius.

The following is sample output from the **show environment** command the with the **leds** keyword:

```
RP/0/RP0/CPU0:router# show environment leds
```

```
0/2/*: Module (host) LED status says: OK
0/2/*: Module (plimasic) LED status says: OK
0/SM0/*: Module (host) LED status says: OK
```

Table 8 describes the significant fields shown in the display.

Table 8 *show environment leds Field Descriptions*

Field	Description
<i>rack_num/slot_num/*</i> :	Rack number and slot number where the node resides.
Module (host) LED status says:	Current LED status of the specified node.

R3.5.0 Beta Draft—Cisco Confidential Information

show facility-alarm contacts

To display audio and visual facility alarm information for the router, use the **show facility-alarm contacts** command in administration EXEC mode.

show facility-alarm contacts

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Administration EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.3.0	The show facility-alarm contacts command was moved from the root-system task ID to the system task ID.
		The show facility-alarm contacts command was removed from EXEC mode.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	system	read

Examples The following is sample output from the **show facility-alarm contacts** command:

```
RP/0/0/CPU0:router# admin
RP/0/0/CPU0:router(admin)# show facility-alarm contacts

Alarm Contacts
+-----+-----+-----+
| Severity | Audio | Visual |
+-----+-----+-----+
| Critical | off   | off    |
| Major    | off   | off    |
| Minor    | off   | off    |
+-----+-----+-----+
```

R3.5.0 Beta Draft—Cisco Confidential Information

Table 9 describes the significant fields shown in the display.

Table 9 *show facility-alarm contacts Field Descriptions*

Field	Description
Severity	Severity level of the alarm. Can be critical, major, or minor.
Audio	Describes whether there are audio alarms of the indicated severity on the router. “off” means there are no alarms. “on” means there are alarms.
Visual	Describes whether there are visual alarms of the indicated severity on the router. “off” means there are no alarms. “on” means there are alarms.

Related Commands

Command	Description
facility-alarm contacts	Sets or unsets facilities for processing alarms related to temperature and power supply conditions.

R3.5.0 Beta Draft—Cisco Confidential Information

show fmgr interface

To display ternary content addressable memory (TCAM) entries for QoS, enter the **show fmgr interface** command in EXEC mode.

show fmgr interface *type instance* **feature** {fabqos | policer | qos | qos-all} {in | out} [[hw | sw] [all | ipv4-mpls | ipv6] [dup-bank] location *node-id*]

Syntax Description

<i>type</i>	Interface type from which candidate route processor (RP) packets are sourced. For more information, use the question mark (?) online help function.
<i>instance</i>	Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is rack/slot/module/port and a slash mark 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. - port: Physical port number of the interface. Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
feature	Displays feature specific information.
fabqos	Displays fabric quality of service (QoS) entries.
policer	Displays policer entries.
qos	Displays QoS entries.
qos-all	Displays QoS and policer entries.
in	Specifies the ingress direction.
out	Specifies the egress direction.
hw	(Optional) Reads from the hardware.
sw	(Optional) Reads from the software.
all	(Optional) Displays all TCAM entries.
ipv4-mpls	(Optional) Displays ipv4-mpls entries.
ipv6	(Optional) Displays ipv6 entries.

R3.5.0 Beta Draft—Cisco Confidential Information

dup-bank	(Optional) Displays entries from the duplicate bank in turbo mode.
location <i>node-id</i>	(Optional) Identifies the location of the interface whose TCAM information you want to display. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.
Note	Enter the show platform command to see the location of all nodes installed in the router.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	qos	read

Examples The following example shows how to display all ingress QoS and policer TCAM entries for a Gigabit Ethernet interface:

```
RP/0/RP0/CPU0:router# show fmgr interface GigabitEthernet 0/1/5/0 feature qos-all in
```

```
QOS ENTRIES
```

```
=====
Interface = GigabitEthernet0_1_5_0      Feature = qos      Direction = in
TCAM Fields:
ip/mppls  bndl  vlq_id  cid  dscp  exp  dc  qos-id
```

```
CSRAM Fields:
```

```
prio sh_q red_ctr qos_grp dc l2_mark l3_mark l3_mark_val max_th seg_size min_th
l1st_seg pol_has_hpq
```

```
=====
No QoS configured on this interface
```

```
POLICER ENTRIES
```

```
=====
Interface = GigabitEthernet0_1_5_0      Feature = policer      Direction = in
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

TCAM Fields:
IPv4: ip/mppls vlg_id l2_cos drid ip_src l4_proto frag dscp ip_dest qos_grp dc d
st_port qos-id
MPLS: ip/mppls vlg_id l2_cos label exp qos_grp dc qos-id

CSRAM Fields:
cid token1 stats_ptr conform1 exceed1 violate1 token2 conform2 exceed2 violate2
=====
No QoS configured on this interface

POLICER ENTRIES
=====
Interface = GigabitEthernet0_1_5_0      Feature = policer      Direction = in
TCAM Fields:
IPv6: ipv6 vlg_id l2_cos dest_port src_port ip_dest ip_src ext_dst ext_rtg ext_
h ext_frag dest_rng_id dc qos_grp l4_proto dscp/prec qos-id

CSRAM Fields:
cid token1 stats_ptr conform1 exceed1 violate1 token2 conform2 exceed2 violate2
=====
No QoS configured on this interface

RP/0/RP0/CPU0:router#

```

Table 10 describes the significant fields shown in the display.

Table 10 *show fmgr interface Field Descriptions*

QOS ENTRIES	Displays the following QoS information: - Interface—Interface type and identifier. - Feature—Feature currently running on the specified interface. - Direction—Direction of interface (ingress or egress).
CSRAM Fields	General CSRAM ¹ information.
POLICER ENTRIES	General policer and TCAM information for the specified interface.

1. Cisco SRAM

R3.5.0 Beta Draft—Cisco Confidential Information

show fpd package

To display which shared port adapters (SPA) and SIPs are supported with your current Cisco IOS XR software release, which field-programmable device (FPD) image you need for each SPA and SIP, and what the minimum hardware requirements are for the SPA and SIP modules, use the **show fpd package** command, in administration EXEC.

show fpd package

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Administration EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.4.1	The show fpd package command output was updated to display the rommon images.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If there are multiple FPD images for your card, use the **show fpd package** command to determine which FPD image to use if you only want to upgrade a specific FPD type.

Task ID	Task ID	Operations
	sysmgr	read

Examples The following example shows partial sample output from the **show fpd package** command:

```
RP/0/0/CPU0:Router# admin
RP/0/0/CPU0:Router(admin)# show fpd package
```

```
=====
                                Field Programmable Device Package
=====
```

R3.5.0 Beta Draft—Cisco Confidential Information

Card Type	FPD Description	Type	Subtype	SW Version	Min Req HW Vers
=====	=====	=====	=====	=====	=====
CRS1-SIP-800	JACKET FPGA swv2.0	lc	fpga	2.0	0.0
	FPGA swv2.0 hww80	lc	fpga	2.0	0.80

8-10GBE	FPGA swvA.0	lc	fpga	10.0	0.0

Route Processor	ROMMON2 swv1.43 asmp	lc	rommon2	1.43	0.0
	ROMMON2 swv1.43 dsmp	lc	rommon2	1.43	0.0
	ROMMON swv1.43 asmp	lc	rommon	1.43	0.0
	ROMMON swv1.43 dsmp	lc	rommon	1.43	0.0

SC	ROMMON2 swv1.43 asmp	lc	rommon2	1.43	0.0
	ROMMON2 swv1.43 dsmp	lc	rommon2	1.43	0.0
	ROMMON swv1.43 asmp	lc	rommon	1.43	0.0
	ROMMON swv1.43 dsmp	lc	rommon	1.43	0.0

HQ Route Processor	ROMMON2 swv1.43 asmp	lc	rommon2	1.43	0.0
	ROMMON2 swv1.43 dsmp	lc	rommon2	1.43	0.0
	ROMMON swv1.43 asmp	lc	rommon	1.43	0.0
	ROMMON swv1.43 dsmp	lc	rommon	1.43	0.0

Shelf Controller GE	ROMMON2 swv1.43 asmp	lc	rommon2	1.43	0.0
	ROMMON2 swv1.43 dsmp	lc	rommon2	1.43	0.0
	ROMMON swv1.43 asmp	lc	rommon	1.43	0.0
	ROMMON swv1.43 dsmp	lc	rommon	1.43	0.0

Route Processor B	ROMMON2 swv1.43 asmp	lc	rommon2	1.43	0.0
	ROMMON2 swv1.43 dsmp	lc	rommon2	1.43	0.0
	ROMMON swv1.43 asmp	lc	rommon	1.43	0.0
	ROMMON swv1.43 dsmp	lc	rommon	1.43	0.0

Shelf Controller GE2	ROMMON2 swv1.43 asmp	lc	rommon2	1.43	0.0
	ROMMON2 swv1.43 dsmp	lc	rommon2	1.43	0.0
	ROMMON swv1.43 asmp	lc	rommon	1.43	0.0
	ROMMON swv1.43 dsmp	lc	rommon	1.43	0.0

DRP	ROMMON2 swv1.43 asmp	lc	rommon2	1.43	0.0
	ROMMON2 swv1.43 dsmp	lc	rommon2	1.43	0.0
	ROMMON2 swv1.43 sp	lc	rommon2	1.43	0.0
	ROMMON swv1.43 asmp	lc	rommon	1.43	0.0
	ROMMON swv1.43 dsmp	lc	rommon	1.43	0.0
	ROMMON swv1.43 sp	lc	rommon	1.43	0.0

DRP_B	ROMMON2 swv1.43 asmp	lc	rommon2	1.43	0.0
	ROMMON2 swv1.43 dsmp	lc	rommon2	1.43	0.0
	ROMMON2 swv1.43 sp	lc	rommon2	1.43	0.0
	ROMMON swv1.43 asmp	lc	rommon	1.43	0.0
	ROMMON swv1.43 dsmp	lc	rommon	1.43	0.0
	ROMMON swv1.43 sp	lc	rommon	1.43	0.0

S1S2S3	ROMMON2 swv1.43 sp	lc	rommon2	1.43	0.0
	ROMMON swv1.43 sp	lc	rommon	1.43	0.0

S1S3	ROMMON2 swv1.43 sp	lc	rommon2	1.43	0.0
	ROMMON swv1.43 sp	lc	rommon	1.43	0.0

S2	ROMMON2 swv1.43 sp	lc	rommon2	1.43	0.0
	ROMMON swv1.43 sp	lc	rommon	1.43	0.0

Fabric HS123	ROMMON2 swv1.43 sp	lc	rommon2	1.43	0.0
	ROMMON swv1.43 sp	lc	rommon	1.43	0.0

R3.5.0 Beta Draft—Cisco Confidential Information

Fabric HS123 Star	ROMMON2 swv1.43 sp	lc	rommon2	1.43	0.0
	ROMMON swv1.43 sp	lc	rommon	1.43	0.0
Fabric HS13 Star	ROMMON2 swv1.43 sp	lc	rommon2	1.43	0.0
	ROMMON swv1.43 sp	lc	rommon	1.43	0.0
Fabric QQS123	ROMMON2 swv1.43 sp	lc	rommon2	1.43	0.0
	ROMMON swv1.43 sp	lc	rommon	1.43	0.0
LED	ROMMON2 swv1.43 sp	lc	rommon2	1.43	0.0
	ROMMON swv1.43 sp	lc	rommon	1.43	0.0
YYY-XXXIface	ROMMON2 swv1.43 asmp	lc	rommon2	1.43	0.0
	ROMMON2 swv1.43 dsmp	lc	rommon2	1.43	0.0
	ROMMON2 swv1.43 sp	lc	rommon2	1.43	0.0
	ROMMON swv1.43 asmp	lc	rommon	1.43	0.0
	ROMMON swv1.43 dsmp	lc	rommon	1.43	0.0
	ROMMON swv1.43 sp	lc	rommon	1.43	0.0
PSAL	ROMMON2 swv1.43 sp	lc	rommon2	1.43	0.0
	ROMMON swv1.43 sp	lc	rommon	1.43	0.0
FAN	ROMMON2 swv1.43 sp	lc	rommon2	1.43	0.0
	ROMMON swv1.43 sp	lc	rommon	1.43	0.0
FC Fan Controller	ROMMON2 swv1.43 sp	lc	rommon2	1.43	0.0
	ROMMON swv1.43 sp	lc	rommon	1.43	0.0
LED	ROMMON2 swv1.43 sp	lc	rommon2	1.43	0.0
	ROMMON swv1.43 sp	lc	rommon	1.43	0.0
SPA-4XT3/E3	SPA E3 Subrate FPGA	spa	fpga2	1.4	0.0
	SPA T3 Subrate FPGA	spa	fpga3	1.4	0.0
	SPA I/O FPGA	spa	fpga	1.0	0.0
	SPA ROMMON	spa	rommon	2.12	0.0
SPA-2XT3/E3	SPA E3 Subrate FPGA	spa	fpga2	1.4	0.0
	SPA T3 Subrate FPGA	spa	fpga3	1.4	0.0
	SPA I/O FPGA	spa	fpga	1.0	0.0
	SPA ROMMON	spa	rommon	2.12	0.0
SPA-OC192POS	SPA FPGA swv1.3	spa	fpga	1.3	0.0
SPA-8XOC12-POS	SPA FPGA swv1.0	spa	fpga	1.0	0.5
SPA-4XOC3-POS	SPA FPGA swv3.4	spa	fpga	3.4	0.0
SPA-OC192POS-XFP	SPA FPGA swv1.2	spa	fpga	1.2	0.0
SPA-8X1GE	SPA FPGA swv1.8	spa	fpga	1.8	0.0
SPA-2XOC48POS/RPR	SPA FPGA swv1.0	spa	fpga	1.0	0.0
SPA-4XOC48POS/RPR	SPA FPGA swv1.0	spa	fpga	1.0	0.0
SPA-10X1GE-V2	SPA FPGA swv1.10	spa	fpga	1.10	0.0
SPA-8X1GE-V2	SPA FPGA swv1.10	spa	fpga	1.10	0.0
SPA-5X1GE-V2	SPA FPGA swv1.10	spa	fpga	1.10	0.0
SPA-1X10GE-L-V2	SPA FPGA swv1.9	spa	fpga	1.9	0.0

R3.5.0 Beta Draft—Cisco Confidential Information

Table 11 describes the significant fields shown in the display.

Table 11 *show fpd package Field Descriptions*

Field	Description
Card Type	Type of card that is associated with this FPD.
FPD Description	Currently running FPD type and image version.
Type	Hardware type. Can be one of the following types: • spa—shared port adapter • lc—line card.
Subtype	FPD type. Can be one of the following types: • fabldr—fabric downloader • fpga1—field-programmable gate array • fpga2—field-programmable gate array 2 • fpga3—field-programmable gate array 3 • fpga4—field-programmable gate array 4 • fpga5—field-programmable gate array 5 • rommon—read-only memory monitor • rommon2—read-only memory monitor 2
SW Version	Currently running FPD image version.
Min Req HW Version	Minimum required hardware version for the associated FPD image.

Related Commands

Command	Description
show hw-module fpd	Displays FPD compatibility for all modules or for a specific module.
upgrade hw-module fpd	Manually upgrades the current FPD image package on a module.

R3.5.0 Beta Draft—Cisco Confidential Information

show hw-module fpd

To display field-programmable device (FPD) compatibility for all modules or a specific module, use the **show hw-module fpd** command in the appropriate mode.

show hw-module fpd location {all | node-id}

Syntax Description	location	Specifies the location of the module.
	all	Specifies all modules in the router.
	<i>node-id</i>	Location of the module in the <i>rack/slot/module</i> notation.

Defaults	No default behavior or values

Command Modes	EXEC Administration EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.4.1	The show hw-module fpd command output was updated to display the common images.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	sysmgr	read
	root-lr	read

Examples	The following example shows how to display FPD compatibility for all modules in the router:

```
RP/0/0/CPU0:Router# show hw-module fpd location all
```

```
=====
Existing Field Programmable Devices
=====
```

```
show hw-module fpd
```

R3.5.0 Beta Draft—Cisco Confidential Information

Location	Card Type	HW Version	Type	Subtype	Inst	Current SW Version	Upg/ Dng?
0/0/SP	YYY-XXXIface	255.254	lc	rommon	0	1.43	No
			lc	rommon2	0	1.43	No
0/0/CPU0	CRS1-SIP-800	0.104	lc	fpga	0	2.0	No
			lc	rommon	0	1.43	No
			lc	rommon2	0	1.43	No
0/0/0	SPA-OC192POS-XFP	2.1	spa	fpga	0	1.2	No
0/0/1	SPA-10X1GE-V2	1.0	spa	fpga	1	1.10	No
0/0/2	SPA-1X10GE-L-V2	1.0	spa	fpga	2	1.9	No
0/0/5	SPA-5X1GE-V2	1.0	spa	fpga	5	1.10	No
0/2/SP	YYY-XXXIface	255.254	lc	rommon	0	1.43	No
			lc	rommon2	0	1.43	No
0/2/CPU0	YYY-XXXIface	255.254	lc	rommon	0	1.43	No
			lc	rommon2	0	1.43	No
0/RP0/CPU0	HQ Route Processor	0.1	lc	rommon	0	1.43	No
			lc	rommon2	0	1.43	No
0/SM0/SP	Fabric HS123	0.1	lc	rommon	0	1.43	No
			lc	rommon2	0	1.43	No
0/SM1/SP	Fabric HS123	0.1	lc	rommon	0	1.43	No
			lc	rommon2	0	1.43	No
0/SM2/SP	Fabric HS123	0.1	lc	rommon	0	1.43	No
			lc	rommon2	0	1.43	No
0/SM3/SP	Fabric HS123	0.1	lc	rommon	0	1.43	No
			lc	rommon2	0	1.43	No

Table 12 describes the significant fields shown in the display.

Table 12 *show hw-module fpd Field Descriptions*

Field	Description
Location	Location of the module in the <i>rack/slot/module</i> notation.
Card Type	Module part number.
HW Version	Hardware model version for the module.
Type	Hardware type. Can be one of the following types: - spa—shared port adapter - lc—line card.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 12** *show hw-module fpd Field Descriptions*

Field	Description
Subtype	FPD type. Can be one of the following types: - fabldr—fabric downloader - fpga1—field-programmable gate array - fpga2—field-programmable gate array 2 - fpga3—field-programmable gate array 3 - fpga4—field-programmable gate array 4 - fpga5—field-programmable gate array 5 - rommon—read-only memory monitor - rommon2—read-only memory monitor 2
Inst	FPD instance. The FPD instance uniquely identifies an FPD and is used by the FPD process to register an FPD.
Current SW Version	Currently running FPD image version.
Upg/Dng	Specifies whether an FPD upgrade or downgrade is required. A downgrade will be required in rare cases when the version of the FPD image has a higher major revision than the version of the FPD image in the current Cisco IOS XR software package.

Related Commands

Command	Description
show fpd package	Displays which FPD image package is needed for the router to properly support the modules for the running Cisco IOS XR software release. It also indicates all available FPD images that are available for a specific module.
upgrade hw-module fpd	Manually upgrades the current FPD image package on a module.

R3.5.0 Beta Draft—Cisco Confidential Information

show hw-module subslot brief

To display summary diagnostic information about internal hardware devices for a shared port adapter (SPA), use the **show hw-module subslot brief** command in EXEC mode.

show hw-module subslot [*node-id*] **brief** [*device* [*device-index* [*device-subindex*]]]

Syntax Description	<i>node-id</i> (Optional) Location for which to display the specified information. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
	<i>device</i> (Optional) Internal hardware device for which to display the specified information. Valid devices include: • analog-digital-converter—Displays analog-to-digital converter information. • c2w—Displays Cisco-to-wire bus device information. • fpga—Displays shared port adapter (SPA) field-programmable gate array information. • framer—Displays SONET framer information. (Not applicable to Ethernet SPAs.) • l2-tcam—Displays SPA Layer 2 ternary content addressable memory information. (Not applicable to POS SPAs.) • mac—Displays SPA MAC information. (Not applicable to POS SPAs.) • pluggable-optics—Displays pluggable-optics module information. • power-margining—Displays power-margining device information. • sdcc—Displays section data communications channel device information. (Not applicable to Ethernet SPAs.) • serdes—Displays SPA serializer/deserializer information. • spi4—Displays system packet interface level 4.2 bus device information. • temperature-sensor—Displays temperature sensor information.
	<i>device-index</i> (Optional) Index of the specific device if there are multiple devices of the same type.
	<i>device-subindex</i> (Optional) Subindex of the specific device if there are multiple devices of the same device index.

Defaults No default behavior or values

Command Modes EXEC

R3.5.0 Beta Draft—Cisco Confidential Information**Command History**

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the command to display the nodes on the router.

You can enter a partially qualified location specifier by using the wildcard (*) character. For example, 0/1/* would display information for all modules on slot 1 in rack 0.

Use the **show hw-module subslot brief** command to obtain summary diagnostic information about an interface on the SPA.

Task ID

Task ID	Operations
root-lr	read

Examples

The following is sample output for the **show hw-module subslot brief** command:

```
RP/0/RP1/CPU0:router# show hw-module subslot brief
```

```
BAY 0 brief info:
-----
SPA inserted: YES
SPA type:      1xOC192 POS/RPR HHSPA with XFP
SPA operational state: READY
SPA cfg admin up: YES
```

```
BAY 1 brief info:
-----
SPA inserted: YES
SPA type:      1xOC192 POS/RPR FHSPA
SPA operational state: READY
SPA cfg admin up: YES
```

[Table 13](#) describes the significant fields shown in the display.

Table 13 *show hw-module subslot brief Field Descriptions*

Field	Description
SPA inserted	Indicates if a SPA is currently detected in the subslot.
SPA type	Description of SPA including the technology type, number of ports, height of SPA (HHSPA—single height, FHSPA—double height), and optics type.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 13** *show hw-module subslot brief Field Descriptions (continued)*

Field	Description
SPA operational state	Current state of the SPA module.
SPA cfg admin	Configured state of the SPA: YES—the SPA is not shut down, NO—the SPA is shut down.

The following is sample output for the **show hw-module subslot brief** command with the **c2w** option:

```
RP/0/RP1/CPU0router# show hw-module subslot 0/2/cpu0 brief c2w
```

```
SPA device c2w index 0 subindex 0 info:
```

```
Auxiliary C2W (0x0803bfbcb), name AUX C2W (busywait), state 4
```

```
SPA device c2w index 0 subindex 0 info:
```

```
Auxiliary C2W (0x080638c4), name AUX C2W (busywait), state 4
```

Related Commands

Command	Description
show controllers	Displays the controller type and other information.

R3.5.0 Beta Draft—Cisco Confidential Information

show hw-module subslot config

To display information related to configuration of the specified internal hardware device on a shared port adapter (SPA), use the **show hw-module subslot config** command in EXEC mode.

show hw-module subslot [*node-id*] **config** [*device* [*device-index* [*device-subindex*]]]

Syntax Description		
<i>node-id</i>	(Optional) Location for which to display the specified information. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.	
<i>device</i>	(Optional) Internal hardware device for which to display the specified information. Valid devices include:	• analog-digital-converter—Displays analog-to-digital converter information. • c2w—Displays Cisco-to-wire bus device information. • fpga—Displays SPA field-programmable gate array information. • framer—Displays SONET framer information. (Not applicable to Ethernet SPAs.) • l2-tcam—Displays SPA Layer 2 ternary content addressable memory information. (Not applicable to POS SPAs.) • mac—Displays SPA MAC information. (Not applicable to POS SPAs.) • pluggable-optics—Displays pluggable-optics module information. • power-margining—Displays power-margining device information. • sdcc—Displays section data communications channel device information. (Not applicable to Ethernet SPAs.) • serdes—Displays SPA serializer/deserializer information. • spi4—Displays system packet interface level 4.2 bus device information. • temperature-sensor—Displays temperature sensor information.
<i>device-index</i>	(Optional) Index of the specific device if there are multiple devices of the same type.	
<i>device-subindex</i>	(Optional) Subindex of the specific device if there are multiple devices of the same device index.	

Defaults No default behavior or values

Command Modes EXEC

R3.5.0 Beta Draft—Cisco Confidential Information**Command History**

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You can also enter a partially qualified location specifier by using the wildcard (*) character. For example, 0/1/* would display information for all modules on slot 1 in rack 0.

Use the **show hw-module subslot config** command to obtain diagnostic information about the configuration of an interface on the SPA.

Task ID

Task ID	Operations
root-lr	read

Examples

The following is sample output for the **show hw-module subslot config** command:

```
RP/0/RP1/CPU0router# show hw-module subslot 0/2/cpu0 config
```

```
BAY 0 config info:
-----
SPA inserted: YES
SPA cfg admin up: YES
SPA cfg power up: YES

BAY 1 config info:
-----
SPA inserted: YES
SPA cfg admin up: YES
SPA cfg power up: YES
```

[Table 14](#) describes the significant fields shown in the display.

Table 14 show hw-module subslot config Field Descriptions

Field	Description
SPA inserted	Indicates if a SPA is currently detected in the subslot.
SPA cfg admin up	Configured state of the SPA: YES—the SPA is not shut down, NO—the SPA is shut down.
SPA cfg power up	Indicates whether the subslot is currently configured as powered or not.

Related Commands

R3.5.0 Beta Draft—Cisco Confidential Information

Command	Description
show controllers	Displays the controller type and other information.

R3.5.0 Beta Draft—Cisco Confidential Information

show hw-module subslot counters

To display statistics related to the processing of internal hardware devices for a shared port adapter (SPA), use the **show hw-module subslot counters** command in EXEC mode.

show hw-module subslot [*node-id*] **counters** [*device* [*device-index* [*device-subindex*]]]

Syntax Description	<i>node-id</i> (Optional) Location for which to display the specified information. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
	<i>device</i> (Optional) Internal hardware device for which to display the specified information. Valid devices include: • analog-digital-converter—Displays analog-to-digital converter information. • c2w—Displays Cisco-to-wire bus device information. • fpga—Displays SPA field-programmable gate array information. • framer—Displays SONET framer information. (Not applicable to Ethernet SPAs.) • l2-tcam—Displays SPA Layer 2 ternary content addressable memory information. (Not applicable to POS SPAs.) • mac—Displays SPA MAC information. (Not applicable to POS SPAs.) • pluggable-optics—Displays pluggable-optics module information. • power-margining—Displays power-margining device information. • sdcc—Displays section data communications channel device information. (Not applicable to Ethernet SPAs.) • serdes—Displays SPA serializer/deserializer information. • spi4—Displays system packet interface level 4.2 bus device information. • temperature-sensor—Displays temperature sensor information.
	<i>device-index</i> (Optional) Index of the specific device if there are multiple devices of the same type.
	<i>device-subindex</i> (Optional) Subindex of the specific device if there are multiple devices of the same device index.

Defaults No default behavior or values

Command Modes EXEC

R3.5.0 Beta Draft—Cisco Confidential Information**Command History**

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You can also enter a partially qualified location specifier by using the wildcard (*) character. For example, 0/1/* would display information for all modules on slot 1 in rack 0.

Use the **show hw-module subslot counters** command to display statistics related to the processing by the specified internal hardware device.

Task ID

Task ID	Operations
root-lr	read

Examples

The following is sample output for the **show hw-module subslot counters** command:

```
RP/0/RP1/CPU0router# show hw-module subslot 0/2/cpu0 counters

BAY 0 counts info:
-----
SPA inserted: YES
SPA type:      5xGE SPA
SPA operational state: READY
SPA insertion time:  Fri Nov 19 01:49:07 2004
SPA last time ready: Fri Nov 19 01:49:42 2004
SPA uptime [HH:MM:SS]: 49:49:29

BAY 1 counts info:
-----
SPA inserted: YES
SPA type:      1xOC192 POS/RPR HHSPA with XFP
SPA operational state: READY
SPA insertion time:  Fri Nov 19 01:49:08 2004
SPA last time ready: Fri Nov 19 01:49:35 2004
SPA uptime [HH:MM:SS]: 49:49:36
```

Table 15 describes the significant fields shown in the display.

Table 15 show hw-module subslot counters Field Descriptions

Field	Description
SPA inserted	Indicates if a SPA is currently detected in the subslot.
SPA type	Description of SPA including the technology type, number of ports, height of SPA (HHSPA—single height, FHSPA—double height), and optics type.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 15** *show hw-module subslot counters Field Descriptions (continued)*

Field	Description
SPA operational state	Current state of the SPA module.
SPA insertion time	Time the SPA module was last physically inserted or power-cycled.
SPA last time ready	Time the SPA module last changed state to up or ready (the last time the module was loaded or reloaded).
SPA uptime	The time in service or amount of time since the module was last out of service due to a reload, power-cycle, or configuration event.

The following is sample output for the **show hw-module subslot counters** command with the **framer** option:

```
RP/0/RP1/CPU0router# show hw-module subslot counters framer

SPA device framer index 0 subindex 0 info:

Milan Framer counters:
STREAM 0
Rx Bytes (48-bit) (#0x381fa078-0x883c): 163857232569448
Rx Good Bytes (48-bit) (#0x381fa080-0x8840): 1964924
Rx Good Packets (48-bit) (#0x381fa040-0x8820): 26234
Tx Byte Cnt Reg (48-bit) (#0x381fe070-0xa838): 9375380
Tx Good Bytes Cnt Reg (48-bit) (#0x381fe068-0xa834): 8909442
Tx Transmitted Packet Cnt Reg (48-bit) (#0x381fe040-0xa820): 114692
```

R3.5.0 Beta Draft—Cisco Confidential Information

show hw-module subslot errors

To display error information about internal hardware devices for a shared port adapter (SPA), use the **show hw-module subslot errors** command in EXEC mode.

show hw-module subslot [*node-id*] **errors** [*device* [*device-index* [*device-subindex*]]]

Syntax Description	<i>node-id</i> (Optional) Location for which to display the specified information. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
	<i>device</i> (Optional) Internal hardware device for which to display the specified information. Valid devices include: • analog-digital-converter—Displays analog-to-digital converter information. • c2w—Displays Cisco-to-wire bus device information. • fpga—Displays SPA field-programmable gate array information. • framer—Displays SONET framer information. (Not applicable to Ethernet SPAs.) • l2-tcam—Displays SPA Layer 2 ternary content addressable memory information. (Not applicable to POS SPAs.) • mac—Displays SPA MAC information. (Not applicable to POS SPAs.) • pluggable-optics—Displays pluggable-optics module information. • power-margining—Displays power-margining device information. • sdcc—Displays section data communications channel device information. (Not applicable to Ethernet SPAs.) • serdes—Displays SPA serializer/deserializer information. • spi4—Displays system packet interface level 4.2 bus device information. • temperature-sensor—Displays temperature sensor information.
	<i>device-index</i> (Optional) Index of the specific device if there are multiple devices of the same type.
	<i>device-subindex</i> (Optional) Subindex of the specific device if there are multiple devices of the same device index.

Defaults No default behavior or values

Command Modes EXEC

R3.5.0 Beta Draft—Cisco Confidential Information**Command History**

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You can also enter a partially qualified location specifier by using the wildcard (*) character. For example, 0/1/* would display information for all modules on slot 1 in rack 0.

Use the **show hw-module subslot errors** command to display error information related to the specified internal hardware device on a SPA.

Task ID

Task ID	Operations
root-lr	read

Examples

The following is sample output for the **show hw-module subslot errors** command with the **pluggable-optics** option:

```
RP/0/RP1/CPU0router# show hw-module subslot 0/2/cpu0 errors pluggable-optics
```

```
SPA device pluggable-optics index 0 subindex 0 info:
```

```
Phased Initialization
  Phase Reached: 4
  Phase Exit Code: 0
  Phase Read Offset: 256
```

```
Socket Verification
  Not supported
```

```
SPA device pluggable-optics index 0 subindex 0 info:
```

```
Phased Initialization
  Phase Reached: 2
  Phase Exit Code: 3
  Phase Read Offset: 256
```

```
Socket Verification
  Not supported
```

Related Commands

Command	Description
show controllers	Displays the controller type and other information.

R3.5.0 Beta Draft—Cisco Confidential Information

show hw-module subslot registers

To display register information about internal hardware devices for a shared port adapter (SPA), use the **show hw-module subslot registers** command in EXEC mode.

show hw-module subslot [*node-id*] **registers** [*device* [*device-index* [*device-subindex*]]]

Syntax Description	<i>node-id</i> (Optional) Location for which to display the specified information. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
	<i>device</i> (Optional) Internal hardware device for which to display the specified information. Valid devices include: • analog-digital-converter—Displays analog-to-digital converter information. • c2w—Displays Cisco-to-wire bus device information. • fpga—Displays SPA field-programmable gate array information. • framer—Displays SONET framer information. (Not applicable to Ethernet SPAs.) • l2-tcam—Displays SPA Layer 2 ternary content addressable memory information. (Not applicable to POS SPAs.) • mac—Displays SPA MAC information. (Not applicable to POS SPAs.) • pluggable-optics—Displays pluggable-optics module information. • power-margining—Displays power-margining device information. • sdcc—Displays section data communications channel device information. (Not applicable to Ethernet SPAs.) • serdes—Displays SPA serializer/deserializer information. • spi4—Displays system packet interface level 4.2 bus device information. • temperature-sensor—Displays temperature sensor information.
	<i>device-index</i> (Optional) Index of the specific device if there are multiple devices of the same type.
	<i>device-subindex</i> (Optional) Subindex of the specific device if there are multiple devices of the same device index.

Defaults No default behavior or values

Command Modes EXEC

R3.5.0 Beta Draft—Cisco Confidential Information**Command History**

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the command to display the nodes on the router.

You can also enter a partially qualified location specifier by using the wildcard (*) character. For example, 0/1/* would display information for all modules on slot 1 in rack 0.

Use the **show hw-module subslot registers** command to display register information for the specified internal hardware device on the SPA.

Task ID

Task ID	Operations
root-lr	read

Examples

The following example shows sample output for the **show hw-module subslot registers** command:

```
RP/0/RP1/CPU0router# show hw-module subslot 0/2/CPU0 registers
```

```
BAY 0 registers info:
```

```
-----
```

```
SPA hardware ID : 0x1
```

```
SPA SW FPGA rev.: 0x10
```

```
BAY 1 registers info:
```

```
-----
```

```
SPA hardware ID : 0x90000000
```

```
SPA SW FPGA rev.: 0xD
```

Related Commands

Command	Description
show controllers	Displays the controller type and other information.

R3.5.0 Beta Draft—Cisco Confidential Information

show hw-module subslot status

To display status information about internal hardware devices for a shared port adapter (SPA), use the **show hw-module subslot status** command in EXEC mode.

show hw-module subslot [*node-id*] **status** [*device* [*device-index* [*device-subindex*]]]

Syntax Description		
<i>node-id</i>	(Optional) Location for which to display the specified information. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.	
<i>device</i>	(Optional) Internal hardware device for which to display the specified information. Valid devices include:	• analog-digital-converter—Displays analog-to-digital converter information. • c2w—Displays Cisco-to-wire bus device information. • fpga—Displays SPA field-programmable gate array information. • framer—Displays SONET framer information. (Not applicable to Ethernet SPAs.) • l2-tcam—Displays SPA Layer 2 ternary content addressable memory information. (Not applicable to POS SPAs.) • mac—Displays SPA MAC information. (Not applicable to POS SPAs.) • pluggable-optics—Displays pluggable-optics module information. • power-margining—Displays power-margining device information. • sdcc—Displays section data communications channel device information. (Not applicable to Ethernet SPAs.) • serdes—Displays SPA serializer/deserializer information. • spi4—Displays system packet interface level 4.2 bus device information. • temperature-sensor—Displays temperature sensor information.
<i>device-index</i>	(Optional) Index of the specific device if there are multiple devices of the same type.	
<i>device-subindex</i>	(Optional) Subindex of the specific device if there are multiple devices of the same device index.	

Defaults No default behavior or values

Command Modes EXEC

R3.5.0 Beta Draft—Cisco Confidential Information**Command History**

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You can also enter a partially qualified location specifier by using the wildcard (*) character. For example, 0/1/* would display information for all modules on slot 1 in rack 0.

Use the **show hw-module subslot status** command to obtain status information about an interface on the SPA.

Task ID

Task ID	Operations
root-lr	read

Examples

The following example shows sample output for the **show hw-module subslot status** command with the **temperature-sensor** option:

```
RP/0/RP1/CPU0router# show hw-module subslot 0/2/cpu0 status temperature-sensor
```

```
SPA device temperature-sensor index 0 subindex 0 info:
```

```
DS1631 (0x0803c2e4) device status:
temperature = 0x1c80 (28.5 degree C)
```

```
SPA device temperature-sensor index 0 subindex 0 info:
```

```
DS1631 (0x08063bec) device status:
temperature = 0x1e00 (30.0 degree C)
```

Related Commands

Command	Description
show controllers	Displays the controller type and other information.

R3.5.0 Beta Draft—Cisco Confidential Information

show inventory

To retrieve and display information about all the Cisco products that are installed in the router, use the **show inventory** command in EXEC or administration EXEC mode.

In EXEC mode:

```
show inventory [node-id | all | location {node-id | all} | raw]
```

In administration EXEC mode:

```
show inventory [node-id | all | chassis | fans | location {node-id | all} | power-supply | raw]
```

Syntax Description

<i>node-id</i>	(Optional) Identifies the location of a specific node whose inventory information you want to display. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.
all	(Optional) Displays inventory information for all the physical entities in the chassis.
location { <i>node-id</i> all }	(Optional) Displays inventory information for a specific node, or for all nodes in the chassis.
raw	(Optional) Displays raw information about the chassis for diagnostic purposes.
chassis	(Optional) Displays inventory information for the entire chassis.
fans	(Optional) Displays inventory information for the fans.
power-supply	(Optional) Displays inventory information for the power supply.

Defaults

All inventory information for the entire chassis is displayed.

Command Modes

EXEC
Administration EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.3.0	This command was first supported on the Cisco CRS-1. The root-system task ID was removed from the show inventory command.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If a Cisco entity is not assigned a PID, that entity is not retrieved or displayed.

R3.5.0 Beta Draft—Cisco Confidential Information

Enter the **show inventory** command with the **raw** keyword to display every RFC 2737 entity installed in the router, including those without a PID, UDI, or other physical identification.

**Note**

The **raw** keyword is primarily intended for troubleshooting problems with the **show inventory** command itself.

If any of the Cisco products do not have an assigned PID, then the output may display incorrect PIDs, and the VID and SN elements may be missing.

For UDI compliance products, the PID, VID, and SN are stored in EEPROM and NVRAM. Use the **show inventory** command to display this information.

Task ID**Task ID****Operations**

sysmgr

read

Examples

The following is partial sample output from the **show inventory** command with the **raw** keyword:

```
RP/0/0/CPU0:router(admin)# show inventory raw
```

```
NAME: "0/0/CPU0", DESCR: "Cisco 12000 Series Performance Route Processor  
PID: PRP-2, VID: V01, SN: SAD091702N9
```

```
NAME: "voltages 0/0/CPU0", DESCR: "host__PLIM_V7_HDD_5V"  
PID: , VID: N/A, SN:
```

```
NAME: "voltages 0/0/CPU0", DESCR: "host__PLIM_V6_1.5V"  
PID: , VID: N/A, SN:
```

```
NAME: "voltages 0/0/CPU0", DESCR: "host__PLIM_V4_1.3V"  
PID: , VID: N/A, SN:
```

```
NAME: "voltages 0/0/CPU0", DESCR: "host__PLIM_V5_1.8V"  
PID: , VID: N/A, SN:
```

```
NAME: "voltages 0/0/CPU0", DESCR: "host__PLIM_V3_2.5V"  
PID: , VID: N/A, SN:
```

```
NAME: "voltages 0/0/CPU0", DESCR: "host__3.3V"  
PID: , VID: N/A, SN:
```

```
NAME: "voltages 0/0/CPU0", DESCR: "host__5V"  
PID: , VID: N/A, SN:
```

```
--More--
```

R3.5.0 Beta Draft—Cisco Confidential Information

Table 16 describes the significant fields shown in the display.

Table 16 *show inventory Field Descriptions*

Field	Description
NAME	Hardware for which the inventory information is displayed. If you are displaying the chassis inventory, this field shows, “chassis.” If you are displaying raw inventory, or all inventory information for all nodes in the chassis, this field shows the node name. For a node, the NAME is expressed in <i>node_type/rack</i> notation.
DESCR	Describes the chassis or the node. Chassis descriptions provide the name of the chassis and its Gbps. Node descriptions provide the type of node and its software version.
PID	Physical model name of the chassis or node.
VID	Physical hardware revision of the chassis or node.
SN	Physical serial number for the chassis or node.

R3.5.0 Beta Draft—Cisco Confidential Information

show led

To display LED information for the router, or for a specific LED location, use the **show led location** command in EXEC mode.

show led [**location** {*node-id* | **all**}]

Syntax Description

location {*node-id* | **all**}

(Optional) Displays LED information for a single LED location or for the entire router.

Enter the **all** keyword to display LED information for the entire router, or use the *node-id* argument to specify LED location. The *node-id* argument is expressed in the *rack/slot/module* notation.

Note Enter the **show platform** command to see the location of all nodes installed in the router.

Defaults

The default is to enter the **show led** command without including any optional parameters to display information about all LEDs on the router.

Command Modes

EXEC

Administration EXEC

Command History**Release****Modification**

Release 2.0

This command was introduced on the Cisco CRS-1.

Release 3.0

No modification.

Release 3.2

This command was introduced on the Cisco XR 12000 Series Router.

Release 3.3.0

The **show led** command was moved from the root-system task ID to the system task ID.

The **show led** command was supported in Administration EXEC mode.

Release 3.4.0

No modification.

Release 3.5.0

No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID**Task ID****Operations**

system

read

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following is sample output from the **show led location** command with the **all** keyword on a Cisco CRS-1:

```
RP/0/RP0/CPU0:router# show led location all
```

LOCATION	MESSAGE	MODE	STATUS
0/1/*	IOS XR	DEFAULT	UNLOCKED
0/6/*	IOS XR	DEFAULT	UNLOCKED
0/RP0/*	ACTV RP	DEFAULT	UNLOCKED
0/RP1/*	STBYRDY	DEFAULT	UNLOCKED

Table 17 describes the significant fields shown in the display.

Table 17 *show led location Field Descriptions*

Field	Description
LOCATION	Identifies the location of the node. The LOCATION is expressed in the <i>rack/slot/module</i> notation.
MESSAGE	Current message displayed by the LED.
MODE	Current operating mode of the specified node.
STATUS	Current status of the specified node.

The following is sample output from the **show led location** command with the **all** keyword on a Cisco XR 12000 Series Router:

```
RP/0/0/CPU0:router#show led location all
```

LOCATION	MESSAGE	MODE	STATUS
0/0/CPU0	ACTVRP	DEFAULT	UNLOCKED
0/1/CPU0	PSC1	DEFAULT	UNLOCKED
0/2/CPU0	IOX RUN	DEFAULT	UNLOCKED
0/3/CPU0	IOX RUN	DEFAULT	UNLOCKED
0/4/CPU0	IOX RUN	DEFAULT	UNLOCKED
0/5/CPU0	IOX RUN	DEFAULT	UNLOCKED

Related Commands

Command	Description
led mode	Specifies the LED mode parameters.

R3.5.0 Beta Draft—Cisco Confidential Information

show mbus

To display Mbus Controller Area Network (CAN) errors and interface counters, use the **show mbus** command in administration EXEC mode.

show mbus {**can-error** | **counters**} **location** {*node-id* | **all**}

Syntax Description

can-error	Displays CAN bus error statistics.
counters	Displays information about the firmware packets that were dropped.
location all	Displays Mbus information for all nodes installed in the router.
location <i>node-id</i>	Identifies the location of the node whose CAN errors and interface counters you want to display. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.
Note Enter the show platform command to see the location of all nodes installed in the router.	

Defaults

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.3.0	The root-system task ID was removed from the show mbus command.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
sysmgr	read

Examples

The following is sample output from the **show mbus** command with the **can-error** and **location** keywords:

```
RP/0/0/CPU0:router# admin
RP/0/0/CPU0:router(admin)# show mbus can-error location 0/0/CPU0
```

```
Slot #   Stuff   Form   Ack   Bit_1   Bit_0   CRC
0         0         0         0         0         0         0
```

R3.5.0 Beta Draft—Cisco Confidential Information

Table 18 describes the significant fields shown in the display.

Table 18 *show mbus can-error Field Descriptions*

Field	Description
Slot	Slot that contains the node whose Mbus counters are displayed.
Stuff	Number of stuff errors on the node.
Form	Number of form errors on the node.
Ack	Number of acknowledgement errors on the node.
Bit_1	Number of Bit_1 errors on the node.
Bit_0	Number of Bit_0 errors on the node.
CRC	Number of CRC ¹ errors.

1. cyclic redundancy check

The following is sample output from the **show mbus** command with the **location** keyword:

```
RP/0/0/CPU0:router# admin
RP/0/0/CPU0:router(admin)# show mbus counters location 0/0/CPU0

Slot #   Mbox      Mbox      Mbus      Mbus      Obj
        Xmit      Rcv       Xmit      Rcv       Ovr_wr
0         0         0         0         0         0
```

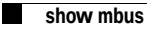
Table 19 describes the significant fields shown in the display.

Table 19 *show mbus counters Field Descriptions*

Field	Description
Slot	Identifies the slot that contains the node whose Mbus counters are displayed.
Mbox Xmit	Number of packets dropped due to Mbox transmit errors. Note MBox is a chunk of the MP DMEM ¹ that receives MIPC messages. The Norm Priority mailbox has a buffer of 32 KB, while the high-priority Mbox has a buffer of 8 KB.
Mbox Rcv	Number of packets dropped due to Mbox receive errors.
Mbus Xmit	Number of packets dropped due to Mbus transmit errors. Note The Mbus is a low-bandwidth (1 megabit per second) serial bus that connects cards, switch fabric cards, power supplies, and blower/fan assemblies to the PRPs ² and counters.
Mbus Rcv	Number of packets dropped due to Mbus receive errors.
Obj Ovr_wr	Number of packets that were overwritten.

1. Maintenance Processor Data Memory

2. performance route processors

***R3.5.0 Beta Draft—Cisco Confidential Information***

Related Commands	Command	Description
	clear mbus-statistics location	Clears all MBUS interface counters on a specific node.

R3.5.0 Beta Draft—Cisco Confidential Information

show platform

To display information and status on each node in the system, use the **show platform** command in EXEC mode or administration EXEC mode.

On the Cisco CRS-1 router:

```
show platform [node-id]
```

On the Cisco XR 12000 Series Router:

```
show platform
```

Syntax Description	<i>node-id</i>	(Optional) Specifies the node whose information you want to display. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
	Note	The <i>node-id</i> argument is available on the Cisco CRS-1 only.

Defaults	Cisco CRS-1 router: Status and information are displayed for all nodes in the system
	Cisco XR 12000 Series Router: No default behavior or values

Command Modes	EXEC
	Administration EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	The show platform was first supported in administration EXEC mode. On the Cisco CRS-1, the EXEC mode show platform command was moved from the root-system task ID to the system task ID.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	The show platform command provides a summary of the nodes in the system, including node type and status.
	Enter the show platform command in administration EXEC mode to display output for the entire system. Enter the show platform command in EXEC mode to display output for only those nodes that belong to the SDR on which the command is executed.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	sysmgr	read (on the Cisco XR 12000 Series Router only)
	system	read (in EXEC mode on the Cisco CRS-1 only)
	root-system	read (in administration EXEC mode on the Cisco CRS-1 only)

Examples

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

```
RP/0/RP0/CPU0:router# show platform
```

Node	Type	PLIM	State	Config State
0/1/CPU0	MSC	Jacket Card	IOS XR RUN	PWR, NSHUT, MON
0/1/0	MSC (SPA)	4XOC3-POS	OK	PWR, NSHUT, MON
0/1/5	MSC (SPA)	8X1GE	OK	PWR, NSHUT, MON
0/6/CPU0	MSC	Jacket Card	IOS XR RUN	PWR, NSHUT, MON
0/6/0	MSC (SPA)	4XOC3-POS	OK	PWR, NSHUT, MON
0/6/4	MSC (SPA)	8XOC3/OC12-POS	OK	PWR, NSHUT, MON
0/6/5	MSC (SPA)	8X1GE	OK	PWR, NSHUT, MON
0/RP0/CPU0	RP (Active)	N/A	IOS XR RUN	PWR, NSHUT, MON
0/RP1/CPU0	RP (Standby)	N/A	IOS XR RUN	PWR, NSHUT, MON

The following is sample output for the **show platform** command with the *node-id* argument:

```
RP/0/RP0/CPU0:router# show platform 0/1/0
```

Node	Type	PLIM	State	Config State
0/1/0	MSC (SPA)	4XOC3-POS	OK	PWR, NSHUT, MON

Table 20 describes the significant fields shown in the display.

Table 20 *show platform Field Descriptions*

Field	Description
Node	Identifies the node, in the <i>rack/slot/module</i> format.
Type	Type of node.
PLIM	Type of PLIM ¹ currently supported on the module.
State	Current state of the specified node.
Config State	Current status of the specified node.

1. physical layer interface module

Related Commands	Command	Description
	show environment	Displays environmental monitor parameters for the system.

R3.5.0 Beta Draft—Cisco Confidential Information

show redundancy

To display the status of route processor redundancy, use the **show redundancy** command in EXEC mode.

show redundancy [**location** {*node-id* | **all**} | **summary**]

Syntax Description	location	(Optional) Specifies the location of the node or nodes whose redundancy information you want to display. You can display information about a specific node, or about all nodes in the router.
	<i>node-id</i>	Specifies the location of the node whose redundancy information you want to display. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.
	all	Displays redundancy information for all nodes installed in the router.
	summary	(Optional) Displays a summary of all redundant node pairs in the router.

Defaults	Route processor redundancy information is displayed for all nodes in the system.

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the show redundancy command to display the redundancy status of the route processors. The show redundancy command also displays the boot and switch-over history for the RPs.

Task ID	Task ID	Operations
	system	read

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following is sample output from the **show redundancy** command on a Cisco CRS-1:

```
RP/0/RP0/CPU0:router# show redundancy

Redundancy information for node 0/RP0/CPU0:
=====
Node 0/RP0/CPU0 is in ACTIVE role
Partner node (0/RP1/CPU0) is in STANDBY role
Standby node in 0/RP1/CPU0 is ready

Reload and boot info
-----
RP reloaded Tue Mar 28 09:02:26 2006: 5 hours, 41 minutes ago
Active node booted Tue Mar 28 09:02:56 2006: 5 hours, 41 minutes ago
Last switch-over Tue Mar 28 09:09:26 2006: 5 hours, 34 minutes ago
Standby node boot Tue Mar 28 09:10:37 2006: 5 hours, 33 minutes ago
Standby node last went not ready Tue Mar 28 09:25:49 2006: 5 hours, 18 minutes a
go
Standby node last went ready Tue Mar 28 09:25:51 2006: 5 hours, 18 minutes ago
There has been 1 switch-over since reload
```

Table 21 describes the significant fields shown in the display.

Table 21 *show redundancy Field Descriptions*

Field	Description
Node */*/* is in XXX role	Current role of the primary route processor, where (*/*/) is the route processor ID in the format <i>rack/slot/module</i> , and XXX is the role of the route processor (active or standby). In the example, this field shows that the node with the ID 0/RP0/CPU0 is in active role.
Partner node (*/*/) is in XXX role	Current role of the secondary (or partner) route processor, where (*/*/) is the route processor ID in the <i>rack/slot/module</i> format, and XXX is the role of the route processor (active or standby). In the example, this field shows that the node with the ID 0/RP1/CPU0 is in standby role.
Standby node in(*/*/) is ready	Current state of the standby node, where (*/*/) is the standby route processor ID. In the example, the standby node is ready.
Reload and boot info	General overview of the active and standby route processors' reload and boot history.

The following is sample output from the **show redundancy** command on a Cisco XR 12000 Series Router:

```
RP/0/0/CPU0:router# show redundancy

Redundancy information for node 0/0/CPU0:
=====
Node 0/0/CPU0 is in ACTIVE role
Node 0/0/CPU0 has no valid partner

Reload and boot info
-----
PRP reloaded Wed Mar 15 19:50:31 2006: 1 week, 5 days, 18 hours, 57 minutes ago
Active node booted Wed Mar 15 19:50:31 2006: 1 week, 5 days, 18 hours, 57 minute
```

R3.5.0 Beta Draft—Cisco Confidential Information

s ago

Redundancy information for node 0/1/CPU0:

=====

Node 0/1/CPU0 is in ACTIVE role

Node 0/1/CPU0 has no valid partner

Reload and boot info

PSC1 reloaded Wed Mar 15 19:51:31 2006: 1 week, 5 days, 18 hours, 56 minutes ago

Active node booted Wed Mar 15 19:51:31 2006: 1 week, 5 days, 18 hours, 56 minutes ago

Table 22 describes the significant fields shown in the display.

Table 22 *show redundancy Field Descriptions*

Field	Description
Node */*/* is in XXX role	Current role of the primary route processor, where (*/*/*) is the route processor ID in the format <i>rack/slot/module</i> , and XXX is the role of the route processor (active or standby). In the example, this field shows that the node with the ID 0/RP0/CPU0 is in active role.
Partner node (*/*/*) is in XXX role	Current role of the secondary (or partner) route processor, where (*/*/*) is the route processor ID in the <i>rack/slot/module</i> format, and XXX is the role of the route processor (active or standby). In the example, this field shows that the node with the ID 0/RP1/CPU0 is in standby role.
Standby node in(*/*/*) is ready	Current state of the standby node, where (*/*/*) is the standby route processor ID. In the example, the standby node is ready.
Reload and boot info	General overview of the active and standby route processors' reload and boot history.

Related Commands

Command	Description
redundancy switchover	Causes the primary (active) RP to fail over to the redundant standby RP, if the standby RP is available.

R3.5.0 Beta Draft—Cisco Confidential Information

show screddrv

To display system controller (SC) redundancy information, use the **show screddrv** command in EXEC mode.

show screddrv [**all** | **standby** | **trace**]

Syntax Description

all	(Optional) Displays redundancy details for the entire router.
standby	(Optional) Displays detailed redundancy information for the standby node.
trace	(Optional) Displays detailed ltrace information for the arbitration mechanism.

Defaults

SC redundancy information is displayed for all nodes in the system.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	No modification.
Release 3.3.0	The show screddrv command was moved from the root-system task ID to the system task ID.
	The arbitration keyword was removed from the show screddrv command.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Enter the **show screddrv** command without any of the optional parameters to display summarized SC redundancy and arbitration information for the router.

Task ID

Task ID	Operations
system	read

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following is sample output from the **show screddrv** command with the **all** keyword:

```
RP/0/RP0/CPU0:router# show screddrv all

Redundancy Driver Info for slot 32:
Slot=32
Role=active role
State=ACTIVE STATE
Prefer_slot=0
Registers: ICreg=[1], MSreg=[33], MPPReg=[c0005cc8]
Tx error count=0
Rx error count=22
Comm Statistics=5632
SHOW REDDRV ARBITRATION is not supported.
```

Table 23 describes the significant fields shown in the display.

Table 23 *show screddrv Field Descriptions*

Field	Description
Role	Current role of the card in the specified slot; for example, it may be active, standby, and so forth.
State	Current state of the card in the specified slot.
Prefer_slot	Information about the preferred redundancy slot.
Registers	Information about the following registers: • ICreg • MSreg • MPPReg
Tx error count	Number of transmit errors that have occurred on the card in the specified slot.
Rx error count	Number of receive errors that have occurred on the card in the specified slot.
Comm Statistics	Command statistics.
SHOW REDDRV ARBITRATION	Describes whether arbitration is supported or not on this slot. If arbitration is supported, this field provides arbitration information.

Related Commands

Command	Description
redundancy reddrv	Enables the RP and displays SC redundancy.

R3.5.0 Beta Draft—Cisco Confidential Information

show version

To display the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images, use the **show version** command in EXEC mode.

show version

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	The show version command was moved from the sysmgr task ID to the basic-services task ID.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **show version** command displays a variety of system information, including hardware and software version, router uptime, boot settings (configuration register), and active software.

Task ID	Task ID	Operations
	basic-services	read

Examples The following example show partial output from the **show version** command:

```
RP/0/RP0/CPU0:router# show version
```

```
Cisco IOS XR Software, Version 3.4.0
Copyright (c) 2006 by cisco Systems, Inc.
```

```
ROM: System Bootstrap, Version 1.32(20050525:193559) [CRS-1 ROMMON],
```

```
CRS-8_P1 uptime is 1 week, 22 hours, 27 minutes
```


R3.5.0 Beta Draft—Cisco Confidential Information

System image file is "disk0:hfr-os-mbi-3.3.90/mbihfr-rp.vm"

R3.5.0 Beta Draft—Cisco Confidential Information

```

cisco CRS-8/S (7457) processor with 4194304K bytes of memory.
7457 processor at 1197Mhz, Revision 1.2

16 Packet over SONET/SDH network interface(s)
16 SONET/SDH Port controller(s)
2 Ethernet/IEEE 802.3 interface(s)
16 GigabitEthernet/IEEE 802.3 interface(s)
2043k bytes of non-volatile configuration memory.
38079M bytes of hard disk.
1000592k bytes of ATA PCMCIA card at disk 0 (Sector size 512 bytes).
1000640k bytes of ATA PCMCIA card at disk 1 (Sector size 512 bytes).

Package active on node 0/1/SP:
hfr-diags, V 3.3.90[1I], Cisco Systems, at disk0:hfr-diags-3.3.90
  Built on Mon Mar 27 12:29:00 UTC 2006
  By edde-bld1 in /vws/aga/production/3.3.90.1I/hfr/workspace for c2.95.3-p8

hfr-admin, V 3.3.90[1I], Cisco Systems, at disk0:hfr-admin-3.3.90
  Built on Mon Mar 27 09:22:26 UTC 2006
  By edde-bld1 in /vws/aga/production/3.3.90.1I/hfr/workspace for c2.95.3-p8

hfr-base, V 3.3.90[1I], Cisco Systems, at disk0:hfr-base-3.3.90
  Built on Mon Mar 27 09:13:04 UTC 2006
  By edde-bld1 in /vws/aga/production/3.3.90.1I/hfr/workspace for c2.95.3-p8

hfr-os-mpi, V 3.3.90[1I], Cisco Systems, at disk0:hfr-os-mpi-3.3.90
  Built on Mon Mar 27 08:34:13 UTC 2006
  By edde-bld1 in /vws/aga/production/3.3.90.1I/hfr/workspace for c2.95.3-p8
--More--

```

Table 24 describes the significant fields shown in the display.

Table 24 *show version Field Descriptions*

Field	Description
Cisco IOS XR software, Version	Cisco IOS XR software version number currently running on the router.
ROM	System bootstrap version number currently running on the router.
router uptime	Number of uninterrupted days, hours, minutes, and seconds the system has been up and running.
System image file is	Location and name of the system image file currently running on the router.
Packet over SONET/SDH network interface(s)	Number of Packet-over-SONET/SDH interfaces available on the current router.
SONET/SDH Port controller(s)	Number of SONET or SDH ¹ interfaces available on the current router.
Ethernet/IEEE 802.3 interface(s)	Number of Ethernet or IEEE 802.3 interfaces available on the current router.
GigabitEthernet/IEEE interface(s)	Number of Gigabit Ethernet or IEEE 802.3 interfaces available on the current router.
bytes of non-volatile configuration memory	Available volatile configuration memory, in bytes.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 24** *show version Field Descriptions (continued)*

Field	Description
bytes of ATA PCMCIA card at disk 0	ATA PCMCIA ² available on the card in disk 0, in bytes.
Package active on node 0/1/SP	Provides details about the current software package that is running on the SP node in slot 1.

1. Synchronous Digital Hierarchy

2. AT Attachment Personal Computer Memory Card Industry Association

R3.5.0 Beta Draft—Cisco Confidential Information

upgrade all

To upgrade the fabric-downloader, ROMMON, Mbus, and current field-programmable device (FPD) image package on a module or on all modules installed in a router, use the **upgrade all** command in administration EXEC mode.

upgrade all location {*node-id* | **all**} [**force**]

Syntax Description

location all	Upgrades all ROM images on all line cards (LCs) that are installed in the router.
location node-id	Upgrades all ROM images on a specific node. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation. Note Enter the show platform command to see the location of all nodes installed in the router.
force	(Optional) Skips the version check and forces an upgrade.

Defaults

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
sysmgr	read, write

Examples

The following example shows how to upgrade the all ROM images on all line cards that are installed in the router:

```
RP/0/0/CPU0:Router# admin
RP/0/0/CPU0:router(admin)# upgrade all all
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	clear mbus-statistics location	Clears all MBUS interface counters on a specific node.
	show mbus	Displays Mbus CAN errors and interface counters.
	show platform	Displays information and status on each node in the system.

R3.5.0 Beta Draft—Cisco Confidential Information

upgrade cpuctrlbits

To upgrade the CPU controller bits on all nodes that are installed in the router or on a specific node, use the **upgrade cpuctrlbits** command in administration EXEC mode.

upgrade cpuctrlbits {**all** | **location** *node-id*} [**bootflash** | **disk0** | **disk1** | **internal**]

Syntax Description

all	Upgrades the CPU controller bits on all nodes installed in the router.
location <i>node-id</i>	Upgrades the CPU controller bits on a specific node. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation. Note Enter the show platform command to see the location of all nodes installed in the router.
bootflash	(Optional) Use the images located on the bootflash to upgrade the CPU controller on all nodes, or on the specified node.
disk0	(Optional) Use the images located on disk0 to upgrade the CPU controller on all nodes, or on the specified node.
disk1	(Optional) Use the images located on disk1 to upgrade the CPU controller on all nodes, or on the specified node.
internal	(Optional) Use the images located in the /pkg/bin. Note This is the default location for the ROMMON image.

Defaults

Default location for the ROMMON image = **internal**

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	The upgrade cpuctrlbits command was moved from the sysmgr task ID to the system task ID.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
system	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to upgrade the CPU controller bits on all nodes in a router:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# upgrade cpuctrlbits all
```

Please do not power cycle, reload the router or reset any nodes until all upgrades are completed.
Please check the syslog to make sure that all nodes are upgraded successfully.
If you need to perform multiple upgrades, please wait for current upgrade to be completed before proceeding to another upgrade.
Failure to do so may render the cards under upgrade to be unusable.

Related Commands

Command	Description
show platform	Displays information and status on each node in the system.

R3.5.0 Beta Draft—Cisco Confidential Information

upgrade fabric-downloader

To upgrade the fabric-downloader image package on a module or on all modules installed in a router, use the **upgrade fabric-downloader** command in administration EXEC mode.

upgrade fabric-downloader location {*node-id* | **all**} [**force**]

Syntax Description

location *node-id*

Upgrades the fabric-downloader on a specific LC. The *node-id* is expressed in the *rack/slot/module* notation.

Note Enter the **show platform** command to see the location of all nodes installed in the router.

location all

Upgrades the fabric-downloader on all LCs that are installed in the router.

force

(Optional) Skips the version check and forces an upgrade.

Defaults

No default behavior or values

Command Modes

Administration EXEC

Command History**Release****Modification**

Release 3.2

This command was introduced on the Cisco XR 12000 Series Router.

Release 3.3.0

No modification.

Release 3.4.0

No modification.

Release 3.5.0

No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID**Task ID****Operations**

sysmgr

read, write

Examples

The following example shows how to upgrade the fabric-downloader image package on a specific node:

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

```
RP/0/0/CPU0:router(admin)# upgrade fabric-downloader location 0/0/CPU0
```

Related Commands

R3.5.0 Beta Draft—Cisco Confidential Information

Command	Description
show platform	Displays information and status on each node in the system.

R3.5.0 Beta Draft—Cisco Confidential Information

upgrade hw-module fpd

To manually upgrade the current field-programmable device (FPD) image package on a module, use the **upgrade hw-module fpd** command in administration EXEC mode.

```
upgrade hw-module fpd {all | fabldr | fpga-type | rommon | rommon2} [force] location [all | node-id] [reload]
```

Syntax Description

all	Upgrades all FPD images on the selected module.
fabldr	Upgrades the fabric-downloader image on the module.
<i>fpga-type</i>	Upgrades a specific field-programmable gate array (FPGA) image on the module. Use the show fpd package command to view all available FPGA images available for a specific module.
rommon	Upgrades the rommon on the module.
rommon2	Upgrades the rommon on the module.
force	(Optional) Forces the update of the indicated FPD image package on a shared port adapter (SPA) that meets the minimum version requirements. Without this option, the manual upgrade upgrades only incompatible FPD images.
location	Specifies the location of the module.
all	(Optional) Upgrades the FPD image of all modules in the router.
<i>node-id</i>	(Optional) Location of the module. Naming notation is <i>rack/slot/subslot</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the SPA interface processor (SIP). <i>subslot</i>: Subslot number of the SPA. For more information about the syntax for the router, use the question mark (?) online help function.
reload	(Optional) Reloads the module after the FPD image has been updated. If you do not use the reload keyword, you must manually reload the module before the FPD upgrade is complete. Use the hw-module reset or hw-module subslot reload command in EXEC mode to reload the module.

Defaults

No default behavior or values

Command Modes

Administration EXEC

R3.5.0 Beta Draft—Cisco Confidential Information**Command History**

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.3.0	The reload keyword was added to this command. Support for multiple FPGA images was added.
Release 3.4.0	No modification.
Release 3.4.1	The rommon2 keyword was added to this command.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

During the upgrade procedure, the module needs to be offline (shut down but powered).

Task ID

Task ID	Operations
system	read, write (on the Cisco CRS-1 router only)
sysmgr	read, write

Examples

The following example shows how to upgrade the default FPGA on a SPA in the Cisco CRS-1 router:

```
RP/0/RP0/CPU0:Router# admin
RP/0/RP0/CPU0:Router(admin)# upgrade hw-module fpd fpga force location 0/1/4

% RELOAD REMINDER:
- The upgrade operation of the target module will not interrupt its normal
  operation. However, for the changes to take effect, the target module
  will need to be manually reloaded after the upgrade operation. This can
  be accomplished with the use of "hw-module <target> reload" command.
- If automatic reload operation is desired after the upgrade, please use
  the "reload" option at the end of the upgrade command.
- The output of "show hw-module fpd location" command will not display
  correct version information after the upgrade if the target module is
  not reloaded.
Continue? [confirm] y

SP/0/1/SP:Dec 22 05:41:17.920 : upgrade_daemon[125]: programming...with file /ne
t/node0_RP1_CPU0/hfr-1c-3.3.83/fpd/ucode/fpga_gladiator_sw0.6.xsvf
SP/0/1/SP:Dec 22 05:41:28.900 : upgrade_daemon[125]: ...programming...
SP/0/1/SP:Dec 22 05:41:28.906 : upgrade_daemon[125]: ...it will take a while...
SP/0/1/SP:Dec 22 05:41:29.004 : upgrade_daemon[125]: ...it will take a while...
SP/0/1/SP:Dec 22 05:43:03.432 : upgrade_daemon[125]: ...programming...
SP/0/1/SP:Dec 22 05:43:03.438 : upgrade_daemon[125]: ...it will take a while...
Successfully upgraded spa fpga instance 4 on location 0/1/4.
```

The following example shows how to upgrade the default FPGA on a SPA in the Cisco XR 12000 Series Router:

```
RP/0/0/CPU0:Router# admin
RP/0/0/CPU0:Router(admin)# upgrade hw-module fpd fpga force location 0/3/0

% RELOAD REMINDER:
```

R3.5.0 Beta Draft—Cisco Confidential Information

- The upgrade operation of the target module will not interrupt its normal operation. However, for the changes to take effect, the target module will need to be manually reloaded after the upgrade operation. This can be accomplished with the use of "hw-module <target> reload" command.
- If automatic reload operation is desired after the upgrade, please use the "reload" option at the end of the upgrade command.
- The output of "show hw-module fpd location" command will not display correct version information after the upgrade if the target module is not reloaded.

Continue? [confirm] **y**

```
LC/0/3/CPU0:Dec 22 06:46:59.732 : spa_192_jacket_v2[203]: %SPA_FPD-6-UPDATE_STAR
T : SPA-4XCT3/DS0[0]: Starting update of FPD 'fpga' image
LC/0/3/CPU0:Dec 22 06:47:23.518 : spa_192_jacket_v2[203]: %SPA_FPD-6-UPDATE_PASS
ED : SPA-4XCT3/DS0[0]: Successfully updated FPD 'fpga' image
Successfully upgraded spa fpga instance 0 on location 0/3/0.
```

Related Commands

Command	Description
show hw-module fpd	Displays the FPD compatibility for all modules or a specific module.
show fpd package	Displays which FPD image package is needed for the router to properly support the modules for the running Cisco IOS XR software release. It also indicates all available FPD images that are available for a specific module.

R3.5.0 Beta Draft—Cisco Confidential Information

upgrade mbus

To upgrade the Mbus agent ROM image on a module or on all modules installed in a router, use the **upgrade mbus** command in administration EXEC mode.

upgrade mbus [**force**] **location** {**all** | *node-id*}

Syntax Description	force	(Optional) Skips the version check and forces an upgrade.
	location all	Upgrades the Mbus agent ROM on all line cards (LCs) that are installed in the router.
	location <i>node-id</i>	Upgrades the Mbus agent ROM on a specific node. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.
	Note	Enter the show platform command to see the location of all nodes installed in the router.

Defaults No default behavior or values

Command Modes Administration EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	sysmgr	read, write

Examples The following example shows how to upgrade the Mbus agent ROM on a specific node:

```
RP/0/0/CPU0:router# admin
RP/0/0/CPU0:router(admin)# upgrade mbus location 0/0/CPU0
```

```
Upgrading the MBUS agent rom on slot 0
RP/0/0/CPU0:Nov 18 16:52:23.296 : upgrade_mbus[65703]: %MBUS-6-API_INFO_DUMP : d
ownload status slot 0, DOWNLOAD_SUCCESS
RP/0/0/CPU0:Nov 18 16:52:33.422 : upgrade_mbus[65703]: %MBUS-6-API_INFO_DUMP : d
```

R3.5.0 Beta Draft—Cisco Confidential Information

```
ownload status slot 0, PROGRAM_ROM SUCCESS
Upgrade complete. Use admin CLI "test mbus soft-reset-agent" or OIR the card to
force new MBUS Rom image to execute.
```

Related Commands

Command	Description
clear mbus-statistics location	Clears all MBUS interface counters on a specific node.
show mbus	Displays Mbus CAN errors and interface counters.
show platform	Displays information and status on each node in the system.

R3.5.0 Beta Draft—Cisco Confidential Information

upgrade rommon (Cisco CRS-1 Router)

To upgrade the ROMMON on all nodes that are installed in the router or on a specific node, use the **upgrade rommon** command in administration EXEC mode.

upgrade rommon {a | b} {all | location *node-id*} [bootflash | disk0 | disk1 | internal]

Syntax Description		
a		Upgrades ROMMON A.
b		Upgrades ROMMON B.
all		Upgrades the CPU controller bits on all nodes installed in the router.
location <i>node-id</i>		Upgrades the CPU controller bits on a specific node. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.
	Note	Enter the show platform command to see the location of all nodes installed in the router.
bootflash		(Optional) Uses the images located on the bootflash to upgrade the CPU controller on all nodes, or on the specified node.
disk0		(Optional) Uses the images located on disk0 to upgrade the CPU controller on all nodes, or on the specified node.
disk1		(Optional) Uses the images located on disk1 to upgrade the CPU controller on all nodes, or on the specified node.
internal		(Optional) Uses the images in the /pkg/bin location.
	Note	This is the default location for the ROMMON image.

Defaults Default location for the ROMMON image = **internal**

Command Modes Administration EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	The upgrade rommon command was moved from the sysmgr task ID to the system task ID.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.5.0 Beta Draft—Cisco Confidential Information**Task ID**

Task ID	Operations
system	read, write

Examples

The following example shows how to upgrade ROMMON A on all nodes in a router:

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

```
RP/0/RP0/CPU0:router(admin)# upgrade rommon a all
```

Please do not power cycle, reload the router or reset any nodes until all upgrades are completed.

Please check the syslog to make sure that all nodes are upgraded successfully.

If you need to perform multiple upgrades, please wait for current upgrade to be completed before proceeding to another upgrade.

Failure to do so may render the cards under upgrade to be unusable.

Related Commands

Command	Description
show platform	Displays information and status on each node in the system.

R3.5.0 Beta Draft—Cisco Confidential Information

upgrade rommon (Cisco XR 12000 Series Router)

To upgrade the ROMMON image on a module or on all modules installed in the router, use the **upgrade rommon** command in administration EXEC mode.

upgrade rommon location {*node-id* | **all**} [**force**]

Syntax Description	location <i>node-id</i>	Upgrades the ROMMON on a specific line card. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.
	Note	Enter the show platform command to see the location of all nodes installed in the router.
	location all	Upgrades the ROMMON on all modules installed in a router.
	force	(Optional) Skips the version check and forces an upgrade.

Defaults No default behavior or values

Command Modes Administration EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	sysmgr	read, write

Examples The following example shows how to upgrade the ROMMON image on a specific node:

```
RP/0/0/CPU0:router# admin
RP/0/0/CPU0:router(admin)# upgrade rommon location 0/4/CPU0

===== Line Card (Slot 4) =====
Upgrading linecard rom-monitor
Erasing sectors: eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
Programming image: pppppppppp
Verifying image: vvvvvvvvvv
```

R3.5.0 Beta Draft—Cisco Confidential Information

Upgraded linecard rom-monitor successfully

Related Commands	Command	Description
	show platform	Displays information and status on each node in the system.



Fabric Management and Control Network Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

This chapter describes the Cisco IOS XR software commands used to monitor and control application-specific integrated circuit (ASIC) fabric queues for the Cisco XR 12000 Series Router line cards or Cisco CRS-1 modular services cards running Cisco IOS XR software.

R3.5.0 Beta Draft—Cisco Confidential Information

clear controller fabric statistics

To clear fabric plane statistics from the counters information table, use the **clear controller fabric statistics** command in administration EXEC mode.

clear controller fabric statistics plane [*plane-id* | **all**]

Syntax Description

plane <i>plane-id</i>	(Optional) The fabric plane and plane ID. Range is from 0 to 7.
plane all	(Optional) Specifies fabric statistics for all planes.

Defaults

Information for all planes is cleared

Command Modes

Administration EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	No modification.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **clear controller fabric statistics** command clears the fabric statistics for the specified fabric plane or all planes.

Task ID

Task ID	Operations
root-system	read, write, execute
fabric	read, write

Examples

The following example shows how to clear all fabric plane statistics from the router:

```
RP/0/RP0/CPU0:router(admin)# clear controller fabric statistics plane all
```

R3.5.0 Beta Draft—Cisco Confidential Information

clear controller fabricq statistics

To clear application-specific integrated circuit (ASIC) statistics for specific fabric queues, use the **clear controller fabricq statistics** command in EXEC mode.

clear controller fabricq statistics [**instance** *asic_instance*] [**location** *node-id*]

Syntax Description	instance <i>asic_instance</i>	(Optional) Identifies the fabric queue instance whose ASIC statistics you want to clear. Range is from 1 through 3.
	location <i>node-id</i>	(Optional) Identifies a node on which to clear ASIC statistics for a specific fabric queue, or for all fabric queues. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults	The default is to enter the clear controller fabricq statistics command without any optional keyword arguments to clear ASIC statistics for all fabric queues on the router.

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	No modification.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Only locations that contain a fabric queue ASIC can be specified for the **location** *node-id*.

This command is intended for use while performing special maintenance, test, or debugging procedures. It should not be necessary to use this command when fabric connectivity is performing normally.

Task ID	Task ID	Operations
	root-system	execute
	drivers	read, write

R3.5.0 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to clear ASIC statistics on all fabric queues on the node located in 0/1/CPU0:

```
RP/0/RP0/CPU0:router# clear controller fabricq statistics location 0/1/CPU0
```

The following example shows how to clear ASIC statistics for a specific fabric queue on all nodes that are installed in the router:

```
RP/0/RP0/CPU0:router# clear controller fabricq statistics instance 2
```

The following example shows how to clear ASIC statistics for a specific fabric queue on a specific node:

```
RP/0/RP0/CPU0:router# clear controller fabricq statistics instance 2 location 0/1/CPU0
```

Related Commands

Command	Description
show controllers fabricq statistics	Displays statistics about packet flow through the fabric queue ASIC.

R3.5.0 Beta Draft—Cisco Confidential Information

clear controller ingressq statistics

To clear application-specific integrated circuit (ASIC) statics from the ingress fabric queue on a specific node, or on all nodes installed in the router, use the **clear controller ingressq statistics** command in EXEC mode.

clear controller ingressq statistics [**location** *node-id*]

Syntax Description

location <i>node-id</i>	(Optional) Identifies the node whose ASIC statistics you want to clear from the ingress fabric queue. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults

Enter the **clear controller ingressq statistics** command without the optional **location** *node-id* keyword argument to clear the ASIC statistics from the ingress queues on all nodes that are installed in the router.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	No modification.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Only locations that contain a fabric queue ASIC can be specified for the **location** *node-id*.

The **clear controller ingressq statistics** command is intended for use while performing special maintenance, test, or debugging procedures. It should not be necessary to use this command when fabric connectivity is performing normally.

Task ID

Task ID	Operations
drivers	read, write

Examples

The following example shows how to use the **clear controller ingressq statistics** command to clear all ASIC statistics in the ingress fabric queue from the location 0/1/CPU0:

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router# clear controller ingressq statistics location 0/1/CPU0
```

Related Commands	Command	Description
	show controllers ingressq statistics	Displays statistical information for the ingress queue ASIC.

R3.5.0 Beta Draft—Cisco Confidential Information

clear controller switch

To clear the statistics for the Broadcom switches for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card, use the **clear controller switch** command in administration EXEC mode.

clear controller switch {*instance*} {*statistics*} {**all** {*location node-id*} | *location node-id* | **ports** *number*{*location node-id*}}

Syntax Description	<i>instance</i>	Switch instance identifier. The switch number is either 0 or 1.
	statistics	Clears statistics for packets transmitted/received on switch ports.
	all	Clears statistics for all ports.
	location <i>node-id</i>	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the <i>node-id</i> argument as entered in the <i>rack/slot/module</i> notation.
	ports <i>number</i>	Clears statistics for a specific switch port.

Defaults No default behavior or values

Command Modes Administration EXEC

Command History	Release	Modification
	Release 3.4.1	This command was updated on the Cisco CRS-1 to include inter-rack switches.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **clear controller switch** command is used to specify intra-rack switches.

Task ID	Task ID	Operations
	root-system	execute

Examples :The following example shows how to clear the statistics for the Broadcom switches:

```
RP/0/0/CPU0:router(admin)# clear controller switch 1 statistics all location f0/sc0/cpu0
```

R3.5.0 Beta Draft—Cisco Confidential Information

clear controller switch errdisable

To clear the err-disable state of the switch port for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card, use the **clear controller switch errdisable** command in administration EXEC mode.

clear controller switch errdisable {port {FE | GE} {0 | 1}} {location *node-id*}

Syntax Description

port	Specifies the port.
FE	Specifies the ports for the Fast Ethernet (FE).
GE	Specifies the ports for the Gigabit Ethernet (GE).
0	Specifies port number 0 for the backplane FE.
1	Specifies port number 1 for the backplane FE.
location <i>node-id</i>	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the <i>node-id</i> argument as entered in the <i>rack/slot/module</i> notation.

Defaults

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.4.1	This command was updated on the Cisco CRS-1 to include inter-rack switches.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
root-system	execute

Examples

The following example shows how to clear the error disable state for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card:

```
RP/0/RP0/CPU0:router(admin)## clear controller switch errdisable port GE 1 location
f0/sc0/cpu0
```

R3.5.0 Beta Draft—Cisco Confidential Information

clear controller switch inter-rack

To clear the ISC switch counters, use the **clear controller switch inter-rack** command in administration EXEC mode.

```
clear controller switch inter-rack {errdisable {ports {number | all} | statistics {all | ports  
number}} {location node-id}}
```

Syntax Description	errdisable	Clears the err-disabled state of the port if the port was brought down by Unidirectional Link Detection (UDLD).
	ports	Specifies the port.
	number	Number for the port. The range is from 0 to 21.
	all	Specifies all ports for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card.
	statistics	Clears the statistics for the switch.
	all	Specifies all of the ports.
	location node-id	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the <i>node-id</i> argument as entered in the <i>rack/slot/module</i> notation.

Defaults	No default behavior or values

Command Modes	Administration EXEC

Command History	Release	Modification
	Release 3.4.1	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **clear controller switch inter-rack** command is used to specify inter-rack switches.

Task ID	Task ID	Operations
	root-system	execute

Examples

The following example shows how to clear statistics for all the ports for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card:

 clear controller switch inter-rack

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(admin)# clear controller switch inter-rack statistics all location  
f0/sc0/cpu0
```

R3.5.0 Beta Draft—Cisco Confidential Information

clear fabricq counters

To clear to fabric or from fabric counters associated with the fabric queue driver, use the **clear fabricq counters** command in administration EXEC mode.

clear fabricq counters {frfab | tofab} [all | error | packet] location node-id

Syntax Description	frfab	Clears the from fabric queue counters.
	tofab	Clears to fabric queue counters.
	all	(Optional) Clears all counters.
	error	(Optional) Clears error counters.
	packet	(Optional) Clears packet counters.
	location node-id	Identifies the node whose fabric counters you want to clear. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults All fabric queue driver counters are cleared

Command Modes Administration EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	fabric	read
	root-system	read

Examples The following example shows how to clear all to fabric queue counters for the location 0/1/CPU0:

```
RP/0/0/CPU0:router(admin)# clear fabricq counters tofab location 0/1/CPU0
```

The following example shows how to clear all fabricq counters for the location 0/1/CPU0:

```
RP/0/0/CPU0:router(admin)# clear fabricq counters all location 0/1/CPU0
```

 clear fabricq counters

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show controllers fabricq frfab	Displays from fabric statistics.
	show controllers fabricq tofab	Displays to fabric statistics.

R3.5.0 Beta Draft—Cisco Confidential Information

controllers fabric plane

To configure optical interface module (OIM) fabric plane properties, use the **controllers fabric plane** command in administration configuration mode. To return the OIM fabric plane properties to their default configuration, use the **no** form of this command.

controllers fabric plane *plane-id* **oim** {**count** {**1** | **3**} | **width** {**1** | **2**} | **instance** *oim-instance*
location *node-id*}

no controllers fabric plane *plane-id* **oim** {**count** {**1** | **3**} | **width** {**1** | **2**} | **instance** *oim-instance*
location *node-id*}

Syntax Description

<i>plane-id</i>	Identifies the fabric plane. Range is from 0 to 7.
count { 1 3 }	Configures the number of OIMs used in this plane. Enter 1 to configure all cables in the plane to connect to the same OIM. Enter 3 to configure the cables from each fabric card to connect to different OIMs.
width { 1 2 }	Width of OIMs) in the current fabric plane. Enter 1 to indicate a single-width OIM that covers one slot only. Enter 2 to indicate a dual-width OIM that covers two slots.
instance { <i>oim-instance</i> }	Specifies the properties a specific OIM. Range is from 0 through 2.
location <i>node-id</i>	Identifies the node whose OIM fabric plane properties you want to configure. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults

No default behavior or values

Command Modes

Administration configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	- The topology keyword was removed from the controllers fabric plane command syntax. - The oim, count, width, and instance keywords were added to the controllers fabric plane command syntax.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.5.0 Beta Draft—Cisco Confidential Information**Task ID****Task ID****Operations**

fabric

read, write

Examples

The following example shows how to configure all cables in the fabric plane to connect to the same OIM:

```
RP/0/RP0/CPU0:router(admin-config)# controllers fabric plane 3 oim count 1
```


R3.5.0 Beta Draft—Cisco Confidential Information

controllers fabric plane shutdown

To shut down the state of a fabric plane, use the **controllers fabric plane shutdown** command in administration configuration mode. To disable the state of a fabric plane, use the **no** form of this command.

controllers fabric plane *plane-id* shutdown

no controllers fabric plane *plane-id* shutdown

Syntax Description

<i>plane-id</i>	Fabric plane identifier. Range is from 0 to 7.

Defaults

The controller fabric plane is not shut down, and data continues to flow through the plane.

Command Modes

Administration configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **controllers fabric plane shutdown** command to perform a graceful shutdown of the fabric plane before a fabric reconfiguration or fabric plane migration. This ensures that data is not flowing through the plane.

Task ID

Task ID	Operations
fabric	read, write

Examples

The following example shows fabric plane 3 being shut down:

```
RP/0/RP0/CPU0:router(admin-config)# controllers fabric plane 3 shutdown
```

R3.5.0 Beta Draft—Cisco Confidential Information

controllers fabric rack

To put the rack into installation mode so that no traffic is sent over the switch fabric, use the **controllers fabric rack** command in administration configuration mode. To reenale traffic to be sent over the switch fabric, use the **no** form of this command.

controllers fabric rack *rack_number* **install-mode**

no controllers fabric rack *rack_number* **install-mode**

Syntax Description	<i>rack_number</i>	Rack number. Range is from 0 through 17.
	install-mode	Puts the specified rack into installation mode, so that no traffic is sent over the switch fabric.

Defaults	No default behavior or values

Command Modes	Administration configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	fabric	read, write

Examples	The following example shows how to put the rack into installation mode so that no traffic is sent over the switch fabric:

```
RP/0/RP0/CPU0:router # admin
RP/0/RP0/CPU0:router (config)# configure
RP/0/RP0/CPU0:router (admin-config)# controllers fabric rack 1 install-mode
```

R3.5.0 Beta Draft—Cisco Confidential Information

controllers fabric statistics collection

To enable the collection of fabric statistics data and configure the interval at which statistics are collected, use the **controllers fabric statistics collection** command in administration configuration mode. To return the system to the default interval setting, use the **no** form of this command.

controllers fabric statistics collection {**control** [**refresh**] | **interval** *seconds*}

no controllers fabric statistics collection {**control** [**refresh**] | **interval** *seconds*}

Syntax Description

control	Enables fabric statistics data collection.
refresh	(Optional) Causes the system to collect data immediately.
interval <i>seconds</i>	Specifies the interval, in seconds, between collection of data for fabric statistics. Range is from 10 to 180 seconds. Default is 30 seconds.

Defaults

Control of fabric statistics data collection = enabled
Interval= 30 seconds.

Command Modes

Administration configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
fabric	read, write

Examples

The following example shows statistic data collection on the fabric being disabled:

```
RP/0/RP0/CPU0:router(admin-config)# controllers fabric statistics collection control  
disable
```

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers fabric

To display fabric card information, use the **show controllers fabric** command in administration EXEC mode.

show controllers fabric [**clock** | **csc-fpga** | **fab-clk** | **fab-control** | **sca** | **xbar**]

Syntax Description	clock	(Optional) Displays which fabric clock each slot is synchronized to and whether the clock is redundant or not.
	csc-fpga	(Optional) Displays registers associated with the csc-fpga on each fabric card (FC).
	fab-clk	(Optional) Displays registers associated with the fabric clock FPGA on all route processors (RPs), line cards (LCs), and FCs.
	fab-control	(Optional) Displays the state of all RPs, LCs, and FCs in the chassis from a fabric control software perspective.
	sca	(Optional) Displays registers associated with Scheduler Control ASIC on the CSC cards.
	xbar	(Optional) Displays registers associated with the Cross Bar (XBAR) ASIC on the clock scheduler card (CSC) and switch fabric card (SFC).

Defaults All fabric card information is displayed

Command Modes Administration EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show controllers fabric** command to display various registers associated with the fabric cards and state information associated with the fabric control software.

Task ID	Task ID	Operations
	root-system	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following is sample output from the **show controllers fabric clock** command:

```
RP/0/0/CPU0:router(admin)# show controllers fabric clock
```

```
The Primary Clock for system is CSC_0  
System Fabric Clock is Redundant
```

Slot #	Primary Clock	Mode
3	CSC_0	Redundant
4	CSC_0	Redundant
5	CSC_0	Redundant
11	CSC_0	Redundant
12	CSC_0	Redundant
15	CSC_0	Redundant
16	CSC_0	Redundant
17	CSC_0	Redundant
18	CSC_0	Redundant
19	CSC_0	Redundant
20	CSC_0	Redundant

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers fabric bundle

To display fabric card bundle information, use the **show controllers fabric bundle** command in administration EXEC mode.

show controllers fabric bundle {*node-id* [**brief** | **detail**] | **all** [**brief** | **detail**] | **port** *port-id* [**brief** | **detail** | **statistics**] | **summary**}

Syntax Description	
<i>node-id</i>	Identifies a node whose fabric bundle information you want to display. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation. Follow the <i>node-id</i> argument with one of the following optional keywords to display the data a specific format: brief—Displays brief information about the fabric bundle. detail—Displays detailed information about the fabric bundle.
brief	(Optional) Displays brief information about the specified fabric bundle port or ports. This is the default.
detail	(Optional) Displays detailed information about the specified fabric bundle port or ports.
all	Displays bundle information for all fabric bundles. Follow the all keyword with one of the following optional keywords to display the data a specific format: brief—Displays brief information about the fabric bundles. detail—Displays detailed information about the fabric bundles.
port <i>port-id</i>	Identifies a port whose fabric bundle information you want to display. The <i>port-id</i> argument is entered in the <i>rack/slot/module/port</i> notation. Follow the <i>port-id</i> argument with one of the following optional keywords to display the data a specific format: brief—Displays brief information about the fabric bundle. detail—Displays detailed information about the fabric bundle. statistics—Displays fabric bundle statistics for the specified port.
statistics	Displays fabric bundle statistics.
summary	Displays summarized fabric bundle information.

Defaults Information is displayed for all fabric bundle ports on the router.

Command Modes Administration EXEC

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1.

R3.5.0 Beta Draft—Cisco Confidential Information

Release	Modification
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
fabric	read

Examples

The following is sample output from the **show controllers fabric bundle** command:

```
RP/0/0/CPU0:router(admin)# show controllers fabric bundle all
```

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers fabric connectivity

To display controller fabric connectivity information, use the **show controllers fabric connectivity** command in administration EXEC mode.

show controllers fabric connectivity {all | *node-id*} [brief | detail]

Syntax Description

all	Specifies all controller fabric ports.
<i>node id</i>	Specifies the fabric port associated with the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
brief	(Optional) Specifies brief information about controller fabric connectivity. This is the default.
detail	(Optional) Specifies detailed information about controller fabric connectivity.

Defaults

Brief information about controller fabric connectivity is displayed.

Command Modes

Administration EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	No modification.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show controllers fabric connectivity** command to monitor a modular services card as it sends data to the fabric or receives data from the fabric.

Task ID

Task ID	Operations
fabric	read

Examples

The following is sample output from the **show controllers fabric connectivity** command that displays fabric connectivity information in brief form for all resources:

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(admin)# show controllers fabric connectivity all brief
```

Card Percent R/S/M Uptime	In Use	Tx Planes 01234567	Rx Planes 01234567	Monitored For (s)	Total Uptime (s)
0/2/CPU0 100.0000	1	.1.....	.1.....	20913	20913
0/RP0/CPU0	1	.1.....	.1.....	20913	20913

The following is sample output from the **show controllers fabric connectivity** command that displays detailed fabric connectivity information for all resources:

```
RP/0/RP0/CPU0:router(admin)# show controllers fabric connectivity all
```

Card R/S/M	In Use	Tx Planes 01234567	Rx Planes 01234567	Monitored For (s)	Total Uptime (s)	Percent Uptime
0/1/CPU0	1	.1.....	.1.....	8561	8561	100.0000
0/2/CPU0	1	.1.....	.1.....	8561	8561	100.0000
0/RP1/CPU0	1	.1.....	.1.....	8561	8561	100.0000

The following is sample output from the **show controllers fabric connectivity** command that displays fabric connectivity information for the modular services card on node 0/0/CPU0:

```
RP/0/RP0/CPU0:router(admin)# show controller fabric connectivity 0/0/CPU0
```

Card R/S/M	In Use	Tx Planes 01234567	Rx Planes 01234567	Monitored For (s)	Total Uptime (s)	Percent Uptime
0/0/CPU0	1	.1.....	.1.....	8805	8805	100.0000

Table 25 describes the significant fields shown in the display.

Table 25 *show controllers fabric connectivity Field Descriptions*

Field	Description
Card R/S/M	Identifies the fabric card, in the format <i>rack/slot/module</i> .
In Use	Indicates the number of fabric ports that are in use on the card.
Tx Planes	Indicates activity on the transmit fabric plane.
Rx Planes	Indicates activity on the receive fabric plane.
Monitored For (s)	Elapsed time in seconds since monitoring began.
Total Uptime	Total uptime expressed in seconds.
Percent Uptime	Percentage of time the card has been up since monitoring began.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers fabric fgid resource

To display information about the fabric resources that are allocated to specific Secure Domain Router (SDR) fabric group IDs (FGIDs), use the **show controllers fabric fgid resource** command in administration EXEC mode.

```
show controllers fabric fgid resource {all | sdr {Owner | sdr_name} {all | application {CLI |
GSP | LPTS} id fabric_fgid [elements number_of_fgids]}}
```

Syntax Description		
all		Displays FGID resource information for all Secure Domain Routers (SDRs) on the current system.
sdr		Specifies an individual Secure Domain Router (SDR).
<i>sdr_name</i>		Identifies a specific SDR that is configured on the router.
{ Owner <i>sdr_name</i> }		Displays information for all resources allocated to the specified Secure Domain Routers (SDRs).
all		
Owner		Specifies the owner SDR.
application		Displays information for a specific resource allocated to the owner Secure Domain Routers (SDRs). follow the sdr Owner application keywords with one of the following keywords to specify a particular resource application: • CLI • GSP • LPTS
CLI		Displays command line interface (CLI) information for the owner SDR.
GSP		Displays Gateway Service Protocol (GSP) information for the owner SDR.
LPTS		Displays Local Packet Transport Services (LPTS) information for the owner SDR.
id <i>fabric_fgid</i>		Fabric FGID whose SDR resource information you want to display. Replace with an FGID. Range is from 0 through 1000000
elements <i>number_of_fgids</i>		(Optional) Number of fabric FGIDs to display in the command output. Replace <i>number_of_fgids</i> with the number of FGIDs to list in the command output. Range is from 1 through 1000000.

Defaults No default behavior or values

Command Modes Administration EXEC

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show controllers fabric fgid resource** command to verify the multicast resource ID for the fabric card multicast bit set.

Task ID

Task ID	Operations
fabric	read

Examples

The following example shows sample output from the show controllers fabric fgid resource command. In this example, LPTS information is displayed for the SDR owner FGID 1000:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# show controllers fabric fgid resource sdr Owner application
lpts id 1000 elements 1
```

```
=====
Displaying FGID Info for:
SDR: Owner APPLICATION : LPTS
**** No FGID's allocated ****
RP/0/RP0/CPU0:P1_CRS-8(admin)#show controllers fabric fgid resource sdr Owner $
```

```
=====
Displaying FGID Info for:
SDR: Owner APPLICATION : LPTS
**** No FGID's allocated ****
```

The following example shows sample output from the show controllers fabric fgid resource command. In this example, fabric resource information is displayed for all SDRs in the system:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# show controllers fabric fgid resource all
```

```
=====
Displaying FGID Info for:
SDR: Owner APPLICATION : CLI
**** No FGID's allocated ****

=====
Displaying FGID Info for:
SDR: Owner APPLICATION : GSP
1024, 1025, 1026, 1027, 1028, 1029, 1030, 1031, 1032, 1033
1034, 1035, 1036, 1037, 1038, 1039, 1040, 1041, 1042, 1043
1044, 1045, 1046, 1047, 1048, 1049, 1050, 1051, 1052, 1053
1054, 1055, 1056, 1057, 1058, 1059, 1060, 1061, 1062, 1063
1064, 1065, 1066, 1067, 1068, 1069, 1070, 1071, 1072, 1073
1074, 1075, 1076, 1077, 1078, 1079, 1080, 1081, 1082, 1083
1084, 1085, 1086, 1087, 1088, 1089, 1090, 1091, 1092, 1093
1094, 1095, 1096, 1097, 1098, 1099, 1100, 1101, 1102, 1103
1104, 1105, 1106, 1107, 1108, 1109, 1110, 1111, 1112, 1113
1114, 1115, 1116, 1117, 1118, 1119, 1120, 1121, 1122, 1123
1124, 1125, 1126, 1127, 1128, 1129, 1130, 1131, 1132, 1133
1134, 1135, 1136, 1137, 1138, 1139, 1140, 1141, 1142, 1143
1144, 1145, 1146, 1147, 1148, 1149, 1150, 1151, 1152, 1153
1154, 1155, 1156, 1157, 1158, 1159, 1160, 1161, 1162, 1163
1164, 1165, 1166, 1167, 1168, 1169, 1170, 1171, 1172, 1173
```

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers fabric fgid statistics

To display resource statistical information for the fabric group ID (FGID), use the **show controllers fabric fgid statistics** command in administration EXEC mode.

show controllers fabric fgid statistics {all | pool | sdr | system} [brief | detail]

Syntax Description

all	Specifies all FGID resource statistical information for the logical router and FGID resource pools.
sdr	Specifies FGID resource statistics about the secure domain router (SDR).
pool	Specifies FGID statistical information about the resource pool.
system	Specifies FGID resource statistics for the entire physical router.
brief	(Optional) Specifies brief information about FGIDs. This is the default.
detail	(Optional) Specifies detailed information about FGIDs.

Defaults

Brief information is displayed

Command Modes

Administration EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	No modification.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show controllers fabric fgid statistics** command to monitor FGID resource usage based on a system, pool, or client view.

Task ID

Task ID	Operations
fabric	read
root-system	read, execute

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following is sample output from the **show controllers fabric fgid statistics** command that displays resource statistics for the fabric FGID in detailed form with all resources activated:

```
RP/0/RP0/CPU0:router(admin)# show controllers fabric fgid statistics all detail
```

Fabric FGID Resource Statistics Information:

System wide Fabric multicast resource statistics:

```
Total number of FGIDs in the system is 1000000
Current number of InUse FGIDs in the system is 500
High Water Mark of InUse FGIDs in the system is 500
```

Per SDR basis Fabric multicast resource statistics:

```
Secure Domain Router Name is Owner
InUse FGIDs is 500
High Water Mark InUse FGIDs is 500
```

Per client basis FGID resource utilization:

	Appl Name	Appl ID	Pool ID	Current InUse FGIDs	HighWater Mark InUse FGIDs

	CLI	0	2	0	0
	LPTS	1	1	0	0
	GSP	2	0	500	500

Per Pool basis Fabric multicast resource statistics:

```
Pool Identifier is 0
Pool Name is GSP
Pool type is Dedicated
The starting FGID of this pool is 1024
Total FGIDs of this pool is 10240
InUse FGIDs of this pool is 500
High Water Mark InUse FGIDs of this pool is 500
```

```
Pool Identifier is 1
Pool Name is LPTS
Pool type is Dedicated
The starting FGID of this pool is 11264
Total FGIDs of this pool is 32768
InUse FGIDs of this pool is 0
High Water Mark InUse FGIDs of this pool is 0
```

```
Pool Identifier is 2
Pool Name is COMMON
Pool type is Shared
The starting FGID of this pool is 44032
Total FGIDs of this pool is 955968
InUse FGIDs of this pool is 0
High Water Mark InUse FGIDs of this pool is 0
```

Table 26 describes the significant fields shown in the display.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 26** *show controllers fabric fgid statistics Field Descriptions*

Field	Description
Total number of FGIDs in the system	Total number of fabric FGIDs in the system.
Current number of Inused FGIDs in the system	Total number of fabric FGIDs in use in the system.
High Water Mark of Inused FGIDs in the system	Number of in-use fabric FGIDs at the highest point within the system.
Secure Domain Router Name	Name of the SDR.
Inused FGIDs	Inused (in-use) fabric FGID.
High Water Mark inused FGIDs	Number of inused (in-use) FGIDs since monitoring started.
Appl Name	Application name.
Appl ID	Application ID.
Pool ID	Pool ID.
Current InUsed FGIDs	Current number of inused (in-use) FGIDs.
Pool Identifier	Group pool identifier number.
Pool Name	Group pool name.
Pool type	Group pool type.
Total FGIDs of this pool	Number of FGIDs in the pool.
Inused FGIDs of this pool	Number of FGIDs inused (in-use) in the pool.
High Water Mark inused FGIDs of this pool	Number of FGIDs in the pool since the start of monitoring.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers fabric fsdb-pla all

To display plane availability status information for all racks in the system, use the **show controllers fabric fsdb-pla all** command in administration EXEC mode.

show controllers fabric fsdb-pla all

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Administration EXEC

Command History	Release	Modification
	Release 3.3.1	This command was introduced on the Cisco CRS-1.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show controllers fabric fsdb-pla all** command to verify line card connectivity to the fabric planes.

Task ID	Task ID	Operations
	fabric	read

Examples The following example shows sample output from the show controllers fabric fsdb-pla all command:

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

RP/0/RP0/CPU0:router (admin)# show controllers fabric fsdb-pla all

Rack 0:
=====

SrcGrp:0
01234567
Multicast Mask 11111111
Unicast Mask 11111111

Destination S3-Fabricq Reachability Mask Downloaded Mask
Address Mask SrcGrp:0 SrcGrp:0
```

 show controllers fabric fsdb-pla all

R3.5.0 Beta Draft—Cisco Confidential Information

```
01234567 01234567 01234567
```

```
-----
```

```
4 11111111 11111111 11111111
5 11111111 11111111 11111111
12 11111111 11111111 11111111
13 11111111 11111111 11111111
24 11111111 11111111 11111111
25 11111111 11111111 11111111
30 11111111 11111111 11111111
31 11111111 11111111 11111111:
```


R3.5.0 Beta Draft—Cisco Confidential Information

show controllers fabric link port

To display link information for a specific fabric port, use the **show controllers fabric link port** command in administration EXEC mode.

```
show controllers fabric link port {fabricqrx | ingressqtx | s1ro | s1rx | s1tx | s2rx | s2tx | s3rx |
s3tx} {port | all} [brief | detail]
```

Syntax Description		
fabricqrx		Displays information for the fabric queue receive port.
ingressqtx		Displays information for the ingress queue transmit port.
s1ro		Displays information for the S1 Out-of-Band receive port. The out of band ports connect the fabric planes together so that the flow control information collected within a fabric plane is distributed across all fabric planes. This is essential in controlling fabric congestion and the congestion location within fabric.
s1rx		Displays information for the Stage 1 (S1) receive port. The S1 receive port distributes incoming traffic.
s1tx		Displays information for the Stage 1 (S1) transmit port. The S1 transmit port distributes outgoing traffic.
s2rx		Displays information for the Stage 2 (S2) receive port. The S2 receive port forwards incoming cells to Stage 3 (S3) port.
s2tx		Displays information for the Stage 2 (S2) transmit port. The S2 transmit port forwards outgoing cells to Stage 3 (S3) transmit port.
s3rx		Displays information about S3 receive port. The S3 receive port performs switching for incoming traffic.
s3tx		Displays information about S3 transmit port. The S3 receive port performs switching for outgoing traffic.
<i>port</i>		Specifies the port whose fabric link information you want to display. Replace <i>port</i> with a port identifier. The <i>port</i> naming notation is in the <i>rack/slot/module/asic/port</i> format. Note A slash mark between values is required as part of the <i>port</i> naming notation.
all		Displays fabric link information for all specified ports.
brief		(Optional) Displays summarized fabric link information.
detail		(Optional) Specifies that the command output includes detailed fabric link information.

Defaults

Enter the **show controllers fabric link port** command without specifying any of the optional parameters to display summarized fabric link information. This is the same information that is displayed when you include the **brief** option in the **show controllers fabric link port** command string.

Command Modes

Administration EXEC

R3.5.0 Beta Draft—Cisco Confidential Information**Command History**

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show controllers fabric link port** command to check the health of fabric internal connections.

Task ID

Task ID	Operations
fabric	read

Examples

The following example shows partial sample output from the show controllers fabric link port command for all S1RO ports in the system:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router (admin)# show controllers fabric link port s1ro all
```

```
Flags: P - plane admin down, p - plane oper down
C - card admin down, c - card oper down
L - link port admin down, l - linkport oper down
A - asic admin down, a - asic oper down
B - bundle port admin Down, b - bundle port oper down
I - bundle admin down, i - bundle oper down
N - node admin down, n - node down
o - other end of link down d - data down
f - failed component downstream
m - plane multicast down
Sfe Port Admin Oper Down Other Near-end Far-end
R/S/M/A/P State State Flags End Bport Bport
-----
```

```
0/SM0/SP/0/0 UP UP 0/SM0/SP/1/15
0/SM0/SP/0/1 UP UP 0/SM1/SP/0/33
0/SM0/SP/0/2 UP UP 0/SM1/SP/1/33
0/SM0/SP/0/3 UP UP 0/SM2/SP/0/33
0/SM0/SP/0/4 UP UP 0/SM2/SP/1/33
0/SM0/SP/0/5 UP UP 0/SM3/SP/0/33
0/SM0/SP/0/6 UP UP 0/SM3/SP/1/33
0/SM0/SP/1/0 UP UP 0/SM0/SP/0/15
0/SM0/SP/1/1 UP DOWN 1 Unused
0/SM0/SP/1/2 UP UP Unused
0/SM0/SP/1/3 UP DOWN 1 Unused
0/SM0/SP/1/4 UP DOWN 1 Unused
0/SM0/SP/1/5 UP DOWN 1 Unused
0/SM0/SP/1/6 UP DOWN 1 Unused
0/SM1/SP/0/0 UP UP 0/SM1/SP/1/15
0/SM1/SP/0/1 UP UP 0/SM0/SP/0/33
0/SM1/SP/0/2 UP UP 0/SM0/SP/1/33
0/SM1/SP/0/3 UP UP 0/SM2/SP/0/51
--More--
```

R3.5.0 Beta Draft—Cisco Confidential Information

The following example shows partial sample output from the show controllers fabric link port command with the detail keyword included in the command string:

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

```
RP/0/RP0/CPU0:router (admin)# show controllers fabric link port fabricqrx all detail
```

```
Flags: P - plane admin down, p - plane oper down
C - card admin down, c - card oper down
L - link port admin down, l - linkport oper down
A - asic admin down, a - asic oper down
B - bundle port admin Down, b - bundle port oper down
I - bundle admin down, i - bundle oper down
N - node admin down, n - node down
o - other end of link down d - data down
f - failed component downstream
m - plane multicast down
```

```
Sfe Port Admin Oper Down Sfe BP Port BP Other
R/S/M/A/P State State Flags Role Role End
```

```
-----
0/1/CPU0/0/0 UP UP A A 0/SM0/SP/0/15
-----
```

```
Link Type Pin1 Name Pin2 Name
-----
```

```
CHASSIS G5 A4
```

```
Sfe Port Admin Oper Down Sfe BP Port BP Other
R/S/M/A/P State State Flags Role Role End
```

```
-----
0/1/CPU0/0/1 UP UP A B 0/SM0/SP/0/39
-----
```

```
Link Type Pin1 Name Pin2 Name
-----
```

```
CHASSIS G19 A34
```

```
Sfe Port Admin Oper Down Sfe BP Port BP Other
R/S/M/A/P State State Flags Role Role End
```

```
-----
0/1/CPU0/0/2 UP UP A A 0/SM0/SP/0/14
```

```
--More--
```

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers fabric plane

To display system fabric plane information, use the **show controllers fabric plane** command in administration EXEC mode.

show controllers fabric plane {*plane-id* | **all**} [**brief** | **detail** | **statistics** {**brief** | **detail**}]

Syntax Description

<i>plane-id</i>	Plane number. Range is from 0 to 7.
all	Specifies that all information about system fabric planes is displayed.
brief	(Optional) Specifies brief information about the system fabric plane. This is the default.
detail	(Optional) Specifies detailed information about the system fabric plane.
statistics	(Optional) Specifies statistical information for cell activity within the plane.

Defaults

Brief information is displayed

Command Modes

Administration EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	No modification.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show controllers fabric plane** command to monitor the fabric plane status, and the cell traffic and error statistics to or from the fabric plane.

Task ID

Task ID	Operations
root-system	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following is sample output from the **show controllers fabric plane** command that displays system fabric plane information from all fabric planes:

```
RP/0/RP0/CPU0:router(admin)# show controllers fabric plane all
```

Plane Id	Admin State	Oper State	Down Flags	Total Bundles	Down Bundles
0	UP	DOWN	p	0	0
1	UP	UP		0	0
2	UP	DOWN	p	0	0
3	UP	DOWN	p	0	0
4	UP	DOWN	p	0	0
5	UP	DOWN	p	0	0
6	UP	DOWN	p	0	0
7	UP	DOWN	p	0	0

The following is sample output from the **show controllers fabric plane** command that displays system fabric plane statistics from fabric plane 1 in brief form:

```
RP/0/RP0/CPU0:router(admin)# show controllers fabric plane 1 statistics brief
```

Plane	In Cells	Out Cells	CE Cells	UCE Cells	PE Cells
1	0	0	0	0	0

The following is sample output from the **show controllers fabric plane** command that displays system fabric plane statistics from fabric plane 1 in detailed form:

```
RP/0/RP0/CPU0:router(admin)# show controllers fabric plane 1 statistics detail
```

```
The fabric plane number is 1
Total number of providers for the statistics: 0
Total received data cells: 0
Total transmitted data cells: 0
Total received correctable errored cells: 0
Total received uncorrectable errored cells: 0
Total received parity error cells: 0
Total unicast lost cells: 0
Total multicast lost cells: 0
Last clearing of "show controller fabric plane" counters never
```

The following is sample output from the **show controllers fabric plane** command that displays system fabric plane statistics from the fabric for all planes in detailed form:

```
RP/0/RP0/CPU0:router(admin)# show controllers fabric plane all statistics detail
```

```
The fabric plane number is 0
Total number of providers for the statistics: 0
Total received data cells: 0
Total transmitted data cells: 0
Total received correctable errored cells: 0
Total received uncorrectable errored cells: 0
Total received parity error cells: 0
Total unicast lost cells: 0
Total multicast lost cells: 0
Last clearing of "show controller fabric plane" counters never
```

```
The fabric plane number is 1
Total number of providers for the statistics: 0
Total received data cells: 0
Total transmitted data cells: 0
Total received correctable errored cells: 0
```

R3.5.0 Beta Draft—Cisco Confidential Information

```
Total received uncorrectable errored cells: 0
Total received parity error cells: 0
Total unicast lost cells: 0
Total multicast lost cells: 0
Last clearing of "show controller fabric plane" counters never
```

```
The fabric plane number is 2
Total number of providers for the statistics: 0
Total received data cells: 0
Total transmitted data cells: 0
Total received correctable errored cells: 0
Total received uncorrectable errored cells: 0
Total received parity error cells: 0
Total unicast lost cells: 0
Total multicast lost cells: 0
Last clearing of "show controller fabric plane" counters never
```

```
The fabric plane number is 3
Total number of providers for the statistics: 0
Total received data cells: 0
Total transmitted data cells: 0
Total received correctable errored cells: 0
Total received uncorrectable errored cells: 0
Total received parity error cells: 0
Total unicast lost cells: 0
Total multicast lost cells: 0
Last clearing of "show controller fabric plane" counters never
```

```
The fabric plane number is 4
Total number of providers for the statistics: 0
Total received data cells: 0
Total transmitted data cells: 0
Total received correctable errored cells: 0
Total received uncorrectable errored cells: 0
Total received parity error cells: 0
Total unicast lost cells: 0
Total multicast lost cells: 0
Last clearing of "show controller fabric plane" counters never
```

```
The fabric plane number is 5
Total number of providers for the statistics: 0
Total received data cells: 0
Total transmitted data cells: 0
Total received correctable errored cells: 0
Total received uncorrectable errored cells: 0
Total received parity error cells: 0
Total unicast lost cells: 0
Total multicast lost cells: 0
Last clearing of "show controller fabric plane" counters never
```

Table 27 describes the significant fields shown in the display.

Table 27 *show controllers fabric plane Field Descriptions*

Field	Description
The fabric plane number is 1	Fabric plane ID number.
Total number of providers for the statistics	Number of providers (sources) from which statistics were extracted.
Total received data cells	Total of data cells that have been received.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 27** *show controllers fabric plane Field Descriptions (continued)*

Field	Description
Total received correctable errored cells	Total number of cells with errors that can be corrected.
Total received uncorrectable errored cells	Total number of cells with errors that cannot be corrected.
Total received parity error cells	Total number of cells that have parity errors.
Total unicast lost cells	Number of lost unicast cells.
Last clearing of “show controller fabric plane” counters	Indicates when the fabric plane counters were last cleared.

Related Commands

Command	Description
show controllers fabric connectivity	Displays controller fabric connectivity information.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers fabric rack all

To display information about the fabric racks in the current system, use the **show controllers fabric rack all** command in administration EXEC mode.

show controllers fabric rack all [**brief** | **detail**]

Syntax Description

brief	(Optional) Displays summarized fabric rack information.
detail	(Optional) Specifies that the command output includes detailed fabric rack information.

Defaults

Use the **show controllers fabric rack all** command without including any of the optional syntax to display detailed information about all fabric card racks in the current system.

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show controllers fabric rack all** command to display fabric rack topology information.

Task ID

Task ID	Operations
fabric	read

Examples

The following example shows sample output from the **show controllers fabric rack all** command:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:P1_CRS-8(admin)# show controllers fabric rack all

Rack Rack Server
Num Status Status
-----
0  NORMAL  PRESENTRP/0/RP0/CPU0:router(admin)#
```


R3.5.0 Beta Draft—Cisco Confidential Information

show controllers fabric sfe

To display information about a specific switch fabric element, use the **show controllers fabric sfe** command in administration EXEC mode.

show controllers fabric sfe {**fabricq** | **ingressq** | **s1** | **s2** | **s3**} [**port** | **all**] [**backpressure** | **brief** | **detail**]

Syntax Description		
fabricq		Displays information from the fabric queue for the switching fabric element.
ingressq		Displays information from the ingress queue for the switching fabric element.
s1		Displays information about Stage 1 (S1) switch fabric elements. S1 elements distribute traffic.
s2		Displays information about Stage 2 (S2) switch fabric elements. S2 elements forward cells to Stage 3 (S3) elements.
s3		Displays information about S3 switch fabric elements. S3 elements perform switching.
<i>port</i>		Specifies the port that owns the switch fabric element you want to display. Replace <i>port</i> with the port number, in the <i>rack/slot/module/ASIC/port</i> format.
	Note	A slash mark between values is required as part of the <i>port</i> notation.
all		Displays information about the switch fabric elements on all ports in the system.
backpressure		(Optional) Displays backpressure information for the specified switch fabric elements.
brief		(Optional) Displays summarized information for the specified switch fabric elements.
detail		(Optional) Includes detailed information about the specified switch fabric elements in the command output.

Defaults Use the **show controllers fabric sfe** command without specifying any of the optional parameters to display detailed information about a specified switch fabric element.

Command Modes Administration EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
fabric	read

Examples

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

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router (admin)# show controllers fabric sfe fabricq all
```

```
Flags: P - plane admin down, p - plane oper down
C - card admin down, c - card oper down
L - link port admin down, l - linkport oper down
A - asic admin down, a - asic oper down
B - bundle port admin Down, b - bundle port oper down
I - bundle admin down, i - bundle oper down
N - node admin down, n - node down
o - other end of link down d - data down
f - failed component downstream
m - plane multicast down
```

```
Sfe Admin Oper
R/S/M/A State State
```

```
-----
0/1/CPU0/0 UP UP
0/1/CPU0/1 UP UP
0/3/CPU0/0 UP UP
0/3/CPU0/1 UP UP
0/6/CPU0/0 UP UP
0/6/CPU0/1 UP UP
0/RP0/CPU0/0 UP UP
0/RP1/CPU0/0 UP UP
```

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers fabricq drop

To display the number of packets dropped to the fabric or from the fabric on a per slot basis in the fabric queue driver, use the **show controllers fabricq drop** command in administration EXEC mode.

show controllers fabricq drop [**detail**] [**location** *node-id*]

Syntax Description

detail	(Optional) Displays detailed statistical information.
location <i>node-id</i>	(Optional) Displays statistical information for the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults

Information about packet drops for all route processors (RPs) on the router is displayed

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show controllers fabricq drop** command to display statistics about packet drops. Specifying a location displays information only if that location is an RP. Use the **detail** keyword to display detailed output.

**Note**

The **show controllers fabricq drop** command is typically used for debugging purposes.

Task ID

Task ID	Operations
root-system	read, write

Examples

The following is detailed sample output from the **show controllers fabricq drop** command for location 0/1/CPU0:

```
RP/0/0/CPU0:router(admin)# show controllers fabricq drop detail location 0/1/CPU0
```

```
Location 0/1/0:
```

R3.5.0 Beta Draft—Cisco Confidential Information

To Fabric dropped packets:

Slot	Tx-OVS	Tx-NHB	Tx-NPB	Tx-QF	Tx-LP	Tx-DS	Tx-MB	Tx-DIS	Tx-Total
Low Priority:									
0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
mcast	0	0	0	0	0	0	0	0	0
High Priority:									
0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
mcast	0	0	0	0	0	0	0	0	0

Legend:

Tx-OVS: Drops due to oversized packets

Tx-NHB: Drops due to missing packet header buffer

Tx-NPB: Drops due to missing packet payload buffer

Tx-QF: Drops because the queue is full

Tx-LP: Drops because the packet is low priority

Tx-DS: Drops because the destination slot is dead

Tx-MB: Drop counter for packets transmitted over MBUS (Not supported)

Tx-DIS: Drops because the tofab transmission is disabled

From Fabric dropped packets:

Slot	Rx-REF	Rx-PKT	Rx-DEC	Rx-Total
0	0	0	0	0
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

R3.5.0 Beta Draft—Cisco Confidential Information

```

11      0      0      0      0
12      0      0      0      0
13      0      0      0      0
14      0      0      0      0
15      0      0      0      0

```

Legend:

Rx-REF: Drops in the FPGA reassembly

Rx-PKT: Drops due to invalid packet

Rx-DEC: Drops due to decoding the packet

Table 28 describes the significant fields shown in the display.

Table 28 *show controllers fabricq drop Field Descriptions*

Field	Description
To Fabric dropped packets	Displays statistics about the transmitted packets that were dropped.
Slot	Slot that contains the fabric card whose statistics are displayed.
Tx-OVS	Number of transmitted packets that were dropped because they were oversized.
Tx-NHB	Number of transmitted packets that were dropped because they were missing a packet header buffer.
Tx-NPB	Number of transmitted packets that were dropped because they were missing a packet payload buffer.
Tx-QF	Number of transmitted packets that were dropped because the queue is full.
Tx-LP	Number of transmitted packets that were dropped because they were low priority.
Tx-DS	Number of transmitted packets that were dropped because the destination slot is dead.
Tx-MB	Number of dropped transmitted packets that were sent over the Mbus.
Tx-DIS	Number of transmitted packets that were dropped because the tofab transmission is disabled.
Tx-Total	Total number of packets transmitted.
From Fabric dropped packets	Displays statistics about the received packets that were dropped.
Slot	Slot that contains the fabric card whose statistics are displayed.
Rx-REF	Number of received packets that were dropped in the FPGA reassembly.
Rx-PKT	Number of received packets that were dropped because they were invalid.
Rx-DEC	Number of received packets that were dropped due to decoding.
Rx-Total	Total number of received packets that were dropped.

1. Optimized Voice Service

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show controllers fabricq errors	Displays information about errors.
	show controllers fabricq frfab	Displays from fabric statistics.
	show controllers fabricq output	Displays information about to fabric output service.
	show controllers fabricq queue	Displays information about packet queues.
	show controllers fabricq registers	Displays information about chopper and assembler registers.
	show controllers fabricq tofab	Displays to fabric statistics.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers fabricq errors

To display the count of hardware errors associated with the fabric queue driver, use the **show controllers fabricq errors** command in administration EXEC mode.

show controllers fabricq errors [*location node-id*]

Syntax Description	location node-id	(Optional) Displays statistical information for the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults	Information about errors for all route processors (RPs) on the router is displayed

Command Modes	Administration EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **show controllers fabricq errors** command to display statistics about hardware errors. Specifying a location displays information only if that location is a RP.

The **show controllers fabricq errors** command is intended for use while performing debugging procedures.

Task ID	Task ID	Operations
	root-system	read, write

Examples	The following is sample output from the show controllers fabricq errors command for location 0/1/CPU0:

```
RP/0/0/CPU0:router(admin)# show controllers fabricq errors location 0/1/CPU0
```

```
Location 0/1/0:
```

```
ToFab Errors:
```

```
Error Type      Error Count Max Rate Rate Exceeded Count
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

-----
SRAM Parity          0          2          0
DMA Address          0         100         0
DMA Size             0         100         0
Fusilli Parity       0          2          0
PCI TRANS64          0          2          0
PCI Address          0          2          0

```

Table 29 describes the significant fields shown in the display.

Table 29 *show controllers fabricq errors Field Descriptions*

Field	Description
Error Count	Number of errors of each type.
Max Rate	Maximum number of errors of that type that can be received per second.
Rate Exceeded Count	Number of times that error has exceeded the Max Rate. When the rate is exceeded, the software may try to restart the fabric queue driver and associated ASICs or FPGAs to correct the problem.

Related Commands

Command	Description
show controllers fabricq drop	Displays information about packet drops.
show controllers fabricq frfab	Displays from fabric statistics.
show controllers fabricq output	Displays information about to fabric output service.
show controllers fabricq queue	Displays information about packet queues.
show controllers fabricq registers	Displays information about chopper and assembler registers.
show controllers fabricq tofab	Displays to fabric statistics.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers fabricq fabric-backpressure

To display back pressure information for the fabric queue ASICs, use the **show controllers fabricq fabric-backpressure** command in EXEC and administration EXEC mode.

show controllers fabricq fabric-backpressure [**summary**] [**instance** *asic_instance*] [**location** *node-id*]

Syntax Description	summary	(Optional) Displays summarized backpressure information about all fabric queue ASICs in the system.
	instance <i>asic_instance</i>	(Optional) Displays backpressure information for a specific fabric queue ASIC. Replace <i>asic_instance</i> with the instance that identifies the ASIC whose backpressure information you want to display.
	Note	Enter the show controllers fabricq fabric-backpressure command without including any of the optional keywords or arguments to display all fabric queue ASIC instances in the system.
	location <i>node</i>	Displays back pressure information for the fabric queue ASICs on a particular node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
	Note	Use the show platform command to see a list of all nodes currently installed in your system.

Defaults Enter the **show controllers fabricq fabric-backpressure** command without including any of the optional keywords or arguments to display detailed back pressure information about all fabric queue ASICs in the system.

Command Modes EXEC
Administration EXEC

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	fabric	read

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Operations
interface	read
drivers	read

Examples

The following example shows sample output from the **show controllers fabricq fabric-backpressure** command when it is entered with the **summary** keyword:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# show controllers fabricq fabric-backpressure summary
```

```
Rack 0: All Groups Received? : Yes
```

The following example shows sample output from the **show controllers fabricq fabric-backpressure** command when it is entered without any of the optional keywords:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# show controllers fabricq fabric-backpressure
```

```
Location: 0/1/CPU0
Asic Instance: 0
Fabric Destination Address: 4
BP global Configuration Register: 0xff07
```

```
Cluster Number: 0
Primary Link: 0
Secondary Link: 9
Number of Backup links: 14
Backup Links: 8 1 2 10 3 11 27 16 26 17 25 18 24 19
BP enable Mask: 0x4
BP EC: 0
BP IM: 0x1ffe
```

```
+-----+
|BP Engine| Enabled |Current Link |Rx group |P Link |S Link |
+-----+
| 0 | No |Secondary | 255 | 0 | 9 |
+-----+
| 1 | No |Secondary | 255 | 0 | 9 |
+-----+
| 2 | Yes |Primary | 0 | 0 | 9 |
+-----+
```

```
Location: 0/1/CPU0
Asic Instance: 1
Fabric Destination Address: 5
BP global Configuration Register: 0xff07
```

```
Cluster Number: 0
Primary Link: 0
Secondary Link: 9
Number of Backup links: 14
Backup Links: 8 1 2 10 3 11 27 16 26 17 25 18 24 19
BP enable Mask: 0x4
BP EC: 0
BP IM: 0x1ffe
```

```
+-----+
|BP Engine| Enabled |Current Link |Rx group |P Link |S Link |
+-----+
| 0 | No |Secondary | 255 | 0 | 9 |
+-----+
| 1 | No |Secondary | 255 | 0 | 9 |
```

R3.5.0 Beta Draft—Cisco Confidential Information

```
+-----+
| 2 | Yes | Primary | 0 | 0 | 9 |
+-----+
```

```
Location: 0/3/CPU0
Asic Instance: 0
Fabric Destination Address: 12
BP global Configuration Register: 0xff07

Cluster Number: 0
--More--
```

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers fabricq frfab

To display from fabric statistics associated with the fabric queue driver, use the **show controllers fabricq frfab** command in administration EXEC mode.

show controllers fabricq frfab [**detail**] [**location** *node-id*]

Syntax Description

detail	(Optional) Displays detailed statistical information.
location <i>node-id</i>	(Optional) Displays statistical information for the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults

From fabric statistics are displayed for all route processors (RPs) on the router

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show controllers fabricq frfab** command to display from fabric statistics. Specifying a location displays information only if that location is an RP. Use the **detail** keyword to display detailed output.

**Note**

The **show controllers fabricq frfab** command is typically used for debugging purposes.

Task ID

Task ID	Operations
root-system	read, write

Examples

The following is sample output from the **show controllers fabricq frfab** command for location 0/1/CPU0:

```
RP/0/RP0/CPU0:router(admin)## show controllers fabricq frfab location 0/1/CPU0
```

```
Location 0/1/0:
```

```
From Fabric Stats:
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

-----
Slot    Rx-pkts    Rx-TH-pkts Rx-dropped
1       0         3928       0
2       0         37309      0
3       0         43306      0
4       0         42681      0
5       0         35063      0

From Fabric Packet per Queue Stats:
-----
Packets received in queue 0 - 0
Packets received in queue 1 - 3928
Packets received in queue 2 - 150069
Packets received in queue 3 - 8290

From Fabric Error Stats:
-----
Bigger than MTU pkts          - 0
Corrupted pkts                - 0
SPD pkt count                  - 0
No IDB drops                   - 0
IDB queue tail drops          - 0
Chan corrupted pkts            - 0
First/Last err pkts           - 0
Sequence err pkts              - 0
Unknown Rx type                - 0
Output queue 0 full drops      - 0
Output queue 1 full drops      - 0
Output queue 2 full drops      - 0
Output queue 3 full drops      - 0
Output queue unmatched drops   - 0
OQ 0 drops because FQ below threshold - 0
OQ 1 drops because FQ below threshold - 0
OQ 2 drops because FQ below threshold - 0
OQ 3 drops because FQ below threshold - 0

From Fabric Error Events:
-----
Fusilli parity errors - 0
Fusilli interface errors - 0
Free queue drop threshold events - 0
Free queue empty events - 0
Bad descriptors events - 0
Output queue 0 almost empty events - 0
Output queue 1 almost empty events - 0
Output queue 2 almost empty events - 0
Output queue 3 almost empty events - 0
OQ 0 drops because of ptr - 0 (Not implemented)
OQ 1 drops because of ptr - 0 (Not implemented)
OQ 2 drops because of ptr - 0 (Not implemented)
OQ 3 drops because of ptr - 0 (Not implemented)
Interrupt throttle events - 0
Spurious interrupt events - 0

Assembler memory statistics:
-----
Bufs enqueued to free queue    - 163311
Bufs rxed from OQ               - 162287
Bufs copied to public pool      - 0 (Not implemented)
Bufs returned to the pool       - 162287
Bufs returned by driver         - 0 (Not implemented)
Bufs from driver to OS          - 0 (Not implemented)

```

R3.5.0 Beta Draft—Cisco Confidential Information

Table 30 describes the significant fields shown in the display.

Table 30 *show controllers fabricq frfab Field Descriptions*

Field	Description
Rx-pkts	Number of packets received from the fabric.
Rx-TH-pkts	Number of “think hard” packets received from the fabric.
Rx-dropped	Number of packets received from the fabric that had to be dropped.

Related Commands

Command	Description
show controllers fabricq drop	Displays information about packet drops.
show controllers fabricq errors	Displays information about errors.
show controllers fabricq output	Displays information about to fabric output service.
show controllers fabricq queue	Displays information about packet queues.
show controllers fabricq registers	Displays information about chopper and assembler registers.
show controllers fabricq tofab	Displays to fabric statistics.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers fabriccq output

To display to fabric output service statistics associated with the fabric queue driver, use the **show controllers fabriccq output** command in administration EXEC mode.

show controllers fabriccq output [**location** *node-id*]

Syntax Description	location <i>node-id</i>	(Optional) Displays statistical information for the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults	Information is displayed for all route processors (RPs) on the router

Command Modes	Administration EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **show controllers fabriccq output** command to display to fabric output service statistics. Specifying a location displays information only if that location is an RP.

The service time is the time from when the RP CPU has made the packet ready to be sent to the slot to when the FPGA has put the packet on the queue to that particular slot.

**Note**

The **show controllers fabriccq output** command is typically used for debugging purposes.

Task ID	Task ID	Operations
	root-system	read, write

Examples	The following is sample output from the show controllers fabriccq output command for location 0/1/CPU0:

```
RP/0/RP0/CPU0:router(admin)## show controllers fabriccq output location 0/1/CPU0
```

```
Location 0/1/0:
```

R3.5.0 Beta Draft—Cisco Confidential Information

To Fabric servicing time statistics:

Slot	Minimum	Maximum	Average	Timeouts

Low Priority:				
0	0	0	0	0
1	0	0	0	0
2	0	10	0	0
3	0	21	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
mcast	0	0	0	0
High Priority:				
0	0	0	0	0
1	0	22	0	0
2	0	96	0	0
3	0	13	0	0
4	0	12	0	0
5	0	14	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
mcast	0	6	0	0

Table 31 describes the significant fields shown in the display.

Table 31 *show controllers fabricq output Field Descriptions*

Field	Description
Slot	Slot to which the packets are sent.
Minimum	Lowest service time of all the packets sent to that slot.
Maximum	Highest service time of all the packets sent to that slot.
Average	Average service time of all the packets sent to that slot.
Timeouts	Number of times a packet's service time has exceeded a threshold of 200 milliseconds (the packet is dropped).

Related Commands

Command	Description
show controllers fabricq drop	Displays information about packet drops.
show controllers fabricq errors	Displays information about errors.

R3.5.0 Beta Draft – Cisco Confidential Information

Command	Description
show controllers fabricq frfab	Displays from fabric statistics.
show controllers fabricq queue	Displays information about packet queues.
show controllers fabricq registers	Displays information about chopper and assembler registers.
show controllers fabricq tofab	Displays to fabric statistics.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers fabricq statistics

To display statistics about packet flow through the fabric queue application-specific integrated circuit (ASIC), use the **show controllers fabricq statistics** command in EXEC mode.

show controllers fabricq statistics [*instance instance*] [*location node-id*]

Syntax Description

instance <i>instance</i>	(Optional) Specifies instance and number for a single fabric queue ASIC. The <i>instance</i> argument is a number from 0 to 4.
location <i>node-id</i>	(Optional) Specifies statistical packet flow information for the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults

Information for all fabric queue ASICs for all locations is displayed

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	No modification.
Release 3.3.0	The show controllers fabricq packet-stats command was replaced by the show controllers fabricq statistics command.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show controllers fabricq statistics** command to track the number of unicast and multicast packets that are sent from the fabric to the specified node.

Task ID

Task ID	Operations
interface	read
drivers	read

Examples

The following is sample output from the **show controllers fabricq statistics** command that displays statistics about fabric queue packets that have passed through ASIC 0 on node 0/1/CPU0:

```
RP/0/RP0/CPU0:router# show controllers fabricq statistics instance 0 location 0/1/CPU0
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

Fabric Queue Manager Packet Statistics
=====

Location: 0/1/CPU0
Asic Instance: 0
Fabric Destination Address:    32

Input Cell counters:
+-----+
Data cells      :          42356 (+          22 )
Control cells   :       29877224 (+       36372 )
Idle cells      :    219947284936 (+    267358842 )
BP Asserted Count :              0 (+              0 )
MC BP Asserted Count :              0 (+              0 )

Reassembled packet counters
+-----+
Ucast pkts      :              0 (+              0 )
Mcast pkts      :              0 (+              0 )
Cpuctrlcast pkts :         21159 (+             11 )

Dropped packets
+-----+
Ucast pkts      :              0 (+              0 )
Mcast pkts      :              0 (+              0 )
Cpuctrlcast pkts :              0 (+              0 )
Vital denied pkts :              0 (+              0 )
NonVital denied pkts :              0 (+              0 )
Unicast lost pkts :              0 (+              0 )
Ucast partial pkts :              0 (+              0 )
PSM OOR Drops   :              0 (+              0 )

```

Table 32 describes the significant fields shown in the display.

Table 32 *show controllers fabricq statistics Field Descriptions*

Field	Description
Input Cell counters	Number of cells that have reached the fabric queue ASIC.
Reassembled packet counters	Number of packets the fabric queue ASIC has reassembled after transmission over the fabric.
Dropped packets	Number of packets the fabric queue ASIC has had to drop.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers fabricq queue

To display information about the hardware queues of the performance route processor chopper and assembler FPGAs, use the **show controllers fabricq queue** command in administration EXEC mode.

show controllers fabricq queue [**detail**] [**location** *node-id*]

Syntax Description

detail	(Optional) Displays detailed statistical information.
location <i>node-id</i>	(Optional) Displays statistical information for the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults

Information for all performance route processors on the router is displayed

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show controllers fabricq queue** command to display information about packet queues. Specifying a location displays information only if that location is an RP.

This command is intended for use while performing debugging procedures.

Task ID

Task ID	Operations
root-system	read, write

Examples

The following is detailed sample output from the **show controllers fabricq queue** command for the location 0/1/CPU0:

```
RP/0/0/CPU0:router(admin)# show controllers fabricq queue detail location 0/1/CPU0
```

```
Location 0/1/0:
```

```
To Fabric Queue Stats:
```

```
-----
```

```
Slot      EnQueued    DeQueued  Cur-Entrys  Max-Entrys    Blocked    BP count
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

Low Priority:
  0          0          0          0          0          No          0
  1          0          0          0          0          No          0
  2         300         300          0          2          No          0
  3        8428        8428          0         12          No          0
  4          0          0          0          0          No          0
  5          0          0          0          0          No          0
  6          0          0          0          0          No          0
  7          0          0          0          0          No          0
  8          0          0          0          0          No          0
  9          0          0          0          0          No          0
 10          0          0          0          0          No          0
 11          0          0          0          0          No          0
 12          0          0          0          0          No          0
 13          0          0          0          0          No          0
 14          0          0          0          0          No          0
 15          0          0          0          0          No          0
mcast        0          0          0          0          No          0
High Priority:
  0          0          0          0          0          No          0
  1         7882         7882          0          2          No          0
  2        62330        62330          0         36          No          0
  3        60752        60752          0        100          No          0
  4        72588        72588          0         36          No          0
  5        60876        60876          0        100          No          0
  6          0          0          0          0          No          0
  7          0          0          0          0          No          0
  8          0          0          0          0          No          0
  9          0          0          0          0          No          0
 10          0          0          0          0          No          0
 11          0          0          0          0          No          0
 12          0          0          0          0          No          0
 13          0          0          0          0          No          0
 14          0          0          0          0          No          0
 15          0          0          0          0          No          0
mcast      19562      19562          0        200          No          0
Free packet header buffers 7680

From Fabric Queue Stats:
-----
Queue  Allocated      Free
  0          0        512
  1          0        512
  2          0        512
  3          0        512
F/Q          87        937

```

Table 33 describes the significant fields shown in the display.

Table 33 *show controllers fabricq queue Field Descriptions*

Field	Description
Slot	Slot or queue to which the packets are sent.
EnQueued	Number of entries enqueued for that queue.
DeQueued	Number of entries dequeued for that queue.
Cur-Entrys	Number of entries currently for that queue.
Max-Entrys	Highest number of entries for that queue.
Blocked	Yes or No if that queue is blocked.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 33** *show controllers fabricq queue Field Descriptions (continued)*

Field	Description
BP count	Backpressure count, which is the number of times the queue got full.
Queue	Priority queues receiving packets; 0 is the highest priority. The F/Q entry is the software free packet queue.
Allocated	Number of packets in that queue.
Free	Number of packets available for that queue.

Related Commands

Command	Description
show controllers fabricq drop	Displays information about packet drops.
show controllers fabricq errors	Displays information about errors.
show controllers fabricq frfab	Displays from fabric statistics.
show controllers fabricq output	Displays information about to fabric output service.
show controllers fabricq registers	Displays information about chopper and assembler registers.
show controllers fabricq tofab	Displays to fabric statistics.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers fabricq registers

To display the hardware registers of the chopper and assembler FPGAs, use the **show controllers fabricq registers** command in administration EXEC mode.

show controllers fabricq registers [**detail**] [**location** *node-id*]

Syntax Description	detail	(Optional) Displays detailed statistical information.
	location <i>node-id</i>	(Optional) Displays statistical information for the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults	Information for all route processors (RPs) on the router is displayed

Command Modes	Administration EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

Use the **show controllers fabricq registers** command to display the hardware registers of the chopper and assembler FPGAs. Specifying a location displays information only if that location is an RP.

This command is intended for use while performing debugging procedures.

Task ID	Task ID	Operations
	root-system	read, write

Examples	The following is sample output from the show controllers fabricq registers command for location 0/1/CPU0:

```
RP/0/0/CPU0:router(admin)# show controllers fabricq registers location 0/1/CPU0
```

```
Location 0/1/0:
```

```
Chopper Registers:
```

```
-----
```

```
FPGA Version                                00020012
```

```
HP Descriptor fetch enable                 00010000
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

Descriptor array size          000003FF
Interrupt cause                00000000
Interrupt mask                 FC01FFFF
LP Descriptor fetch enable     00000008
HP Interrupt desc afull       00000000
LP Interrupt desc afull       00000000
Discovery low control reg base address F1000840
Discovery next desc reg base address F1000830
Chopper PCI base address      F0000000
HP Descriptor queue empty status 0001FFFF
HP Descriptor queue almost full 00000000
Data queue empty status       0001FFFF
Data queue almost full        00000000
LP Descriptor queue empty status 0001FFFF
LP Descriptor queue almost full 00000000
SRAM Descriptor threshold      000003F0
SRAM Data threshold           000007F0
DMA Control                    000000DD
Back pressure status           00000000
Fusilli Tx Enable             0001FFFF
Cell count                     0030CDA1
Reset VOQ                      00000000
DMA Busy Status                00000000
DMA Done Status                000000DD
HP Descriptor start addr for queue 0 0B448000
HP Descriptor start addr for queue 1 0B44A000
HP Descriptor start addr for queue 2 0B44C000
HP Descriptor start addr for queue 3 0B44E000
HP Descriptor start addr for queue 4 0B450000
HP Descriptor start addr for queue 5 0B452000
HP Descriptor start addr for queue 6 0B454000
HP Descriptor start addr for queue 7 0B456000
HP Descriptor start addr for queue 8 0B458000
HP Descriptor start addr for queue 9 0B45A000
HP Descriptor start addr for queue 10 0B45C000
HP Descriptor start addr for queue 11 0B45E000
HP Descriptor start addr for queue 12 0B460000
HP Descriptor start addr for queue 13 0B462000
HP Descriptor start addr for queue 14 0B464000
HP Descriptor start addr for queue 15 0B466000
HP Descriptor start addr for queue 16 0B468000
LP Descriptor start addr for queue 0 0B426000
LP Descriptor start addr for queue 1 0B428000
LP Descriptor start addr for queue 2 0B42A000
LP Descriptor start addr for queue 3 0B42C000
LP Descriptor start addr for queue 4 0B42E000
LP Descriptor start addr for queue 5 0B430000
LP Descriptor start addr for queue 6 0B432000
LP Descriptor start addr for queue 7 0B434000
LP Descriptor start addr for queue 8 0B436000
LP Descriptor start addr for queue 9 0B438000
LP Descriptor start addr for queue 10 0B43A000
LP Descriptor start addr for queue 11 0B43C000
LP Descriptor start addr for queue 12 0B43E000
LP Descriptor start addr for queue 13 0B440000
LP Descriptor start addr for queue 14 0B442000
LP Descriptor start addr for queue 15 0B444000
LP Descriptor start addr for queue 16 0B446000

```

Assembler Registers:

```

Version          0002000D
Chip Config      0000000F
Int Mask         00000000

```


R3.5.0 Beta Draft—Cisco Confidential Information

```

Output Queue Threshold      00000033
Low Pri Req level          00000030
High Pri Req level         00000060
Free Queue Size            00001000
Free Queue Base            0B3A6000
Free Queue Rd Pointer      0B3A6380
Free Queue Wr Pointer      0B3A61C0
Output Queue Size          00001000
Output Queue 0 Base Addr   0B3A8000
Output Queue 0 Write Addr  0B3A8000
Output Queue 0 Read Addr   0B3A8000
Output Queue 0 Match       C0000200
Output Queue 0 Mask        00003E00
Output Queue 1 Base Addr   0B3AA000
Output Queue 1 Write Addr  0B3AAB58
Output Queue 1 Read Addr   0B3AAB58
Output Queue 1 Match       C0000C00
Output Queue 1 Mask        00003E00
Output Queue 2 Base Addr   0B3AC000
Output Queue 2 Write Addr  0B3AC4D0
Output Queue 2 Read Addr   0B3AC4D0
Output Queue 2 Match       C0000400
Output Queue 2 Mask        00003C00
Output Queue 3 Base Addr   0B3AE000
Output Queue 3 Write Addr  0B3AE360
Output Queue 3 Read Addr   0B3AE360
Output Queue 3 Match       C0000000
Output Queue 3 Mask        00000000
Discard Buffer Addr        0A1AC700
REFIM config               00000000
REFIM Max Packet Len       000000C1

```

Related Commands

Command	Description
show controllers fabricq drop	Displays information about packet drops.
show controllers fabricq errors	Displays information about errors.
show controllers fabricq frfab	Displays from fabric statistics.
show controllers fabricq output	Displays information about to fabric output service.
show controllers fabricq queue	Displays information about packet queues.
show controllers fabricq tofab	Displays to fabric statistics.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers fabricq tofab

To display to fabric statistics associated with the fabric queue driver, use the **show controllers fabricq tofab** command in administration EXEC mode.

show controllers fabricq tofab [**detail**] [**location** *node-id*]

Syntax Description

detail	(Optional) Displays detailed statistical information.
location <i>node-id</i>	(Optional) Displays statistical information for the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults

Information for all route processors (RPs) on the router is displayed

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show controllers fabricq tofab** command to display to fabric statistics. Specifying a location displays information only if that location is an RP.

The **show controllers fabricq tofab** command is intended for use while performing debugging procedures.

Task ID

Task ID	Operations
root-system	read, write

Examples

The following is sample output from the **show controllers fabricq tofab** command for location 0/1/CPU0:

```
RP/0/0/CPU0:router(admin)# show controllers fabricq tofab location 0/1/CPU0
```

```
Location 0/1/0:
```

```
To Fabric Stats:
-----
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

Slot    Tx-pkts    Tx-TH-pkts Tx-dropped Tx-DMA
Low Priority:
3        0          446         0         446
High Priority:
1        0          248         0         248
2        0        13696         0        13696
3        0        14347         0        14347
4        0        15889         0        15889
5        0        14351         0        14351
mcast    0         2182         0         2182

```

To Fabric Errors:

```

Failed sends because of no header bufs - 0
Failed sends because of no payload bufs - 0
SRAM parity errors - 0
DMA errors - 0
Fusilli Parity errors - 0

```

Table 34 describes the significant fields shown in the display.

Table 34 *show controllers fabricq tofab Field Descriptions*

Field	Description
Tx-pkts	Number of packets sent to that slot.
Tx-TH-pkts	Number of “think hard” packets sent to that slot.
Tx-dropped	Number of dropped packets sent to that slot.
Tx-DMA	Number of direct memory accesses (DMA) to send the packet to that slot.

Related Commands

Command	Description
show controllers fabricq drop	Displays information about packet drops.
show controllers fabricq errors	Displays information about errors.
show controllers fabricq frfab	Displays from fabric statistics.
show controllers fabricq output	Displays information about to fabric output service.
show controllers fabricq queue	Displays information about packet queues.
show controllers fabricq registers	Displays information about chopper and assembler registers.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers ingressq statistics

To display statistical information for the ingress queue application-specific integrated circuit (ASIC), use the **show controllers ingressq statistics** command in EXEC mode.

show controllers ingressq statistics [*location node-id*]

Syntax Description

location <i>node-id</i>	(Optional) Specifies statistical ingress queue information for the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults

Information for all locations is displayed

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	No modification.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show controllers ingressq statistics** command to track the number of unicast and multicast packets that are sent to the fabric from the specified node.

Task ID

Task ID	Operations
root-system	read, write

Examples

The following is sample output from the **show controllers ingressq statistics** command that displays packet and cell flow statistics through an ingress queue on node 0/1/CPU0:

```
RP/0/RP0/CPU0:router# show controllers ingressq statistics location 0/1/CPU0

Ingressq Rx Statistics.
-----
rx pkts : 278770 ( 44473109 bytes)
rx pkts from cpu : 263548 ( 36239661 bytes)
rx control pkts from cpu : 263548 ( 36239661 bytes)
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

rx data pkts from cpu : 0 ( 0 bytes)
Ingressq Tx Statistics.
-----
tx pkts : 278768 ( 48162158 bytes)
tx pkts to cpu : 15222 ( 8233448 bytes)
tx control pkts to cpu : 15222 ( 8233448 bytes)
tx data pkts to cpu : 0 ( 0 bytes)
tx pkts shaped : 263546 ( 39928710 bytes)
tx cells to fabric : 529664
Ingressq Drops.
-----
length error drops : 0
crc error drops : 0
OOR error drops : 0
backpressure discard drops : 0
tail drops : 0
cell drops : 2

```

Table 35 describes the significant fields shown in the display.

Table 35 *show controllers ingressq statistics Field Descriptions*

Field	Description
Ingressq Rx Statistics	Receive side statistics, which include Rx packets from metro and Rx packets from the CPU.
Ingressq Tx Statistics	Transmit side statistics, which include Tx packets sent out and the number of cells sent to the fabric.
Ingressq Drops	Count of various packet and cell drops within the ingress queue.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers switch

To display the control Ethernet connection in the route processor (RP), use the **show controllers switch** command in administration EXEC mode.

show controllers switch *instance* {**ports** | **statistics**} **location** *node-id*

Syntax Description

instance	Two intra-rack switches are present on the RP/SC. The instance is from 0 to 1 that identifies the specific switch.
ports	Displays the port states as up, down, or err-disabled. The ports keyword displays control Ethernet switches, port states, statistics, and Spanning Tree Protocol (STP) information.
statistics	Displays switch port statistics.
location <i>node-id</i>	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the <i>node-id</i> argument as entered in the <i>rack/slot/module</i> notation.

Defaults

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.4.1	This command was introduced on the Cisco CRS-1.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **show controllers switch** command is used to specify intra-rack switches.

Task ID

Task ID	Operations
fabric	read
root-system	read

Examples

The following sample output shows how to verify the control Ethernet connection on the RP:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch 0 ports location 0/rp0/Cpu0
```

```
RP/0/RP0/CPU0:router(admin)#show controllers switch 0 ports location 0/rp0/Cpu0
FE Port  0 : Up, STP State : FORWARDING (Connects to - 0/RP0)
FE Port  1 : Up, STP State : FORWARDING (Connects to - 0/RP1)
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

FE Port  2 : Down                      (Connects to - 0/FC0)
FE Port  3 : Down                      (Connects to - 0/FC1)
FE Port  4 : Down                      (Connects to - 0/AM0)
FE Port  5 : Down                      (Connects to - 0/AM1)
FE Port  6 : Down                      (Connects to - )
FE Port  7 : Down                      (Connects to - )
FE Port  8 : Down                      (Connects to - 0/SM0)
FE Port  9 : Up, STP State : FORWARDING (Connects to - 0/SM1)
FE Port 10 : Down                      (Connects to - 0/SM2)
FE Port 11 : Down                      (Connects to - 0/SM3)
FE Port 12 : Down                      (Connects to - 0/SM4)
FE Port 13 : Down                      (Connects to - 0/SM5)
FE Port 14 : Down                      (Connects to - 0/SM6)
FE Port 15 : Down                      (Connects to - 0/SM7)
GE Port  0 : Up, STP State : FORWARDING (Connects to - GE_0)
GE Port  1 : Up, STP State : FORWARDING (Connects to - Switch 1)

```

The following sample output shows how to verify the control Ethernet connection on intra-rack switches for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch 0 ports location f0/sc0/Cpu0
```

```

FE Port  0 : Up, STP State : FORWARDING (Connects to - F0/SC0)
FE Port  1 : Up, STP State : FORWARDING (Connects to - F0/SC1)
FE Port  2 : Down                      (Connects to - F0/FC0)
FE Port  3 : Down                      (Connects to - F0/FC1)
FE Port  4 : Down                      (Connects to - F0/AM0)
FE Port  5 : Down                      (Connects to - F0/AM1)
FE Port  6 : Down                      (Connects to - F0/LM0)
FE Port  7 : Down                      (Connects to - F0/LM1)
FE Port  8 : Down                      (Connects to - F0/SM0)
FE Port  9 : Down                      (Connects to - F0/SM1)
FE Port 10 : Down                      (Connects to - F0/SM2)
FE Port 11 : Down                      (Connects to - F0/SM3)
FE Port 12 : Down                      (Connects to - F0/SM4)
FE Port 13 : Down                      (Connects to - F0/SM5)
FE Port 14 : Down                      (Connects to - F0/SM6)
FE Port 15 : Down                      (Connects to - F0/SM7)
GE Port  0 : Up, STP State : FORWARDING (Connects to - GE_0)
GE Port  1 : Up, STP State : FORWARDING (Connects to - Switch 1)

```

Table 36 describes the significant fields shown in the display.

Table 36 *show controllers switch Field Descriptions*

Field	Description
FE Port	Fast Ethernet (FE) port.
STP State	Spanning Tree Protocol (STP) state of the port.
GE Port	Gigabit Ethernet (GE) port.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers switch inter-rack ports

To display the inter-rack switch port states for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card, use the **show controllers switch inter-rack ports** command in administration EXEC mode.

show controllers switch inter-rack ports {all} {location node-id}

Syntax Description	all	Displays all the ports for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card.
	location node-id	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the <i>node-id</i> argument as entered in the <i>rack/slot/module</i> notation.

Defaults	No default behavior or values

Command Modes	Administration EXEC

Command History	Release	Modification
	Release 3.4.1	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The port numbers, which range from 0 to 21, correspond to those on the front panel.



Note The **show controllers switch inter-rack ports** command is applied only to the 22-port SCGE. When you use the **all** and **location** keywords, all other supported cards are displayed including the route processor (RP).

Task ID	Task ID	Operations
	fabric	read
	root-system	read
	admin	read

Examples

The following example shows sample output of the control Ethernet connection for inter-rack switches on the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card:

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(admin)# show controllers switch inter-rack ports all location  
f0/sc0/CPU0
```

```
GE_Port_0 : Down  
GE_Port_1 : Down  
...  
...  
GE_Port_13 : Up  
GE_Port_14 : Up  
...  
...  
GE_Port_20 : Down  
GE_Port_21 : Down  
To_5618 : Up  
Stacking : Up
```

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers switch inter-rack statistics

To display the statistics on the ports of the inter-rack switches for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card, use the **show controllers switch inter-rack statistics** command in administration EXEC mode.

show controllers switch inter-rack statistics {*interface number* | **all**} {**brief** | **detail**} **location** *node-id*

Syntax Description	<i>interface number</i>	Number for the Gigabit Ethernet interface. The range is from 0 to 21. The interface number identifies the specific front panel GE port on the 22-port SCGE.
	all	Displays statistics of all ports for inter-rack switches.
	brief	Displays transmit and receive statistics on the GE ports.
	detail	Displays MIB like detailed switch port statistics that include transmit, receive, and error packet counts.
	location <i>node-id</i>	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the <i>node-id</i> argument as entered in the <i>rack/slot/module</i> notation.

Defaults No default behavior or values

Command Modes Administration EXEC

Command History	Release	Modification
	Release 3.4.1	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	fabric	read
	root-system	read
	admin	read

Examples The following example shows sample output on the port statistics counters for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card:

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(admin)# show controllers switch inter-rack statistics all brief
location f0/sc0/cpu0
```

Port	Tx Frames	Tx Errors	Rx Frames	Rx Errors
GE_Port_0 :	374423	0	1776848	0
GE_Port_1 :	251232	0	170742	0
GE_Port_2 :	857923	0	414409	0
GE_Port_3 :	239437	0	152772	0
GE_Port_4 :	166166	0	82031	0
GE_Port_5 :	0	0	0	0
GE_Port_6 :	0	0	0	0
...				
GE_Port_16 :	0	0	0	0
GE_Port_17 :	0	0	0	0
GE_Port_18 :	0	0	0	0
GE_Port_19 :	0	0	0	0
GE_Port_20 :	0	0	0	0
GE_Port_21 :	0	0	0	0
To_5618 :	522072	0	293720	0
Stacking :	1482	0	0	0
Stacking :	0	0	0	0

The following example shows sample output for the detailed statistics per port for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch inter-rack statistics 0 detail
location f0/sc0/cpu0
```

```
GE_Port_0
```

Rx fragment	:	0	Tx fragment	:	0
Rx unicast	:	1642337	Tx unicast	:	379927
Rx multicast	:	51619	Tx multicast	:	205950
Rx broadcast	:	91436	Tx broadcast	:	150357
Rx FCS error	:	0	Tx FCS error	:	0
Rx Pause	:	0	Tx Pause	:	0
Rx Undersize	:	0	Tx Oversize	:	0
Rx FFP drop	:	0	Tx CFI drop	:	0
Rx Control frame	:	0	Tx Cell error	:	0
			Tx Jabber	:	0
			Tx excessive collision:		0
			Tx tagged vlan	:	0
			Tx abort	:	0

Table 37 describes the significant fields shown in the display.

Table 37 *show controllers switch inter-rack statistics Field Descriptions*

Field	Description
Port	Logical port number. The range is from 0 to 21 and corresponds to the ports on the front panel.
Tx Frames	Transmit frame counter.
Tx Errors	Transmit cell error counter.
Rx Frames	Receive frame counter.
Rx Errors	Receive code error counter.
Rx fragment	Receive fragment counter.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 37** *show controllers switch inter-rack statistics Field Descriptions (continued)*

Field	Description
Rx unicast	Receive unicast frame counter.
Rx multicast	Receive multicast frame counter.
Rx broadcast	Receive broadcast frame counter.
Rx FCS error	Receive FCS error frame counter.
Rx Pause	Receive pause frame counter.
Rx Undersize	Receive undersize frame counter.
Rx FFP drop	Packets dropped by FFP counter.
Rx Control frame	Receive control frame counter.
Tx fragment	Transmit fragment counter.
Tx unicast	Transmit unicast frame counter.
Tx multicast	Transmit multicast frame counter
Tx broadcast	Transmit broadcast frame counter
Tx FCS error	Transmit FCS error frame counter
Tx Pause	Transmit pause control frame counter.
Tx Oversize	Transmit oversize packet counter.
Tx CFI drop	Number of CFI packets dropped for this port.
Tx Cell error	Transmit cell error counter.
Tx Jabber	Transmit jabber counter.
Tx excessive collision	Transmit excessive collision frame counter.
Tx tagged vlan	Transmit tagged VLAN packet counter.
Tx abort	Transmit aborted packet counter.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers switch inter-rack stp

To display information for the spanning tree protocol (STP) of inter-rack switches for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card, use the **show controllers switch inter-rack stp** command in administration EXEC mode.

show controllers switch inter-rack stp {**location** *node-id* | **ports** *interface number* {**location** *node-id*} | **region** {**location** *node-id*}}

Syntax Description	location <i>node-id</i>	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the <i>node-id</i> argument as entered in the <i>rack/slot/module</i> notation.
	ports <i>interface number</i>	Displays the number for the Gigabit Ethernet interface. The range is from 0 to 21. The interface number that identifies the specific front panel GE port on the 22-port SCGE.
	region	Displays MST region configuration information that includes MST revision number, instance to VLAN mapping, and MST region name.

Defaults No default behavior or values

Command Modes Administration EXEC

Command History	Release	Modification
	Release 3.4.1	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	fabric	read
	root-system	read
	admin	read

Examples The following sample output displays information for STP:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch inter-rack stp location f0/sc0/cpu0
```

```
##### MST      0 vlans mapped:    2-4094
Bridge          address 5246.48f0.20ff  priority      32768 (32768 sysid 0)
```

```
show controllers switch inter-rack stp
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

Root          this switch for the CIST
Operational   hello time 1, forward delay 6, max age 8, txholdcount 6
Configured    hello time 1, forward delay 6, max age 8, max hops 4

Interface      Role Sts Cost      Prio.Nbr Type
-----
##### MST 1 vlans mapped: 1
Bridge         address 5246.48f0.20ff priority 32769 (32768 sysid 1)
Root           this switch for MST1

Interface      Role Sts Cost      Prio.Nbr Type
-----
GE_13 Desg FWD 20000 128. 14 P2p
GE_14 Desg FWD 20000 128. 15 P2p
GE_15 Desg FWD 20000 128. 16 P2p
GE_17 Desg FWD 20000 128. 18 P2p
GE_22 Desg FWD 20000 128. 23 P2p

```

Table 38 describes the significant fields shown in the display.

Table 38 *show controllers switch inter-rack stp Field Descriptions*

Field	Description
MST	Multiple Spanning Tree (MST).
vlans mapped	Number of VLANs mapped.
Bridge	Part of the bridge identifier and is taken as the most significant part of the bridge ID comparisons.
Root	MAC address of Root and Priority.
Operational	Operational STP parameters.
Configured	STP configured parameters.
Interface	Interface running STP.
Role	MSTP role that includes designated, alternate, root, and backup.
Sts	Spanning tree state (STS) that includes forwarding, blocking, and learning.
Cost	Cost associated with the port.
Prio.	Priority associated with the port.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers switch inter-rack uddl

To display the inter-rack connection for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card, use the **show controllers switch inter-rack uddl** command in administration EXEC mode.

show controllers switch inter-rack uddl {*interface number* | **all**} **location** *node-id*

Syntax Description	<i>interface number</i>	Number for the Gigabit Ethernet interface. The range is from 0 to 21. The interface number identifies the specific front panel GE port on the 22-port SCGE.
	all	Displays statistics of all ports for inter-rack switches.
	location <i>node-id</i>	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the <i>node-id</i> argument as entered in the <i>rack/slot/module</i> notation.

Defaults	No default behavior or values

Command Modes	Administration EXEC

Command History	Release	Modification
	Release 3.4.1	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	fabric	read
	root-system	read
	admin	read

Examples	The following sample output shows who is connected to the inter-rack on the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch inter-rack uddl all location  
f0/sc0/cpu0
```

```
Interface Gig port# 13  
---  
...
```

```
show controllers switch inter-rack udd
```

R3.5.0 Beta Draft—Cisco Confidential Information

```
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
...
...
Entry 1
---
...
Device name: 0_RP0_CPU0_Switch
Port ID: GE_Port_0
Neighbor echo 1 device: nodeF0_SC0_CPU0
Neighbor echo 1 port: Gig port# 13
```

Table 39 describes the significant fields shown in the display.

Table 39 *show controllers switch inter-rack udd Field Descriptions*

Field	Description
Interface Gig port	Interface number that identifies the specific front panel GE port on the 22-port SCGE.
Current bidirectional state	Current bidirectional state of the port is undetermined, bidirectional, or unidirectional.
Current operational state	Port operational status that includes up or error-disabled.
Device name	Connected device or neighbor.
Port ID	Port ID.
Neighbor echo 1 device	Device ID of neighbor.
Neighbor echo 1 port	Port ID of neighbor.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers switch stp location

To display the STP information for intra-rack switches, use the **show controllers switch stp location** command in administration EXEC mode.

show controllers switch stp location *node-id*

Syntax Description	<i>node-id</i>	The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults	No default behavior or values

Command Modes	Administration EXEC

Command History	Release	Modification
	Release 3.4.1	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	The spanning tree protocol (STP) runs on links between RPs and SCs.

Task ID	Task ID	Operations
	fabric	read
	root-system	read

Examples	The following sample output shows how to verify information for the spanning tree for location 0/rp0/CPU0 on the RP:
	RP/0/RP0/CPU0:router(admin)# show controllers switch stp location 0/rp0/Cpu0

```
RP/0/RP0/CPU0:router(admin)# show controllers switch stp location 0/rp0/Cpu0

##### MST    0 vlans mapped:    2-4094
Bridge        address 0011.93ef.e392 priority      36864 (36864 sysid 0)
Root          address 5246.48f0.20ff priority      32768 (32768 sysid 0)
              port      GE_Port_0   path cost      0
Regional Root address 5246.48f0.20ff priority      32768 (32768 sysid 0)
              internal cost      20000 rem hops  3
Operational   hello time 1, forward delay 6, max age 8, txholdcount 6
Configured    hello time 1, forward delay 6, max age 8, max hops  4

Interface      Role Sts Cost      Prio.Nbr Type
-----

```

R3.5.0 Beta Draft—Cisco Confidential Information

```
##### MST    1 vlans mapped:    1
Bridge        address 0011.93ef.e392 priority    36865 (36864 sysid 1)
Root          address 5246.48f0.20ff priority    32769 (32768 sysid 1)
              port      GE_Port_0 cost          20000 rem hops  3
```

```
Interface      Role Sts Cost          Prio.Nbr Type
-----
FE_Port_1 Desg FWD  200000 128.    2 P2p
GE_Port_0 Root FWD   20000 128.   49 P2p
```

The following sample output shows how to verify the connection on intra-rack switches for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch stp location f0/sc0/CPU0
```

```
##### MST    0 vlans mapped:    2-4094
Bridge        address 0800.453e.469a priority    36864 (36864 sysid 0)
Root          address 5246.48f0.20ff priority    32768 (32768 sysid 0)
              port      GE_Port_0 path cost      0
Regional Root address 5246.48f0.20ff priority    32768 (32768 sysid 0)
              internal cost 20000 rem hops  3
Operational   hello time 1, forward delay 6, max age 8, txholdcount 6
Configured    hello time 1, forward delay 6, max age 8, max hops  4
```

```
Interface      Role Sts Cost          Prio.Nbr Type
-----
```

```
##### MST    1 vlans mapped:    1
Bridge        address 0800.453e.469a priority    36865 (36864 sysid 1)
Root          address 5246.48f0.20ff priority    32769 (32768 sysid 1)
              port      GE_Port_0 cost          20000 rem hops  3
```

```
Interface      Role Sts Cost          Prio.Nbr Type
-----
FE_Port_1 Desg FWD  200000 128.    2 P2p
GE_Port_0 Root FWD   20000 128.   49 P2p
```

Table 40 describes the significant fields shown in the display.

Table 40 *show controllers switch stp location Field Descriptions*

Field	Description
MST	Multiple Spanning Tree Protocol (MST).
vlans mapped	VLANs mapped to MST instance.
Bridge	MAC address of Bridge and Priority.
Root	MAC address of Root and Priority.
Regional Root	Root of the MST region.
Operational	Operational STP parameters.
Configured	STP configured parameters.
Interface	Interface running STP.
Role	MSTP role that includes designated, alternate, root, and backup.
Sts	Spanning tree state (STS) that includes forwarding, blocking, and learning.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 40** *show controllers switch stp location Field Descriptions (continued)*

Field	Description
Cost	Cost of path to root.
Prio.Nbr Type	Priority of switch port.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers switch stp ports

To display the Spanning Tree Protocol (STP) information for intra-rack switches, use the **show controllers switch stp ports** command in administration EXEC mode.

show controllers switch stp ports {FE {0 | 1} | GE {0 | 1}} **location** *node-id*

Syntax Description

FE {0 1}	Displays information for the Fast Ethernet (FE) port. Choose one of the following values: 0—FE port number 0. 1—FE port number 1.
GE {0 1}	Displays information for the Gigabit Ethernet (GE) port. Choose one of the following values: 0—GE port number 0. 1—GE port number 1.
location <i>node-id</i>	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the <i>node-id</i> argument as entered in the <i>rack/slot/module</i> notation.

Defaults

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.4.1	This command was introduced on the Cisco CRS-1.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

**Note**

The port numbers must match the port numbers that are displayed on the front panel of the 22-port SCGE card.

Task ID

Task ID	Operations
fabric	read
root-system	read

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows the remote-end point that is connected to the GE link even if the remote endpoint is on a different chassis:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch stp ports FE 1 location 0/rp0/CPU0
```

```
FE_Port_1 of MST1 is designated forwarding
Edge port:          no          (default) port guard :    none      (default)
Link type: point-to-point          (auto) bpdu filter: disable  (default)
Boundary : internal                bpdu guard : disable  (default)
Bpdus (MRecords) sent 9190, received 3
```

```
Instance Role Sts Cost      Prio.Nbr Vlans mapped
-----
      1 Desg  FWD   200000 128.    2 1
```

Table 41 describes the significant fields shown in the display.

Table 41 *show controllers switch stp ports Field Descriptions*

Field	Description
GE Port	Gigabit Ethernet (GE) port.
STP State	Spanning Tree Protocol (STP) state of the port

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers switch stp region

To display information for the spanning tree for the Multiple Spanning Tree (MST) region, use the **show controllers switch stp region** command in administration EXEC mode.

show controllers switch stp region location *node-id*

Syntax Description

location <i>node-id</i>	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the <i>node-id</i> argument as entered in the <i>rack/slot/module</i> notation.

Defaults

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.4.1	This command was introduced on the Cisco CRS-1.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
fabric	read
root-system	read

Examples

The following example displays sample output from the **show controllers switch stp region** command:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch stp region location 0/rp0/CPU0
```

```
Name      [STP_1]
Revision   1
Instances configured 2
```

```
-----
0      2-4094
1      1
-----
```

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers switch uddl location

To display the Unidirectional Link Detection (UDLD) information for intra-rack switches., use the **show controllers switch uddl location** command in administration EXEC mode.

show controllers switch uddl location*node-id*

Syntax Description	<i>node-id</i>	The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults	No default behavior or values

Command Modes	Administration EXEC

Command History	Release	Modification
	Release 3.4.1	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	UDLD runs on links between RPs and SCs.

Task ID	Task ID	Operations
	fabric	read
	root-system	read

Examples	The following sample output shows who is connected on the RP:
	<pre>RP/0/RP0/CPU0:router(admin)# show controllers switch uddl location 0/rp0/CPU0 Interface GE_Port_0 Current bidirectional state: Bidirectional Current operational state: Advertisement - Single neighbor detected ... Entry 1 --- Device name: nodeF0_SC0_CPU0 Port ID: Gig port# 13 Neighbor echo 1 device: 0_RP0_CPU0_Switch Neighbor echo 1 port: GE_Port_0</pre>

R3.5.0 Beta Draft—Cisco Confidential Information

The following sample output shows an intra-rack connection for the 22-port Shelf Controller Gigabit Ethernet (22-port SCGE) card:

```
RP/0/RP0/CPU0:router(admin)# show controllers switch udd location f0/sc0/CPU0
```

```
Interface GE_Port_0
---
...
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
...

Entry 1
---
...
Current neighbor state: Bidirectional
Device name: nodeF0_SC0_CPU0
Port ID: Gig port# 22
Neighbor echo 1 device: F0_SC0_CPU0_Switch
Neighbor echo 1 port: GE_Port_0
```

Table 42 describes the significant fields shown in the display.

Table 42 *show controllers switch udd location Field Descriptions*

Field	Description
Current bidirectional state	Current bidirectional state of the port is undetermined, bidirectional, or unidirectional.
Current operational state	Port operational status that includes up or error-disabled.
Current neighbor state	Neighbor state states that the link state is observed from the neighbor (undetermined, bidirectional, or unidirectional).
Device name	Connected device or neighbor.
Port ID	Port ID.
Neighbor echo 1 device	Device ID of neighbor.
Neighbor echo 1 port	Port ID of neighbor.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers switch uddl ports

To display the information for Unidirectional Link Detection (UDLD) for a specified location, use the **show controllers switch uddl ports** command in administration EXEC mode.

show controllers switch uddl ports {FE {0 | 1} | GE {0 | 1}} **location** *node-id*

Syntax Description	FE {0 1}	Displays information for the Fast Ethernet (FE) port. Choose one of the following values: 0—FE port number 0. 1—FE port number 1.
	GE {0 1}	Displays information for the Gigabit Ethernet (GE) port. Choose one of the following values: 0—GE port number 0. 1—GE port number 1.
	location <i>node-id</i>	Specifies the specific RP/SC in the system in which the switches are present. This applies to location descriptions for the <i>node-id</i> argument as entered in the <i>rack/slot/module</i> notation.

Defaults	No default behavior or values

Command Modes	Administration EXEC

Command History	Release	Modification
	Release 3.4.1	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. UDLD runs on links between RPs and SCs.

Task ID	Task ID	Operations
	fabric	read
	root-system	read

Examples	The following example displays sample output from the show controllers switch uddl ports command:

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(admin)# show controllers switch udd ports FE 1 location 0/rp0/CPU0
```

```
Interface FE_PORT_1
```

```
---
```

```
Port enable administrative configuration setting: Enabled
```

```
Port enable operational state: Enabled
```

```
Current bidirectional state: Bidirectional
```

```
Current operational state: Advertisement - Single neighbor detected
```

```
Message interval: 7
```

```
Time out interval: 5
```

```
Entry 1
```

```
---
```

```
Expiration time: 16
```

```
Device ID: 1
```

```
Current neighbor state: Bidirectional
```

```
Device name: 0_RP1_CPU0_Switch
```

```
Port ID: FE_PORT_0
```

```
Neighbor echo 1 device: 0_RP0_CPU0_Switch
```

```
Neighbor echo 1 port: FE_PORT_1
```

```
Message interval: 7
```

```
Time out interval: 5
```

```
CDP Device name: BCM_SWITCH
```



ASIC Driver Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

This module describes the commands used to configure and monitor the ASICs on a router running Cisco IOS XR software.

R3.5.0 Beta Draft—Cisco Confidential Information

asic-scan pse

To run a generic ASIC scan on the Packet Switching Engine (PSE), use the **asic-scan pse** command in EXEC mode.

```
asic-scan pse {egress | ingress} [disable | enable | help-subblock | subblock_number [error_cause
[disable | enable] | disable | enable | help_cause] | quick-scan [filename [filename] | allscan]
location node-id
```

Syntax Description

egress	Runs the ASIC scan on the egress PSE device.
ingress	Runs the ASIC scan on the ingress PSE device.
disable	(Optional) Disables the ASIC scan on all sub-blocks.
enable	(Optional) Enables the ASIC scan on all sub-blocks.
help-subblock	(Optional) Lists all sub-block numbers.
<i>subblock_number</i> error_cause [disable enable]	(Optional) Enables or disables the ASIC scan on a specific error cause in the specified sub-block. Replace <i>subblock_number</i> with the number that identifies the sub-block on which to enable or disable the ASIC scan. Replace <i>error_cause</i> with the number that identifies an error cause in the specified sub-block.
<i>subblock_number</i> disable	(Optional) Disables the ASIC scan on the specified sub-block
<i>subblock_number</i> enable	(Optional) Enables the ASIC scan on the specified sub-block
<i>subblock_number</i> help_cause	(Optional) Lists all block numbers in the specified sub-block.
quick-scan <i>filename</i>	(Optional) Performs a quick ASIC scan on a specific file. Replace <i>filename</i> with the name of the .xsvf file on which to run the quick ASIC scan
<i>filename</i>	Name of the file on which to write the ASIC scan output.
quick-scan allscan	(Optional) Performs a quick ASIC scan on all bits of the chip, including the preread for Metro.
location <i>node-id</i>	Identifies the location of the node hosting the PSE on which to run the ASIC scan. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation. Note Use the show platform command to see the location of all nodes installed in the router.

Defaults

No default behavior or values

Command Modes

EXEC

R3.5.0 Beta Draft—Cisco Confidential Information**Command History**

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	No modification.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
drivers	read, write

Examples

The following example shows how to run a quick ASIC scan on all bits of the chip on the egress PSE device that is located on the CPU node in slot 1:

```
RP/0/RP0/CPU0:router# asic-scan pse egress quick-scan allscan location 0/1/CPU0
```

```
quick_scan: {'sysdb' detected the 'warning' condition 'An EDM took too long to process a request and was timed out'} Scan in progress... Please wait for completion mesaage
```

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

The following command shows how to run an ASIC scan on the ingress PSE device that is located on the CPU node in slot 1:

```
RP/0/RP0/CPU0:P2_CR8-8# asic-scan pse ingress location 0/1/CPU0
```

```
RP/0/RP0/CPU0:P2_CR8-8#
```

R3.5.0 Beta Draft—Cisco Confidential Information

clear controller egressq queue

To clear a specific controller egress queue, use the **clear controller egressq queue** command in EXEC mode.

clear controller egressq queue *queue-id1* [*queue-id2*] **location** *node-id*

Syntax Description

<i>queue-id1</i>	Queue you want to clear. Replace <i>queue-id1</i> with a queue number. Range is from 1 through 8191.
<i>queue-id2</i>	(Optional) Last queue in a range of queues to clear. Replace <i>queue-id2</i> with a queue number. Range is from 1 through 8191.
location <i>node-id</i>	Identifies the location of the node whose egress queue you want to clear. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.
Note Use the show platform command to see the location of all nodes installed in the router.	

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	No modification.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

**Note**

If you enter the optional [*queue-id2*] argument after you enter the *queue-id1* argument, then the *queue-id1* argument specifies the first queue in a range of queues to be cleared. If you enter the *queue-id1* argument without specifying the *queue-id2* argument, then only the queue specified for *queue-id1* is cleared.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	root-system	read
	basic-services	read, write
	drivers	read, write

Examples

The following example shows how to clear a specific controller egress queue:

```
RP/0/RP0/CPU0:router# clear controller egress queue 1 location 0/1/CPU0
```

Related Commands

Command	Description
clear controller egressq queue all	Clears all controller egress queues in the specified location.

R3.5.0 Beta Draft—Cisco Confidential Information

clear controller egressq queue all

To clear all controller egress queues on a specific node, use the **clear controller egressq queue all** command in EXEC mode.

clear controller egressq queue all location *node-id*

Syntax Description	all	Clears all egress queues in the specified <i>location</i> .
	location <i>node-id</i>	Identifies the location of the egressq queue you want to clear. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.
	Note	Use the show platform command to see the location of all nodes installed in the router.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	No modification.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	root-system	read
	basic-services	read, write
	drivers	read, write

Examples

The following example shows how to clear all controller egress queues on a specific node:

```
RP/0/RP0/CPU0:router# clear controller egress queue all location 0/1/CPU0
```

Related Commands

Command	Description
show asic errors	Clears a specific controller egress queue.

R3.5.0 Beta Draft—Cisco Confidential Information

clear controller egressq statistics

To clear the egress queue statistics in a specific location, use the **clear controller egressq statistics** command in EXEC mode.

clear controller egressq statistics location *node-id*

Syntax Description

location *node-id*

Identifies the location of the egressq queue whose statistics you want to clear. The *node-id* is expressed in the *rack/slot/module* notation.

Note Use the **show platform** command to see the location of all nodes installed in the router.

Defaults

No default behavior or values

Command Modes

EXEC

Command History**Release****Modification**

Release 2.0

This command was introduced on the Cisco CRS-1.

Release 3.0

No modification.

Release 3.2

No modification.

Release 3.3.0

No modification.

Release 3.4.0

No modification.

Release 3.5.0

No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID**Task ID****Operations**

drivers

read, write

Examples

The following example shows how to clear all controller egress queue statistics on a specific node:

```
RP/0/RP0/CPU0:router# clear controller egressq statistics location 0/1/CPU0
```

Related Commands**Command****Description**

[show controllers egressq statistics](#)

Displays egress queue manager statistics.

R3.5.0 Beta Draft—Cisco Confidential Information

clear controller pse statistics

To clear statistics maintained by the packet switching engine (PSE) on a specific PSE device instance, or on a specific node, use the **clear controller pse statistics** command in EXEC mode.

clear controller pse statistics [**instance** {**0** | **1**}] [**location** *node-id*]

Syntax Description	instance { 0 1 }	(Optional) Identifies the PSE device whose statistics you want to clear. Enter 0 to specify the ingress PSE device, or enter 1 to specify the egress PSE device. Note Follow the instance { 0 1 } argument with the location <i>node-id</i> argument to restrict the command to specific node containing the specified device instance.
	location <i>node-id</i>	(Optional) Identifies the location of the node whose PSE device statistics you want to clear. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation. Note Use the show platform command to see the location of all nodes installed in the router. Note Include the instance { 0 1 } argument before the location <i>node-id</i> argument to restrict the command to a specific device instance on the specified node.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	No modification.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

R3.5.0 Beta Draft—Cisco Confidential Information

The **instance** keyword directs the **clear controller pse statistics** command to a specific PSE device, and the **location** keyword directs the **clear controller pse statistics** command to that device or devices on the specified modular services card. You can specify the **instance** and **location** keywords together in the same command. If the **instance** and **location** keywords are not specified, the **clear controller pse statistics** command takes effect on both device instances on all modular services cards.

Task ID	Task ID	Operations
	root-system	execute
	drivers	read, write

Examples

The following example shows how to clear PSE statistics on a specific instance of the controller (instance 1):

```
RP/0/RP0/CPU0:router# clear controller pse statistics instance 1
```

The following example shows how to clear all PSE statistics on a specific node (0/1/CPU0):

```
RP/0/RP0/CPU0:router# clear controller pse statistics location 0/1/CPU0
```

Related Commands

Command	Description
show controllers pse eio links	Displays PSE information for EIO (Elastic I/O) links, or for a specific controller.
show controllers pse ipc	Displays PSE information for IPC connections, or for a specific IPC controller.
show controllers pse mp	Displays PSE information for the maintenance processor on a specific controller or node.
show controllers pse statistics	Displays PSE statistics for a specific controller instance, or for a specific node.
show controllers pse summary	Displays a summary of PSE information for a specific controller or node.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers cpuctrl cdma

To display information about the CPU controller Code Division Multiplex Access (CDMA) engine, use the **show controllers cpuctrl cdma** command in EXEC mode.

show controllers cpuctrl cdma {**all** | **cdma0** {*queue* | **all**} | **cdma1** {*queue* | **all**} {**active** | **detail**} [**location** *node-id*]

Syntax Description		
all		Displays CDMA information for channel 0 and channel 1.
cdma0 <i>queue</i>		Displays CDMA information for a specific Division Multiplex Access (DMA) queue on channel 0. Replace <i>queue</i> with a number. Range is from 1 through 7.
cdma0 all		Displays CDMA engine information for all DMA queues on channel 0.
cdma1 <i>queue</i>		Displays CDMA information for a specific Division Multiplex Access (DMA) queue on channel 1. Replace <i>queue</i> with a number. Range is from 1 through 7.
cdma1 all		Displays CDMA engine information for all DMA queues on channel 1.
active		Displays descriptions for active DMA queues only.
detail		Displays descriptions for any DMA queues, regardless of whether they are active.
location <i>node-id</i>		(Optional) Identifies the location of the node whose CPU controller CDMA information you want to display. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	No modification.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	drivers	read

Examples

The following example shows how to display CPU controller CDMA information from the active DMA queues on channel 1:

```
RP/0/RP0/CPU0:router# show controllers cpuctrl cdma cdma0 1 active
```

```
-----
DMA queue:
Channel:      0          queue:      1
client handle: 1          queue state: Active
OS Interrupt Level:108      Cpuctrl Interrupt Level:12
OS Run Priority:45  Queue Created 1 times
Pakmode = 0x2
CDMA out_of_desc failures = 0
CDMA transactions = 3, Bytes DMA'd = 67584
DMA IWA = 0
ISR pointer is at 0x78043224  Descriptor List at 0xec032300
Pakman/Bufman Instance: /dev/bufman/misc
client callback function pointer 0x48203424
client cleanup function pointer 0x48203424
```

```
Queue descriptor list info:
list_size=32  current_index=3  tx_index=3
active descriptors number:0
```

```
-----
DMA queue:
Channel:      0          queue:      1
client handle: 1          queue state: Active
OS Interrupt Level:108      Cpuctrl Interrupt Level:12
OS Run Priority:45  Queue Created 1 times
Pakmode = 0x2
CDMA out_of_desc failures = 0
CDMA transactions = 3, Bytes DMA'd = 67584
DMA IWA = 0
ISR pointer is at 0x7804316c  Descriptor List at 0xec032300
Pakman/Bufman Instance: /dev/bufman/misc
client callback function pointer 0x48203424
client cleanup function pointer 0x48203424
```

```
Queue descriptor list info:
list_size=32  current_index=3  tx_index=3
--More-
active descriptors number:0
```

```
-----
DMA queue:
Channel:      0          queue:      1
client handle: 1          queue state: Inactive
-----
DMA queue:
Channel:      0          queue:      1
client handle: 1          queue state: Inactive
```

R3.5.0 Beta Draft—Cisco Confidential Information

Table 43 describes the significant fields shown in the display.

Table 43 *show controllers cpuctrl cdma Field Descriptions*

Field	Description
DMA queue	Identifies the DMA queue.
Channel	Identifies the channel whose DMA queue is displayed. 0 is the ingress channel, and 1 is the egress channel
queue	Identifies the queue.
client handle	Internal identifier for the Cisco client.
queue state	Current state of the queue.
OS Interrupt Level	Current interrupt level for the queue.
Cpuctrl Interrupt Level	Current interrupt level for the CPU controller.
OS Run Priority	Run priority level for this queue.
Queue Created 1 times	Number of times this queue was regenerated.
Pakmode	Information about internal data structures and parameters.
CDMA out_of_desc failures	Number of CDMA ¹ failures in the queue.
CDMA transactions	Number of CDMA transactions in the queue.
Bytes DMA'd	Number of bytes that have been processed by the Division Multiplex Access engine.
DMA IWA	Number of IWA bytes that have been processed by the Division Multiplex Access engine.
ISR pointer is at	Internal information about the location of the ISR ² pointer.
Descriptor List at	Internal information about the location of the descriptor list.
Pakman/Bufman Instance	Internal information about the location of the Pakman and Bufman Instance.
client callback function pointer	Internal information about the client callback function pointer.
client cleanup function pointer	Internal information about the client cleanup function pointer.
Queue descriptor list info	Internal information about the queue descriptor list.

1. Code Division Multiple Access

2. intermediate session routing

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers cpuctrl clients

To display information about all CPU controller clients on the router, or for specific CPU controller clients, use the **show controllers cpuctrl clients** command in EXEC mode.

```
show controllers cpuctrl clients {all | cdma {plim asic | dcc | egressq | fabricq | fia | ingressq |
jacketcard | mipc | plim | plimasic | pse | reindeer} | pdma {diag | fia | frf | gsp | mipc | mstats
| netflow | netio}} {active | detail} [location node-id]
```

Syntax Description

all	Displays a summary information for all clients on the router.
cdma	Displays information about Code Division Multiplex Access (CDMA) clients only.
dcc	Displays information for the dcc client.
egressq	Displays information for the egressq client.
fabricq	Displays information for the Fabricq ASIC client.
fia	Displays information for the Fabric Interface ASIC (FIA) client.
ingressq	Displays information for the ingressq ASIC client.
jacketcard	Displays information for the jacketcard client.
mipc	Displays information for the Marvel interprocess communication (MIPC) client.
plim	Displays information for the plim client.
plimasic	Displays information for the plim ASIC client.
pse	Displays information for the pse client.
reindeer	Displays information for the reindeer client.
pdma	Displays information for Provisioning-Driven Memory Administration (PDMA) clients only.
diag	Displays information for the PDMA client called DIAG packet.
fia	Displays information for the Fabric Interface ASIC packet PDMA client.
frf	Displays information for the Fast Reroute (FRR) packet PDMA client.
gsp	Displays information for the Global Support Partner (GSP) packet PDMA client.
mipc	Displays information for the MIPC packet PDMA client.
mstats	Displays information for the MSTATS packet PDMA client.
netflow	Displays information for the NETFLOW packet PDMA client.
netio	Displays information for the NETIO packet PDMA client.
active	Displays descriptions for active queues only.
detail	Displays descriptions for any queues, regardless of whether they are active.
location node-id	(Optional) Identifies the location of the node whose CPU controller information you want to display. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.

Defaults

No default behavior or values

R3.5.0 Beta Draft—Cisco Confidential Information**Command Modes** EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	No modification.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	drivers	read

Examples The following example shows how to display information about the active queues on the CPU controller client called “plimasic”:

```
RP/0/RP0/CPU0:router# show controllers cpuctrl clients plimasic active
```

```
-----
client_name: plimasic client_handle: 10
isr_count:   0          queue_count:  0
client_pid:  0
```

```
-----
client_name: plimasic client_handle: 10
isr_count:   0          queue_count:  0
client_pid:  0
```

```
-----
client_name: plimasic client_handle: 10
isr_count:   0          queue_count:  0
client_pid:  0
```

```
-----
client_name: plimasic client_handle: 10
isr_count:   0          queue_count:  0
client_pid:  0
```

R3.5.0 Beta Draft—Cisco Confidential Information

Table 44 describes the significant fields shown in the display.

Table 44 *show controllers cpuctrl clients Field Descriptions*

Field	Description
client	Client type that whose information is displayed. Can be DMA ¹ or PKT.
client_name	Identifies the client whose information is displayed.
client_handle	Internal client identifier.
isr_count	ISR ² counters.
queue_count	Queue counters.
client_pid	Client PID ³ .

1 Division Multiplex Access

2. Integrated SONET/SDH

3. packet identification

Related Commands

Command	Description
show controllers cpuctrl summary	Displays summarized information about all CPU controller ASICs on the router or on a specific node

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers cpuctrl devices

To display information about the CPU controller devices on the router, use the **show controllers cpuctrl devices** command in EXEC mode.

```
show controllers cpuctrl devices {egressq | epse | fabricq0 | fabricq1 | fabricq2 | fabricq3 |
    fia0 | fia1 | ingressq | ipse | jacketcard0 | jacketcard1 | jacketcard2 | plimasic0 | plimasic1 |
    plimasic2 | plimasic3 | plimfpga} {pdma queue {all | tx | rx} {active | detail} | pio}
[location node-id]
```

Syntax Description		
egressq		Displays information about the egressq ASIC instance 0.
epse		Displays information about the egress packet switching engine (PSE) ASIC.
fabricq0		Displays information about the fabricq ASIC instance 0.
fabricq1		Displays information about the fabricq ASIC instance 1.
fabricq2		Displays information about the fabricq ASIC instance 2.
fabricq3		Displays information about the fabricq ASIC instance 3.
fia0		Displays information about the Fabric Interface ASIC (FIA) instance 0.
fia1		Displays information about the FIA instance 1.
ingressq		Displays information about the ingressq ASIC.
ipse		Displays information about the ingress packet switching engine (PSE) ASIC.
jacketcard0		Displays information about the jacketcard0 ASIC.
jacketcard1		Displays information about the jacketcard1 ASIC.
jacketcard2		Displays information about the jacketcard2 ASIC.
plimasic0		Displays information about the PLIM ASIC instance 0.
plimasic1		Displays information about the PLIM ASIC instance 1.
plimasic2		Displays information about the PLIM ASIC instance 2.
plimasic3		Displays information about the PLIM ASIC instance 3.
plimfpga		Displays information about the field-programmable gate array (FPGA) PLIM.
pdma queue all		Displays transmit and receive Provisioning-Driven Memory Administration (PDMA) information for the specified queue. Replace <i>queue</i> with a queue number. The range is from 1 through 7.
pdma queue tx		Displays transmit PDMA information only for the specified queue. Replace <i>queue</i> with a queue number. The range is from 1 through 7.
pdma queue rx		Displays receive PDMA information only for the specified queue. Replace <i>queue</i> with a queue number. The range is from 1 through 7.
pdma all		Displays transmit and receive PDMA information for all queues.
active		Displays descriptions for active queues only.
detail		Displays detailed descriptions for any queues, regardless of whether they are active.

R3.5.0 Beta Draft—Cisco Confidential Information

pio	Displays transmit and receive Polled I/O (PIO) information for the specified queue.
location <i>node-id</i>	(Optional) Identifies the location of the node whose CPU controller information you want to display. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	No modification.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	drivers	read

Examples The following example shows how to display transmit and receive PDMA information for all active queues on the egressq ASIC instance 0:

```
RP/0/RP0/CPU0:router# show controllers cpuctrl devices egressq pdma all active
```

```
-----
TX PKT queue:
  cpuctrl net Port:      7          queue:      0
  client handle: 6       queue state: Active
  OS Interrupt Level:127   Cpuctrl Interrupt Level:31
  OS Run Priority:20   Queue Created 1 times
  Pakmode = 0x1
  Tx out_of_desc failures = 0
  Packets transmitted = 0, Byte transmitted = 0
  Tx IWA = 0
  ISR pointer is at 0x7804372c   Descriptor List at 0xec27b060
  Pakman/Bufman Instance: /dev/pakman/server
  client callback function pointer 0x00000000
  client cleanup function pointer 0x00000000
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

Queue descriptor list info:
list_size=1024  current_index=0  tx_index=0
active descriptors number:0

```

```

-----
TX PKT queue:
  cpuctrl net Port:      0          queue:      1
client handle: 6         queue state: Inactive
-----

```

```

TX PKT queue:
  cpuctrl net Port:      0          queue:      2
client handle: 6         queue state: Inactive
-----

```

```

TX PKT queue:
  cpuctrl net Port:      0          queue:      3
client handle: 6         queue state: Inactive
-----

```

```

TX PKT queue:
  cpuctrl net Port:      0          queue:      4
client handle: 6         queue state: Inactive
-----

```

```

TX PKT queue:
  cpuctrl net Port:      0          queue:      5
client handle: 6         queue state: Inactive
-----

```

```

TX PKT queue:
  cpuctrl net Port:      0          queue:      6
client handle: 6         queue state: Inactive
-----

```

```

TX PKT queue:
  cpuctrl net Port:      0          queue:      7
client handle: 6         queue state: Inactive
-----

```

```

RX PKT queue:
  cpuctrl net Port:      7          queue:      0
client handle: 3         queue state: Active
--More--

```

Table 45 describes the significant fields shown in the display.

Table 45 *show controllers cpuctrl devices Field Descriptions*

Field	Description
PKT queue:	Displays whether the packet queue is TX ¹ or RX ² .
cpuctrl net Port	Identifies the CPU controller port.
queue	Identifies the queue whose CPU controller device information is displayed.
client handle	Internal Cisco client identifier.
queue state	Current state of the queue. The queue can be <i>Active</i> or <i>Inactive</i> .

1. transmit

2. receive

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show controllers cpuctrl summary	Displays summarized information about all CPU controller ASICs on the router or on a specific node

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers cpuctrl internal

To display information about the internal CPU controller, use the **show controllers cpuctrl internal** command in EXEC mode.

show controllers cpuctrl internal location *node-id*

Syntax Description	location <i>node-id</i>	Identifies the location of the node whose internal CPU controller information you want to display. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	No modification.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	drivers	read

Examples	The following example shows how to display information about the internal CPU controller:

```
RP/0/RP0/CPU0:router# show controllers cpuctrl internal
```

```
Cpuctrl Internal Info for node 0/0/CPU0:
Error Interrupts = 0      Spurious Error Interrupts = 0
PCI Error Overflows = 0      PCI PM Error Overflows = 0
PCIX Error Overflows = 0      Internal Access PCI Overflows = 0
Port Error Overflows = 0      Error Log Overflows = 0
cpuctrl Config Reg = 0x8357ffff cpuctrl Physical Offset = 0x80000000
cpuctrl Window Size = 0x40000000 cpuctrl Port Window Size = 0x04000000
```

R3.5.0 Beta Draft—Cisco Confidential Information

```
cpuctrl SHMem Size = 0x00800000  cpuctrl SHMem Used = 0x00223ee8
cpuctrl version info: Squid FPGA v2.07 Fri Jan 23 16:21:01 2004 ykoren
```

```
Cpuctrl Internal Info for node 0/3/CPU0:
Error Interrupts = 0      Spurious Error Interrupts = 0
PCI Error Overflows = 0      PCI PM Error Overflows = 0
PCIX Error Overflows = 0      Internal Access PCI Overflows = 0
Port Error Overflows = 0      Error Log Overflows = 0
cpuctrl Config Reg = 0x8357ffff  cpuctrl Physical Offset = 0x80000000
cpuctrl Window Size = 0x40000000  cpuctrl Port Window Size = 0x04000000
cpuctrl SHMem Size = 0x00800000  cpuctrl SHMem Used = 0x00223ee8
cpuctrl version info: Squid FPGA v2.07 Fri Jan 23 16:21:01 2004 ykoren
```

```
Cpuctrl Internal Info for node 0/RP0/CPU0:
Error Interrupts = 0      Spurious Error Interrupts = 0
PCI Error Overflows = 0      PCI PM Error Overflows = 0
PCIX Error Overflows = 0      Internal Access PCI Overflows = 0
Port Error Overflows = 0      Error Log Overflows = 0
cpuctrl Config Reg = 0x803f007f  cpuctrl Physical Offset = 0x80000000
cpuctrl Window Size = 0x40000000  cpuctrl Port Window Size = 0x04000000
cpuctrl SHMem Size = 0x00800000  cpuctrl SHMem Used = 0x00223ee8
cpuctrl version info: Squid FPGA v2.07 Fri Feb 6 17:49:22 2004 ykoren

Cpuctrl Internal Info for node 0/RP1/CPU0:
Error Interrupts = 0      Spurious Error Interrupts = 0
PCI Error Overflows = 0      PCI PM Error Overflows = 0
PCIX Error Overflows = 0      Internal Access PCI Overflows = 0
Port Error Overflows = 0      Error Log Overflows = 0
cpuctrl Config Reg = 0x003f007f  cpuctrl Physical Offset = 0x80000000
cpuctrl Window Size = 0x40000000  cpuctrl Port Window Size = 0x04000000
cpuctrl SHMem Size = 0x00800000  cpuctrl SHMem Used = 0x00223ee8
cpuctrl version info: Squid FPGA v2.05 Wed Sep 3 17:37:47 2003 ykoren
```

Table 46 describes the significant fields shown in the display.

Table 46 *show controllers cpuctrl internal Field Descriptions*

Field	Description
Error Interrupts	Total of error interrupts that have occurred on this node.
Spurious Error Interrupts	Current number interrupts that have occurred on this node due to spurious errors.
PCI Error Overflows	Number of times the PCI ¹ error buffer overflowed on the node. Note When an overflow occurs, packets may be dropped.
PCI PM Error Overflows	Number of times PCI PM ² errors buffer overflowed on this node. Note When an overflow occurs, packets may be dropped.
PCIX Error Overflows	Number of times the PCI IX error buffer overflowed on this node. Note When an overflow occurs, packets may be dropped.
Internal Access PCI Overflows	Number of times the Internal Access PCI buffer overflowed on this node. Note When an overflow occurs, packets may be dropped.
Port Error Overflows	Number of times the port error buffer overflowed on this node. Note When an overflow occurs, packets may be dropped.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 46** *show controllers cpuctrl internal Field Descriptions (continued)*

Field	Description
Error Log Overflows	Number of times the error log buffer overflowed on this node. Note When an overflow occurs, packets may be dropped.
cpuctrl Config Reg	CPU controller configuration register, expressed in hexadecimal format.
cpuctrl Physical Offset	CPU controller physical offset, expressed in hexadecimal format.
cpuctrl Window Size	CPU controller window size, expressed in hexadecimal format. CPU controller performance improves as window size increases.
cpuctrl Port Window Size	CPU controller port window size, expressed in hexadecimal format. CPU controller port performance improves as window size increases.
cpuctrl SHMem Size	CPU controller SH memory size, expressed in hexadecimal format.
cpuctrl SHMem Used	CPU controller SH memory that has been used already, expressed in hexadecimal format.
cpuctrl version info	Provides version information for the CPU controller. The information displayed is: • Squid version • Date of the last version install or upgrade • ID of the user who performed the install or upgrade.

1. Peripheral Component Interconnect
2. port manager

Related Commands

Command	Description
show controllers cpuctrl summary	Displays summarized information about all CPU controller ASICs on the router or on a specific node

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers cpuctrl ports

To display port information for the specified CPU controller ASIC, use the **show controllers cpuctrl ports** command in EXEC mode.

```
show controllers cpuctrl ports {cpuctrl | egressq| epse | fabricq0 | fabricq1 | fabricq2 |
    fabricq3 | fia0 | fia1 | ingressq | ipse | jacketcard0 | jacketcard1 | jacketcard2 | plimasic0 |
    plimasic1 | plimasic2 | plimasic3 | reindeer} {pdma queue-id {all | rx | tx} {active | detail} |
    pio} [location node-id]
```

Syntax Description		
cpuctrl		Displays port information for the CPU controller ASIC instance 0.
egressq		Displays port information for the egressq ASIC instance 0.
epse		Displays port information for the egress packet switching engine (EPSE) ASIC.
fabricq0		Displays port information for the fabricq ASIC instance 0.
fabricq1		Displays port information for the fabricq ASIC instance 1.
fabricq2		Displays port information for the fabricq ASIC instance 2.
fabricq3		Displays port information for the fabricq ASIC instance 3.
fia0		Displays port information for the fabric Interface ASIC (FIA) instance 0.
fia1		Displays port information for the fabric Interface ASIC (FIA) instance 1.
ingressq		Displays port information for the ingressq ASIC.
ipse		Displays port information for the ingress packet switching engine (PSE) ASIC.
jacketcard0		Displays port information for the jacketcard0 ASIC.
jacketcard1		Displays port information for the jacketcard1 ASIC.
jacketcard2		Displays port information for the jacketcard2 ASIC.
plimasic0		Displays port information for instance 0 of the plim ASIC.
plimasic1		Displays port information for instance 1 of the plim ASIC.
plimasic2		Displays port information for instance 2 of the plim ASIC.
plimasic3		Displays port information for instance 3 of the plim ASIC.
reindeer		Displays port information for the reindeer ASIC.
pdma queue-id all		Displays transmit and receive Provisioning-Driven Memory Administration (PDMA) information for the specified queue.
pdma queue-id tx		Displays transmit PDMA information only for the specified queue. The information displayed pertains to the ASIC indicated in the show controllers cpuctrl ports command.
pdma queue-id rx		Displays receive PDMA information only for the specified queue. The information displayed pertains to the ASIC indicated in the show controllers cpuctrl ports command.
pdma all		Displays transmit and receive PDMA information for all queues. The information displayed pertains to the ASIC indicated in the show controllers cpuctrl ports command.
active		Displays descriptions for active queues only.

R3.5.0 Beta Draft—Cisco Confidential Information

detail	Displays descriptions for any queues, regardless of whether they are active.
pio	Displays transmit and receive Polled I/O (PIO) information for the specified queue.
location <i>node-id</i>	(Optional) Identifies the location of the node whose CPU controller port information you want to display. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	No modification.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	drivers	read

Examples The following example shows how to display port information for the transmit and receive PIO queues on the EPSE ASIC:

```
RP/0/RP0/CPU0:router# show controllers cpuctrl ports epse pio
```

```
client name: PSE                device instance: 1
cpuctrl net port: 6             pci base: 0x98000000
map reg: 0x6076a12c            OS interrupt level: 102
Cpuctrl interrupt level: 6      OS Run priority: 6
config reg: 0x00000000          channels reg: 0x00000000
int_cause_asic_mask: 0x00000010 int_cause_error_mask: 0x00000020
int_cause_link_error_mask: 0x00000040
crc_errors: 0   sync_errors: 0  reframe_events: 0
```

```
client name: PSE                device instance: 1
cpuctrl net port: 6             pci base: 0x98000000
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

map reg: 0x6076a12c          OS interrupt level: 102
Cpuctrl interrupt level: 6    OS Run priority: 6
config reg: 0x00000000        channels reg: 0x00000000
int_cause_asic_mask: 0x00000010 int_cause_error_mask: 0x00000020
int_cause_link_error_mask: 0x00000040
crc_errors: 0    sync_errors: 0    reframe_events: 0

```

device PSE instance 1 is not detected on node 201/

Table 47 describes the significant fields shown in the display.

Table 47 *show controllers cpuctrl ports Field Descriptions*

Field	Description
client name	Identifies the client whose port CPU controller information is displayed.
device instance	The client's device instance for which the port CPU controller information is displayed.
cpuctrl net port	Identifies the CPU controller net port.
pci base	PCI ¹ base.
map reg	Client map register.
OS interrupt level	Level of Cisco IOS XR interrupt configured for the port. Interrupts are triggered by arrival of a packet that causes the CPU to postpone other tasks and handle the packet.
Cpuctrl interrupt level	Level of CPU controller interrupt configured for the port.
OS Run priority	Cisco IOS XR priority.
config reg	Configuration register, expressed in hexadecimal format.
channels reg	Channel register, expressed in hexadecimal format.
int_cause_asic_mask	Internal ASIC masking information.
int_cause_error_mask	Internal error masking information.
int_cause_link_error_mask	Internal link error masking information.
crc_errors	Number of CRC ² errors that have occurred on this port.
sync_errors	Number of synchronization errors that have occurred on this port.
reframe_events	Number of reframe events that have occurred on this port.

1. Peripheral Component Interconnect

2. cyclic redundancy check

Related Commands

Command	Description
show controllers cpuctrl summary	Displays summarized information about all CPU controller ASICs on the router or on a specific node.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers cpuctrl summary

To display summarized information about all CPU controller ASICs on the router or on a specific node, use the **show controllers cpuctrl summary** command in EXEC mode.

show controllers cpuctrl summary [**location** *node-id*]

Syntax Description

location <i>node-id</i>	(Optional) Identifies the location of the node whose CPU controller ASIC information you want to display. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	No modification.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
drivers	read

Examples

The following example shows how to display summarized information about all CPU controller ASICs on a specific node:

```
RP/0/RP0/CPU0:router# show controllers cpuctrl summary location 0/0/CPU0
```

```
Cpuctrl discovered 11 device on node 0/0/CPU0:
```

```
Cpuctrl HW version string for this node is:  
Squid FPGA v2.07 Fri Jan 23 16:21:01 2004 ykoren
```

```
-----  
device_name:          Fabricq      device instance:      0
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

Cpuctrl net port:      3          pci_base:      0x8c000000

-----

device_name:      Fabricq      device instance:      1
Cpuctrl net port:      4          pci_base:      0x90000000

-----

device_name:      Ingressq      device instance:      0
Cpuctrl net port:      8          pci_base:      0xa0000000

-----

device_name:      Egressq      device instance:      0
Cpuctrl net port:      7          pci_base:      0x9c000000

-----

device_name:      FIA          device instance:      0
Cpuctrl net port:      1          pci_base:      0x84000000

-----

device_name:      FIA          device instance:      1
Cpuctrl net port:      2          pci_base:      0x88000000

-----

device_name:      Cpuctrl      device instance:      0
Cpuctrl net port:      0          pci_base:      0x80000000

-----

device_name:      PSE          device instance:      1
Cpuctrl net port:      6          pci_base:      0x98000000

--More--

```

Table 48 describes the significant fields shown in the display.

Table 48 *show controllers cpuctrl summary Field Descriptions*

Field	Description
device_name	Identifies the device whose CPU controller information is displayed.
device instance	Identifies the CPU device whose information is displayed. Can be 0 or 1.
Cpuctrl net port	Identifies the CPU controller network port.
pci_base	PCI ¹ base, in hexadecimal format.

1. Peripheral Component Interconnect

Related Commands

Command	Description
show controllers cpuctrl cdma	Displays information about the CPU controller CDMA engine.
show controllers cpuctrl clients	Displays information about all CPU controller clients on the router, or for specific CPU controller clients.
show controllers cpuctrl devices	Displays information about the CPU controller devices on the router.

R3.5.0 Beta Draft—Cisco Confidential Information

Command	Description
<code>show controllers cpuctrl internal</code>	Displays information about the internal CPU controller.
<code>show controllers cpuctrl ports</code>	Displays port information for the specified CPU controller ASIC.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers egressq eio links

To display Elastic I/O (EIO) information for the egress queueing ASIC, use the **show controllers egressq eio links** command in EXEC mode.

show controllers egressq eio links *{link-id | all}* **location** *node-id*

Syntax Description

<i>link-id</i>	Identifies the EIO link whose egress queueing ASIC information you want to display. Replace <i>link-id</i> with a link identifier. Range is from 0 through 4294967295.
all	Displays egress queueing ASIC information for all links on the specified node.
location <i>node-id</i>	Identifies the location of the egress queue manager whose EIO link information you want to display. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
interface	read
drivers	read

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to display information for all EIO links on a node's egress queueing ASIC:

```
RP/0/RP0/CPU0:router# show controllers egressq eio links all location 0/2/CPU0
```

```
Node: 0/2/CPU0:
```

```
EIO links:
```

```
-----
ASIC Id      Peer Id      Type Link-Id Attempts Accept Failed State
-----
EGRESSQ_0    PSE_1        RX   11         1         1         0     EIO_LINK_TRAINED
EGRESSQ_0    PSE_1        TX   64         0         0         0     EIO_LINK_TRAINED
EGRESSQ_0    PLIM-ASIC_0  TX   60         0         0         0     EIO_LINK_TRAINED
EGRESSQ_0    PLIM-ASIC_1  TX   61         0         0         0     EIO_ADD_LINK
EGRESSQ_0    PLIM-ASIC_2  TX   62         0         0         0     EIO_ADD_LINK
EGRESSQ_0    PLIM-ASIC_3  TX   63         0         0         0     EIO_ADD_LINK
-----
```

Table 49 describes the significant fields shown in the display.

Table 49 *show controllers egressq eio links Field Descriptions*

Field	Description
ASIC Id	Identifies the ASIC that is associated with the link whose information is displayed.
Peer Id	Identifies the ASIC peer.
Type	Indicates whether the AISC is receiving (RX) or transmitting (TX).
Link-Id	Link identifier.
Attempts	Number of attempts made to send or receive information on the specified link.
Accept	Number of consecutive EIO requests for the link made by the PSE driver to the peer that were accepted.
Failed	Number of consecutive EIO requests for the link that failed.
State	Current link state.

Related Commands

Command	Description
show controllers egressq group	Displays information for about egress queue groups.
show controllers egressq interface	Displays information about interfaces associated with an egress queue.
show controllers egressq port	Displays egress queue information for a port, or for several ports.
show controllers egressq queue	Displays information about a specific egress queue, or a range of egress queues.
show controllers egressq statistics	Displays egress queue manager statistics.
show controllers ingressq statistics	Displays ingress queue manager statistics.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers egressq group

To display information about egress queue groups, use the **show controllers egressq group** command in EXEC mode.

show controllers egressq group {*group1* [*group2*] | **all** | **limits** {**max** | **min**}} **location** *node-id*

Syntax Description

<i>group1</i>	First group whose information you want to display.
<i>group2</i>	(Optional) Last group whose information you want to display.
all	Indicates that you want to display information about all egress queue groups on a specific node.
limits	Indicates that you want to display the limits table. Follow the keyword with max to display the maximum limits table, or min to display the minimum limits table.
max	Display the maximum limits table.
min	Display the minimum limits table.
location <i>node-id</i>	Identifies the location of the egress queue whose group information you want to display.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If you do not specify a group number for the *group2* argument, information is displayed only for the egress queue you specified for the *group1* argument. If you specify *group1* and *group2*, information is displayed for all groups within the range from *group1* through *group2*.

Task ID

Task ID	Operations
interface	read
drivers	read

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to display information for a specific range of egress queue groups on the CPU node in slot 2:

```
RP/0/RP0/CPU0:router# show controllers egressq group 1 3 location 0/2/CPU0
```

```
-----
                        Group 1
-----
Port                   : 0
Priority                : Low
Max LB Tokens          : 7812
Max LB Limit Index     : 38
Min LB Tokens          : 0
Min LB Limit Index     : 0
Quantum                : 27
Default Queue          : 1
High Priority Queue     : N/A
Low Priority Queue      : 1
-----

                        Group 2
-----
Port                   : 1
Priority                : Low
Max LB Tokens          : 7812
Max LB Limit Index     : 38
Min LB Tokens          : 0
Min LB Limit Index     : 0
Quantum                : 27
Default Queue          : 2
High Priority Queue     : N/A
Low Priority Queue      : 2
-----

                        Group 3
-----
Port                   : 256
Priority                : Low
Max LB Tokens          : 7812
Max LB Limit Index     : 38
Min LB Tokens          : 0
Min LB Limit Index     : 0
Quantum                : 27
Default Queue          : 3
High Priority Queue     : N/A
Low Priority Queue      : 3
-----
```

Table 50 describes the significant fields shown in the display.

Table 50 *show controllers egressq group Field Descriptions*

Field	Description
Port	Port identifier.
Priority	Group priority.
Max LB Tokens	Maximum number of port LB tokens.
Max LB Limit Index	Maximum LB limit.
Min LB Tokens	Minimum number of port LB tokens.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 50** *show controllers egressq group Field Descriptions (continued)*

Field	Description
Min LB Limit Index	Minimum LB limit.
Quantum	Quantum value for this group.
Default Queue	Default queue for this group.
High Priority Queue	High priority queue identifier.
Low Priority Queue	Low priority queue identifier.

Related Commands

Command	Description
show controllers egressq eio links	Displays EIO information for the egress queueing ASIC.
show controllers egressq interface	Displays information about interfaces associated with an egress queue.
show controllers egressq port	Displays egress queue information for a port, or for several ports.
show controllers egressq queue	Displays information about a specific egress queue, or a range of egress queues.
show controllers egressq statistics	Displays egress queue manager statistics.
show controllers ingressq statistics	Displays ingress queue manager statistics.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers egressq interface

To display information about interfaces associated with an egress queue, use the **show controllers egressq interface** command in EXEC mode.

```
show controllers egressq interface [Bundle-Ether bundle-id | Bundle-POS bundle-id |
GigabitEthernet interface_instance | Loopback interface | MgmtEth interface_instance |
Null 0 | POS interface_instance | all] location location
```

Syntax Description		
Bundle-Ether <i>bundle-id</i>		Identifies the aggregated Ethernet interfaces whose egress queue information you want to display. Replace <i>bundle-id</i> with the bundle identifier. Range is from 1 through 65535.
Bundle-POS <i>bundle-id</i>		Identifies the aggregated POS interfaces whose egress queue information you want to display. Replace <i>bundle-id</i> with the bundle identifier. Range is from 1 through 65535.
GigabitEthernet <i>interface_instance</i>		Identifies the Gigabit Ethernet or IEEE 802.3 interfaces whose egress queue information you want to display.
Loopback <i>interface</i>		Identifies the loopback interfaces whose egress queue information you want to display. Replace <i>interface</i> with the loopback interface identifier. Range is from 1 through 65535.
MgmtEth <i>interface_instance</i>		Identifies the Ethernet or IEEE 802.3 interfaces whose egress queue information you want to display.
Null 0		Identifies the Null interface.
POS <i>interface_instance</i>		Identifies the POS interfaces whose egress queue information you want to display.
all		Indicates that you want to display egress queue information for all interfaces in the specified location .
location <i>location</i>		Identifies the location of the interface whose egress queue information you want to display.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
interface	read
drivers	read

Examples

The following example shows how to display egress queue information for all configured interfaces on the router:

```
RP/0/RP0/CPU0:router# show controllers egressq interface all
```

```
/CPU0
-----
Interface POS0/0/0/15
-----
Port 776
-----
Max LB Tokens      : 18720
Max LB Limit Index : 41
Quantum            : 27
Default Group      : 24
High Priority Group : N/A
Low Priority Group  : 24
-----
Interface POS0/0/0/14
-----
Port 780
-----
Max LB Tokens      : 18720
Max LB Limit Index : 41
Quantum            : 27
Default Group      : 23
High Priority Group : N/A
Low Priority Group  : 23
-----
Interface POS0/0/0/13
-----
Port 778
-----
Max LB Tokens      : 18720
Max LB Limit Index : 41
Quantum            : 27
Default Group      : 22
High Priority Group : N/A
Low Priority Group  : 22
-----
Interface POS0/0/0/12
-----
Port 782
-----
Max LB Tokens      : 18720
Max LB Limit Index : 41
```

R3.5.0 Beta Draft—Cisco Confidential Information

```
Quantum          : 27
Default Group    : 21
High Priority Group : N/A
Low Priority Group : 21
```

```
-----
Interface POS0/0/0/11
```

```
-----
Port 520
```

```
-----
Max LB Tokens      : 18720
Max LB Limit Index : 41
Quantum            : 27
Default Group      : 20
High Priority Group : N/A
Low Priority Group  : 20
```

```
-----
Interface POS0/0/0/10
```

```
-----
Port 524
```

```
-----
Max LB Tokens      : 18720
Max LB Limit Index : 41
Quantum            : 27
Default Group      : 19
High Priority Group : N/A
Low Priority Group  : 19
```

```
-----
Interface POS0/0/0/9
```

```
-----
Port 522
```

```
-----
Max LB Tokens      : 18720
Max LB Limit Index : 41
Quantum            : 27
Default Group      : 18
High Priority Group : N/A
Low Priority Group  : 18
```

```
-----
Interface POS0/0/0/8
```

```
-----
Port 526
```

```
-----
Max LB Tokens      : 18720
Max LB Limit Index : 41
Quantum            : 27
Default Group      : 17
High Priority Group : N/A
Low Priority Group  : 17
```

Table 51 describes the significant fields shown in the display.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 51** *show controllers egressq interface Field Descriptions*

Field	Description
Interface	Interface identifier, in the <type>rack/slot/module/port format.
Port	Port to which the specified interface belongs.
Max LB Tokens	Maximum number of port LB tokens.
Max LB Limit Index	Maximum LB limit.
Quantum	Quantum value for this interface.
Default Group	Default group.
High Priority Group	High priority group identifier.
Low Priority Group	Low priority group identifier.

Related Commands

Command	Description
show controllers egressq eio links	Displays EIO information for the egress queueing ASIC.
show controllers egressq group	Displays information for about egress queue groups.
show controllers egressq port	Displays egress queue information for a port, or for several ports.
show controllers egressq queue	Displays information about a specific egress queue, or a range of egress queues.
show controllers egressq statistics	Displays egress queue manager statistics.
show controllers ingressq statistics	Displays ingress queue manager statistics.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers egressq port

To display egress queue information for a port, or for several ports, use the **show controllers egressq port** command in EXEC mode.

show controllers egressq port {*port1* [*port2*] | **all** | **limits max**] **location** *node-id*

Syntax Description	<i>port1</i>	Identifies the port whose egress queue information you want to display. Replace <i>port1</i> with a port identifier. Range is from 1 through 1023.
	<i>port2</i>	Identifies the last port whose egress queue information you want to display. Replace <i>port2</i> with a port identifier. Range is from 1 through 1023.
	all	Indicates that you want to display egress queue information for all ports on the node in the specified location.
	limits max	Indicates that you want to display the maximum limits table.
	location <i>node-id</i>	Identifies the location of the egress queue whose group information you want to display. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	interface	read
	drivers	read

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to display egress queue information for ports 1, 2, and 3 on the CPU node in slot 2:

```
RP/0/RP0/CPU0:router# show controllers egressq port 1 3 location 0/2/CPU0
```

```
-----
                        Port 1
-----
Max LB Tokens           : 7812
Max LB Limit Index      : 38
Quantum                 : 27
Default Group           : 2
High Priority Group      : N/A
Low Priority Group       : 2
-----

-----
                        Port 2
-----
Port is not allocated
-----

                        Port 3
-----
Port is not allocated
```

Table 52 describes the significant fields shown in the display.

Table 52 *show controllers egressq port Field Descriptions*

Field	Description
Port	Port identifier.
Max LB Tokens	Maximum number of port LB tokens.
Max LB Limit Index	Maximum LB limit.
Quantum	Quantum value for this interface.
Default Group	Default group.
High Priority Group	High priority group identifier.
Low Priority Group	Low priority group identifier.

Related Commands

Command	Description
show controllers egressq eio links	Displays EIO information for the egress queueing ASIC.
show controllers egressq group	Displays information for about egress queue groups.
show controllers egressq interface	Displays information about interfaces associated with an egress queue.
show controllers egressq queue	Displays information about a specific egress queue, or a range of egress queues.
show controllers egressq statistics	Displays egress queue manager statistics.
show controllers ingressq statistics	Displays ingress queue manager statistics.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers egressq queue

To display information about a specific egress queue, or a range of egress queues, use the **show controllers egressq queue** command in EXEC mode.

```
show controllers egressq queue {queue1 [queue2] | context [max_elements] | all | limits}
location node-id
```

Syntax Description		
<i>queue1</i>		Identifies the first port whose egress queue information you want to display. Replace <i>queue1</i> with a queue identifier. Range is from 1 through 8191.
<i>queue2</i>		(Optional) Identifies the last port whose egress queue information you want to display. Replace <i>queue2</i> with a queue identifier. Range is from 1 through 8191.
context		Specifies the context in which to display the information.
<i>max_elements</i>		(Optional) Maximum number of queue elements to show. Replace <i>max_elements</i> with a maximum number of elements. Range is from 1 through 4096000.
all		Indicates that you want to display egress queue information for all ports on the node in the specified location.
limits		Indicates that you want to display the limits table. Follow the limits keyword with max to display the maximum limits table, or min to display the minimum limits table.
max		Display the maximum limits table.
min		Display the minimum limits table.
location <i>node-id</i>		Identifies the location of the egress queue whose egress queue information you want to display. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	interface	read
	drivers	read

Examples

The following example shows how to display information about egress queues 1 and 2 on the CPU node in slot 2:

```
RP/0/RP0/CPU0:router# show controllers egressq queue 1 2 location 0/2/CPU0
```

```
-----
                        Queue 1
-----
Group                  : 1
Priority                : Low
Max LB Tokens          : 7812
Max LB Limit Index     : 38
Min LB Tokens          : 0
Min LB Limit Index     : 0
Quantum                : 27
Instantaneous length   : 0
Length high watermark  : 0
-----
                        Queue 2
-----
Group                  : 2
Priority                : Low
Max LB Tokens          : 7812
Max LB Limit Index     : 38
Min LB Tokens          : 0
Min LB Limit Index     : 0
Quantum                : 27
Instantaneous length   : 0
Length high watermark  : 0
-----
```

Table 53 describes the significant fields shown in the display.

Table 53 *show controllers egressq queue Field Descriptions*

Field	Description
Group	Group identifier.
Priority	Group priority.
Max LB Tokens	Maximum number of port LB tokens.
Max LB Limit Index	Maximum LB limit.
Min LB Tokens	Minimum number of port LB tokens.
Min LB Limit Index	Minimum LB limit.
Quantum	Quantum value for this queue.
Instantaneous length	Egress queue instantaneous length.
Length high watermark	Length high watermark register.

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	<code>show controllers egressq eio links</code>	Displays EIO information for the egress queueing ASIC.
	<code>show controllers egressq group</code>	Displays information for about egress queue groups.
	<code>show controllers egressq interface</code>	Displays information about interfaces associated with an egress queue.
	<code>show controllers egressq port</code>	Displays egress queue information for a port, or for several ports.
	<code>show controllers egressq statistics</code>	Displays egress queue manager statistics.
	<code>show controllers ingressq statistics</code>	Displays ingress queue manager statistics.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers egressq statistics

To display egress queue manager statistics, use the **show controllers egressq statistics** command in EXEC mode.

show controllers egressq statistics location *node-id*

Syntax Description

location <i>node-id</i>	Identifies the location of the egress queue whose statistics you want to display. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
interface	read
drivers	read

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to display egress queue manager statistics:

```
RP/0/RP0/CPU0:router# show controllers egressq statistics location 0/2/CPU0
```

```
-----
Egressq Statistics
-----
egressq ASIC version: 1
egressq ASIC state: Normal
plimasic link0 output packets: 0
plimasic link0 output bytes: 0
plimasic link1 output packets: 0
plimasic link1 output bytes: 0
plimasic link2 output packets: 0
plimasic link2 output bytes: 0
plimasic link3 output packets: 0
plimasic link3 output bytes: 0
cpuctrl input packets: 0
cpuctrl output bytes: 1433250
pse input packets: 29250
pse dropped packets: 0
cpuctrl dropped packets: 0
-----
```

Table 54 describes the significant fields shown in the display.

Table 54 *show controllers egressq statistics Field Descriptions*

Field	Description
egressq ASIC version	Version identifier for the egress queue ASIC.
egressq ASIC state	Current state of the egress queue ASIC.
plimasic link0 output packets	Number of output packets on link 0 of the ASIC.
plimasic link0 output bytes	Output bytes on link 0 of the ASIC.
plimasic link1 output packets	Number of output packets on link 1 of the ASIC.
plimasic link1 output bytes	Number of output packets on link 1 of the ASIC.
plimasic link2 output packets	Number of output packets on link 2 of the ASIC.
plimasic link2 output bytes	Number of output packets on link 2 of the ASIC.
plimasic link3 output packets	Number of output packets on link 3 of the ASIC.
plimasic link3 output bytes	Number of output packets on link 3 of the ASIC.
cpuctrl input packets	Number of CPU controller input packets received on this ASIC.
cpuctrl output bytes	CPU controller output bytes transmitted on this ASIC.
pse input packets	Number of PSE input packets received on this ASIC.
pse dropped packets	Number of PSE packets that were dropped by this ASIC due to errors.
cpuctrl dropped packets	Number of CPU controller packets that were dropped by this ASIC due to errors.

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show controllers egressq eio links	Displays EIO information for the egress queueing ASIC.
	show controllers egressq group	Displays information for about egress queue groups.
	show controllers egressq interface	Displays information about interfaces associated with an egress queue.
	show controllers egressq port	Displays egress queue information for a port, or for several ports.
	show controllers egressq queue	Displays information about a specific egress queue, or a range of egress queues.
	show controllers ingressq statistics	Displays ingress queue manager statistics.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers ingressq statistics

To display ingress queue manager statistics, use the **show controllers ingressq statistics** command in EXEC mode.

show controllers ingressq statistics location *node-id*

Syntax Description

location *node-id*

Identifies the location of the ingress queue whose statistics you want to display. The *node-id* is expressed in the *rack/slot/module* notation.

Note Use the **show platform** command to see the location of all nodes installed in the router.

Defaults

No default behavior or values

Command Modes

EXEC

Command History**Release****Modification**

Release 3.2

This command was introduced on the Cisco CRS-1.

Release 3.3.0

No modification.

Release 3.4.0

No modification.

Release 3.5.0

No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

**Note**

In the **show controllers ingressq statistics** command display, the *rx pkts* counter field may wrap if it is calculating line rate traffic.

Task ID**Task ID****Operations**

interface

read

drivers

read

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to display ingress queue manager statistics:

```
RP/0/RP0/CPU0:router# show controllers ingressq statistics location 0/2/CPU0
```

Ingressq Rx Statistics.

```
-----
rx pkts                :          131827 (          33509182 bytes)
rx pkts from cpu       :          102509 (          16422606 bytes)
rx control pkts from cpu :          102509 (          16422606 bytes)
rx data pkts from cpu   :              0 (              0 bytes)
```

Ingressq Tx Statistics.

```
-----
tx pkts                :          131826 (          35086366 bytes)
tx pkts to cpu         :           29318 (          17086576 bytes)
tx control pkts to cpu :           29318 (          17086576 bytes)
tx data pkts to cpu    :              0 (              0 bytes)
tx pkts shaped         :          102508 (          17999790 bytes)
tx cells to fabric     :           223190
```

Ingressq Drops.

```
-----
length error drops - PSE      :          0
length error drops - Cpuctrl  :          0
crc error drops - PSE        :          0
crc error drops - Cpuctrl    :          0
OOR error drops - PSE        :          0
OOR error drops - Cpuctrl    :          0
discard drops              :          0
tail drops                 :          0
tail drops - no QE         :          0
cell drops                  :          0
```

Related Commands

Command	Description
show controllers egressq eio links	Displays EIO information for the egress queueing ASIC.
show controllers egressq group	Displays information for about egress queue groups.
show controllers egressq interface	Displays information about interfaces associated with an egress queue.
show controllers egressq port	Displays egress queue information for a port, or for several ports.
show controllers egressq queue	Displays information about a specific egress queue, or a range of egress queues.
show controllers egressq statistics	Displays egress queue manager statistics.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers plim asic

To display physical layer interface module (PLIM) ASIC information for a specific node or interface, use the **show controllers plim asic** command in EXEC mode.

Use the following syntax on a Cisco CRS-1:

```
show controllers plim asic {statistics {interface {POS interface_instance |
TenGigE interface_instance} summary} | summary} [location node-id]
```

Use the following syntax on a Cisco XR 12000 Series Router:

```
show controllers plim asic {rx-channel bay {0 | 1} channel channel_number | spa {0 | 1} |
tx-channel bay {0 | 1} channel channel_number} [location node-id]
```

Syntax Description		
statistics		Displays PLIM ASIC statistics for a specific interface, or summarized statistics information for all PLIM ASICs on a specific node.
interface POS <i>interface_instance</i>		Displays statistical information for POS interfaces only. The <i>interface</i> argument is expressed in the <i>rack/slot/module/port</i> notation. Note Use the show interfaces command in EXEC mode to see a list of all interfaces the router.
interface TenGigE <i>interface_instance</i>		Displays statistical information for TenGigE interfaces only. The <i>interface</i> argument is expressed in the <i>rack/slot/module/port</i> notation. Note Use the show interfaces command in EXEC mode to see a list of all interfaces the router.
summary		Displays a summarized information for PLIM ASICs on a specified node, or for all interfaces on the router.
location node-id		Identifies the location of the node whose PLIM ASIC information you want to display. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation. Note Use the show platform command to see the location of all nodes installed in the router.
rx-channel bay {0 1}		Displays statistical information for the SPI4.2 receive channel that is specified with the channel channel_number argument. Use 0 to indicate the bottom bay, or 1 to indicate the top bay.
spa {0 1}		Displays statistical information for the SPA that is specified with the channel channel argument. Use 0 to indicate the bottom bay, or 1 to indicate the top bay.
tx-channel bay {0 1}		Displays statistical information for the SPI4.2 transmit channel. Use 0 to indicate the bottom bay, or 1 to indicate the top bay.
channel channel_number		Identifies the channel whose statistics you want to display. Replace <i>channel_number</i> with the number of the channel whose statistics you want to display. Range is from 1 through 255.

Defaults

No default behavior or values

R3.5.0 Beta Draft—Cisco Confidential Information

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

To display statistics for a specific PLIM ASIC on a Cisco CRS-1, include the **interface interface** option in the command, as shown in the following example:

```
show controllers plim asic statistics interface interface
```

To display summarized statistics information for all PLIM ASICs on a specific node in a Cisco CRS-1, include the **summary** option in the command, as shown in the following example:

```
show controllers plim asic statistics summary
```

To display summarized PLIM ASIC port information on a Cisco CRS-1, use the **show controllers plim asic summary location node-id** command.

To display a summary of PLIM ASIC statistics on a Cisco CRS-1, use the **show controllers plim asic statistics summary location node-id** command.

Task ID	Task ID	Operations
	interface	read
	root-system	read

Examples The following example shows how to display PLIM ASIC statistics information for a POS interface on a Cisco CRS-1:

```
RP/0/RP0/CPU0router# show controllers plim asic statistics interface POS 0/2/0/0
```

```
Node: 0/2/CPU0
```

```
-----
POS0/2/0/0 Tx Statistics
-----
```

TotalOctets	: 78904040	TotalPkts	: 1622308
UnicastPkts	: 1622308	MulticastPkts	: 0
BroadcastPkts	: 0	<64Octets	: 1610433
64Octets	: 0	65to127Octets	: 11875
128to255Octets	: 0	256to511Octets	: 0
512to1023Octets	: 0	1024to1518Octets	: 0
1519to1548Octets	: 0	1549to9216Octets	: 0

R3.5.0 Beta Draft—Cisco Confidential Information

```

>9216Octet      : 0          BadCRCPkts      : 0
802.1QPkts      : 0          Underrun       : 0
Runt            : 0          Giant           : 0
PausePkts       : 0          Jabbers         : 0
DeferralAbort   : 0          LateCollision    : 0
CollisionAbort  : 0          OneCollision     : 0
MultiCollision  : 0          TotalCollisions : 0
TotalDefer      : 0          LateCollisionAbort: 0
LengthAbort     : 0          TxBP count      : 0

POS0/2/0/0 Rx Statistics
-----
--More-- failed to get stats
TotalOctets     : 91010808
TotalPkts       : 1815571    UnicastPkts    : 1815571
MulticastPkts   : 0          BroadcastPkts   : 0
64Octets        : 63846     65to127Octets : 11844
128to255Octets  : 7         256to511Octets : 0
512to1023Octets : 0         1024to1518Octets : 0
1519to1548Octets : 0        1549to9216Octets : 0
>9216Octets     : 0          BadCRCPkts     : 0
BadCodedPkts    : 0          Runt           : 0
ShortPkts       : 1739874   802.1QPkts    : 0
Drop            : 0          PausePkts      : 0
ControlPkts     : 0          Jabbers        : 0
BadPreamble     : 0

POS0/2/0/0 Drop
-----
RxFIFO Drop     : 0          PAR Tail Drop  : 0
TxFIFO Drop     : 0

```

Table 55 describes the significant fields shown in the display.

Table 55 *show controllers plim asic Field Descriptions*

Field	Description
TotalOctets	Number of octets received or transmitted on the interface.
TotalPkts	Number of Total packets received or transmitted on the interface.
UnicastPkts	Number of unicast packets received or transmitted on the interface.
MulticastPkts	Number of multicast packets received or transmitted on the interface. Received packets were directed to the multicast address.
BroadcastPkts	Number of good broadcast packets received or transmitted. Received packets were directed to the broadcast address.
64Octets	Number of packets (including bad packets) received or transmitted that were less than 64 octets in length (excluding framing bits but including FCS octets).
64Octets	Number of packets (including bad packets) received or transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65to127Octets	Number of packets (including bad packets) received or transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

R3.5.0 Beta Draft—Cisco Confidential Information**Table 55** *show controllers plim asic Field Descriptions (continued)*

Field	Description
128to255Octets	Number of packets (including bad packets) received or transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256to511Octets	Number of packets (including bad packets) received or transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512to1023Octets	Number of packets (including bad packets) received or transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024to1518Octets	Number of packets (including bad packets) received or transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
1519to1548Octets	Number of packets (including bad packets) received or transmitted that were between 1519 and 1548 octets in length inclusive (excluding framing bits but including FCS octets).
1549to9216Octets	Number of packets (including bad packets) received or transmitted that were between 1549 and 9216 octets in length inclusive (excluding framing bits but including FCS octets).
>9216Octet	Number of packets (including bad packets) received or transmitted that were greater than 9216 octets in length (excluding framing bits but including FCS octets).
BadCRCPkts	Number of packets received or transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS error) or a bad FCS with a nonintegral number of octets (alignment error).
802.1QPkts	Number of 802.1QPkts received or transmitted on the interface.
Underrun	Number of packets that were not retrieved quickly enough from shared memory to be transmitted/received.
Runt	Number of packets received or transmitted that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Giant	Number of packets received or transmitted that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
PausePkts	Number of pause packets transmitted/received on the interface. Pause packets that tell remote devices to delay sending more packets for a specified period of time.
Jabbers	Number of packets received or transmitted that were longer than 1518 octets (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS error) or a bad FCS with a nonintegral number of octets (assigned error).
DeferralAbort	Number of deferral aborts that occurred on this segment.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 55** *show controllers plim asic Field Descriptions (continued)*

Field	Description
LateCollision	Number of late collisions on this segment
CollisionAbort	Number of collisions that were aborted.
OneCollision	Number of single collisions that occurred on this segment.
MultiCollision	Number multiple collisions that occurred on this segment.
TotalCollisions	Number of collisions on this segment.
TotalDefer	Number of deferrals on this segment.
LateCollisionAbort	Number of late collision aborts that occurred on this segment.
LengthAbort	Number of length aborts that occurred on this segment.
TxBP count	Number of transmit BP on this segment.
Rx Statistics	Indicates the statistics that follow were received by the interface.
TX statistics	Indicates the statistics that follow were transmitted by the interface.
RxFIFO Drop	Displays the receive FIFO drop information.
PAR Tail Drop	Displays PAR tail drop information.
TxFIFO Drop	Displays transmitted FIFO drop information.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers pse eio links

To display packet switching engine (PSE) information for Elastic I/O (EIO) links, use the **show controllers pse eio links** command in EXEC mode.

show controllers pse eio links [*link_number* | **all**] [**location** *node-id*]

Syntax Description

links <i>link_number</i>	Displays PSE information for the specified link. Replace <i>link_number</i> with a link number in the range from 1 through 4294967295. Note Use the show controllers pse eio links all location node-id command to display all available EIO link IDs on a node.
links all	Displays PSE information for all links on the specified node.
location <i>node-id</i>	(Optional) Displays all EIO links on a specific node only. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation. Note Use the show platform command to see the location of all nodes installed in the router.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	No modification.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
interface	read
drivers	read

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following is sample output from the **show controllers pse eio links** command for a specific EIO link:

```
RP/0/RP0/CPU0:router# show controllers pse eio links 50 location 0/0/CPU0

Node: 0/0/CPU0:
-----

EIO link: 50
-----
ASIC Id      Peer Id      Type Link-Id Attempts Accept Failed State
-----
PSE_1        FABRICQ_0    RX   50         1         1         0     EIO_LINK_TRAINED
-----
Macro-id Windage Diag status
-----
0           4           0x0000
1           4           0x0000
2           4           0x0000
3           4           0x0000
-----
```

Table 56 describes the significant fields shown in the display.

Table 56 *show controllers pse eio links Field Descriptions*

Field	Description
Node	Node whose PSE information is displayed.
EIO link	EIO link whose information is displayed.
ASIC Id	ASIC associated with this EIO link.
Peer Id	ASIC of the remote peer of this EIO link.
Type	Indicates whether this link is receiving or transmitting (re)training requests.
Link-Id	Unique ID assigned by the system to the EIO link.
Attempts	Number of consecutive EIO training requests for the link made by the PSE driver to the peer. Note Typically, the PSE driver at the receive end of a link initiates the training of that EIO link. Therefore, the EIO links whose PSE driver is at the transmit end show a value of 0 for the <i>Attempts</i> field, even though those links are in the EIO_LINK_TRAINED state.
Accept	Number of PSE driver requests for training that were accepted by the peer. When a PSE driver request is accepted, training is started. Note Typically, the PSE driver at the receive end of a link initiates the training of that EIO link. Therefore, the EIO links whose PSE driver is at the transmit end show a value of 0 for the <i>Accept</i> field, even though those links are in the EIO_LINK_TRAINED state.
Failed	Number of times the training for this link failed for any reason.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 56** *show controllers pse eio links Field Descriptions (continued)*

Field	Description
State	Current state of the EIO link.
Macro-id Windage Diag status	Windage value used for the training, and the final status of the training for that windage. Note The Macro-id Windage Diag status field is displayed only when you ask EIO info for specific link.

Related Commands

show controllers pse ipc	Displays PSE device information for IP connections, or for a specific IPC controller.
show controllers pse mp	Displays PSE information for the maintenance processor on a specific controller or node.
show controllers pse statistics	Displays PSE statistics for a specific controller instance, or for a specific node.
show controllers pse summary	Displays a summary of PSE information for a specific controller or node.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers pse ipc

To display packet switching engine (PSE) device information for interprocess communication (IPC) connections, or for a specific IPC controller, use the **show controllers pse ipc** command in EXEC mode.

show controllers pse ipc {**client-connection** {*connID* | **all**} | **cpuctrlif**} [**instance** {**0** | **1**}]
[**location** *node-id*]

Syntax Description		
client-connection <i>connID</i>		Displays IPC information about the specified client connection. Replace <i>connID</i> with the client connection ID. Range is from 1 through 255.
client-connection all		Displays IPC information about the all client connection.
cpuctrlif		Displays IPC information about the specified PSE IPC CPU controller instance.
instance { 0 1 }		(Optional) Identifies the PSE device whose information you want to display. Enter 0 to specify the ingress PSE device, or 1 to specify the egress PSE device. Note Follow the instance { 0 1 } argument with the location node-id argument to restrict the command to a specific node containing the specified device instance.
location <i>node-id</i>		(Optional) Identifies the location of the node whose PSE device information you want to display. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation. Note Use the show platform command to see the location of all nodes installed in the router. Note Include the instance { 0 1 } argument before the location node-id argument to restrict the command to a specific device instance on the specified node.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	No modification.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

To display client connection IPC information for a specific device instance, include the **instance** {0 | 1} argument with the command, as shown in the following example:

```
show controllers pse ipc client-connection connId instance instance
```

To display client connection IPC information for a specific node location, include the **location** node-id argument with the command, as shown in the following example:

```
show controllers pse ipc client-connection connId location node-id
```

Task ID

Task ID	Operations
interface	read
drivers	read

Examples

The following command shows how to display PSE information for a specific IPC client-connection:

```
RP/0/RP0/CPU0:router# show controllers pse ipc client-connection 13
```

```
Node: 0/0/CPU0:
```

```
PSE IPC Conn Info:
```

```
-----
ConnId:      13 (Backdoor)
ConnOptions: 0
Clnfos:      0x482bf9f8 (Notif) 0 (Reply)
ConnStateFlags: 0
ConnNotifFlags: 0
SendReqs:    0 (iHP) 4 (iNP) 0 (eHP) 0 (eNP)
SendFiltered: 0 (iHP) 0 (iNP) 0 (eHP) 0 (eNP)
SendFailed:  0 (iHP) 0 (iNP) 0 (eHP) 0 (eNP)
RecvReqs:    0
RecvReqTouts: 0
RecvDatTouts: 0
RecvQState:  0/16
```

```
Node: 0/3/CPU0:
```

```
PSE IPC Conn Info:
```

```
-----
ConnId:      13 (Backdoor)
ConnOptions: 0
Clnfos:      0x482bf9f8 (Notif) 0 (Reply)
ConnStateFlags: 0
ConnNotifFlags: 0
SendReqs:    0 (iHP) 4 (iNP) 0 (eHP) 0 (eNP)
SendFiltered: 0 (iHP) 0 (iNP) 0 (eHP) 0 (eNP)
SendFailed:  0 (iHP) 0 (iNP) 0 (eHP) 0 (eNP)
RecvReqs:    0
RecvReqTouts: 0
RecvDatTouts: 0
RecvQState:  0/16
```

R3.5.0 Beta Draft—Cisco Confidential Information

Table 57 describes the significant fields shown in the display.

Table 57 *show controllers pse ipc client-connection Field Descriptions*

Field	Description
ConnId	Connection identifier.
ConnOptions	Connection bind time options requested by the client creating this connection.
Clinfos	Client information (clinfo) index number. The memory database is organized as a table of clinfos, which are indexed by the region id and maintained in shared memory.
ConnStateFlags	Bitmask containing the current state of the connection.
ConnNotifFlags	Bitmask of the types of notifications that the client creating this connection has registered for.
SendReqs	Number of PSE IPC send requests that client has made on this connection.
SendFiltered	Number of send requests that were filtered out (dropped) from the PSE driver due to any internal filter policy.
SendFailed	Number of send requests that could not be handled by the PSE driver due to error conditions such as hardware I/O failures, lack of buffering space, and so forth.
RecvReqs	Number of data receive requests that the client has made on this connection.
RecvReqTouts	Number of data receive requests from the client that timed out because no data was received from PSE device.
RecvDatTouts	Number of times data was received from PSE device, but timed out because there was no receive request from client to pick up that data from the connection.
RecvQState	Current state of the internal data receive FIFO queue. The internal data receive FIFO queue buffers data arriving from the PSE device for the connection, until the client sends a receive request for that data. The RecvQState is expressed in the X/Y notation, where X is current depth of the queue, and Y is the maximum depth allowed for the queue.

The following command shows how to display PSE information for a specific IPC controller connection:

```
RP/0/RP0/CPU0:router# show controllers pse ipc cpuctrlif
```

```
Node: 0/0/CPU0:
```

```
-----
Pse IPC cpuctrl if Information
```

```
-----
Cpuctrl interface is up
```

```
Normal Priority Tx I/F:
```

```
BufBase 0x112190 BufSize 32768 PadBufp 0xec0af118 Seqnum 854
```

```
RORegNum 10 RORegVal 0x49f0 WOREgNum 2 WOREgVal 0x49f0
```

```
CDMACh 0 CDMAQ 3
```

```
HoldQ 0/512 CDMAPendQ 0/128 UnackQ 0/256
```

```
NumEnqs 854 NumRejs 0 NumDmaReqFails 0
```

```
NumDmaPendFails 0 NumMbxSpcFails 0 NumHldqOvflows 0
```

```
Normal Priority Rx I/F:
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

NumPDMAEntries 64 NumEnqs 15 NumRejs 0

Pse IPC cpuctrl if Information
-----
Cpuctrl interface is up
Normal Priority Tx I/F:
    BufBase 0x112190  BufSize 32768 PadBufp 0xec0af14c Seqnum 424
    RORegNum 10 RORegVal 0x1c60 WOREgNum 2 WOREgVal 0x1c60
    CDMACH 1 CDMAQ 3
    HoldQ 0/512 CDMAPendQ 0/128 UnackQ 0/256
    NumEnqs 424 NumRejs 0 NumDmaReqFails 0
    NumDmaPendFails 0 NumMbxSpcFails 0 NumHldqOvflows 0
Normal Priority Rx I/F:
    NumPDMAEntries 64 NumEnqs 2 NumRejs 0

Node: 0/3/CPU0:
-----

Pse IPC cpuctrl if Information
-----
Cpuctrl interface is up
Normal Priority Tx I/F:
    BufBase 0x112190  BufSize 32768 PadBufp 0xec0af118 Seqnum 833
    RORegNum 10 RORegVal 0xdb8 WOREgNum 2 WOREgVal 0xdb8
    CDMACH 0 CDMAQ 3
    HoldQ 0/512 CDMAPendQ 0/128 UnackQ 0/256
    NumEnqs 833 NumRejs 0 NumDmaReqFails 0
    NumDmaPendFails 0 NumMbxSpcFails 0 NumHldqOvflows 0
Normal Priority Rx I/F:
    NumPDMAEntries 64 NumEnqs 9 NumRejs 0

Pse IPC cpuctrl if Information
-----
Cpuctrl interface is up
Normal Priority Tx I/F:
    BufBase 0x112190  BufSize 32768 PadBufp 0xec0af14c Seqnum 409
    RORegNum 10 RORegVal 0x5f70 WOREgNum 2 WOREgVal 0x5f70
    CDMACH 1 CDMAQ 3
    HoldQ 0/512 CDMAPendQ 0/128 UnackQ 0/256
    NumEnqs 409 NumRejs 0 NumDmaReqFails 0
    NumDmaPendFails 0 NumMbxSpcFails 0 NumHldqOvflows 0
Normal Priority Rx I/F:
    NumPDMAEntries 64 NumEnqs 2 NumRejs 0

```

R3.5.0 Beta Draft—Cisco Confidential Information

Table 58 describes the significant fields shown in the display.

Table 58 *show controllers pse ipc cpuctrlif Field Descriptions*

Field	Description
Cpuctrl interface is up	Whether the connection is currently up or down.
Cpuctrl interface is down	
Normal Priority Tx I/F	Displays the following transmit buffer information for the connection: • BufBase • BufSize • PadBufp • Seqnum • RORegNum • RORegVal • WORegNum • WORegVal • CDMACH • CDMAQ • HoldQ • CDMAPendQ • UnackQ • NumEnqs • NumRejs • NumDmaReqFails • NumDmaPendFails • NumMbxSpcFails • NumHldqOvflows
Normal Priority Rx I/F:	Displays the following receive buffer information for the connection: • NumPDMAEntries • NumEnqs • NumRejs

Related Commands

show controllers pse eio links	Displays PSE information for EIO (Elastic I/O) links, or for a specific controller.
show controllers pse mp	Displays PSE information for the maintenance processor on a specific controller or node.
show controllers pse statistics	Displays PSE statistics for a specific controller instance, or for a specific node.
show controllers pse summary	Displays a summary of PSE information for a specific controller or node.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers pse mp

To display packet switching engine (PSE) information for the maintenance processor on a specific controller or node, use the **show controllers pse mp** command in EXEC mode.

show controllers pse mp [**egress** | **ingress**] [**location** *node-id*]

Syntax Description	egress	(Optional) Displays information for the egress PSE device only. Note Follow the egress argument with the location <i>node-id</i> argument to restrict the command to a specific node.
	ingress	(Optional) Displays information for the ingress PSE device only. Note Follow the ingress argument with the location <i>node-id</i> argument to restrict the command to a specific node.
	location <i>node-id</i>	(Optional) Identifies the location of the node whose PSE device information you want to display. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation. Note Use the show platform command to see the location of all nodes installed in the router. Note Include the instance {0 1} argument before the location <i>node-id</i> argument to restrict the command to a specific device instance on the specified node.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	No modification.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

R3.5.0 Beta Draft—Cisco Confidential Information

The **instance** and **location** optional keywords are not mutually exclusive. The **instance** keyword directs the command to a specific PSE device, and the **location** keyword directs the command to that device or devices on the specified modular services card. You can specify the **instance** and **location** options together in the same command. If you do not specify the **instance** {0 | 1} and **location** *node-id* arguments, the **show controllers pse mp** command takes effect on both device instances on all modular services cards.

Task ID**Task ID Operations**

interface	read
drivers	read

Examples

The following command shows how to display PSE maintenance processor information for a specific controller instance:

```
RP/0/RP0/CPU0:router# show controllers pse mp instance 1
```

```
Node: 0/0/CPU0:
```

```
-----
```

```
PSE 1, MP Info:
```

```
-----
```

```
MIPC Subtask Context Information
```

```
  High Priority MIPC Mbox Info
```

```
    NumProc 0 NumUnsupp 0
```

```
    NxtSeqNum 0 NumOOSeq 0
```

```
  Norm Priority MIPC Mbox Info
```

```
    NumProc 429 NumUnsupp 0
```

```
    NxtSeqNum 425 NumOOSeq 0
```

```
  NumMsgsGtrred 93 NumDMAErrDrops 5 NumGtrDisDrops 2
```

```
MSTAT Subtask Context Information
```

```
  NumSegs 9 CntrsPerBrst 93 MinCycleMsecs 4000
```

```
  ----- Seg[0] config -----
```

```
  SegId 0 SegBeg 0 SegEnd 3071
```

```
  ExpBeg 0 ExpEnd 0 ExpRate 0 CycBefExp 0
```

```
  ----- Seg[1] config -----
```

```
  SegId 1 SegBeg 3072 SegEnd 74239
```

```
  ExpBeg 3072 ExpEnd 3072 ExpRate 0 CycBefExp 0
```

```
  ----- Seg[2] config -----
```

```
  SegId 2 SegBeg 74240 SegEnd 107007
```

```
  ExpBeg 74240 ExpEnd 74240 ExpRate 0 CycBefExp 0
```

```
  ----- Seg[3] config -----
```

```
  SegId 3 SegBeg 107008 SegEnd 262143
```

```
  ExpBeg 107008 ExpEnd 107008 ExpRate 0 CycBefExp 0
```

```
  ----- Seg[4] config -----
```

```
  SegId 4 SegBeg 262144 SegEnd 265215
```

```
  ExpBeg 262144 ExpEnd 262144 ExpRate 0 CycBefExp 0
```

```
  ----- Seg[5] config -----
```

```
  SegId 5 SegBeg 265216 SegEnd 336383
```

```
  ExpBeg 265216 ExpEnd 265216 ExpRate 0 CycBefExp 0
```

```
  ----- Seg[6] config -----
```

```
  SegId 6 SegBeg 336384 SegEnd 442367
```

```
  ExpBeg 336384 ExpEnd 336385 ExpRate 1 CycBefExp 1
```

```
  ----- Seg[7] config -----
```

```
  SegId 7 SegBeg 442368 SegEnd 458751
```

```
  ExpBeg 442368 ExpEnd 442368 ExpRate 0 CycBefExp 0
```

```
  ----- Seg[8] config -----
```

```
  SegId 8 SegBeg 458752 SegEnd 491519
```

```
show controllers pse mp
```

R3.5.0 Beta Draft—Cisco Confidential Information

```
ExpBeg 458752 ExpEnd 458752 ExpRate 0 CycBefExp 0
CurrTokens 9 MaxTokens 44 MinTokens 11
CurrSeg 5 CurrCntr 289954 CntrsExp 66532
PktsExp 33266 DMAErrDrops 0 REDDrops 0
REDDelays 0 GtrDisDelays 0
CfgUpdsApp 1 SegUpdsApp 10 UpdsRej 0
```

```
Node: 0/3/CPU0:
```

```
PSE 1, MP Info:
```

```
-----
MIPC Subtask Context Information
    High Priority MIPC Mbox Info
        NumProc 0 NumUnsupp 0
        NxtSeqNum 0 NumOOSeq 0
    Norm Priority MIPC Mbox Info
        NumProc 416 NumUnsupp 0
        NxtSeqNum 412 NumOOSeq 0
    NumMsgsGtred 71 NumDMAErrDrops 4 NumGtrDisDrops 3
MSTAT Subtask Context Information
    NumSegs 9 CntrsPerBrst 93 MinCycleMsecs 4000
    ----- Seg[0] config -----
    SegId 0 SegBeg 0 SegEnd 3071
    ExpBeg 0 ExpEnd 0 ExpRate 0 CycBefExp 0
    ----- Seg[1] config -----
    SegId 1 SegBeg 3072 SegEnd 74239
    ExpBeg 3072 ExpEnd 3072 ExpRate 0 CycBefExp 0
    ----- Seg[2] config -----
    SegId 2 SegBeg 74240 SegEnd 107007
    ExpBeg 74240 ExpEnd 74240 ExpRate 0 CycBefExp 0
    ----- Seg[3] config -----
    SegId 3 SegBeg 107008 SegEnd 262143
    ExpBeg 107008 ExpEnd 107008 ExpRate 0 CycBefExp 0
    ----- Seg[4] config -----
    SegId 4 SegBeg 262144 SegEnd 265215
    ExpBeg 262144 ExpEnd 262144 ExpRate 0 CycBefExp 0
    ----- Seg[5] config -----
    SegId 5 SegBeg 265216 SegEnd 336383
    ExpBeg 265216 ExpEnd 265216 ExpRate 0 CycBefExp 0
    ----- Seg[6] config -----
    SegId 6 SegBeg 336384 SegEnd 442367
    ExpBeg 336384 ExpEnd 336415 ExpRate 1 CycBefExp 0
    ----- Seg[7] config -----
    SegId 7 SegBeg 442368 SegEnd 458751
    ExpBeg 442368 ExpEnd 442368 ExpRate 0 CycBefExp 0
    ----- Seg[8] config -----
    SegId 8 SegBeg 458752 SegEnd 491519
    ExpBeg 458752 ExpEnd 458752 ExpRate 0 CycBefExp 0
    CurrTokens 5 MaxTokens 44 MinTokens 11
    CurrSeg 6 CurrCntr 398633 CntrsExp 1064256
    PktsExp 33258 DMAErrDrops 0 REDDrops 0
    REDDelays 0 GtrDisDelays 0
    CfgUpdsApp 1 SegUpdsApp 10 UpdsRej 0
```

R3.5.0 Beta Draft—Cisco Confidential Information

Table 59 describes the significant fields shown in the display.

Table 59 *show controllers pse mp Field Descriptions*

Field	Description
MIPC Subtask Context Information	MIPC subtask information from the following mailboxes (queues): - High Priority MIPC Mbox - Norm Priority MIPC Mbox Note The MIPC MBox is a chunk of the MP DMEM that receives MIPC messages. The Norm Priority mailbox has buffer of 32 KB, while the High Priority Mbox has an 8 KB buffer.
High Priority MIPC Mbox Info	Mailbox (or queue) that receives high-priority MIPC messages. The following information is displayed for the High Priority MIPC Mbox: - NumProc—Number of MIPC messages that have been processed. - NumUnsupp—Number of unsupported MIPC messages. - NxtSeqNum—Sequence number of the message with respect to other messages sent on the same MIPC channel. - NumOOSeq—Number of MIPC messages that were received out of sequence.
Norm Priority MIPC Mbox info	Mailbox (or queue) that receives normal-priority MIPC messages. The following information is displayed for the High Priority MIPC Mbox: - NumProc—Number of MIPC messages that have been processed. - NumUnsupp—Number of unsupported MIPC messages. - NxtSeqNum—Identifies the sequence number of the message with respect to other messages sent on the same MIPC channel. - NumOOSeq—Number of MIPC messages that were received out of sequence.
NumMsgsGtred	Number of MIPC gather messages that have been processed.
NumDMAErrDrops	Number of MIPC gather messages that were dropped due to DMA errors.
NumGtrDisDrops	Number of MIPC gather messages that were dropped due to distribution errors.
MSTAT Subtask Context Information	MSTAT subtask information from the following queues: - High Priority MIPC Mbox - Norm Priority MIPC Mbox The MIPC MBox is a chunk of the MP DMEM that receives MIPC messages. The Norm Priority mailbox has buffer of 32 KB, while the High Priority Mbox has an 8 KB buffer.

R3.5.0 Beta Draft—Cisco Confidential Information**Related Commands**

show controllers pse eio links	Displays PSE information for EIO links, or for a specific controller.
show controllers pse ipc	Displays PSE device information for IPC connections, or for a specific IPC controller.
show controllers pse statistics	Displays PSE statistics for a specific controller instance, or for a specific node.
show controllers pse summary	PSE displays a summary of PSE information for a specific controller or node.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers pse statistics

To display packet switching engine (PSE) statistics for a specific controller instance, or for a specific node, use the **show controllers pse statistics** command in EXEC mode.

show controllers pse statistics [**instance** {**0** | **1**}] [**location** *node-id*]

Syntax Description	instance { 0 1 }	(Optional) Identifies the PSE device whose statistics you want to display. Enter 0 to specify the ingress PSE device, or 1 to specify the egress PSE device. Note Follow the instance { 0 1 } argument with the location <i>node-id</i> argument to restrict the command to specific node containing the specified device instance.
	location <i>node-id</i>	(Optional) Identifies the location of the node whose PSE device information you want to display. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation. Note Use the show platform command to see the location of all nodes installed in the router. Note Include the instance { 0 1 } argument before the location <i>node-id</i> argument to restrict the command to a specific device instance on the specified node.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	No modification.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

R3.5.0 Beta Draft—Cisco Confidential Information

The **instance** and **location** optional keywords are not mutually exclusive. The **instance** keyword directs the command to specific PSE device, and the **location** keyword directs the command to that device or devices on the specified modular services card. You can specify the **instance** and **location** options together in the same command. If you do not specify the **instance** {0 | 1} and **location** *node-id* arguments, the **show controllers pse statistics** command takes effect on both device instances on all modular services cards.

Task ID

Task ID Operations

interface	read
drivers	read

Examples

The following command shows how to display PSE statistics for a specific controller instance:

```
RP/0/RP0/CPU0:router# show controllers pse statistics instance 0
```

```
Node: 0/0/CPU0:
```

```
-----
PSE 0, Statistics Info:
```

```
-----
NULL_STATS_PTR : 0
MPLS_FWD_STATS_MEM_OOR : 0
LAYER2_LOW_PRIORITY : 0
CDP : 0
CONTROL : 0
ARP : 0
RARP : 0
CGMP : 0
LOOP : 0
IPV4_OPTIONS : 0
DROP_IPV4_LENGTH_ERROR : 0
DROP_IPV4_CHECKSUM_ERROR : 0
IPV4_TTL_ERROR : 0
DROP_TCP_FLAG : 0
DROP_ACL_NO_MATCH : 0
UNKNOWN_PKT_TYPE : 0
DROP_ERROR_DISTR : 0
DROP_UNKNOWN_DISTR : 0
PLU_EXCEPTION : 0
IPV4_UNKNOWN_PLU_TYPE : 0
IPV4_PLU_PUNT : 0
IPV4_PLU_DROP_PKT : 0
UNKNOWN_LAYER2 : 0
IPV4_DF_SET_FRAG_NEEDED_PUNT : 0
IPV4_FRAG : 0
INCOMPLETE_ADJ_PUNT : 0
UNKNOWN_IFIB : 0
IPV4_MCAST_EMPTY_OLIST_COUNTER : 0
IPV4_MCAST_MAX_COPIES_EXCEEDED_COUNTER : 0
IPV4_MCAST_LAST_PACKET_TIME_WASTED_COUNTER : 0
BAD_SKIP_GATHER : 0
RP_PUNT : 0
UNKNOWN_PUNT_REASON : 0
DROP_BAD_RESOURCE_ERROR : 0
IPV4_LOAD_INFO_DROP : 0
DROP_IPV4_LINE_STATUS : 0
DROP_PUNT_EXCEED_Q_THRESH : 0
```

R3.5.0 Beta Draft—Cisco Confidential Information

```
DROP_IPV6_LINE_STATUS : 0
PLU_LEAF_UNTERMINATED : 0
PLU_LEAF_UNUSED : 0
PLU_LEAF_ECC : 0
PLU_LEAF_NO_MATCH : 0
PLU_LEAF_BAD_CHANNEL : 0
PLU_LEAF_INVALID : 0
QUEUE_THRESHOLD_DROP : 0
DROP_IPV6_SANITY : 0
DROP_IPV6_PLU : 0
DROP_IPV6_UNKNOWN_PLU_TYPE : 0
DROP_IPV6_LENGTH_ERROR : 0
PUNT_IPV6_MISS_SRC_COMP : 0
IPV6_LINK_LOCAL : 0
IPV6_HOP_BY_HOP : 0
IPV6_TTL_ERROR : 0
IPV6_PLU_PUNT : 0
IFIB_DROP : 0
IPV4_MCAST_DROP_DF_PACKET : 0
IPV6_TOO_BIG : 0
IPV4_MCAST_DO_ALL_BUT_FWD : 0
IPV4_NO_MATCH : 0
GRE_NON_IPV4 : 0
GRE_BAD_FLAGS : 0
IPV4_TUNNEL_NOT_CONFIGD : 0
MPLS_LOADINFO_DROP : 0
IPV4_DOUBLE_TUNNEL : 0
GLOBAL_IFHANDLE_TCAM_MISS : 0
L2TP_COOKIE_MISMATCH : 0
L2TP_TUNNEL_DOWN : 0
RECIRCULATE_UIDB_INDEX : 0
DUMMY_COUNTER : 2622348240762
MPLS_LINE_STATUS_DN_DROP : 0
MPLS_TTL_ERROR : 0
MPLS_PLU_DROP_PKT : 0
MPLS_INVALID_EXPNULL : 0
MPLS_NOT_ENABLED_DROP : 0
MPLS_UNSUPP_PLU_LABEL_TYPE : 0
IPV6_MED_PRI : 0
IPV4_TUNNEL_UNEXP_PHYSINTF_ADJ : 0
IPV4_TUNNEL_UNEXP_TUNINTF_ADJ : 0
IPV4_MCAST_DO_ALL : 0
DROP_IPV4_L4HDR_LENGTH_ERROR : 0
UNKNOWN_OSI : 0
MPLS_PLU_ERROR : 0
MPLS_PLU_NO_MATCH : 0
MPLS_TTL_EXP_GEN_ICMP : 0
MPLS_PLU_PUNT : 0
MPLS_NON_IP_PKT_GT_MTU : 0
MPLS_IPV4_DF : 0
DROP_L2TP_TOO_SHORT_ERROR : 0
DROP_L2TP_TOO_LONG_ERROR : 0
DROP_GRE_LENGTH_ERROR : 0
DROP_IPIP_LENGTH_ERROR : 0
DROP_PUNT_POL_EXCEED : 0
IPV4_TUNNEL_FORUS : 0
IPV4_PLU_RCV : 0
IPV4_FRAG_TUNNEL_PUNT : 0
IPV4MC_NO_MATCH : 0
MPLS_IPV4_FRAGMENTED : 0
MPLS_IPV4_PKT_WITH_OPT_NEEDS_FRAG : 0
IPV4_CANNOT_FRAG : 0
IPV4_NULL_RTE_DROP_PKT : 0
IPV6_NULL_RTE_DROP_PKT : 0
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

IPV4_OPTIONS_RSVP : 0
IPV4_IGMP : 0
IPV4_OPTIONS_PIM : 0
PLIM_ASIC_HDR_ERROR : 0
IPV6_PLU_RCV : 0
IPV4_LOAD_INFO_PUNT : 0
IPV6_LOAD_INFO_PUNT : 0
IPV6_LOAD_INFO_DROP : 0
RP_DEST_DROP : 0
DROP_IPV6_ENABLE : 0
PUNT_ACL_ICMP : 0
PUNT_ACL_LOG : 0
SAP_PUNT : 0
MPLS_INCOMPLETE_ADJ : 0
PKT_LARGE_PADDING_PUNT : 0

```

```

Node: 0/3/CPU0:

```

```

PSE 0, Statistics Info:

```

```

NULL_STATS_PTR : 0
MPLS_FWD_STATS_MEM_OOR : 0
LAYER2_LOW_PRIORITY : 0
CDP : 0
CONTROL : 0
ARP : 0
RARP : 0
CGMP : 0
LOOP : 0
IPV4_OPTIONS : 0
DROP_IPV4_LENGTH_ERROR : 0
DROP_IPV4_CHECKSUM_ERROR : 0
IPV4_TTL_ERROR : 0
DROP_TCP_FLAG : 0
DROP_ACL_NO_MATCH : 0
UNKNOWN_PKT_TYPE : 0
DROP_ERROR_DISTR : 0
DROP_UNKNOWN_DISTR : 0
PLU_EXCEPTION : 0
IPV4_UNKNOWN_PLU_TYPE : 0
IPV4_PLU_PUNT : 0
IPV4_PLU_DROP_PKT : 0
UNKNOWN_LAYER2 : 0
IPV4_DF_SET_FRAG_NEEDED_PUNT : 0
IPV4_FRAG : 0
INCOMPLETE_ADJ_PUNT : 0
UNKNOWN_IFIB : 0
IPV4_MCAST_EMPTY_OLIST_COUNTER : 0
IPV4_MCAST_MAX_COPIES_EXCEEDED_COUNTER : 0
IPV4_MCAST_LAST_PACKET_TIME_WASTED_COUNTER : 0
BAD_SKIP_GATHER : 0
RP_PUNT : 0
UNKNOWN_PUNT_REASON : 0
DROP_BAD_RESOURCE_ERROR : 0
IPV4_LOAD_INFO_DROP : 0
DROP_IPV4_LINE_STATUS : 0
DROP_PUNT_EXCEED_Q_THRESH : 0
DROP_IPV6_LINE_STATUS : 0
PLU_LEAF_UNTERMINATED : 0
PLU_LEAF_UNUSED : 0
PLU_LEAF_ECC : 0
PLU_LEAF_NO_MATCH : 0
PLU_LEAF_BAD_CHANNEL : 0

```


R3.5.0 Beta Draft—Cisco Confidential Information

```
PLU_LEAF_INVALID : 0
QUEUE_THRESHOLD_DROP : 0
DROP_IPV6_SANITY : 0
DROP_IPV6_PLU : 0
DROP_IPV6_UNKNOWN_PLU_TYPE : 0
DROP_IPV6_LENGTH_ERROR : 0
PUNT_IPV6_MISS_SRC_COMP : 0
IPv6_LINK_LOCAL : 0
IPv6_HOP_BY_HOP : 0
IPv6_TTL_ERROR : 0
IPv6_PLU_PUNT : 0
IFIB_DROP : 0
IPv4_MCAST_DROP_DF_PACKET : 0
IPv6_TOO_BIG : 0
IPv4_MCAST_DO_ALL_BUT_FWD : 0
IPv4_NO_MATCH : 0
GRE_NON_IPV4 : 0
GRE_BAD_FLAGS : 0
IPv4_TUNNEL_NOT_CONFIGD : 0
MPLS_LOADINFO_DROP : 0
IPv4_DOUBLE_TUNNEL : 0
GLOBAL_IFHANDLE_TCAM_MISS : 0
L2TP_COOKIE_MISMATCH : 0
L2TP_TUNNEL_DOWN : 0
RECIRCULATE_UIDB_INDEX : 0
DUMMY_COUNTER : 2668152738279
MPLS_LINE_STATUS_DN_DROP : 0
MPLS_TTL_ERROR : 0
MPLS_PLU_DROP_PKT : 0
MPLS_INVALID_EXPNULL : 0
MPLS_NOT_ENABLED_DROP : 0
MPLS_UNSUPP_PLU_LABEL_TYPE : 0
IPv6_MED_PRI : 0
IPv4_TUNNEL_UNEXP_PHYSINTF_ADJ : 0
IPv4_TUNNEL_UNEXP_TUNINTF_ADJ : 0
IPv4_MCAST_DO_ALL : 0
DROP_IPV4_L4HDR_LENGTH_ERROR : 0
UNKNOWN_OSI : 0
MPLS_PLU_ERROR : 0
MPLS_PLU_NO_MATCH : 0
MPLS_TTL_EXP_GEN_ICMP : 0
MPLS_PLU_PUNT : 0
MPLS_NON_IP_PKT_GT_MTU : 0
MPLS_IPV4_DF : 0
DROP_L2TP_TOO_SHORT_ERROR : 0
DROP_L2TP_TOO_LONG_ERROR : 0
DROP_GRE_LENGTH_ERROR : 0
DROP_IPIP_LENGTH_ERROR : 0
DROP_PUNT_POL_EXCEED : 0
IPv4_TUNNEL_FORUS : 0
IPv4_PLU_RCV : 0
IPv4_FRAG_TUNNEL_PUNT : 0
IPv4MC_NO_MATCH : 0
MPLS_IPV4_FRAGMENTED : 0
MPLS_IPV4_PKT_WITH_OPT_NEEDS_FRAG : 0
IPv4_CANNOT_FRAG : 0
IPv4_NULL_RTE_DROP_PKT : 0
IPv6_NULL_RTE_DROP_PKT : 0
IPv4_OPTIONS_RSVP : 0
IPv4_IGMP : 0
IPv4_OPTIONS_PIM : 0
PLIM_ASIC_HDR_ERROR : 0
IPv6_PLU_RCV : 0
IPv4_LOAD_INFO_PUNT : 0
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

IPV6_LOAD_INFO_PUNT : 0
IPV6_LOAD_INFO_DROP : 0
RP_DEST_DROP : 0
DROP_IPV6_ENABLE : 0
PUNT_ACL_ICMP : 0
PUNT_ACL_LOG : 0
SAP_PUNT : 0
MPLS_INCOMPLETE_ADJ : 0
PKT_LARGE_PADDING_PUNT : 0

```

Table 60 describes the significant fields shown in the display.

Table 60 *show controllers pse statistics Field Descriptions*

Field	Description
Node	Identifies the node whose PSE statistics are displayed. The node ID is expressed in the <i>rack/slot/module</i> notation.
PSE 0, Statistics Info	Displays all statistics maintained by the PSE.

Related Commands

show controllers pse eio links	Displays PSE information for EIO links, or for a specific controller.
show controllers pse ipc	Displays PSE device information for IPC connections, or for a specific IPC controller.
show controllers pse mp	Displays PSE information for the maintenance processor on a specific controller or node.
show controllers pse summary	Displays a summary of PSE information for a specific controller or node.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers pse summary

To display a summary of packet switching engine (PSE) information for a specific controller or node, use the **show controllers pse summary** command in EXEC mode.

show controllers pse summary [**instance** {**0** | **1**}] [**location** *node-id*]

Syntax Description	instance { 0 1 }	(Optional) Identifies the PSE device whose information you want to display. Enter 0 to specify the ingress PSE device, or 1 to specify the egress PSE device. Note Follow the instance { 0 1 } argument with the location <i>node-id</i> argument to restrict the command to specific node containing the specified device instance.
	location <i>node-id</i>	(Optional) Identifies the location of the node whose PSE device information you want to display. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation. Note Use the show platform command to see the location of all nodes installed in the router. Note Include the instance { 0 1 } argument before the location <i>node-id</i> argument to restrict the command to a specific device instance on the specified node.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	No modification.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

R3.5.0 Beta Draft—Cisco Confidential Information

The **instance** and **location** optional keywords are not mutually exclusive. The **instance** keyword directs the command to specific PSE device, and the **location** keyword directs the command to that device or devices on the specified modular services card. You can specify the **instance** and **location** options together in the same command. If you do not specify the **instance** {0 | 1} and **location** *node-id* arguments, the **show controllers pse summary** command takes effect on both device instances on all modular services cards.

Task ID

Task ID Operations

interface	read
drivers	read

Examples

The following command shows how to display a summary of PSE information for a specific controller instance:

```
RP/0/RP0/CPU0:router# show controllers pse summary instance 1
```

```
Node: 0/0/CPU0:
```

```
-----
```

```
PSE 1, Summary Info:
```

```
-----
```

```
IBM P/N       : 47P0595   LotNum       : D2300123
SerialNum     : 0x00001c  BadPPECls   : 0000
Version      : 1         CpuctrlPort  : 6
DeviceState   : 0 (UP)
StartupOpts   : 00000000  MmappedBase : 0x60669000
ClsDisMask    : 0000     NFusedPPEs   : 0    (0 hwf, 0 swf)
MPUCodeName   : /pkg/ucode/egress_mp_v1.mucode
PPEUCodeName  : /pkg/ucode/egress_turbo_pos_v1.mucode
INTR-Status   : 00000000  INTR-Enable : 0x7ffffe
NColdResets   : 1         NWarmResets  : 0
NPPEUCldds    : 1         NResetRetry  : 0
NIntrtps      : 1         NIntrptThrot: 0
```

```
Node: 0/3/CPU0:
```

```
-----
```

```
PSE 1, Summary Info:
```

```
-----
```

```
IBM P/N       :          LotNum       :
SerialNum     : 0xffffffff BadPPECls   : 0000
Version      : 3         CpuctrlPort  : 6
DeviceState   : 0 (UP)
StartupOpts   : 00000000  MmappedBase : 0x60669000
ClsDisMask    : 0000     NFusedPPEs   : 4    (0 hwf, 4 swf)
MPUCodeName   : /pkg/gsr/ucode/egress_mp_v3.mucode
PPEUCodeName  : /pkg/gsr/ucode/egress_turbo_pos_v3.mucode
INTR-Status   : 00000000  INTR-Enable : 0x7ffffe
NColdResets   : 1         NWarmResets  : 0
NPPEUCldds    : 1         NResetRetry  : 0
NIntrtps      : 1         NIntrptThrot: 0
```

R3.5.0 Beta Draft—Cisco Confidential Information

Table 61 describes the significant fields shown in the display.

Table 61 *show controllers pse summary Field Descriptions*

Field	Description
Node	Node whose PSE information is displayed.
IBM P/N	IBM part number.
SerialNum	Serial number of the node.
BadPPECIs	Number of bad PPECIs on the PSE.
Version	PSE version.
CpuctrlPort	Cpuctrl port associated with the PSE instance.
DeviceState	Whether the node is up (active) or down (inactive).
StartupOpts	Internal information about the PSE startup options.
MmappedBase	Internal mapping information.
ClsDisMask	Internal masking information.
NFusedPPEs	Internal PPE information.
MPUcodeName	Information about the MPU code.
PPEUcodeName	Information about the PPEU code.
INTR-Status	Internal status information.
INTR-Enable	Internal enable information.
NColdResets	Number of cold resets experienced by the router.
NWarmResets	Number of warm resets experienced by the router.
NPPEUCDids	Internal information about the PSE.
NResetRetry	Number of times the router attempted to reset itself.
NIntrtps	Internal information about interrupts on the PSE.
NIntrptThrot	Internal throttling information for the PSE.

Related Commands

show controllers pse eio links	Displays PSE information for EIO links, or for a specific controller.
show controllers pse ipc	Displays PSE device information for IPC connections, or for a specific IPC controller.
show controllers pse mp	Displays PSE information for the maintenance processor on a specific controller or node.
show controllers pse statistics	Displays PSE statistics for a specific controller instance, or for a specific node.

R3.5.0 Beta Draft—Cisco Confidential Information

show packet-memory

To display information for packet memory, use the **show packet-memory** command in EXEC mode.

show packet-memory [**location** *node-id*]

Syntax Description	location <i>node-id</i>	(Optional) Displays detailed packet memory information for the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults	Displays information about all packet memory.

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	No modification.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	The show packet-memory command can be used to display the total number of packet and particle headers, along with the packet memory that is currently allocated in the system.

Task ID	Task ID	Operations
	basic-services	read

Examples	The following example shows how to display packet memory information:

```
RP/0/RP0/CPU0:router# show packet-memory
```

```
Packet memory statistics :
=====
Packet headers
total: 32000, free: 32000, size: 448
Particle Pools(8)
Pool(0):total: 8000, free: 8000, size: 256
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

fallback: 0, region: 0
Pool(1):total: 4000, free: 3968, size: 512
fallback: 1, region: 0
Pool(2):total: 16, free: 16, size: 512
fallback: 2, region: 0
Pool(3):total: 8000, free: 7936, size: 768
fallback: 3, region: 0
Pool(4):total: 12800, free: 9172, size: 1648
fallback: 4, region: 0
Pool(5):total: 320, free: 320, size: 2560
fallback: 5, region: 0
Pool(6):total: 1600, free: 1088, size: 4608
fallback: 6, region: 0
Pool(7):total: 640, free: 640, size: 6240
fallback: 7, region: 0
Particle clone
total: 8000, free: 8000, size: 256
Packet Feature Specific Variable (FSV)
total: 16000, free: 16000, size: 88
Packet trace
total: 16384, free: 16384, size: 40

```

Table 62 describes the significant fields shown in the display.

Table 62 *show packet memory Field Descriptions*

Field	Description
Packet headers	Data structure that defines and controls an aggregation of data structures, collectively known as a packet. Includes information about every packet in the system.
Particle Pools	Data structure that describes a particle and may be chained to other particles in a linked list. Includes information about the actual data of the packet and other particle headers in this packet if present in this packet.
Particle clone	Duplicate particle header that points to a previously allocated particle. Differs from a particle header in that a particle clone shares the particle with another particle header.
Packet Feature Specific Variable (FSV)	Scratch pad shared among the features in the packet path, listing hangs of the packet header.
Packet trace	Data associated with the packet header to help tracing a packet in the system.

R3.5.0 Beta Draft—Cisco Confidential Information



SONET Controller Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

This module describes the Cisco IOS XR software commands used to configure SONET operation on a router port using Layer 1 SONET transport technology. The configuration of the SONET controller includes SONET Automatic Protection Switch (APS), which is a feature offering recovery from fiber (external) or equipment (interface and internal) failures at the SONET line layer. You must configure a SONET controller before you can configure a Packet-over-SONET/SDH (POS) interface or a Spatial Reuse Protocol (SRP) interface.

All SONET-related configurations of a SONET-based physical port are grouped under the SONET controller configuration submode. The SONET path-related configuration commands are grouped under the SONET path submode.

R3.5.0 Beta Draft—Cisco Confidential Information

ais-shut (SONET)

To enable automatic insertion of a line alarm indication signal (LAIS) in the sent SONET signal whenever the SONET port enters the administrative shutdown state, use the **ais-shut** command in SONET configuration mode. To disable automatic insertion of a LAIS, use the **no** form of this command.

ais-shut

no ais-shut

Syntax Description This command has no arguments or keywords.

Defaults This command is disabled by default; no AIS is sent.

Command Modes SONET configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When the line is placed in administrative shutdown state, use the **ais-shut** command to send a signal to downstream equipment that indicates that there is a problem with the line.

The **ais-shut** command is ignored if automatic protection switching (APS) is running for the corresponding port, because the setting must be enabled for proper APS operation.

For SONET ports that do not have hardware support for LAIS insertion, the **ais-shut** command is disabled.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples In the following example, the alarm indication is forced on the SONET OC-3 controller:

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/RP0/CPU0:router(config-sonet)# ais-shut
```

Related Commands	Command	Description
	show controllers sonet	Displays information about the operational status of SONET layers.

R3.5.0 Beta Draft—Cisco Confidential Information

ais-shut (SONET path)

To enable automatic insertion of path alarm indication signal (PAIS) in the sent SONET signal whenever the SONET path enters the administratively down state, use the **ais-shut** command in SONET path configuration mode. To disable automatic insertion of PAIS in the SONET signal, use the **no** form of this command.

ais-shut

no ais-shut

Syntax Description This command has no arguments or keywords.

Defaults This command is disabled by default; no AIS is sent.

Command Modes SONET path configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **ais-shut** command to enable automatic insertion of PAIS in the appropriate sent SONET path overhead whenever the corresponding SONET path enters the administratively down state.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows the alarm indication being enabled on all paths:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RP0/CPU0:router(config-sonet)# path
RP/0/RP0/CPU0:router(config-sonet-path)# ais-shut
```

R3.5.0 Beta Draft—Cisco Confidential Information**Related Commands**

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

R3.5.0 Beta Draft—Cisco Confidential Information

aps group

To add an automatic protection switching (APS) group and enter APS group configuration mode, use the **aps group** command in global configuration mode. To remove a group, use the **no** form of this command.

aps group *number*

no aps group *number*

Syntax Description	<i>number</i>	Number of the group. Range is from 1 through 255.

Defaults	No groups exist.

Command Modes	Global configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **aps group** command to enter APS group configuration mode and configure APS connections with other SONET equipment. The following commands are available in APS group configuration submode:

- **authenticate**—Configure sending path alarm indication signal (PAIS) when shut down
- **channel**—Assign a channel to an APS group
- **commit**—Commit the configuration changes to the running configuration
- **describe**—Describe a command without taking real actions
- **do**—Run an EXEC command
- **exit**—Exit from this submode
- **lockout**—Set APS Lockout user request
- **no**—Negate a command or set its defaults
- **revert**— Enable automatic switchover from the protect interface to the working interface after the working interface becomes available

R3.5.0 Beta Draft—Cisco Confidential Information

- **show**—Show contents of the current configuration
- **signalling**—Set APS signaling mode
- **timers**—Modify the time between hello packets and the time before the protect interface process declares a working interface router to be down
- **unidirectional**—Set unidirectional mode

An APS group contains one protect (P) SONET port and one working (W) SONET port. The working and protect ports can reside on the same logical channel (LC), on different LCs in the same router, or on different routers. One APS group must be configured for each protect port and its corresponding working ports.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples The following example shows how the **aps group** command is used to configure APS group 1 and enter APS group configuration mode:

```
RP/0/RP0/CPU0:router(config)# aps group 1
```

Related Commands	Command	Description
	show aps	Displays SONET APS group operational status.

R3.5.0 Beta Draft—Cisco Confidential Information

authenticate (PGP)

To configure the authentication string for the Protect Group Protocol (PGP) message exchange between the protect and working routers, use the **authenticate** command in APS group configuration mode. To revert to the default authentication string, use the **no** form of this command.

authenticate *string*

no authenticate *string*

Syntax Description	<i>string</i>	Authentication string that the router uses to authenticate PGP message exchange between protect or working routers. The maximum length of the string is eight alphanumeric characters. Spaces are not accepted.

Defaults	Authentication is always disabled by using the string cisco .

Command Modes	APS group configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.

Use the **authenticate** command to configure the authentication string for the PGP message exchange between the protect and working routers. Use the **no** form of this command to revert to the default authentication string.

The **authenticate** command applies only in multirouter automatic protection switching (APS) group configurations.

In multirouter APS topologies, the protect and working routers communicate with each other through the User Datagram Protocol (UDP)-based Pretty Good Privacy protocol. Each Pretty Good Privacy packet contains an authentication string used for packet validation. The authentication string on all routers involved in the same APS group operation must match for proper APS operation.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples

The following example enables authentication for APS group 1 in abctown:

```
RP/0/RP0/CPU0:router(config)# aps group 1
```

```
RP/0/RP0/CPU0:router(config-aps)# authenticate abctown
```

Related Commands

Command	Description
channel local	Assigns a port and interface local to the router as a SONET APS channel.
channel remote	Assigns a port and interface that is physically located in a remote router as a SONET APS channel.
show aps	Displays SONET APS group operational status.

R3.5.0 Beta Draft—Cisco Confidential Information

channel local

To assign local SONET physical ports as SONET automatic protection switching (APS) channels in the current APS group, use the **channel local** command in APS group configuration mode. To return to the default setting, use the **no** form of this command.

channel {**0** | **1**} **local** {**sonet** | **preconfigure**} **sonet** *instance*

no channel {**0** | **1**} **local** {**sonet** | **preconfigure**} **sonet** *instance*

Syntax Description

0 1	Assigned channel number: 0 = protect, 1 = working.
sonet	Configures SONET port controllers.
preconfigure	Specifies a SONET preconfiguration. This keyword is used only when a modular services or line card is not physically installed in a slot.
sonet	Specifies a SONET interface type.
<i>instance</i>	Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults

A SONET APS local channel is not assigned.

Command Modes

APS group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **channel local** command to designate SONET physical ports as SONET APS channels in the current APS group. Use the **channel remote** command to assign channels that are physically located in a different router.

Preconfigured interfaces are supported.

If the protect channel is local, it must be assigned using a **channel** command *before* any of the working channels are assigned. The reason is that having only a working channel assigned is a valid configuration for a working router in a multirouter APS topology and further attempts to configure a local protect channel will be rejected.

The interface type must be a SONET controller.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to configure SONET 0/2/0/2 as a local protect channel:

```
RP/0/RP0/CPU0:router(config)# aps group 1
```

```
RP/0/RP0/CPU0:router(config-aps)# channel 0 local SONET 0/2/0/2
```

Related Commands

Command	Description
channel remote	Assigns a port and interface that is physically located in a remote router as a SONET APS channel.
show aps	Displays SONET APS group operational status.

R3.5.0 Beta Draft—Cisco Confidential Information

channel remote

To assign a port and interface that is physically located in a remote router as a SONET automatic protection switching (APS) channel (working or protect), use the **channel remote** command in APS group configuration mode. To return to the default setting, use the **no** form of this command.

channel {0 | 1} **remote** *ip-address*

no channel {0 | 1} **remote** *ip-address*

Syntax Description

{0 1}	Assigned channel number. Replace the <i>channel-number</i> argument with a number that identifies the channel. Enter 0 to designate the channel as protect channel, or 1 to designate the channel as a working channel.
<i>ip-address</i>	Remote router IP address in A.B.C.D format.

Defaults

A SONET APS remote channel is not assigned.

Command Modes

APS group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **channel remote** command to assign working or protect channels that are physically located in a different router.

Use the **channel local** command to assign channels in the local router.

**Note**

The **channel remote** command should not be used in single-router APS topologies.

The IP address of the remote router is required only if a working channel configured as the protect router contacts all working routers.

R3.5.0 Beta Draft—Cisco Confidential Information

Specifying a remote protect channel is optional. If you do not specify a remote protect channel, the default value of 0.0.0.0 is used. The protect router is always the one that contacts the working router. The working router replies to the protect router using the source address extracted from the incoming messages as the destination address. If an address other than 0.0.0.0 (the default value) is specified, the working router always uses that address when sending messages to the protect router.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples

In the following examples, a remote channel with IP address 192.168.1.1 is assigned as the working channel:

```
RP/0/RP0/CPU0:router(config)# aps group 1
```

```
RP/0/RP0/CPU0:router(config-aps)# channel 1 remote 192.168.1.1
```

Related Commands	Command	Description
	channel local	Assigns a port and interface local to the router as a SONET APS channel.
	show aps	Displays SONET APS group operational status.

R3.5.0 Beta Draft—Cisco Confidential Information

clear counters sonet

To clear SONET counters for a specific SONET controller, use the **clear counters sonet** command in EXEC mode.

clear counters sonet *instance*

Syntax Description	<i>instance</i>	Either a physical interface instance or a virtual interface instance as follows: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. Note For more information about the syntax for the router, use the question mark (?) online help function.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the clear counters sonet command to clear SONET counters for a specific SONET controller.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	sonet-sdh	read, write
	basic-services	read, write

Examples

The following example shows the SONET counters being cleared on the SONET interface:

```
RP/0/RP0/CPU0:router# clear counters sonet 0/1/0/0
```

Related Commands

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

R3.5.0 Beta Draft—Cisco Confidential Information

clock source (SONET)

To set the clock source of the sent signal on SONET ports, use the **clock source** command in SONET configuration mode. To cancel a clock source setting, use the **no** form of this command.

clock source {**internal** | **line**}

no clock source {**internal** | **line**}

Syntax Description	internal	Specifies that the controller will clock its sent data from its internal clock.
	line	Specifies that the controller will clock its sent data from a clock recovered from the receive data stream of the line. This is the default value.

Defaults The clock source for the controller is **line**.

Command Modes SONET configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **clock source** command to configure which reference clock is used by the sender.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples In the following example, the SONET controller is configured to clock its sent data from its internal clock:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/2/0/2
```

```
RP/0/RP0/CPU0:router(config-sonet)# clock source internal
```


R3.5.0 Beta Draft—Cisco Confidential Information**Related Commands**

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

R3.5.0 Beta Draft—Cisco Confidential Information

controller (SONET)

To enter SONET configuration mode so that you can configure a specific SONET controller, use the **controller** command in global configuration mode. To return to the default state, use the **no** form of this command.

controller [**preconfigure**] **sonet** *instance*

no controller [**preconfigure**] **sonet** *instance*

Syntax Description	preconfigure	(Optional) Specifies a SONET preconfiguration. Use the preconfigure keyword only when a modular services card is not physically installed in a slot.
	sonet	Configures SONET port controllers.
	<i>instance</i>	Either a physical interface instance or a virtual interface instance as follows: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. Note For more information about the syntax for the router, use the question mark (?) online help function.

Defaults No default behavior or values

Command Modes Global configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter SONET configuration mode for the SONET controller in slot number 2:

```
RP/0/RP0/CPU0:router(config)# controller SONET 0/2/0/1  
RP/0/RP0/CPU0:router(config-sonet)#
```

Related Commands

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

R3.5.0 Beta Draft—Cisco Confidential Information

delay trigger

To configure SONET line delay trigger values, use the **delay trigger** command in SONET configuration mode. To cancel the line delay trigger value and return to the default, use the **no** form of this command.

delay trigger line value

no delay trigger line value

Syntax Description	line value	Sets the SONET line delay trigger value in milliseconds. Range is from 0 to 511. Default is 0 (no delay).

Defaults	value: 0

Command Modes	SONET configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples	In the following example, the SONET line delay trigger value is set to 5:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/2/0/2
```

```
RP/0/RP0/CPU0:router(config-sonet)# delay trigger line 5
```

Related Commands	Command	Description
	show controllers sonet	Displays information about the operational status of SONET layers.

R3.5.0 Beta Draft—Cisco Confidential Information

force

To initiate a forced automatic protection switching (APS) request at the local end of the SONET link, use the **force** command in APS group configuration mode. To cancel the switch, use the **no** form of this command.

force {0 | 1}

no force {0 | 1}

Syntax Description

0 | 1 Assigned channel number. 0 = protect, 1 = working.

Defaults

No default behavior or values

Command Modes

APS group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

**Note**

If a request of equal or higher priority is in effect, you cannot use the **force** command to initiate a forced APS request at the local end of the SONET link.

Use the **force** command to manually switch the traffic to a protect channel. For example, if you need to change the fiber connection, you can manually force the working channel to switch to the protect interface.

The 0 or 1 keyword (by default 1) identifies on which channel the traffic should be stopped and moved on the protect channel. The **force 1** command moves traffic from the working channel to the protect channel; the **force 0** command moves traffic from the protect channel back to the working channel.

A forced switch can be used to override an automatic (Signal Failed Signal Degraded) or a manual switch request. A lockout request (via the **lockout** command) overrides a force request.

In a multirouter APS topology, a force request is allowed only on the protect router.

R3.5.0 Beta Draft—Cisco Confidential Information

This command remains in effect until it is unconfigured by using the **no** form of the command.

Task ID

Task ID	Operations

sonet-sdh	read, write

Examples

The following example shows how to move traffic from the working channel back to the protect channel:

```
RP/0/RP0/CPU0:router(config)# aps group 1
```

```
RP/0/RP0/CPU0:router(config-aps)# force 1
```

Related Commands

Command	Description

lockout	Initiates an APS lockout switch request at the local end of the SONET link.

manual	Initiates an APS manual switch request at the local end of the SONET link.

R3.5.0 Beta Draft—Cisco Confidential Information

framing (SONET)

To specify the framing used on the SONET controller, use the **framing** command in SONET configuration mode. To disable framing on the SONET controller, use the **no** form of this command.

framing {sdh | sonet}

no framing {sdh | sonet}

Syntax Description	sdh	Selects Synchronous Digital Hierarchy (SDH) framing. This framing mode is typically used in Europe.
	sonet	Selects SONET framing. This is the default.

Defaults	The default framing on SONET controllers is sonet .

Command Modes	SONET configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.

Use the **framing** command to select either SONET or SDH framing on the selected physical port, if supported. For physical ports that do not support either of these two options, the **framing** command is disabled.

Use the **no** form of this command to disable SONET or SDH framing on the SONET controller.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples	In the following example, the SONET controller is configured for SDH framing:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/2/0/2
```

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(config-sonet)# framing sdh
```

Related Commands	Command	Description
	show controllers sonet	Displays information about the operational status of SONET layers.

R3.5.0 Beta Draft—Cisco Confidential Information

lockout

To initiate a forced automatic protection switching (APS) request at the local end of the SONET link, use the **lockout** command in APS group configuration mode. To remove the lockout, use the **no** form of this command.

lockout {0 | 1}

no lockout {0 | 1}

Syntax Description

channel-number (Optional) Assigned channel number. **0** = protect, **1** = working. Default is **0**.

Defaults

The default is **0**.

Command Modes

APS group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The optional **0** or **1** keyword (by default **0**) identifies the channel from which the traffic should not be moved on the protect channel:

- The **lockout 1** command keeps traffic away from the working router.
- The **lockout 0** command keeps traffic away from the protect router.

A lockout switch request can be used to override a force, an automatic (Signal Failed or Signal Degraded), or a manual switch request. No other request can override a lockout request; it has the highest possible priority.

In a multirouter APS topology, a lockout request is allowed only on the protect router.

This command remains in effect until it is unconfigured by using the **no** form of the command.

Task ID

Task ID	Operations
sonet-sdh	read, write

R3.5.0 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to lock out or prevent the circuit from switching to a working router in the event that the protect circuit becomes unavailable:

```
RP/0/RP0/CPU0:router(config)# aps group 1

RP/0/RP0/CPU0:router(config-aps)# lockout 0
```

Related Commands

Command	Description
force	Initiates an APS force switch request at the local end of the SONET link.
manual	Initiates an APS manual switch request at the local end of the SONET link.

R3.5.0 Beta Draft—Cisco Confidential Information

loopback (SONET)

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

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

no loopback {**internal** | **line**}

Syntax Description

internal	Specifies that all the packets be looped back from the source.
line	Specifies that the incoming network packets be looped back to the SONET network.

Defaults

This command is disabled by default.

Command Modes

SONET configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The SONET and Synchronous Digital Hierarchy (SDH) transport layers support two loopback operation modes for diagnostic purposes: internal and line. In the terminal (internal) loopback, the sent signal is looped back to the receiver. In the facility (line) loopback, the signal received from the far end is looped back and sent on the line. The two loopback modes cannot be active at the same time. In normal operation mode, neither of the two loopback modes is enabled.

Task ID

Task ID	Operations
sonet-sdh	read, write

R3.5.0 Beta Draft—Cisco Confidential Information

Examples

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

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/2/0/2

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

Related Commands

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

R3.5.0 Beta Draft—Cisco Confidential Information**manual**

To initiate a forced automatic protection switching (APS) request at the local end of the SONET link, use the **manual** command in APS group configuration mode. To cancel the switch, use the **no** form of this command.

manual *channel-number* {**0** | **1**}

no manual *channel-number* {**0** | **1**}

Syntax Description

channel-number The assigned channel number: **0** = protect, **1**= working.

Defaults

No circuit is switched.

Command Modes

APS group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **manual** command to manually switch the circuit to a protect channel. For example, you can use this feature when you need to perform maintenance on the working channel. If a protection switch is already up, you can also use the **manual** command to revert the communication link to the working channel before the wait to restore (WTR) time period has expired. The WTR time period is set by the **revert** command. Use the **no** form of this command to cancel the switch.

A manual switch request can be used to control which channel carries the traffic when no other higher-priority user-initiated or automatic requests are in effect.

The **0** or **1** keyword identifies the channel from which the traffic should be moved on the protect channel:

- The **manual 1** command moves traffic on to the protect channel.
- The **manual 0** command moves traffic on to the working channel.

The manual request has the lowest priority among all user-initiated or automatic requests. Any other such requests override a manual request.

In a multirouter APS topology a **manual** request is allowed only on the protect router.

R3.5.0 Beta Draft—Cisco Confidential Information

This command remains in effect until it is unconfigured by using the **no** form of the command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to move traffic on to the protect router:

```
RP/0/RP0/CPU0:router(config)# aps group 1
```

```
RP/0/RP0/CPU0:router(config-aps)# manual 1
```

Related Commands

Command	Description
force	Initiates an APS force switch request at the local end of the SONET link.
lockout	Initiates an APS lockout switch request at the local end of the SONET link.

R3.5.0 Beta Draft—Cisco Confidential Information

overhead (SONET)

To set the SONET overhead bytes in the frame header to a specific standards requirement, or to ensure interoperability with equipment from another vendor, use the **overhead** command in SONET configuration mode. To remove the setting of the SONET overhead bytes from the configuration file and restore the default condition, use the **no** form of this command.

overhead {**j0** | **s1s0**} *byte-value*

no overhead {**j0** | **s1s0**} *byte-value*

Syntax Description	j0	Sets the J0/C1 byte value in the SONET section overhead. For interoperability with Synchronous Digital Hierarchy (SDH) equipment in Japan, use the value 0x1. Default is 0xcc.
	s1s0	Sets the SS bits value of the H1 byte in the SONET line overhead. Use the following values to tell the SONET transmission equipment the S1 and S0 bit: - For SONET mode, use 0 (this is the default). - For SDH mode, use 2. Range is from 0 to 3. Default is 0. Values 1 and 3 are undefined.
	<i>byte-value</i>	Byte value to which the j1 or s1s0 keyword should be set. Range is from 0 to 255.

Defaults	j0 = 0x01
	s1s0 = 0

Command Modes	SONET configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Use the overhead command to set the SONET overhead bytes in the frame header to a specific standards requirement.

R3.5.0 Beta Draft—Cisco Confidential Information

Use the **no** form of this command to remove the setting of the SONET overhead bytes from the configuration file and restore the default condition.

For the **j0** keyword, the value that you use for the trace byte depends on the type of equipment being used. For the **s1s0** keyword, the value that you use depends on whether you are using the SONET or SDH mode. For SONET mode, use the value 0 (the default). For SDH mode, use the value 2.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples

The following example shows how to set the SS bits value of the H1 byte in the SONET line overhead to 2 for SDH:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/1/0/1
```

```
RP/0/RP0/CPU0:router(config-sonet)# overhead s1s0 2
```


R3.5.0 Beta Draft—Cisco Confidential Information

overhead (SONET path)

To set the SONET path overhead bytes in the frame header to a specific standards requirement or to ensure interoperability with equipment from another vendor, use the **overhead** command in SONET path configuration mode. To remove the setting of the SONET path overhead bytes from the configuration file and restore the system to its default condition, use the **no** form of this command.

overhead {**c2** *byte-value* | **j1** *ascii-value*}

no overhead {**c2** *byte-value* | **j1** *ascii-value*}

Syntax Description	c2 <i>byte-value</i>	Specifies Synchronous Transport Signal (STS) synchronous payload envelope (SPE) content (C2) byte. The transmitted c2 value is automatically set to 0xCF for unscrambled payload and 0x16 for scrambled payload. If c2 is configured to a user-specified value, the user-specified value is always applied regardless of scrambling. Replace the <i>byte-value</i> argument with the byte value to which the c2 keyword should be set. Range is from 0 to 255. Default value is 0.
	j1 <i>ascii-value</i>	Configures the SONET path trace (j1) buffer. Replace the <i>ascii-value</i> argument with a text string that describes the SONET path trace buffer. Default is a 64-byte path trace ASCII message, which includes default information such as router name, (Layer 2—POS) interface name, and IP address, if applicable.

Defaults	c2 = 0xCF
	j1 = 0

Command Modes	SONET path configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

R3.5.0 Beta Draft—Cisco Confidential Information

The SONET standards permit or require user access for configuration of some bytes or bits in the SONET path overhead. Use the **overhead** command to set the SONET path overhead bytes in the frame header to a specific standards requirement. Use the **no** form of this command to remove the setting of the SONET path overhead bytes from the configuration file and restore the system to its default condition.

Use the **c2** keyword to configure the desired C2 byte value in the SONET path overhead.

Use the **j1** keyword to configure a user-defined path trace message in the j1 bytes of the SONET path overhead. For the **j1** keyword, use the default message or insert your own message that has a maximum of 62 characters. If no user-defined message is configured, a default message is automatically generated, containing the router name, the controller name, its IP address, and the values of the sent and received K1 and K2 bytes in the SONET line overhead.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to set the STS SPE C2 byte in the SONET path frame header:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/2/0/2
```

```
RP/0/RP0/CPU0:router(config-sonet)# path
```

```
RP/0/RP0/CPU0:router(config-sonet-path)# overhead c2 0x13
```

Related Commands

scrambling disable (SONET path)	Disables SONET payload scrambling on a SONET path.

R3.5.0 Beta Draft—Cisco Confidential Information

path (SONET)

To enter the SONET path configuration submode, use the **path** command in SONET controller configuration mode.

path

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values

Command Modes	SONET controller configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.

Use the **path** command to access SONET path configuration submode. The following commands are available in SONET path configuration submode:

- **ais-shut**—Configure sending path alarm indication signal (PAIS) when shut down
- **commit**—Commit the configuration changes to the running configuration.
- **default**—Set a command to its defaults
- **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
- **overhead**—Configure SONET Path OverHead (POH) byte or bit values
- **report**—Configure SONET path alarm reporting
- **scrambling**—Disables synchronous payload envelope (SPE) scrambling
- **show**—Show contents of the current configuration
- **threshold**—Configure SONET path bit error rate (BER) threshold values

R3.5.0 Beta Draft—Cisco Confidential Information

- **uneq-shut**—Configure sending “Unequipped” (UNEQ) when shut down

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples

The following example shows how to access SONET path submode from SONET controller configuration mode:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/1/0/0
```

```
RP/0/RP0/CPU0:router(config-sonet)# path
```

R3.5.0 Beta Draft—Cisco Confidential Information

report (SONET)

To permit selected SONET alarms to be logged to the console for a SONET controller, use the **report** command in SONET configuration mode. To disable logging of select SONET alarms, use the **no** form of this command.

report [b1-tca | b2-tca | lais | lrdi | sd-ber | sf-ber | slof | slos]

no report [b1-tca | b2-tca | lais | lrdi | sd-ber | sf-ber | slof | slos]

Syntax Description	b1-tca	(Optional) Reports bit 1 (B1) bit error rate (BER) threshold crossing alert (TCA) errors.
	b2-tca	(Optional) Reports bit 2 (B2) BER TCA errors.
	lais	(Optional) Reports line alarm indication signal (LAIS) errors.
	lrdi	(Optional) Reports line remote defect indication errors.
	sd-ber	(Optional) Reports signal degradation BER errors.
	sf-ber	(Optional) Reports signal failure BER errors.
	slof	(Optional) Reports section loss of frame (SLOF) errors.
	slos	(Optional) Reports section loss of signal (SLOS) errors.

Defaults

Alarms from the following keywords are reported by default:

- **b1-tca**
- **b2-tca**
- **sd-ber**
- **sf-ber**
- **slof**
- **slos**

Command Modes

SONET configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Reporting an alarm means that the alarm can be logged to the console, but it is no guarantee that it will be logged. SONET alarm hierarchy rules dictate that only the most severe alarm of an alarm group is reported. Whether an alarm is reported or not, you can check the current state of masked alarm, a problem indication that is a candidate for an alarm, by displaying the “Masked Alarms” line in the **show controllers sonet** command output.

For B1, the bit interleaved parity (BIP) error report is calculated by comparing the BIP-8 code with the BIP-8 code that is extracted from the B1 byte of the following frame. Differences indicate that section-level bit errors have occurred.

For B2, the BIP error report is calculated by comparing the BIP-8/24 code with the BIP-8 code that is extracted from the B2 byte of the following frame. Differences indicate that line-level bit errors have occurred.

Path AIS is sent by line terminating equipment to alert the downstream path terminating equipment (PTE) that it has detected a defect on its incoming line signal.

Path loss of pointer (LOP) is reported as a result of an invalid pointer (H1, H2) or an excess number of new data flag enabled indications.

SLOF is detected when an error-framing defect on the incoming SONET signal persists for 3 microseconds.

SLOS is detected when an all-zeros pattern on the incoming SONET signal is observed. This defect might also be reported if the received signal level drops below the specified threshold.

To determine the alarms that are reported on the controller, use the **show controllers sonet** command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to enable the reporting of line AIS alarms on the path controller:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/1/0/1
```

```
RP/0/RP0/CPU0:router(config-sonet)# report lais
```

Related Commands

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

R3.5.0 Beta Draft—Cisco Confidential Information

report (SONET path)

To configure whether or not selected SONET alarms are logged to the console for a SONET path controller, use the **report** command in SONET path configuration mode. To disable or re-enable the logging of select SONET alarms, use the **no** form of this command.

report [b3-tca disable | pais | plop disable | prdi]

no report [b3-tca disable | pais | plop disable | prdi]

Syntax Description

b3-tca disable	(Optional) Disables the reporting of bit 3 (B3) bit error rate (BER) threshold crossing alert (TCA) errors.
pais	(Optional) Reports path alarm indication signal (PAIS) errors.
plop disable	(Optional) Disables the reporting of path loss of pointer (LOP) errors.
prdi	(Optional) Reports path remote defect indication (PRDI) errors.

Defaults

Alarms from the following keywords are reported:

- **b3-tca**
- **plop**

Command Modes

SONET path configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Reporting an alarm means that the alarm can be logged to the console, but it is no guarantee that it will be logged. SONET alarm hierarchy rules dictate that only the most severe alarm of an alarm group is reported. Whether an alarm is reported or not, you can view the current state of a masked alarm, a problem indication that is a candidate for an alarm, by inspecting the “Masked Alarms” line displayed in the **show controllers sonet** command output.

For B3, the bit interleaved parity (BIP) error report is calculated by comparing the BIP-8 code with the BIP-8 code that is extracted from the B3 byte of the following frame. Differences indicate that path-level bit errors have occurred.

R3.5.0 Beta Draft—Cisco Confidential Information

Path AIS is sent by line-terminating equipment to alert the downstream path-terminating equipment (PTE) that it has detected a defect on its incoming line signal.

Path LOP is reported as a result of an invalid pointer (H1, H2) or an excess number of new data flag enabled indications.

To determine the alarms that are reported on the controller, use the **show controllers sonet** command.

All report commands accept the default option. The default reporting values are determined based upon the SONET standards specifications and are clearly identified in the corresponding command's help string.

**Note**

The reporting of B3 BER TCA errors and path LOP errors is enabled by default.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

In the following example, reporting of path PAIS alarms is enabled:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/2/0/2
```

```
RP/0/RP0/CPU0:router(config-sonet)# path
```

```
RP/0/RP0/CPU0:router(config-sonet-path)# report pais
```

Related Commands

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

R3.5.0 Beta Draft—Cisco Confidential Information

revert

To enable automatic switchover from the protect interface to the working interface after the working interface becomes available, use the **revert** command in APS configuration mode. To disable automatic switchover, use the **no** form of this command.

revert *minutes*

no revert *minutes*

Syntax Description	<i>minutes</i>	Number of minutes until the circuit is switched back to the working interface after the working interface is available.

Defaults	<i>minutes: 0</i> Automatic switchover is disabled.

Command Modes	APS group configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **revert** command to enable and disable revertive APS operation mode, if needed. The revertive APS operation mode of the routers should be matched with the APS operation mode of the connected SONET equipment. Use the **no** form of this command to disable automatic switchover.

The revertive APS operation mode is the recommended operation mode because it offers better traffic protection during various possible software failures and upgrade or downgrade scenarios.

The *minutes* argument indicates how many minutes will elapse until automatic protection switching (APS) decides to switch traffic back from protect to working after the condition that caused an automatic (Signal Failed or Signal Degrade) switch to protect disappears. A value of 0 (default) disables APS revertive mode.

In a multirouter APS topology, the **revert** command is allowed only on the protect router.

R3.5.0 Beta Draft—Cisco Confidential Information**Task ID**

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to enable APS to revert to the protect or working channel after 5 minutes have elapsed:

```
RP/0/RP0/CPU0:router(config)# aps group 1
```

```
RP/0/RP0/CPU0:router(config-aps)# revert 5
```

Related Commands

Command	Description
show aps	Displays SONET APS group operational status.

R3.5.0 Beta Draft—Cisco Confidential Information

scrambling disable (SONET path)

To disable payload scrambling on a SONET path, use the **scrambling disable** command in SONET path configuration mode. To enable payload scrambling after it has been disabled, use the **no** form of this command.

scrambling disable

no scrambling disable

Syntax Description

This command has no arguments or keywords.

Defaults

The default is enable (SONET payload scrambling is on).

Command Modes

SONET path configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

SONET payload scrambling applies a self-synchronous scrambler (x43+1) to the synchronous payload envelope (SPE) of the controller to ensure sufficient bit transition density. Both ends of the connection must be configured using SONET path scrambling.

If the hardware payload scrambling support is not user-configurable, or is not supported, the **scrambling disable** command may be rejected.

Task ID

Task ID	Operations
sonet-sdh	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

In the following example, scrambling is disabled for the path:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/2/0/2
```

```
RP/0/RP0/CPU0:router(config-sonet)# path
```

```
RP/0/RP0/CPU0:router(config-sonet-path)# scrambling disable
```

Related Commands

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

R3.5.0 Beta Draft—Cisco Confidential Information

show aps

To display the operational status for all configured SONET automatic protection switching (APS) groups, use the **show aps** command in EXEC mode.

show aps

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values.

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.

Use the **show aps** command to display operational status for all configured SONET APS groups.

Displaying the SONET APS operational data is considered of lower priority than the APS operation itself. Because the information is collected from several sources scattered across the various nodes involved, there is a small probability that some states will change while the command is being run.

The command should be reissued for confirmation before decisions are made based on the results displayed.

Task ID	Task ID	Operations
	sonet-sdh	read

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following is sample output from the **show aps** command:

```
RP/0/RP0/CPU0:router# show aps

APS Group 1:
  Protect ch 0 (SONET3_0):Enabled
    SONET framing, SONET signalling, bidirectional, revertive (300 sec)
    Rx K1:0x21 (Reverse Request - Working)
      K2:0x15 (bridging Working, 1+1, bidirectional)
    Tx K1:0x81 (Manual Switch - Working)
      K2:0x15 (bridging Working, 1+1, bidirectional)
  Working ch 1 (SONET2_0):Disabled
    Rx K1:0x00 (No Request - Null)
      K2:0x00 (bridging Null, 1+1, non-aps)
    Tx K1:0x00 (No Request - Null)
      K2:0x00 (bridging Null, 1+1, non-aps)

APS Group 3:
  PGP:protocol version: native 2 adopted 2
  PGP:Authentication "cisco", hello timeout 1 sec, hold timeout 3 sec
  Protect ch 0 (SONET3_1):Disabled
    SONET framing, SONET signalling, bidirectional, non-revertive
    Rx K1:0x00 (No Request - Null)
      K2:0x05 (bridging Null, 1+1, bidirectional)
    Tx K1:0x00 (No Request - Null)
      K2:0x05 (bridging Null, 1+1, bidirectional)
  Working ch 1 (192.168.1.1):Enabled

APS Group 5:
  Protect ch 0 (SONET3_2):Disabled
    SONET framing, SONET signalling, unidirectional (auto), non-revertive
    Rx K1:0x00 (No Request - Null)
      K2:0x04 (bridging Null, 1+1, unidirectional)
    Tx K1:0x00 (No Request - Null)
      K2:0x05 (bridging Null, 1+1, bidirectional)
  Working ch 1 (SONET3_3):Enabled
    Rx K1:0x00 (No Request - Null)
      K2:0x00 (bridging Null, 1+1, non-aps)
    Tx K1:0x00 (No Request - Null)
      K2:0x00 (bridging Null, 1+1, non-aps)

APS Group 6:
  PGP:protocol version: native 2 adopted 2
  PGP:Authentication "cisco", hello timeout 1 sec, hold timeout 3 sec
  Protect ch 0 (192.168.3.2 - auto):Disabled
  Working ch 1 (SONET6_0):Enabled
    Rx K1:0x00 (No Request - Null)
      K2:0x00 (bridging Null, 1+1, non-aps)
    Tx K1:0x00 (No Request - Null)
      K2:0x00 (bridging Null, 1+1, non-aps)
```

Table 63 describes the significant fields shown in the display.

Table 63 *show aps Field Descriptions*

Field	Description
APS Group	Assigned number of the APS group. Range is from 1 through 255.
Protect ch	Number and address of the protect channel interface.
Working ch	Number and address of the working channel interface.

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show aps agents	Displays the status of the APS WP distributed communication subsystem.
	show aps group	Displays information about the APS groups.

R3.5.0 Beta Draft—Cisco Confidential Information

show aps agents

To display the status of the automatic protection switching (APS) working to protect (WP) distributed communication subsystem, use the **show aps agents** command in EXEC mode.

show aps agents

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show aps agents** command to display the status of the APS WP distributed communication subsystem.

The WP communication is critical for the APS functionality. The **show aps agents** command is typically used as a debugging aid for unexpected or unusual APS operation.

Displaying the APS operational data is considered of lower priority than the APS operation itself. Because the information is collected from several sources scattered across the various nodes involved, there is a small probability that some states will change while the command is being run.

The command should be reissued for confirmation before decisions are made based on the results displayed.

Task ID	Task ID	Operations
	sonet-sdh	read

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following is sample output from the **show aps agents** command:

```
RP/0/RP0/CPU0:router# show aps agents

SONET APS Manager working-Protect (WP) connections:
Remote peer (192.168.3.2 - auto) is up:
  Group 6   [P.Ch0] 192.168.3.2 === Manager --- SONET6_0 (node6) --- [W.Ch1]
Remote peer (10.1.1.1) is up:
  Group 3   [W.Ch1] 192.168.1.1 === Manager --- SONET3_1 (node3) --- [P.Ch0]
Local agent (node2) is up:
  Group 1   [W.Ch1] --- SONET2_0 --- SONET3_0 (node3) --- [P.Ch0]
Local agent (node3) is up:
  Group 1   [P.Ch0] --- SONET3_0 --- SONET2_0 (node2) --- [W.Ch1]
  Group 3   [P.Ch0] --- SONET3_1 --- Manager === 192.168.1.1 [W.Ch1]
  Group 5   [P.Ch0] --- SONET3_2 --- SONET3_3 (node3) --- [W.Ch1]
  Group 5   [W.Ch1] --- SONET3_3 --- SONET3_2 (node3) --- [P.Ch0]
Local agent (node6) is up:
  Group 6   [W.Ch1] --- SONET6_0 --- Manager === 192.168.3.2 [P.Ch0]
```

Table 64 describes the significant fields shown in the display.

Table 64 *show aps agents Field Descriptions*

Field	Description
Remote peer	IP address of the remote Protect Group Protocol (PGP) peer for the working router in an APS group. An IP address of 0.0.0.0 indicates a dynamically discovered PGP peer not yet contacted, shown on working routers only. (The protect router contacts the working router.)
Local agent	Node name of the local agent, such as (node2).
Group	The interface location or IP address of the SONET APS group. Internal WP communication channel segments are represented as “---” if the segment is operational or “-/-” if the connection is broken. PGP segments are represented as “===” if operational or “==” if broken.

Related Commands

Command	Description
show aps	Displays SONET APS group operational status.

R3.5.0 Beta Draft—Cisco Confidential Information

show aps group

To display information about the automatic protection switching (APS) groups, use the **show aps group** command in EXEC mode.

show aps group [*number*]

Syntax Description

<i>number</i>	(Optional) The assigned group number.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **show aps group** command displays information about APS groups, and is useful if multiple APS groups are configured.

Displaying the APS operational data is considered of lower priority than the APS operation itself. Because the information is collected from several sources scattered across the various nodes involved, there is a small probability that some states will change while the command is being run.

The command should be reissued for confirmation before decisions are made based on the results displayed.

Task ID

Task ID	Operations
sonet-sdh	read

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

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

```
RP/0/RP0/CPU0:router# show aps group 3
```

```
APS Group 3:
```

```
PGP:Authentication "cisco", hello timeout 1 sec, hold timeout 3 sec
Protect ch 0 (SONET3_1):Admin Down, Disabled
  SONET framing, SONET signalling, bidirectional, non-revertive
  Rx K1:0x00 (No Request - Null)
    K2:0x05 (bridging Null, 1+1, bidirectional)
  Tx K1:0x00 (No Request - Null)
    K2:0x05 (bridging Null, 1+1, bidirectional)
Working ch 1 (192.168.1.1):Admin Down, Enabled
```

[Table 65](#) describes the significant fields shown in the display.

Table 65 *show aps group Field Descriptions*

Field	Description
APS Group	Group number assigned to the displayed APS group. For each channel in the group, the following information is displayed: • Authentication string • Hello timer value • Hold timer value • Role of the channel (working or protect) • Channel number • Name of the assigned physical port • Channel status (Enabled, Disabled, Admin Down, Signal Fail, Signal Degraded, or Not Contacted) • Group-related information (for protect channels only) that includes: – Framing of the SONET port – Kilobytes signaling protocol – Unidirectional or bidirectional APS mode – APS revert time, in seconds (in revertive operation mode only)
Rx	Received error signaling bytes and their APS decoded information.
Tx	Sent error signaling bytes and their APS decoded information.
Working ch	IP address of the corresponding Protect Group Protocol (PGP) peer.

The information displayed for the channels local to the routers is identical to the channel information displayed for single-router APS groups.

Related Commands

Command	Description
show aps	Displays SONET APS group operational status.
show aps agents	Displays the status of the APS WP distributed communication subsystem.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers pos

To display information on the Packet-over-SONET/SDH (POS) controllers, use the **show controllers pos** command in EXEC mode.

```
show controllers pos instance [all | framer {internal | register | statistics} | internal]
[begin line | exclude line | file filename | include line]
```

Syntax Description		
	<i>instance</i>	Either a physical interface instance or a virtual interface instance as follows: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
	all	(Optional) Displays information for all POS interface controllers.
	framer	(Optional) Displays all POS framer information.
	internal	(Optional) Displays all POS internal information.
	register	(Optional) Displays the POS framer registers.
	statistics	(Optional) Displays the POS framer cumulative counters.
	begin <i>line</i>	(Optional) Displays information beginning with the line that includes the regular expression given by the <i>line</i> argument.
	exclude <i>line</i>	(Optional) Displays information excluding all lines that contain regular expressions that match the <i>line</i> argument.
	file <i>filename</i>	(Optional) Saves the configuration to the designated file. For more information on which standard filenames are recognized, use the question mark (?) online help function.
	include <i>line</i>	(Optional) Displays only those lines that contain the regular expression given by the <i>line</i> argument.

Defaults	No default behavior or values

Command Modes	EXEC

R3.5.0 Beta Draft—Cisco Confidential Information**Command History**

Releases	Modifications
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The information displayed is generally useful for diagnostic tasks performed by technical support personnel only.

Task ID

Task ID	Operations
interface	read

Examples

The following is sample output from the **show controllers pos** command:

```
RP/0/RP0/CPU0:router# show controllers POS 0/3/0/2
```

```
Port Number      : 2
Interface        : POS0_3_0_2
Ifhandle         : 0x1380120
CRC              : 32
MTU              : 4474
Port Bandwidth Kbps : 2488320
Admin state      : Up
Driver Link state : Up
```

```
Bundle member    : No
Bundle MTU       : 4474
Bundle Adminstate : Up
```

The following is sample output from the **show controllers pos all** command:

```
RP/0/RP0/CPU0:router# show controllers POS 0/3/0/2 all
```

```
Port Number      : 2
Interface        : POS0_3_0_2
Ifhandle         : 0x1380120
CRC              : 32
MTU              : 4474
Port Bandwidth Kbps : 2488320
Admin state      : Up
Driver Link state : Up
```

```
Bundle member    : No
Bundle MTU       : 4474
Bundle Adminstate : Up
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

POS Driver Internal Cooked Stats Values for port 2
=====
Rx Statistics                      Tx Statistics
-----
Total Bytes:      1200              Total Bytes:      0
Good Bytes:       1200              Good Bytes:       0
Good Packets:     25                Good Packets:     0
Aborts:           0                 Aborts:           0
FCS Errors:       0                 Min-len errors:   0
Runs:             0                 Max-len errors:   0
FIFO Overflows:   0                 FIFO Underruns:   0
Giants:           0
Drops:            0

```

```

Sky4402 asic #2 registers:

```

```

0x000 general_cntrl              0x00
0x002 sys_intf_cntrl_1          0x06
0x003 sys_intf_cntrl_2          0x00
0x004 JTAG3                      0x10
0x005 JTAG2                      0x10
0x006 JTAG1                      0x10
0x007 JTAG0                      0x2f
0x010 active_led                 0x01
0x011 gpio_port_mode             0x01
0x012 gpio_port_fault            0x00
0x013 gpio_port_data             0x58
0x015 gpio_port_cntrl            0x3f
0x017 gpio_port_transition        0x00
0x019 gpio_port_intr_mask        0xff
0x01b gpio_port_intr             0x3f
0x01c master_intr_status         0x00
0x01d master_mask                0x00
0x020 interrupt_4                0x04
0x021 interrupt_3                0x00
0x022 interrupt_2                0x00
0x023 interrupt_1                0x00
0x024 status_4                   0x04
0x025 status_3                   0x00
0x026 status_2                   0x0c
0x027 status_1                   0x80
0x028 mask_4                     0x07
0x029 mask_3                     0x03
0x02a mask_2                     0x1c
0x02b mask_1                     0x8f
0x02d link_state_cntrl           0x80
0x041 diag                       0x00
0x042 stcks                      0x03
0x043 short_frame_cntrl          0x00
0x0c0 ror_ram_c2                 0x16
0x0c1 ror_ram_g1                 0x00
0x0c2 ror_ram_f2                 0x00
0x0c3 ror_ram_h4                 0x00
0x0c4 ror_ram_z3                 0x00
0x0c5 ror_ram_z4                 0x00
0x0c6 ror_ram_z5                 0x00
0x0c7 ror_ram_db_c2              0x16
0x0c8 ror_ram_db_g1              0x00
0x142 tor_ram_c2                 0x16

```

R3.5.0 Beta Draft—Cisco Confidential Information

0x143	tor_ram_g1	0x00
0x144	tor_ram_f2	0x00
0x145	tor_ram_h4	0x00
0x146	tor_ram_z3	0x00
0x147	tor_ram_z4	0x00
0x148	tor_ram_z5	0x00
0x170	tor_ram_s1	0x00
0x171	tor_ram_e2	0x00
0x172	tor_ram_e1	0x00
0x173	tor_ram_f1	0x00
0x174	tor_ram_k1	0x00
0x175	tor_ram_k2	0x00
0x177	tor_ram_z2	0x00
0x180	rsp_cntrl_1	0x00
0x181	rsp_cntrl_2	0x02
0x184	rtop_f1_ovrhd	0x00
0x185	rtop_k1_ovrhd	0x00
0x186	rtop_k2_ovrhd	0x00
0x187	rtop_s1_ovrhd	0x00
0x188	rtop_e1_ovrhd	0x00
0x189	rtop_e2_ovrhd	0x00
0x18a	rtop_deb_s1_ovrhd	0x00
0x18c	rtop_b1_mismatch_cnt_u	0x00
0x18d	rtop_b1_mismatch_cnt_l	0x00
0x190	rtop_b2_mismatch_cnt_u	0x00
0x191	rtop_b2_mismatch_cnt_l	0x00
0x194	rtop_rei_l_cnt_u	0x00
0x195	rtop_rei_l_cnt_l	0x00
0x198	rtop_ber_thresh_u	0x00
0x199	rtop_ber_thresh_l	0x00
0x19a	rtop_ber_leak_u	0x00
0x19b	rtop_ber_leak_l	0x00
0x19c	rtop_ber_delay_u	0x00
0x19d	rtop_ber_delay_l	0x00
0x1c0	rpop_signal_lbl_c2	0x16
0x1c2	rpop_valid_ptr_u	0x02
0x1c3	rpop_valid_ptr_l	0x0a
0x1c4	rpop_b3_mismatch_cnt_u	0x00
0x1c5	rpop_b3_mismatch_cnt_l	0x00
0x1c8	rpop_rei_p_cnt_u	0x00
0x1c9	rpop_rei_p_cnt_l	0x00
0x1cc	rpop_ber_thresh_u	0x00
0x1cd	rpop_ber_thresh_l	0x00
0x1ce	rpop_ber_leak_u	0x00
0x1cf	rpop_ber_leak_l	0x00
0x1d0	rpop_ber_delay_u	0x00
0x1d1	rpop_ber_delay_l	0x00
0x200	rpp_cntrl_1	0x11
0x201	rpp_cntrl_2	0x03
0x202	rpp_cntrl_3	0x3e
0x203	rpp_cntrl_4	0x00
0x204	rpp_cntrl_5	0x00
0x208	rpp_max_pkt_len_u	0x08
0x209	rpp_max_pkt_len_l	0xbd
0x20a	rpp_min_pkt_len	0x04
0x244	tpp_inter_pkt_u	0x00
0x245	tpp_inter_pkt_l	0x00
0x246	tpp_idle_cell_hdr	0x00
0x247	tpp_idle_cell_filldata	0x00
0x248	tpp_cntrl	0x04
0x280	tpog_cntrl	0x20
0x2c0	ttog_cntrl	0x00
0x2c2	ttog_ovrhd_src_1	0x00
0x2c3	ttog_ovrhd_src_2	0x00

R3.5.0 Beta Draft—Cisco Confidential Information

0x2c9 ttog_ovrhd_fill

0x00

Table 66 describes the significant fields shown in the display.

Table 66 *show controllers pos Field Descriptions*

Field	Description
Cisco POS ASIC Register Dump (Receive)	Header for display of the contents of the receive ASIC ¹ register log.
asic mode	Address in hex of the ASIC mode flag.
error source	Address in hex of the error source flag.
error mask	Address in hex of the error mask flag.
error detail 1	Address in hex of the error detail 1 flag.
error detail 2	Address in hex of the error detail 2 flag.
rx offset	Address in hex of the receive offset.
Channel Modes	Location in hex of the channel mode flag.
Port 0:	Port 0 (the first port) statistics display.
Port 1:	Port 1 (the second port) statistics display.
Port 2:	Port 2 (the third port) statistics display.
Port 3:	Port 3 (the fourth port) statistics display.
Runt Threshold	Limit in packets set for runs on the specified port.
Tx Delay	Transmit delay that has been set for the specified port.
Cisco POS ASIC Register Dump (Transmit)	Header for display of the contents of the transmit ASIC register log.
POS Driver Internal Cooked Stats Values for port 0	Statistics relating to the specified POS port (POS port 0).
Rx Statistics	Receive statistics for the indicated POS port.
Total Bytes	Total number of bytes, including data and MAC encapsulation, received by the system.
Good Bytes	Number of bytes received without errors.
Good Packets	Number of packets received without errors.
Aborts	Number of receive bytes that have been aborted
FCS Errors	Number of FCS ² errors that have been received.
Runs	Number of received packets that are discarded because they are smaller than the minimum packet size of the medium.
FIFO Overflows	Number of received packets that exceeded the FIFO stack limit.
Giants	Number of received packets that are discarded because they exceed the maximum packet size of the medium.
Drops	Number of received packets that have been dropped from the system.
Tx Statistics	Transmit statistics for the indicated POS port.
Total Bytes	Total number of bytes, including data and MAC encapsulation, sent by the system.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 66** *show controllers pos Field Descriptions (continued)*

Field	Description
Good Bytes	Number of bytes sent without errors.
Good Packets	Number of packets sent without errors.
Aborts	Number of sent bytes that have been aborted.
Min-len errors	Minimum queue length violations.
Max-len errors	Maximum queue length violations.
FIFO Underruns	First-in, first-out, a buffering scheme where the first byte of data entering the buffer is the first byte retrieved by the CPU. FIFO underruns reports the number of times that the transmitter has been running faster than the router can handle.

1. application-specific integrated circuit
2. frame check sequence

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers sonet

To display information about the operational status of SONET layers, use the **show controllers sonet** command in EXEC mode.

show controllers sonet *instance* {**all** | **framers** | **internal-state**}

Syntax Description

<i>instance</i>	Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. – <i>rack</i>: Chassis number of the rack. – <i>slot</i>: Physical slot number of the modular services card or line card. – <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. – <i>port</i>: Physical port number of the interface. Note For more information about the syntax for the router, use the question mark (?) online help function.
all	Displays all information.
framers	Displays framer information.
internal-state	Displays internal SONET state.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.3.2	SONET MIB support was added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show controllers sonet** command to display information about the operational status of SONET layers on a particular SONET port.

R3.5.0 Beta Draft—Cisco Confidential Information

If the manageability PIE is not installed, you can use the **show controllers sonet** command to display the counters for the current 15 minutes only without history data. However, the SONET MIB is still available but is limited to the current bucket of data. History data is still available only when the manageability PIE is loaded. The **show controllers sonet** command is available at any time to display current data, and history data is stored in the line card rather in the history bucket.

Task ID	Task ID	Operations
	interface	read

Examples

The following is sample output from the **show controllers sonet** command:

```
RP/0/RP0/CPU0:router# show controllers sonet 0/1/2/1
```

```
Port SONET0/1/2/1:
```

```
Status: Up
```

```
Loopback: None
```

```
SECTION
```

```
  LOF = 1          LOS      = 1          BIP(B1) = 14892
```

```
LINE
```

```
  AIS = 2          RDI      = 0          FEBE = 0          BIP(B2) = 21
```

```
PATH
```

```
  AIS = 1          RDI      = 0          FEBE = 0          BIP(B3) = 6
```

```
  LOP = 0          NEWPTR = 0          PSE  = 0          NSE    = 0
```

```
  PLM = 0
```

```
Detected Alarms: None
```

```
Line triggers delayed 100 ms
```

```
Asserted Alarms: None
```

```
Mask for Detected->Asserted: None
```

```
Detected Alerts: None
```

```
Reported Alerts: None
```

```
Mask for Detected->Reported: None
```

```
Alarm reporting enabled for: SLOS SLOF SF_BER PLOP
```

```
Alert reporting enabled for: B1-TCA B2-TCA B3-TCA
```

```
Framing: SONET
```

```
SPE Scrambling: Enabled
```

```
C2 State: Stable   C2_rx = 0x16 (22)   C2_tx = 0x16 (22) / Scrambling Derived
```

```
S1S0(tx): 0x0   S1S0(rx): 0x0 / Framing Derived
```

```
PATH TRACE BUFFER : STABLE
```

```
  Remote hostname : brisbane
```

```
  Remote interface: POS0_2_3_1
```

```
  Remote IP addr  : 10.0.0.2
```

```
APS
```

```
No APS Group Configured
```

```
  Rx(K1/K2) : 0x00/0x00
```

```
  Tx(K1/K2) : 0x00/0x00
```

```
  Remote Rx(K1/K2): 00/00   Remote Tx(K1/K2): 00/00
```

```
BER thresholds: SF = 10e-3   SD = 10e-6
```

```
TCA thresholds: B1 = 10e-6   B2 = 10e-6   B3 = 10e-6
```

R3.5.0 Beta Draft—Cisco Confidential Information

Clock source: line (actual) line (configured)

Optical Power Monitoring (accuracy: +/- 1dB)
Not Supported

RP/0/RP1/CPU0:router#

The following is sample output from the **show controllers sonet** command with the **framers** option:

RP/0/RP0/CPU0:router# **show controllers sonet 0/1/2/1 framers**

```
Common Regs
reg[0]                Master Reset and Identity 0x01
reg[1]                Master Cfg 0000
reg[3]                Master Clock Monitors 0x37
reg[100]              Master Intr Status 1 0000
reg[101]              Master Intr Status Ch 0-7 0000
reg[102]              Master Intr Status Ch 8-15 0000
reg[1000]             Master Clock Source Cfg 0000
reg[1001]             Master DCC Interface Cfg 1 0x0f
reg[1002]             Master DCC Interface Cfg 2 0000
reg[1004]             APS Cfg and Status 0000
reg[1005]             APS FIFO Cfg and Status 0x0f
reg[1006]             APS Intr Status 1 0000
reg[1007]             APS Intr Status 2 0000
reg[1008]             APS Reset Ctrl 0000
reg[1010]             TUL3 Interface Cfg 0x80
reg[1011]             TUL3 Intr Status/Enable 1 0000
reg[1012]             TUL3 Intr Status/Enable 2 0000
reg[1013]             TUL3 ATM Level 3 FIFO Cfg 0x03
reg[1014]             TUL3 ATM Level 3 Signal Label 0x01
reg[1015]             TUL3 POS Level 3 FIFO Low Water Mark 0x15
reg[1016]             TUL3 POS Level 3 FIFO High Water Mark 0x17
reg[1017]             TUL3 POS Level 3 Signal Label 0000
reg[1018]             TUL3 burst 0x0f
--More--
```

Table 67 describes the significant fields shown in the display.

Table 67 *show controllers sonet Field Descriptions*

Field	Description
Port	Slot number of the POS interface.
Status	Displays whether the link associated with the specified port is up or down.
Loopback	Loopback identifier, if applicable.
LOF	Section loss of frame is detected when a severely error-framing (SEF) defect on the incoming SONET signal persists for 3 milliseconds.
LOS	Section loss of signal is detected when an all-zeros pattern on the incoming SONET signal lasts 19(+3) microseconds or longer. This defect might also be reported if the received signal level drops below the specified threshold.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 67** *show controllers sonet Field Descriptions (continued)*

Field	Description
BIP	Bit interleaved parity error reported. - For B1, the bit interleaved parity error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B1 byte of the following frame. Differences indicate that section-level bit errors have occurred. - For B2, the bit interleaved parity error report is calculated by comparing the BIP-8/24 code with the BIP-8 code extracted from the B2 byte of the following frame. Differences indicate that line-level bit errors have occurred. - For B3, the bit interleaved parity error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B3 byte of the following frame. Differences indicate that path-level bit errors have occurred.
AIS	Alarm indication signal. - Line alarm indication signal is sent by the STE¹ to alert the downstream LTE² that a LOS or LOF defect has been detected on the incoming SONET section. - Path alarm indication signal is sent by the LTE to alert the downstream PTE³ that it has detected a defect on its incoming line signal.
RDI	Remote defect indication. - Line remote defect indication is reported by the downstream LTE when it detects LOF⁴, LOS⁵, or AIS⁶. - Path remote defect indication is reported by the downstream PTE when it detects a defect on the incoming signal.
FEBE	Far-end block errors. - Line far-end block error (accumulated from the M0 or M1 byte) is reported when the downstream LTE detects BIP⁷ (B2) errors. - Path far-end block error (accumulated from the G1 byte) is reported when the downstream PTE detects BIP (B3) errors.
LOP	Path loss of pointer is reported as a result of an invalid pointer (H1, H2) or an excess number of NDF ⁸ enabled indications.
NEWPTR	Inexact count of the number of times the SONET framer has validated a new SONET pointer value (H1, H2).
PSE	Inexact count of the number of times the SONET framer has detected a positive stuff event in the received pointer (H1, H2).
NSE	Inexact count of the number of times the SONET framer has detected a negative stuff event in the received pointer (H1, H2).

R3.5.0 Beta Draft—Cisco Confidential Information**Table 67** *show controllers sonet Field Descriptions (continued)*

Field	Description
Detected/Asserted/Reported Alarms	Any alarms detected by the controller are displayed here. Alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver is getting AIS. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms.
Line triggers delayed	Line triggers delayed, in milliseconds.
Alarm reporting enabled for	Types of alarms that generate an alarm message.
Alert reporting enabled for	Types of alarms that generate an alert message.
Framing	Type of framing enabled on the controller.
SPE Scrambling	Status of synchronous payload envelope (SPE) scrambling: Enabled, Disabled.
C2 State	Value extracted from the SONET path signal label byte (C2).
S1S0(tx)	Two S bits received in the last H1 byte.
PATH TRACE BUFFER	SONET path trace buffer is used to communicate information regarding the remote hostname, interface name/number, and IP address. This use of the J1 (path trace) byte is proprietary to Cisco.
Remote hostname	Name of the remote host.
Remote interface	Interface of the remote host.
Remote IP addr	IP address of the remote host.
Remote Rx(K1/K2)/Tx(K1/K2)	Contents of the received and transmitted K1 and K2 bytes.
BER thresholds	List of the bit error rate (BER) thresholds you configured with the threshold (SONET) command.
TCA thresholds	List of threshold crossing alarms (TCA) you configured with the threshold (SONET) command.
Clock source	Actual and configured clock source.
Optical Power Monitoring	Power status of the SONET controller.
PM 5355 asic #0 registers	Header for framer register data.

1. section terminating equipment
2. line terminating equipment
3. path terminating equipment
4. loss of frame
5. loss of synchronization
6. alarm indication signal
7. bit interleaved parity

R3.5.0 Beta Draft – Cisco Confidential Information

8. new data flag

The following is sample output from the **show controllers sonet** command with the **internal-state** keyword:

```
RP/0/RP0/CPU0:router# show controllers sonet 0/1/2/1 internal-state

Interface(layer)      admin_up  if_state
-----
SONET0/1/2/1          up        up
(SONET Section)       up        up
(SONET Line)          up        up
(SONET Path)          up        up
  SonetPath0/1/2/1    up        up
    POS0/1/2/1        up        up
```

Table 68 describes the significant fields shown in the display.

Table 68 show controllers sonet Field Descriptions

Field	Description
Interface (layer)	Slot number of the POS interface.
admin_up	Whether the interface and its associated layers are in the admin-up state.
if_state	Whether the interface and its associated layers are in the up or down state.

R3.5.0 Beta Draft—Cisco Confidential Information

shutdown (SONET)

To disable SONET controller processing, use the **shutdown** command in SONET configuration mode. To bring back up a SONET controller and enable SONET controller processing, use the **no** form of this command.

shutdown

no shutdown

Syntax Description This command has no arguments or keywords.

Defaults The SONET controller is up, and SONET controller processing is enabled.

Command Modes SONET configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **shutdown** command to shut down a SONET controller and disable SONET controller processing. Use the **no shutdown** command to bring back up a SONET controller and enable SONET controller processing.

The SONET controller must be brought up for the proper operation of the Layer 2 interface. The Layer 2 interface has a separate **shutdown** command available, which does not operate on the SONET controller's administrative state.

Task ID	Task ID	Operations
	sonet-sdh	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to bring down the SONET controller and disable SONET controller processing:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/1/0/2
```

```
RP/0/RP0/CPU0:router(config-sonet)# shutdown
```

Related Commands

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

R3.5.0 Beta Draft—Cisco Confidential Information

signalling

To configure the K1K2 overhead byte signaling protocol used for automatic protection switching (APS), use the **signalling** command in APS group configuration mode. To reset APS signaling to the default, use the **no** form of this command.

signalling {sonet | sdh}

no signalling {sonet | sdh}

Syntax Description

sonet	Sets signaling to SONET.
sdh	Sets signaling to Synchronous Digital Hierarchy (SDH).

Defaults

SONET signaling is set by default.

Command Modes

APS group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

By default, APS uses the signaling mode matching the framing mode. The **signalling** command may be required, depending upon the transport equipment capabilities, only on “transition” links interconnecting SONET and SDH networks.

In a multirouter APS topology, the **signalling** command is allowed only on the protect router.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to reset the signaling protocol from the default SONET value to SDH:

```
RP/0/RP0/CPU0:router(config)# aps group 1
```

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(config-aps)# signalling sdh
```

Related Commands	Command	Description
	show aps group	Displays information about the automatic protection switching (APS) groups.

R3.5.0 Beta Draft—Cisco Confidential Information

timers (APS)

To change the time between hello packets and the time before the protect interface process declares a working interface router to be down, use the **timers** command in APS group configuration mode. To return to the default timers, use the **no** form of this command.

timers *hello-seconds hold-seconds*

no timers

Syntax Description	<i>hello-seconds</i>	Number of seconds to wait before sending a hello packet (hello timer). Range is from 1 through 255 seconds. Default is 1 second.
	<i>hold-seconds</i>	Number of seconds to wait to receive a response from a hello packet before the interface is declared down (hold timer). Range is from 1 through 255 seconds. Default is 3 seconds.

Defaults

hello-seconds: 1

hold-seconds: 3

Command Modes

APS group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **timers** command to change the time between hello packets and the time before the protect interface process declares a working interface router to be down.

The hello time, in seconds, represents the interval between the periodic message exchange between the Protect Group Protocol (PGP) peers. The hold time, in seconds, represents the interval starting with the first failed periodic message after which, if no successful exchange takes place, the PGP link is declared dead.

If many multirouter APS groups are configured and the CPU load or the User Datagram Protocol (UDP) traffic associated with the PGP communication is considered too high, then the hello interval should be increased.

R3.5.0 Beta Draft—Cisco Confidential Information

Increasing the hold time is suggested if the PGP link is flapping. The possible causes include high route processor (RP) CPU load, high traffic, or high error rates on the links between the working and the protect routers.

We recommend that you have a hold time at least three times longer than the hello time (allowing three or more consecutive failed periodic message exchange failures).

The **timers** command is typically used only on the protect router. After the PGP connection is established, the working router learns about the timer settings from the protect router and automatically adjusts accordingly, regardless of its own timer configuration.

The **timers** command is meaningful only in multirouter automatic protection switching (APS) topologies and is ignored otherwise.

Task ID

Task ID	Operations

sonet-sdh	read, write

Examples

The following example shows how to configure APS group 3 with the hello timer at 2 seconds and the hold timer at 6 seconds:

```
RP/0/RP0/CPU0:router(config)# aps group 3
```

```
RP/0/RP0/CPU0:router(config-aps)# timers 2 6
```

Related Commands

Command	Description

show aps group	Displays information about the automatic protection switching (APS) groups.

R3.5.0 Beta Draft—Cisco Confidential Information

threshold (SONET)

To set the bit error rate (BER) threshold values of the specified alarms for a SONET controller, use the **threshold** command in SONET configuration mode. To remove the setting of the threshold from the configuration file and restore the default condition, use the **no** form of this command.

threshold {**b1-tca** | **b2-tca** | **sd-ber** | **sf-ber**} *bit-error-rate*

no threshold {**b1-tca** | **b2-tca** | **sd-ber** | **sf-ber**} *bit-error-rate*

Syntax Description	b1-tca	Sets the B1 BER threshold crossing alarm (TCA). Range is from 3 through 9. Default is 10e-6.
	b2-tca	Sets the B2 BER threshold crossing alarm (TCA). Range is from 3 through 9. Default is 10e-6.
	sd-ber	Sets the signal degrade BER threshold. Range is from 3 through 9. Default is 10e-6.
	sf-ber	Sets the signal failure BER threshold. Range is from 3 through 9. Default is 10e-3.
	<i>bit-error-rate</i>	BER from 3 to 9 (10 to the minus <i>x</i>).

Defaults	b1-tca = 10e-6
	b2-tca = 10e-6
	sd-ber = 10e-6
	sf-ber = 10e-3

Command Modes	SONET configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

R3.5.0 Beta Draft—Cisco Confidential Information

For B1, the bit interleaved parity (BIP) error report is calculated by comparing the BIP-8 code with the BIP-8 code that is extracted from the B1 byte of the following frame. Differences indicate that section-level bit errors have occurred.

For B2, the BIP error report is calculated by comparing the BIP-8/24 code with the BIP-8 code that is extracted from the B2 byte of the following frame. Differences indicate that line-level bit errors have occurred.

Signal failure BER and signal degrade BER are sourced from B2 BIP-8 error counts (as is B2-TCA). The **b1-tca** and **b2-tca** keywords print only a log message to the console (if reports for them are enabled).

To determine the BER thresholds configured on the controller, use the **show controllers sonet** command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to configure thresholds on the SONET controller:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/2/0/2
```

```
RP/0/RP0/CPU0:router(config-sonet)# threshold sd-ber 8
```

```
RP/0/RP0/CPU0:router(config-sonet)# threshold sf-ber 4
```

```
RP/0/RP0/CPU0:router(config-sonet)# threshold b1-tca 4
```

Related Commands

Command	Description
report (SONET)	Permits selected SONET alarms to be logged to the console for a SONET controller.
show controllers sonet	Displays information about the operational status of SONET layers.

R3.5.0 Beta Draft—Cisco Confidential Information

threshold (SONET path)

To set the bit error rate (BER) threshold values of the specified alarms for a SONET path, use the **threshold** command in SONET path configuration mode. To remove the setting of the SONET path threshold from the configuration file and restore the default condition, use the **no** form of this command.

threshold b3-tca *bit-error-rate*

no threshold b3-tca *bit-error-rate*

Syntax Description	b3-tca	Sets the B3 BER threshold crossing alarm (TCA). Default is 6.
	<i>bit-error-rate</i>	BER from 3 to 9 (10 to the minus x).

Defaults	b3-tca = 6

Command Modes	SONET path configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

For B3, the bit interleaved parity (BIP) error report is calculated by comparing the BIP-8 code with the BIP-8 code that is extracted from the B3 byte of the following frame. Differences indicate that path-level bit errors have occurred.

In addition to BIP errors detected at the local end in the receive direction, B3 error counts detected in the G1 byte (P-REI or P-FEBE) by the far-end SONET equipment are returned.

The **b3-tca** keyword prints only a log message to the console (if reports for them are enabled).

Task ID	Task ID	Operations
	sonet-sdh	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

In the following example, the BER is set to 4:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/1/0/1
```

```
RP/0/RP0/CPU0:router(config-sonet)# path
```

```
RP/0/RP0/CPU0:router(config-sonet-path)# threshold b3-tca 4
```

Related Commands

Command	Description
show controllers sonet	Displays information that is specific to SONET controllers.
report (SONET)	Permits selected SONET alarms to be logged to the console for a SONET controller.

R3.5.0 Beta Draft—Cisco Confidential Information

uneq-shut (SONET path)

To enable automatic insertion of P-UNEQ code (0x00) in the sent SONET path overhead C2 byte, use the **uneq-shut** command in SONET path configuration mode. To disable this feature, use the **no** form of this command.

uneq-shut

no uneq-shut

Syntax Description This command has no arguments or keywords.

Defaults Automatic insertion is enabled.

Command Modes SONET path configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **uneq-shut** command to disable automatic insertion of P-UNEQ code in the sent SONET path overhead C2 byte whenever the SONET path enters the administratively down state.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

In the following example, automatic insertion of P-UNEQ code is disabled in the sent SONET path overhead C2 byte:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/2/0/2
```

```
RP/0/RP0/CPU0:router(config-sonet)# path
```

```
RP/0/RP0/CPU0:router(config-sonet-path)# uneq-shut
```

R3.5.0 Beta Draft—Cisco Confidential Information

unidirectional

To configure a protect interface for unidirectional mode, use the **unidirectional** command in APS group configuration mode. To restore the default setting, bidirectional mode, use the **no** form of this command.

unidirectional

no unidirectional

Syntax Description

This command has no arguments or keywords.

Defaults

Bidirectional mode is the default mode for the protect interface.

Command Modes

APS group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **unidirectional** command to configure a protect interface for unidirectional mode. Use the **no** form of this command to restore the default setting.

The unidirectional or bidirectional automatic protection switching (APS) operation mode of the routers should be matched with the APS operation mode of the connected SONET equipment.



Note

We recommend using bidirectional APS mode when it is supported by the interconnecting SONET equipment. When the protect interface is configured as unidirectional, the working and protect interfaces must cooperate to switch the transmit and receive SONET channel in a bidirectional fashion. Cooperation occurs automatically when the SONET network equipment is in bidirectional mode.

In a multirouter APS topology, the **unidirectional** command is allowed only on the protect router.

Task ID

Task ID	Operations
sonet-sdh	read, write

R3.5.0 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to configure an APS group for unidirectional mode:

```
RP/0/RP0/CPU0:router(config)# aps group 1
```

```
RP/0/RP0/CPU0:router(config-aps)# unidirectional
```

Related Commands

Command	Description
show aps	Displays SONET APS group operational status.



T3/E3 and T1/E1 Controller Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

This module describes the commands to configure T3/E3 and T1/E1 controllers on routers supporting Cisco IOS XR software.

R3.5.0 Beta Draft—Cisco Confidential Information

bert e1

To start or stop a configured bit error rate test (BERT) on an E1 controller or channel group, use the **bert e1** command in EXEC mode. To return to the default state, use the **no** form of this command.

bert e1 *instance* [**channel-group** *channel-group-number*] {**start** | **stop**}

no bert e1 *instance* [**channel-group** *channel-group-number*] {**start** | **stop**}

Syntax Description	channel-group	(Optional) Channel group number. When an E1 data line is configured, channel group numbers can be values from 0 to 30.
	<i>channel-group-number</i>	
	Note	For any of the DS0 time slots within the time slot range provided for the channel group, use time slot -1 as the channel number.
	start	Starts the BERT on the E1 controller or channel.
	stop	Stops the BERT on the E1 controller or channel.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You need to use the **bert pattern** command in E1 configuration mode or channel configuration mode to configure a BERT pattern before you can start a BERT on an E1 controller or channel group.

To view the BERT results, use the **show controllers e1** command in EXEC mode. The BERT results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BERT
- Total bit errors
- Total bits received

R3.5.0 Beta Draft—Cisco Confidential Information

BERT is data intrusive. Regular data cannot flow on a line while the test is in progress. The line is put in an alarm state when a BERT is in progress and restored to a normal state after a BERT has been terminated.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples

The following example shows how to start a BERT on an E1 controller:

```
RP/0/0/CPU0:Router# bert e1 0/3/0/0/0 start
RP/0/0/CPU0:Router# bert e1 0/3/0/0/0 stop
```

Related Commands	Command	Description
	bert interval	Specifies the duration of a BERT.
	bert pattern	Enables a BERT on a T3/E3 or T1/E1 line.
	show controllers e1	Displays information about the E1 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

bert e3

To start or stop a configured bit error rate test (BERT) on an E3 controller or channel group, use the **bert e3** command in EXEC mode. To return to the default state, use the **no** form of this command.

bert e3 *instance* [**channel-group** *channel-group-number*] [**error**] {**start** | **stop**}

no bert e3 *instance* [**channel-group** *channel-group-number*] [**error**] {**start** | **stop**}

Syntax Description	channel-group <i>channel-group-number</i>	(Optional) Channel group number. When an E3 data line is configured, channel group numbers can be values from 0 to 30.
	Note	For any of the DS0 time slots within the time slot range provided for the channel group, use time slot -1 as the channel number.
	error	(Optional) Injects errors into the running BERT stream.
	start	Starts the BERT on the E3 controller or channel.
	stop	Stops the BERT on the E3 controller or channel.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You need to use the **bert pattern** command in E3 configuration mode or channel configuration mode to configure a BERT pattern before you can start a BERT on an E3 controller or channel group.

To view the BERT results, use the **show controllers e3** command in EXEC mode. The BERT results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BERT
- Total bit errors
- Total bits received

R3.5.0 Beta Draft—Cisco Confidential Information

BERT is data intrusive. Regular data cannot flow on a line while the test is in progress. The line is put in an alarm state when a BERT is in progress and restored to a normal state after a BERT has been terminated.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples

The following example shows how to start a BERT on an E3 controller:

```
RP/0/0/CPU0:Router# bert e3 0/3/0/0/0 start
RP/0/0/CPU0:Router# bert e3 0/3/0/0/0 stop
```

Related Commands	Command	Description
	bert interval	Specifies the duration of a BERT.
	bert pattern	Enables a BERT on a T3/E3 or T1/E1 line.
	show controllers e3	Displays information about the E3 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

bert error

To insert errors into a BERT stream on a T3/E3 or T1/E1 line, use the **bert error** command in T3 or T1 configuration mode. To disable a BERT pattern, use the **no** form of this command.

bert error [*number*]

no bert error [*number*]

Syntax Description	<i>number</i>	Specifies the number of BERT errors to introduce into the bit stream. Range is from 1 to 255.

Defaults	Default is 1

Command Modes	T3 configuration T1 configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the bert error command with the bert pattern command.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples	The following example shows how to insert 10 errors into the BERT bit stream on the T1 controller in slot 0, subslot 3:

```
RP/0/0/CPU0:Router(config)# controller t1 0/0/3/1/10
RP/0/0/CPU0:Router(config-t1e1)# bert error 10
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	bert interval	Specifies the duration of a BERT.
	bert pattern	Enables a BERT on a T3/E3 or T1/E1 line.
	show controllers e1	Displays information about the E1 controllers.
	show controllers e3	Displays information about the E3 controllers.
	show controllers t1	Displays information about the T1 controllers.
	show controllers t3	Displays information about the T3 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

bert interval

To specify the duration of a bit error rate test (BERT) pattern on a T3/E3 or T1/E1 line, use the **bert interval** command in T3, E3, T1, E1, or channel group configuration mode. To revert to the default interval, use the **no** form of this command.

bert interval *time*

no bert interval *time*

Syntax Description

<i>time</i>	Duration (in minutes) of the BERT. The interval can be a value from 1 to 14400.

Defaults

BERT runs for a default of 1 minute if this command is not used.

Command Modes

T3 configuration
E3 configuration
T1 configuration
E1 configuration
channel group configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **bert interval** command with the **bert pattern** command. If the **bert interval** command is not used, then the BERT runs for a default of 1 minute.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to limit the BERT to 10 minutes on the T1 controller in slot 0, subslot 3:

```
RP/0/0/CPU0:Router(config)# controller t1 0/0/3/1/10
RP/0/0/CPU0:Router(config-t1e1)# bert interval 10
```

R3.5.0 Beta Draft—Cisco Confidential Information**Related Commands**

Command	Description
bert error	Inserts errors into a BERT stream on a T3/E3 or T1/E1 line
bert pattern	Enables a BERT on a T3/E3 or T1/E1 line.
show controllers e1	Displays information about the E1 controllers.
show controllers e3	Displays information about the E3 controllers.
show controllers t1	Displays information about the T1 controllers.
show controllers t3	Displays information about the T3 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

bert pattern

To enable a bit error rate test (BERT) pattern on a T3/E3 or T1/E1 line or an individual channel group, use the **bert pattern** command in T3, E3, T1, E1, or channel group configuration mode. To disable a BERT pattern, use the **no** form of this command.

bert pattern {0s | 1s | 2^15 | 2^20 | 2^20-QRSS | 2^23 | alt-0-1 | none}

no bert pattern {0s | 1s | 2^15 | 2^20 | 2^20-QRSS | 2^23 | alt-0-1 | none}

Syntax Description		
	0s	Invokes a repeating pattern of zeros (...000...).
	1s	Invokes a repeating pattern of ones (...111...).
	2^15	Invokes a pseudorandom O.151 test pattern that is 32,768 bits in length.
	2^20	Invokes a pseudorandom O.153 test pattern that is 1,048,575 bits in length.
	2^20-QRSS	Invokes a pseudorandom quasi-random signal sequence (QRSS) 0.151 test pattern that is 1,048,575 bits in length.
	2^23	Invokes a pseudorandom O.151 test pattern that is 8,388,607 bits in length.
	alt-0-1	Invokes a repeating pattern of alternating zeros and ones (...01010...).
	none	BERT is not configured.

Defaults	Disabled

Command Modes	T3 configuration E3 configuration T1 configuration E1 configuration channel group configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

BERT is supported on each of the T3/E3 or T1/E1 links. It is done only over an unframed T3/E3 or T1/E1 signal and is run on only one port at a time. It is also supported on an individual channel group.

To begin a BERT, commit the configuration and use the **bert t1**, **bert e1**, **bert t3**, or **bert e3** command in EXEC mode.

R3.5.0 Beta Draft—Cisco Confidential Information

To view the BERT results, use the **show controllers t1** or **show controllers t3** command in EXEC mode. The BERT results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BERT
- Total bit errors
- Total bits received

BERT is data intrusive. Regular data cannot flow on a line while the test is in progress. The line is put in an alarm state when a BERT is in progress and restored to a normal state after a BERT has been terminated.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples

The following example shows how to enable the running of a BERT pattern of all zeros on the T1 controller in slot 0, subslot 3:

```
RP/0/0/CPU0:Router(config)# controller t1 0/0/3/1/10
RP/0/0/CPU0:Router(config-t1e1)# bert pattern 0s
```

Related Commands

Command	Description
bert error	Inserts errors into a BERT stream on a T3/E3 or T1/E1 line
bert interval	Specifies the duration of a BERT.
show controllers e1	Displays information about the E1 controllers.
show controllers e3	Displays information about the E3 controllers.
show controllers t1	Displays information about the T1 controllers.
show controllers t3	Displays information about the T3 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

bert t1

To start or stop a configured bit error rate test (BERT) on a T1 controller or channel group, use the **bert t1** command in EXEC mode.

bert t1 *instance* [**channel-group** *channel-group-number*] {**start** | **stop**}

no bert t1 *instance* [**channel-group** *channel-group-number*] {**start** | **stop**}

Syntax Description	channel-group	(Optional) Channel group number. When a T1 data line is configured, channel group numbers can be values from 0 to 23.
	Note	For any of the DS0 time slots within the time slot range provided for the channel group, use time slot -1 as the channel number.
	start	Starts the BERT on the T1 controller or channel.
	stop	Stops the BERT on the T1 controller or channel.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You need to use the **bert pattern** command in T1 configuration mode or channel configuration mode to configure BERT pattern before you can start a BERT on a T1 controller or channel group.

To view the BERT results, use the **show controllers t1** command in EXEC mode. The BERT results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BERT
- Total bit errors
- Total bits received

R3.5.0 Beta Draft—Cisco Confidential Information

BERT is data intrusive. Regular data cannot flow on a line while the test is in progress. The line is put in an alarm state when a BERT is in progress and restored to a normal state after a BERT has been terminated.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples

The following example shows how to start a BERT on a T1 controller:

```
RP/0/0/CPU0:Router# bert t1 0/3/0/0/0 start
RP/0/0/CPU0:Router# bert t1 0/3/0/0/0 stop
```

Related Commands	Command	Description
	bert interval	Specifies the duration of a BERT.
	bert pattern	Enables a BERT on a T3/E3 or T1/E1 line.
	show controllers t1	Displays information about the T1 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information**bert t3**

To start or stop a configured bit error rate test (BERT) on a T3 controller or channel group, use the **bert t3** command in EXEC mode.

bert t3 *instance* [**channel-group** *channel-group-number*] [**error**] {**start** | **stop**}

no bert t3 *instance* [**channel-group** *channel-group-number*] [**error**] {**start** | **stop**}

Syntax Description	channel-group	(Optional) Channel group number. When an E1 data line is configured, channel group numbers can be values from 0 to 30.
	Note	For any of the DS0 time slots within the time slot range provided for the channel group, use time slot -1 as the channel number.
	error	(Optional) Injects errors into the running BERT stream.
	start	Starts the BERT on the T3 controller or channel.
	stop	Stops the BERT on the T3 controller or channel.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You need to use the **bert pattern** command in T3 configuration mode or channel configuration mode to configure a BERT pattern before you can start a BERT on a T3 controller or channel group.

To view the BERT results, use the **show controllers t3** command in EXEC mode. The BERT results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BERT

R3.5.0 Beta Draft—Cisco Confidential Information

- Total bit errors
- Total bits received

BERT is data intrusive. Regular data cannot flow on a line while the test is in progress. The line is put in an alarm state when a BERT is in progress and restored to a normal state after a BERT has been terminated.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples

The following example shows how to start a BERT on a T3 controller:

```
RP/0/0/CPU0:Router# bert t3 0/3/0/0 start
RP/0/0/CPU0:Router# bert t3 0/3/0/0 stop
```

Related Commands

Command	Description
bert interval	Specifies the duration of a BERT.
bert pattern	Enables a BERT on a T3/E3 or T1/E1 line.
show controllers t3	Displays information about the T3 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

cablelength

To specify the distance of the cable from the routers to the network equipment, use the **cablelength** command in T3 or E3 configuration mode. To restore the default cable length, use the **no** form of this command.

cablelength *feet*

no cablelength

Syntax Description	<i>feet</i>	Number of feet in the range from 0 to 450.

Defaults	feet: 224

Command Modes	T3 configuration E3 configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	You can specify a cable length from 0 to 450 feet; however, the hardware recognizes only two ranges: 0 to 49 and 50 to 450. For example, entering 35 feet uses the 0 to 49 range. If you later change the cable length to 40 feet, there is no change because 40 is still within the 0 to 49 range. However, if you change the cable length to 50, the 50 to 450 range is used. The actual number you enter is stored in the configuration file.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples	The following example shows how to set the cable length for the router to 300 feet:

```
RP/0/0/CPU0:Router(config)# controller t3 0/6/0/0
RP/0/0/CPU0:Router(config-t3)# cablelength 300
```

R3.5.0 Beta Draft—Cisco Confidential Information**Related Commands**

Command	Description
controller e3	Configures an E3 controller and enters E3 configuration mode.
controller t3	Configures a T3 controller and enters T3 configuration mode.

R3.5.0 Beta Draft—Cisco Confidential Information

channel-group

To configure a DS0 channel group and enter channel group configuration mode, use the **channel-group** command in T1 or E1 configuration mode. To unassign a channel group, use the **no** form of this command.

channel-group *channel-group-number*

no channel-group *channel-group-number*

Syntax Description

channel-group-number Channel group number. When a T1 controller is configured, channel group numbers can be values from 0 to 23. When an E1 controller is configured, channel group numbers can be values from 0 to 30.

Note For any of the DS0 time slots within the time slot range provided for the channel group, use time slot -1 as the channel number.

Defaults

No default behavior or values

Command Modes

T1 configuration

E1 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **channel-group** command is available only on channelized SPAs.

Use the **channel-group** command in configurations in which the router must communicate with a T1 or an E1 fractional data line. The channel group number may be arbitrarily assigned and must be unique for the controller. An associated serial interface is created with each defined channel group.

Before the channel group configuration is valid, you must define the associated DS0 time slots using the **timeslots** command.

Use the **no channel group** command to delete a channel group.

Task ID

Task ID	Operations
sonet-sdh	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to enter channel group configuration mode for channel group number 5:

```
RP/0/0/CPU0:Router(config)# controller t1 0/6/0/0/10  
RP/0/0/CPU0:Router(config-t1e1)# channel-group 5  
RP/0/0/CPU0:Router(config-t1-channel_group)#
```

Related Commands

Command	Description
bert pattern	Enables a bit error rate test (BERT) pattern on an individual channel group.
framing (E1)	Specifies the frame type for the E1 data line.
framing (T1)	Specifies the frame type for the T1 data line.
mode	Specifies the mode of the T1/E1 controller.
speed (DS0)	Specifies the speed of the underlying DS0s in a channel group.
timeslots	Associates one or more DS0 time slots with the channel group.

R3.5.0 Beta Draft—Cisco Confidential Information

clock source (T1/E1)

To set clocking for individual T1 or E1 links, use the **clock source** command in T1 or E1 configuration mode. To return to the default, use the **no** form of this command.

clock source {**internal** | **line**}

no clock source

Syntax Description	internal	Specifies that the clock is generated from the internal clock of the T1 or E1 controller.
	Note	When configuring clocking on a serial link, you need to configure one end to be internal and the other end to be line . If you configure internal clocking on both ends of a connection, framing slips occur. If you configure line clocking on both ends of a connection, the line does not come up.
	line	Specifies that the clock on this controller derives its clocking from the external source to which the controller is connected, which is generally the telephone company central office (CO).

Defaults The default clock source is **internal**.

Command Modes T1 configuration
E1 configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples The following example shows how to set the clocking on the T1 controller in slot 6, subslot 0 to internal:

```
RP/0/0/CPU0:Router(config)# controller t1 0/6/0/0
RP/0/0/CPU0:Router(config-t1e1)# clock source internal
```


R3.5.0 Beta Draft—Cisco Confidential Information**Related Commands**

Command	Description
controller e1	Configures an E1 controller and enters E1 configuration mode.
controller t1	Configures a T1 controller and enters T1 configuration mode.

R3.5.0 Beta Draft—Cisco Confidential Information

clock source (T3/E3)

To set clocking for individual T3 or E3 links, use the **clock source** command in T3 or E3 configuration mode. To return to the default, use the **no** form of this command.

clock source {**internal** | **line**}

no clock source

Syntax Description	internal	Specifies that the clock is generated from the internal clock of the T3 or E3 controller.
	Note	When configuring clocking on a serial link, you need to configure one end to be internal and the other end to be line . If you configure internal clocking on both ends of a connection, framing slips occur. If you configure line clocking on both ends of a connection, the line does not come up.
	line	Specifies that the clock on this controller derives its clocking from the external source to which the controller is connected, which is generally the telephone company central office (CO).

Defaults The default clock source is **internal**.

Command Modes T3 configuration
E3 configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If you do not specify the **clock source** command, the default clock source is used.

Configure the **clock source line** command if your telephone company or the remote data service unit provides the master clock of the T3 or E3 connection.

Configure the **clock source internal** command if your router provides the master clock of the T3 or E3 connection.

**Note**

For a back-to-back connection between two T3 or E3 network modules, one controller must be configured for internal clocking while the other controller must be configured for line clocking.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples

The following example shows how to set the clocking on the T3 controller in slot 6, subslot 0 to line:

```
RP/0/0/CPU0:Router(config)# controller t3 0/6/0/0
RP/0/0/CPU0:Router(config-t3)# clock source line
```

Related Commands	Command	Description
	controller e3	Configures an E3 controller and enters E3 configuration mode.
	controller t3	Configures a T3 controller and enters T3 configuration mode.

R3.5.0 Beta Draft—Cisco Confidential Information

controller e1

To configure an E1 controller and enter E1 configuration mode, use the **controller e1** command in global configuration mode. To return to the default state, use the **no** form of this command.

controller e1 *instance*

no controller e1 *instance*

Syntax Description	<i>instance</i>	Physical interface instance. Naming notation is <i>rack/slot/module/port/t1-num</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. <i>port</i>: Physical port number of the T3 controller. <i>t1-num</i>: E1 channel number. Channels range from 0 to 30. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults	No default behavior or values

Command Modes	Global configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **controller e1** command is used in configurations in which the router is intended to communicate with an E1 fractional data line. The **controller e1** command is available only on channelized interfaces.

Use the **mode** command in T3 configuration mode to specify the mode for the port. The default mode for 2-Port and 4-Port Channelized T3 SPAs is T1.

**Note**

If you do not use the **mode** command to define the port to be E1, you cannot configure the E1 controller.

R3.5.0 Beta Draft—Cisco Confidential Information

To view the status of the controllers, use the **show controllers e1** command.

Task ID	Task ID	Operations
	interface	read, write

Examples

The following example shows how to enter E1 configuration mode for a controller in slot 6, on the SPA in subslot 2, on T3 port number 0 and E1 channel number 3:

```
RP/0/0/CPU0:Router(config)# controller e1 0/6/2/0/3
RP/0/0/CPU0:Router(config-t1e1)#
```

Related Commands

Command	Description
mode	Configures the mode of the port to be E1, T1, or serial.
show controllers e1	Displays information about the E1 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

controller e3

To configure an E3 controller and enter E3 configuration mode, use the **controller e3** command in global configuration mode. To return to the default state, use the **no** form of this command.

controller e3 *instance*

no controller e3 *instance*

Syntax Description	<i>instance</i> Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. <i>port</i>: Physical port number of the E3 controller. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults	No default behavior or values

Command Modes	Global configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. The controller e3 command applies only to the 2-Port and 4-Port Clear Channel T3/E3 SPAs. Use the card type command to define the controller type to be E3. To view the status of the controllers, use the show controllers e3 command.

Task ID	Task ID	Operations
	interface	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to enter E3 configuration mode for a controller in slot 6, on the SPA in subslot 2, on E3 controller 0:

```
RP/0/0/CPU0:Router(config)# controller e3 0/6/2/0
RP/0/0/CPU0:Router(config-e3)#
```

Related Commands

Command	Description
hw-module subslot cardtype	Configures the ports on a clear channel SPA to be T3 or E3.
show controllers e3	Displays information about the E3 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

controller t1

To configure a T1 controller and enter T1 configuration mode, use the **controller t1** command in global configuration mode. To return to the default state, use the **no** form of this command.

controller t1 *instance*

no controller t1 *instance*

Syntax Description	<i>instance</i> Physical interface instance. Naming notation is <i>rack/slot/module/port/t1-num</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. <i>port</i>: Physical port number of the T3 controller. <i>t1-num</i>: T1 channel number. T1 channels range from 0 to 23. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults	No default behavior or values

Command Modes	Global configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

The **controller t1** command is used in configurations in which the router is intended to communicate with a T1 fractional data line. The **controller t1** command is available only on channelized SPAs.

Use the **mode** command in T3 configuration mode to specify the mode for each T3 port. The default mode for 2-Port and 4-Port Channelized T3 SPAs is T1.

To view the status of the controllers, use the **show controllers t1** command.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	interface	read, write

Examples

The following example shows how to enter T1 configuration mode for a controller in slot 6, on the SPA in subslot 2, on T3 port number 0 and T1 channel number 3:

```
RP/0/0/CPU0:Router(config)# controller t1 0/6/2/0/3
RP/0/0/CPU0:Router(config-t1e1)#
```

Related Commands

Command	Description
mode	Configures the mode of the port to be E1, T1, or serial.
show controllers t1	Displays information about the T1 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

controller t3

To configure a T3 controller and enter T3 configuration mode, use the **controller t3** command in global configuration mode. To return to the default state, use the **no** form of this command.

controller t3 *instance*

no controller t3 *instance*

Syntax Description	<i>instance</i> Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. <i>port</i>: Physical port number of the T3 controller. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults	No default behavior or values

Command Modes	Global configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	For the 2-Port and 4-Port Clear Channel T3/E3 SPAs, use the card type command to define the controller type to be T3.
	To view the status of the controllers, use the show controllers t3 command.

Task ID	Task ID	Operations
	interface	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to enter T3 configuration mode for a controller in slot 6, on the SPA in subslot 2, on T3 controller 0:

```
RP/0/0/CPU0:Router(config)# controller t3 0/6/2/0  
RP/0/0/CPU0:Router(config-t3)#
```

Related Commands

Command	Description
hw-module subslot cardtype	Configures the ports on a clear channel SPA to be T3 or E3.
show controllers t3	Displays information about the T3 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

dsu bandwidth

To specify the maximum allowable bandwidth used by a T3 or an E3 controller, use the **dsu bandwidth** command in T3 or E3 configuration mode. To return to the default state, use the **no** form of this command.

dsu bandwidth *kbps*

no dsu bandwidth

Syntax Description	<i>kbps</i>	Maximum bandwidth, in kilobits per second (kbps). Range is from 75 to 44210.

Defaults	44210 is the default bandwidth.

Command Modes	T3 configuration E3 configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

The local interface configuration must match the remote interface configuration. For example, if you reduce the maximum bandwidth to 16,000 on the local port, you must also do the same on the remote port.

The **dsu bandwidth** command reduces the bandwidth by padding the E3 and T3 frame.

To verify the data service unit (DSU) bandwidth configured on the interface, use the **show controllers t3** or **show controllers e3** command in EXEC mode.

When G.751 framing is used on E3 links, DSU bandwidth can be used to select a payload subrate from 34,010 kbps down to 22 kbps. Before framing bypass can be used, a DSU bandwidth of 34,010 kbps must be configured.

Although software allows the user to configure a continuous range of bandwidths in subrate modes, vendors support bandwidths only in quantum (for example, in an E3 digital link, bandwidth must be in multiples of 358 kbps). Therefore, the software sets the user-configured bandwidth to the closest vendor-supported bandwidth. Use the **show controllers t3** or **show controllers e3** command to display the actual bandwidth that is configured.

R3.5.0 Beta Draft—Cisco Confidential Information

The following table shows DSU modes and vendor-supported bandwidths.

Table 69 DSU Modes and Vendor-supported Bandwidths

Mode	Bandwidth (in kbps)	Bandwidth Multiples (in kbps)
Digital Link or Cisco	358–34010 for E3 300–44210 for T3	358 300.746
ADC Kentrox T3/E3 IDSU	1000–34010 for E3 1500–44210 for T3	500 500
Larscom Access T45	3100–44210 kbps	3158
Adtran T3SU 300	75–44210 kbps	75.186
Verilink HDM 2182	1500–44210 kbps	1579

Task ID**Task ID Operations**

sonet-sdh	read, write

Examples

The following example shows how to set the maximum allowable DSU bandwidth to 16,000 kbps on a controller in slot 6, on the SPA in subslot 2, on T3 controller 0:

```
RP/0/0/CPU0:Router(config)# controller t3 0/6/2/0
RP/0/0/CPU0:Router(config-t3)# dsu bandwidth 16000
```

The following example shows the user-configured subrate bandwidth and the actual configured subrate bandwidth as displayed in the output of the **show controllers t3** command:

```
RP/0/0/CPU0:Router# show controllers t3 0/3/2/0

Transmitter is sending RAI.
Receiver has loss of signal.
FEAC code received: DS3 Out-Of-Frame
Framing is C-BIT Parity, Line Code is B3ZS, Clock Source is Internal
Subrate is enabled. Mode: Cisco(default), Bandwidth: 44210 kbps
Remote accept is enabled
Remote fullrate has no request outstanding
INTERVAL      LCV  PCV  CCV  PES  PSES  SEFS  UAS  LES  CES  CSES
23:36-23:42    0    0    0    0    0    0    380  0    0    0
.
.
.
```

Related Commands

Command	Description
show controllers e3	Displays information about the E3 controllers.
show controllers t3	Displays information about the T3 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

dsu mode

To specify the interoperability mode used by a T3 or an E3 controller, use the **dsu mode** command in T3 or E3 configuration mode. To return to the default state, use the **no** form of this command.

dsu mode *mode*

no dsu mode

Syntax Description	<i>mode</i>	DSU mode. The mode can be: adtran , cisco , digital-link , kentrox , larscom , or verilink .

Defaults	cisco is the default mode.

Command Modes	T3 configuration E3 configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Refer to [Table 69](#) for more information regarding the modes.

The local interface configuration must match the remote interface configuration. For example, if you define the data service unit (DSU) interoperability mode as **digital-link** on the local port, you must also do the same on the remote port.

You must know what type of DSU is connected to the remote port to determine if it interoperates with a T3 or an E3 controller. The **dsu mode** command enables and improves interoperability with other DSUs.

To verify the DSU mode configured on the interface, use the **show controllers t3** command in EXEC mode.

Task ID	Task ID	Operations
	sonet-sdh	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to set the DSU mode to **digital-link** for a controller in slot 6, on the SPA in subslot 2, on T3 controller 0:

```
RP/0/0/CPU0:Router(config)# controller t3 0/6/2/0
RP/0/0/CPU0:Router(config-t3)# dsu mode digital-link
```

Related Commands

Command	Description
show controllers e3	Displays information about the E3 controllers.
show controllers t3	Displays information about the T3 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

dsu remote

To control the bandwidth usage with the remote port, use the **dsu remote** command in T3 or E3 configuration mode. To return to the default state, use the **no** form of this command.

dsu remote {accept | fullrate}

no dsu remote

Syntax Description	accept	Allows incoming remote requests to reset the bandwidth to the full rate.
	fullrate	Requests that the remote port set its bandwidth to full rate.

Defaults	Remote accept is the default.

Command Modes	T3 configuration E3 configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. To verify the DSU remote settings configured on the interface, use the show controllers t3 or show controllers e3 command in EXEC mode.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples	The following example shows how to specify that the connected remote port set its bandwidth to full rate: <pre>RP/0/0/CPU0:Router(config)# controller t3 0/6/2/0 RP/0/0/CPU0:Router(config-t3)# dsu remote fullrate</pre>

Related Commands

R3.5.0 Beta Draft—Cisco Confidential Information

Command	Description
show controllers e3	Displays information about the E3 controllers.
show controllers t3	Displays information about the T3 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

fdl ansi

To enable or disable the transmission of ANSI T1.403 once-per-second remote performance reports through Facility Data Link (FDL) for a T1 channel on the channelized T3 interface, use the **fdl ansi** command in T1 configuration mode. To return to the default state of remote performance reporting, use the **no** form of this command.

fdl ansi {enable | disable}

no fdl ansi {enable | disable}

Syntax Description	enable	Enables remote performance reports.
	disable	Disables remote performance reports.

Defaults	FDL ansi is enabled by default.

Command Modes	T1 configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

The **fdl ansi** command applies only to T1 lines and can be used only if the T1 framing type is Extended Super Frame (ESF).

The default state of the **fdl ansi** command is enabled. If you disable reporting and want to reenable it, you can use the **no** form of the command. Alternatively, you can use the **fdl ansi enable** command.

To display the remote performance report information, use the **show controllers t1** command.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples	The following example shows how to disable the performance reports for T1 channel 10:

```
RP/0/0/CPU0:Router(config)# controller t1 0/6/0/1/10
RP/0/0/CPU0:Router(config-t1e1)# fdl ansi disable
```

R3.5.0 Beta Draft—Cisco Confidential Information**Related Commands**

Command	Description
show controllers t1	Displays information about the T1 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

framing (E1)

To select the frame type for an E1 data line, use the **framing** command in E1 configuration mode. To disable E1 framing, use the **no** form of this command.

framing {**crc** | **no-crc** | **unframed**}

no framing {**crc** | **no-crc** | **unframed**}

Syntax Description	crc	Specifies framing with CRC-4 error-monitoring capabilities.
	no-crc	Specifies framing with no CRC.
	unframed	Specifies unframed E1.

Defaults	crc is the default

Command Modes	E1 configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Use the framing command in configurations in which the router or access server is intended to communicate with E1 fractional data lines. The service provider determines the framing type required for your E1 circuit.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples	The following example shows how to select E1 framing as the E1 frame type:

```
RP/0/0/CPU0:Router(config)# controller e1 0/6/0/0/10
RP/0/0/CPU0:Router(config-t1e1)# framing e1
```

R3.5.0 Beta Draft—Cisco Confidential Information**Related Commands**

Command	Description
show controllers e1	Displays information about the E1 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

framing (E3)

To select the frame type for E3 data lines, use the **framing** command in E3 configuration mode. To disable E3 framing, use the **no** form of this command.

framing {g751 | g832}

no framing {g751 | g832}

Syntax Description	g751	Specifies that G.751 framing is used as the E3 framing type.
	g832	Specifies that G.832 framing is used as the E3 framing type.

Defaults	G.751 is the default

Command Modes	E3 configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	If you do not use the framing command, the default is used by the E3 controllers to automatically determine the framing type received from the far-end equipment. You can also set the framing for each T1/E1 channel by using the framing command in T1 or E1 configuration mode.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples	The following example shows how to select G751 as the E3 frame type:

```
RP/0/0/CPU0:Router(config)# controller e3 0/6/0/0
RP/0/0/CPU0:Router(config-e3)# framing g751
```

R3.5.0 Beta Draft—Cisco Confidential Information**Related Commands**

Command	Description
show controllers e3	Displays information about the E3 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

framing (T1)

To select the frame type for a T1 data line, use the **framing** command in T1 configuration mode. To disable T1 framing, use the **no** form of this command.

framing {esf | sf}

no framing {esf | sf}

Syntax Description	esf	Specifies extended super frame as the T1 frame type.
	sf	Specifies super frame as the T1 frame type.

Defaults	Extended super frame is the default

Command Modes	T1 configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Use the framing command in configurations in which the router or access server is intended to communicate with T1 fractional data lines. The service provider determines the framing type required for your T1/E1 circuit.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples	The following example shows how to select super frame as the T1 frame type:

```
RP/0/0/CPU0:Router(config)# controller t1 0/6/0/0/10
RP/0/0/CPU0:Router(config-t1)# framing sf
```


R3.5.0 Beta Draft—Cisco Confidential Information**Related Commands**

Command	Description
show controllers t1	Displays information about the T1 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

framing (T3)

To select the frame type for T3 data lines, use the **framing** command in T3 configuration mode. To disable T3 framing, use the **no** form of this command.

framing {c-bit | m23}

no framing {c-bit | m23}

Syntax Description	c-bit	Specifies that C-bit framing is used as the T3 framing type.
	m23	Specifies that M23 framing is used as the T3 framing type.

Defaults	C-bit framing is the default

Command Modes	T3 configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	If you do not use the framing command, the default is used by the T3 controllers to automatically determine the framing type received from the far-end equipment. You can also set the framing for each T1 or E1 channel by using the framing command in T1 or E1 configuration mode.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples	The following example shows how to select M23 as the T3 frame type:

```
RP/0/0/CPU0:Router(config)# controller t3 0/6/0/0
RP/0/0/CPU0:Router(config-t3)# framing m23
```

Related Commands	Command	Description
	show controllers t3	Displays information about the T3 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

hw-module subslot cardtype

To set the ports on a SPA in T3 or E3 mode, use the **hw-module subslot cardtype** command in global configuration mode. To deselect the card type, use the **no** form of this command.

hw-module subslot *subslot-id* **cardtype** {**t3** | **e3**}

no hw-module subslot *subslot-id* **cardtype** {**t3** | **e3**}

Syntax Description

<i>subslot-id</i>	Subslot to be power cycled. The <i>subslot-id</i> argument is entered in the <i>rack/slot/subslot</i> notation.
t3	Clear-channel T3 with integrated data service units (DSUs).
e3	Clear-channel E3 with integrated data service units (DSUs).

Defaults

The 2-Port and 4-Port Clear Channel T3/E3 SPAs are in T3 mode by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **hw-module subslot cardtype** command applies only to 2-Port and 4-Port Clear Channel T3/E3 SPAs.

By default, the 2-Port and 4-Port Clear Channel T3/E3 SPAs boot in T3 mode. Use the **hw-module subslot cardtype** command to change the setting to E3.

If there are nondefault configurations on the card interfaces, you must delete them before you can change the card type. Use the **no t3 controllers** and **no interface serial** commands to delete any T3 or serial configurations.

Task ID

Task ID	Operations
root-lr	read, write

R3.5.0 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to configure all ports of a T1/E1 SPA, located in slot 5, subslot 2 to T1 mode:

```
RP/0/0/CPU0:Router(config)# hw-module subslot 0/5/2 cardtype e3
```

R3.5.0 Beta Draft—Cisco Confidential Information**Related Commands**

Command	Description
controller t3	Configures a T3 controller and enters T3 configuration mode.
interface serial	Configures a serial interface and enters interface configuration mode.

R3.5.0 Beta Draft—Cisco Confidential Information

loopback (T1/E1)

To loop individual T1 or E1 channels on the channelized T3 controller, use the **loopback** command in T1 or E1 configuration mode. To remove the loop, use the **no** form of this command.

```
loopback {local | network {line | payload} | remote {line {fdl {ansi | bellcore} | inband} |  
payload fdl {ansi | bellcore}}}
```

```
no loopback {local | network {line | payload} | remote {line {fdl {ansi | bellcore} | inband} |  
payload fdl {ansi | bellcore}}}
```

Syntax Description		
local		Loops the router output data back toward the router at the T1 framer and sends an alarm indication signal (AIS) signal out toward the network.
network {line payload }		Loops the data back toward the network before the T1 framer and automatically sets a local loopback at the High-Level Data Link Control (HDLC) controllers (line), or loops the payload data back toward the network at the T1 framer and automatically sets a local loopback at the HDLC controllers (payload).
remote line fdl		Sends a repeating, 16-bit Extended Superframe (ESF) data link code word (00001110 11111111 for FDL ANSI and 00010010 11111111 for FDL Bellcore) to the remote end requesting that it enter into a network line loopback.
remote line inband		Sends a repeating, 5-bit inband pattern (00001) to the remote end requesting that it enter into a network line loopback.
remote payload fdl		Sends a repeating, 16-bit ESF data link code word (00010100 11111111) to the remote end requesting that it enter into a network payload loopback. Enables the remote payload FDL ANSI bit loopback on the T1 channel.
ansi		Enables the remote line Facility Data Link (FDL) ANSI bit loopback on the T1 channel, based on the ANSI T1.403 specification.
bellcore		Enables the remote SmartJack loopback on the T1 channel, based on the TR-TSY-000312 specification.

Defaults	No loops are configured.

Command Modes	T1 configuration E1 configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **loopback** command for troubleshooting purposes. To verify that a loopback is configured on the interface, use the **show controllers t1** or **show controllers e1** command in EXEC mode.

For E1 lines, only the **local** and **network line** options are valid. For T1 lines, all listed options are valid.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to configure the T1 for a local loopback:

```
RP/0/0/CPU0:Router(config)# controller t1 0/6/0/0/10
RP/0/0/CPU0:Router(config-t1)# loopback local
```

Related Commands

Command	Description
framing (E1)	Selects the frame type for the E1 data line.
framing (T1)	Selects the frame type for the T1 data line.
show controllers e1	Displays information about the T1 controllers.
show controllers t1	Displays information about the T1 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

loopback (T3/E3)

To loop the entire T3 or E3 line (all 28 T1 channels or all 21 E1 channels) on the T3 controller or E3 controller, use the **loopback** command in T3 or E3 configuration mode. To remove the loop, use the **no** form of this command.

loopback {**local** | **network** {**line** | **payload**} | **remote**}

no loopback

Syntax Description	local	Loops the data back toward the router and sends an alarm indication signal (AIS) out toward the network.
	network { line payload }	Sets the loopback toward the network before going through the framer (line) or after going through the framer (payload).
	remote	Sends a far-end alarm control (FEAC) request to the remote end requesting that it enter into a network line loopback. FEAC requests (and therefore remote loopbacks) are possible only when the T3 is configured for C-bit framing. The M23 format does not support remote loopbacks.

Defaults	No loops are configured on the T3 line.

Command Modes	T3 configuration E3 configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Use the loopback command for troubleshooting purposes. To verify that a loopback is configured on the interface, use the show controllers t3 or show controllers e3 command in EXEC mode. Note that remote loopback is valid only in C-bit parity mode.
	You can also loopback each T1 or E1 channel by using the loopback command in T1 or E1 configuration mode.

Task ID	Task ID	Operations
	sonet-sdh	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to configure the T3 for a local loopback:

```
RP/0/0/CPU0:Router(config)# controller t3 0/3/0/0  
RP/0/0/CPU0:Router(config-t3)# loopback local
```

Related Commands

Command	Description
framing (E1)	Selects the frame type for the E1 data line.
framing (T1)	Selects the frame type for the T1 data line.
loopback (T1/E1)	Places the specified T1 or E1 channel in loopback mode.
show controllers e3	Displays information about the E3 controllers.
show controllers t3	Displays information about the T3 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information**mdl**

To configure the Maintenance Data Link (MDL) message defined in the ANSI T1.107a-1990 specification, use the **mdl** command in T3 configuration mode. To remove the message, use the **no** form of this command.

mdl {transmit {idle-signal | path | test-signal} {enable | disable} | string {eic | fi | fic | gen-number | lic | port-number | unit} string}

no mdl {transmit {idle-signal | path | test-signal} {enable | disable} | string {eic | fi | fic | gen-number | lic | port-number | unit} string}

Syntax Description

transmit idle-signal	Enables transmission of the MDL Idle Signal message.
transmit path	Enables transmission of the MDL Path message.
transmit test-signal	Enables transmission of the MDL Test Signal message.
string eic string	Specifies the Equipment Identification Code; can be up to 10 characters.
string fi string	Specifies the Facility Identification Code sent in the MDL Path message; can be up to 38 characters.
string fic string	Specifies the Frame Identification Code; can be up to 10 characters.
string gen-number string	Specifies the Generator number string sent in the MDL Test Signal message; can be up to 38 characters.
string lic string	Specifies the Location Identification Code; can be up to 11 characters.
string port-number string	Specifies the Port number string sent in the MDL Idle Signal message; can be up to 38 characters.
string unit string	Specifies the Unit Identification Code; can be up to 6 characters.

Defaults

No MDL message is configured.

Command Modes

T3 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show controllers t3** command to display MDL information (received strings). MDL information is displayed only when framing is set to C-bit.

R3.5.0 Beta Draft—Cisco Confidential Information**Note**

MDL is supported only when the DS3 framing is C-bit parity.

Task ID**Task ID** **Operations**

sonet-sdh read, write

Examples

The following example shows the **mdl** commands on a T3 controller in slot 1, subslot 2, port 0:

```
RP/0/0/CPU0:Router(config)# controller t3 0/1/2/0
RP/0/0/CPU0:Router(config-t3)# clock source line
RP/0/0/CPU0:Router(config-t3)# mdl string eic ID
RP/0/0/CPU0:Router(config-t3)# mdl string fic Building B
RP/0/0/CPU0:Router(config-t3)# mdl string unit ABC
RP/0/0/CPU0:Router(config-t3)# mdl string fi Facility Z
RP/0/0/CPU0:Router(config-t3)# mdl string port-number Port 7
RP/0/0/CPU0:Router(config-t3)# mdl transmit path enable
RP/0/0/CPU0:Router(config-t3)# mdl transmit idle-signal enable
```

Related Commands**Command** **Description**

[show controllers t3](#) Displays information about the T3 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

mode

To set the mode of the T1/E1 controller, use the **mode** command in T3 or E3 configuration mode. To disable the controller mode, use the **no** form of this command.

mode {**e1** | **serial** | **t1**}

no mode {**e1** | **serial** | **t1**}

Syntax Description

e1	Specifies the mode of the port to be channelized E1.
serial	Specifies the mode of the port to be clear channel serial.
t1	Specifies the mode of the port to be channelized T1.

Defaults

The default for the 2-Port and 4-Port Clear Channel T3/E3 SPAs is serial.
There is no default for the 2-Port and 4-Port Channelized T3 SPAs.

Command Modes

T3 configuration
E3 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You can change the mode of a controller only when there are no subinterfaces defined for the controller. For example, if you previously defined channelized T1 subinterfaces on a T3 interface and now you want to change this to E1 subinterfaces or a clear channel interface, you must first clear the subinterfaces. To do this, use the **no controller t1** command for all defined T1/E1 subinterfaces. If you have defined serial parameters, you also need to use the **no interface serial** command.

For channelized SPAs, you must use the **mode** command before you can configure any channelized controllers.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to change the mode of a T3 port to channelized T1:

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/0/CPU0:Router(config)# controller t3 0/6/0/0  
RP/0/0/CPU0:Router(config-t3)# mode t1
```

Related Commands	Command	Description
	show controllers e1	Displays information about the E1 controllers.
	show controllers e3	Displays information about the E3 controllers.
	show controllers t1	Displays information about the T1 controllers.
	show controllers t3	Displays information about the T3 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

national bits (E1)

To specify the national reserved bits for an E1 port, use the **national bits** command in E1 configuration mode. To revert to the default national bits, use the **no** form of this command.

national bits *bits*

no national bits *bits*

Syntax Description	<i>bits</i> Bit pattern. Values can be from 0 to 31.

Defaults	0 is the default, which corresponds to 0x1f.

Command Modes	E1 configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples	The following example shows how to specify the national bits for the E1 controller:

```
RP/0/0/CPU0:Router(config)# controller e1 0/6/0/0/10
RP/0/0/CPU0:Router(config-t1e1)# national bits 3
```

Related Commands	Command	Description
	show controllers e1	Displays information about the E1 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

national bits (E3)

To enable or disable the national reserved bit pattern on an E3 port, use the **national bits** command in E3 configuration mode. To revert to the default value, use the **no** form of this command.

national bits {**disable** | **enable**}

no national bits {**disable** | **enable**}

Syntax Description	disable	Disables national reserved bits for an E3 port.
	enable	Enables national reserved bits for an E3 port.

Defaults	The national reserved bit pattern is enabled on the E3 port.

Command Modes	E3 configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples	The following example shows how to enable the national bits for an E3 controller:

```
RP/0/0/CPU0:Router(config)# controller e3 0/6/2/0
RP/0/0/CPU0:Router(config-e3)# national bits enable
```

Related Commands	Command	Description
	show controllers e3	Displays information about the E3 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers e1

To display information about the E1 links and hardware and software drivers for the E1 controller, use the **show controllers e1** command in EXEC mode.

show controllers e1 *instance* [**all** | **bert** | **brief** | **internal-state** | **tabular**]

Syntax Description

<i>instance</i>	Physical interface instance. Naming notation is <i>rack/slot/module/port/e1-num</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. <i>port</i>: Physical port number of the T3 controller. <i>e1-num</i>: E1 channel number. E1 channels range from 0 to 30. For more information about the syntax for the router, use the question mark (?) online help function.
all	Displays all information for the controllers.
bert	Displays internal E1 bit error rate test results.
brief	Displays summary information for the E1 controller.
internal-state	Displays internal E1 state information.
tabular	Displays E1 controller information in tabular format.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	interface	read

Examples

The following example shows sample output from the **show controllers e1** command for a single E1 channel:

```
RP/0/0/CPU0:Router# show controllers e1 0/0/3/3/0
```

```
E10/0/3/3/0 is down
timeslots:
Receiver has no alarms.
Framing is E1 CRC, Clock Source is internal
Data in current interval (0 seconds elapsed):
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
  0 Unavail Secs, 0 Stuffed Secs
  0 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
```

Table 70 describes the significant fields shown in the display.

Table 70 *show controllers e1 Field Descriptions*

Field	Description
E10_0_3_1_10 1 is down	E1 channel is not operating. The channel state can be up, down, or administratively down. Loopback conditions are shown by (Locally Looped) or (Remotely Looped).
timeslots	DS0 time slots assigned to the E1 channel.
Receiver has no alarms	Any alarms detected by the E1 controller are displayed here. Possible alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver is getting AIS. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms.
Framing	Framing type on the channelized controller.
Clock Source	Clock source controller. Values are internal and line.
Line Code Violations	Line Code Violations (LCVs) is a count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) that occur over the accumulation period. An EXZ increments the LCV by one regardless of the length of the zero string.
P-bit Coding Violation	For all DS3 applications, a P-bit coding violation (PCV) error event is a P-bit parity error event. A P-bit parity error event is the occurrence of a received P-bit code on the DS3 M-frame that is not identical to the corresponding locally calculated code.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 70** *show controllers e1 Field Descriptions (continued)*

Field	Description
Slip Secs	Controlled slip second (CSS) is a 1-second interval that contains one or more controlled slips.
Fr Loss Secs	Frame loss seconds (SELS) is the number of seconds for which an out-of-frame error is detected.
Line Err Secs	Line errored seconds (LES) is a second in which one or more line code violation errors are detected.
Degraded Mins	Degraded minute (DM) is a minute in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3. For more information, see RFC 1406, <i>Definitions of Managed Objects for DS1 and E1 Interface Types</i> .
Errored Secs	Errored seconds (ES) is a second with one or more path coding violations, one or more out-of-frame defects, or one or more controlled slip events or a detected AIS defect.
Bursty Err Secs	Bursty errored seconds (BES) is a second with fewer than 320 and more than one path coding violation error events, no severely errored frame defects, and no detected incoming AIS defects. Controlled slips are not included in this parameter.
Severely Err Secs	Severely errored seconds (SES) is a second with 320 or more path code violation errors events, one or more out-of-frame defects, or a detected AIS defect.
Unavailable Secs	Number of seconds during which the interface was not available in this interval, referred to as UAS.
Stuffed Secs	Stuffed seconds (SS) is a second in which one more bit stuffings take place. This happens when the Pulse Density Enforcer detects a potential violation in the output stream and inserts a 1 to prevent it. Such bit stuffings corrupt user data and indicate that the network is configured incorrectly. This counter can be used to help diagnose this situation.
Near-end path failures	Path failure (PFC)
Far-end path failures	(PFCFE)
SEF/AIS Secs	(SAS)

Related Commands

Command	Description
controller e1	Configures an E1 controller and enters E1 configuration mode.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers e3

To display information about the E3 links and hardware and software drivers for the E3 controller, use the **show controllers e3** command in EXEC mode.

show controllers e3 *instance* [**all** | **bert** | **brief** | **internal-state** | **remote** | **tabular**]

Syntax Description

<i>instance</i>	Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. <i>port</i>: Physical port number of the E3 controller. For more information about the syntax for the router, use the question mark (?) online help function.
all	Displays all information for the controllers.
bert	Displays internal E3 bit error rate test results.
brief	Displays summary information for the E3 controller.
internal-state	Displays internal E3 state information.
tabular	Displays E3 controller information in tabular format.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
interface	read

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows sample output from the **show controllers e3** command for a single E3 port:

```
RP/0/0/CPU0:Router# show controllers e3 0/2/0/0

E30/2/0/0 is down
Transmitter is sending RAI.
Receiver has loss of frame.
Framing is G.751, Line Code is B3ZS, Clock Source is Internal
Subrate is enabled. Mode: Cisco(default), Bandwidth: 34010 kbps
Remote accept is enabled
Remote fullrate has no request outstanding
Data in current interval (360 seconds elapsed):
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation, 0 P-bit Err Secs
  0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
  360 Unavailable Secs, 0 Line Errored Secs
  0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
```

The following example shows sample output from the **show controllers e3** command using the **tabular** keyword, for a single E3 port:

```
RP/0/0/CPU0:Router# show controllers e3 0/2/0/0 tabular

E30/2/0/0 is down
Transmitter is sending RAI.
Receiver has loss of frame.
Framing is G.751, Line Code is B3ZS, Clock Source is Internal
Subrate is enabled. Mode: Cisco(default), Bandwidth: 34010 kbps
Remote accept is enabled
Remote fullrate has no request outstanding
INTERVAL      LCV  PCV  CCV  PES  PSES  SEFS  UAS  LES  CES  CSES
07:49-07:56    0    0    0    0    0    0    380  0    0    0
Data in current interval (380 seconds elapsed):
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation, 0 P-bit Err Secs
  0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
  380 Unavailable Secs, 0 Line Errored Secs
  0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
```

Table 71 describes the significant fields shown in the display.

Table 71 *show controllers e3 Field Descriptions*

Field	Description
Transmitter is sending RAI	Any alarms detected by the controller are displayed here. Possible alarms are as follows: - Transmitter is sending remote alarm. - Transmitter is sending AIS. - Receiver has loss of signal. - Receiver is getting AIS. - Receiver has loss of frame. - Receiver has remote alarm. - Receiver has no alarms.
Framing	Framing type on the controller. Values are G.751 and G.832.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 71** *show controllers e3 Field Descriptions (continued)*

Field	Description
Line Code	Line coding format on the controller.
Clock Source	Clock source on the channelized controller. Values are internal and line.
Data in current interval (seconds elapsed)	Shows the current accumulation period, which rolls into the 24-hour accumulation every 15 minutes. The accumulation period is from 1 to 900 seconds. The oldest 15-minute period falls off the back of the 24-hour accumulation buffer.
Line Code Violations	Line Code Violations (LCVs) is a count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) that occur over the accumulation period. An EXZ increments the LCV by one regardless of the length of the zero string.
P-bit Coding Violation	For all DS3 applications, a P-bit coding violation (PCV) error event is a P-bit parity error event. A P-bit parity error event is the occurrence of a received P-bit code on the DS3 M-frame that is not identical to the corresponding locally calculated code.
C-bit Coding Violation	For C-bit parity and SYNTRAN DS3 applications, the C-bit coding violation (CCV) is the count of coding violations reported by the C-bits. For C-bit parity, it is the count of CP-bit parity errors that occur during the accumulation interval. For SYNTRAN, it is a count of CRC-9 errors that occur during the accumulation interval.
P-bit Err Secs	P-bit errored seconds (PES) is a second with one or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge does not increment when unavailable seconds are counted.
P-bit Severely Err Secs	P-bit severely errored seconds (PSES) is a second with 44 or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge does not increment when unavailable seconds are counted.
Severely Err Framing Secs	Severely errored framing seconds (SEFS) is a second with one or more out-of-frame defects or a detected incoming AIS.
Unavailable Secs	The number of unavailable seconds (UAS) is calculated by counting the number of seconds for which the interface is unavailable. For more information, see RFC 1407, <i>DS3 MIB Variables</i> .
Line Errored Secs	Line errored seconds (LES) is a second in which one or more code violations or one or more LOS defects occurred.
C-bit Errored Secs	C-bit errored seconds (CES) is a second with one or more C-bit code violations (CCV), one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.
C-bit Severely Errored Secs	C-bit severely errored seconds (CSES) is a second with 44 or more CCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.
Total Data (last 24 hours)	Shows the last 15-minute accumulation period.

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands

Command	Description
controller e3	Configures an E3 controller and enters E3 configuration mode.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers t1

To display information about the T1 links and hardware and software drivers for the T1 controller, use the **show controllers t1** command in EXEC mode.

show controllers t1 *instance* [**all** | **bert** | **brief** | **internal-state** | **remote** | **tabular**]

Syntax Description	<i>instance</i>	Physical interface instance. Naming notation is <i>rack/slot/module/port/t1-num</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. <i>port</i>: Physical port number of the T3 controller. <i>t1-num</i>: T1 channel number. T1 channels range from 0 to 23. For more information about the syntax for the router, use the question mark (?) online help function.
	all	Displays all information for the controllers.
	bert	Displays internal T1 bit error rate test results.
	brief	Displays summary information for the T1 controller.
	internal-state	Displays internal T1 state information.
	remote	Displays remote performance information.
	tabular	Displays T1 controller information in tabular format.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.5.0 Beta Draft—Cisco Confidential Information**Task ID****Task ID Operations**

interface	read

Examples

The following example shows sample output from the **show controllers t1** command with the **brief** keyword for a single T1 channel:

```
RP/0/0/CPU0:Router# show controllers t1 0/0/3/0/0 brief
```

```
T10/0/3/0/0 is up
timeslots: 24-1
FDL per AT&T 54016 spec.
No alarms detected.
Framing is ESF, Clock Source is internal
```

The following example shows sample output from the **show controllers t1** command for a single T1 channel:

```
RP/0/0/CPU0:Router# show controllers t1 0/0/3/0/0
```

```
T10/0/3/0/0 is up
timeslots: 24-1
FDL per AT&T 54016 spec.
No alarms detected.
Framing is ESF, Clock Source is internal
Data in current interval (666 seconds elapsed):
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
  0 Unavail Secs, 0 Stuffed Secs
  0 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
Data in Interval 1:
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 56 Severely Err Secs
  0 Unavail Secs, 0 Stuffed Secs
  32256 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
Data in Interval 2:
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
  0 Unavail Secs, 0 Stuffed Secs
  0 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
.
.
.
```

The following example shows sample output from the **show controllers t1** command with the **tabular** keyword for a single T1 channel:

```
RP/0/0/CPU0:Router# show controllers t1 0/0/3/0/0 tabular
```

```
T10/0/3/0/0 is up
timeslots: 24-1
FDL per AT&T 54016 spec.
No alarms detected.
Framing is ESF, Clock Source is internal
```

INTERVAL	LCV	PCV	CSS	SELS	LES	DM	ES	BES	SES	UAS	SS	PFC	PFCFE	SAS
05:05-05:06	0	0	0	0	0	0	0	0	0	0	0	0	0	0
04:50-05:05	0	0	0	0	0	0	0	0	57	0	0	32256	0	0
04:35-04:50	0	0	0	0	0	0	0	0	0	0	0	0	0	0
04:20-04:35	3866624	0	0	0	0	0	0	0	0	0	0	0	0	0

R3.5.0 Beta Draft—Cisco Confidential Information

.
 .
 .

Table 72 describes the significant fields shown in the display.

Table 72 *show controllers t1 Field Descriptions*

Field	Description
T10/0/3/0/0 is up	T1 channel is operating. The channel state can be up, down, or administratively down. Loopback conditions are shown by (Locally Looped) or (Remotely Looped).
timeslots	DS0 time slots assigned to the T1 channel.
FDL per ANSI T1.403 and AT&T 54016 spec.	Performance monitoring is through Facility Data Link based on ANSI T1.403 and AT&T standard specification number 54016.
No alarms detected.	Any alarms detected by the T1 controller are displayed here. Possible alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver is getting AIS. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms.
Framing	Framing type on the channelized controller. Values are ESF, SF and T1-unframed.
Clock Source	Clock source on the T1 channel. Values are internal and line.
Line Code Violations	Line Code Violations (LCVs) is a count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) that occur over the accumulation period. An EXZ increments the LCV by one regardless of the length of the zero string.
P-bit Coding Violation	For all DS3 applications, a P-bit coding violation (PCV) error event is a P-bit parity error event. A P-bit parity error event is the occurrence of a received P-bit code on the DS3 M-frame that is not identical to the corresponding locally calculated code.
Slip Secs	Controlled slip second (CSS) is a 1-second interval that contains one or more controlled slips.
Fr Loss Secs	Frame loss seconds (SELS) is the number of seconds for which an out-of-frame error is detected.
Line Err Secs	Line errored seconds (LES) is a second in which one or more line code violation errors are detected.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 72** *show controllers t1 Field Descriptions (continued)*

Field	Description
Degraded Mins	Degraded minute (DM) is a minute in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3. For more information, see RFC 1406, <i>Definitions of Managed Objects for DS1 and E1 Interface Types</i> .
Errored Secs	Errored seconds (ES) is a second with one or more path coding violations, one or more out-of-frame defects, or one or more controlled slip events or a detected AIS defect.
Bursty Err Secs	Bursty errored seconds (BES) is a second with fewer than 320 and more than one path coding violation error events, no severely errored frame defects, and no detected incoming AIS defects. Controlled slips are not included in this parameter.
Severely Err Secs	Severely errored seconds (SES) is a second with 320 or more path code violation errors events, one or more out-of-frame defects, or a detected AIS defect.
Unavailable Secs	Number of seconds during which the interface was not available in this interval, referred to as UAS.
Stuffed Secs	Stuffed seconds (SS) is a second in which one more bit stuffings take place. This happens when the Pulse Density Enforcer detects a potential violation in the output stream and inserts a 1 to prevent it. Such bit stuffings corrupt user data and indicate that the network is configured incorrectly. This counter can be used to help diagnose this situation.
Near-end path failures	Total number of near-end path failures.
Far-end path failures	Total number of far-end path failures.
SEF/AIS Secs	Total number or Severely Errored Framing (SEF) and Alarm Indication Signal (AIS) errors.

Related Commands

Command	Description
controller t1	Configures a T1 controller and enters T1 configuration mode.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers t3

To display information about the T3 links and hardware and software drivers for the T3 controller, use the **show controllers t3** command in EXEC mode.

show controllers t3 *instance* [**all** | **bert** | **brief** | **internal-state** | **tabular**]

Syntax Description

<i>instance</i>	Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. <i>port</i>: Physical port number of the T3 controller. For more information about the syntax for the router, use the question mark (?) online help function.
all	Displays all information for the controllers.
bert	Displays internal T3 bit error rate test results.
brief	Displays summary information for the T1 controller.
internal-state	Displays internal T3 state information.
tabular	Displays T3 controller information in tabular format.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
interface	read

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows sample output from the **show controllers t3** command using the **brief** keyword for a single T3 port:

```
RP/0/0/CPU0:Router# show controllers t3 0/0/3/0 brief

T30/0/3/0 is up
No alarms detected.
MDL transmission is disabled
  EIC: , LIC: , FIC: , UNIT:
  Path FI:
  Idle Signal PORT_NO:
  Test Signal GEN_NO:
FEAC code received: No code is being received
Framing is C-BIT Parity, Line Code is B3ZS, Clock Source is Internal
```

The following example shows sample output from the **show controllers t3** command using the **tabular** keyword, for a single T3 port:

```
RP/0/0/CPU0:Router# show controllers t3 0/0/3/0 tabular

T30/0/3/0 is up
No alarms detected.
MDL transmission is disabled
  EIC: , LIC: , FIC: , UNIT:
  Path FI:
  Idle Signal PORT_NO:
  Test Signal GEN_NO:
FEAC code received: No code is being received
Framing is C-BIT Parity, Line Code is B3ZS, Clock Source is Internal
INTERVAL      LCV   PCV   CCV   PES   PSES  SEFS  UAS   LES   CES   CSES
05:20-05:30    0     0     0     0     0     0     0     0     0     0
05:05-05:20    0     0     0     0     0     0     0     0     0     0
04:50-05:05    0     0     0     0     0     0     0     0     0     0
04:35-04:50    0     0     0     0     0     0     0     0     0     0
04:20-04:35    0     0     0     0     0     0     0     0     0     0
04:05-04:20    0     0     0     0     0     0     0     0     0     0
03:50-04:05    0     0     0     0     0     0     0     0     0     0
03:35-03:50    0     0     0     0     0     0     0     0     0     0
03:20-03:35    0     0     0     0     0     0     0     0     0     0
03:05-03:20    0     0     0     0     0     0     0     0     0     0
02:50-03:05    0     0     0     0     0     0     0     0     0     0
```

The following example shows sample output from the **show controllers t3** command for a single T3 port:

```
RP/0/0/CPU0:Router# show controllers t3 0/0/3/0

T30/0/3/0 is up
No alarms detected.
MDL transmission is disabled
  EIC: , LIC: , FIC: , UNIT:
  Path FI:
  Idle Signal PORT_NO:
  Test Signal GEN_NO:
FEAC code received: No code is being received
Framing is C-BIT Parity, Line Code is B3ZS, Clock Source is Internal
Data in current interval (695 seconds elapsed):
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation, 0 P-bit Err Secs
  0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
  0 Unavailable Secs, 0 Line Errored Secs
  0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

Data in Interval 1:
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation, 0 P-bit Err Secs
  0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
  0 Unavailable Secs, 0 Line Errored Secs
  0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
Data in Interval 2:
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation, 0 P-bit Err Secs
  0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
  0 Unavailable Secs, 0 Line Errored Secs
  0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
Data in Interval 3:
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation, 0 P-bit Err Secs
  0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
  0 Unavailable Secs, 0 Line Errored Secs
  0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
.
.
.

```

Table 73 describes the significant fields shown in the display.

Table 73 *show controllers t3 Field Descriptions*

Field	Description
T30/0/3/0 is up	T3 channel is operating. The channel state can be up, down, or administratively down. Loopback conditions are shown by (Locally Looped) or (Remotely Looped).
No alarms detected	Any alarms detected by the controller are displayed here. Possible alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver is getting AIS. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms.
MDL transmission	Status of the Maintenance Data Link (either enabled or disabled) and the values of the MDL message fields.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 73** *show controllers t3 Field Descriptions (continued)*

Field	Description
FEAC code received	Whether or not a far-end alarm code request is being received. Possible values are as follows: • DS3 Eqpt. Failure (SA) • DS3 LOS/HBER • DS3 Out-of-Frame • DS3 AIS Received • DS3 IDLE Received • DS3 Eqpt. Failure (NSA) • Common Eqpt. Failure (NSA) • Multiple DS1 LOS/HBER • DS1 Eqpt. Failure • Single DS1 LOS/HBER • DS1 Eqpt. Failure (NSA) • No code is being received
Framing	Framing type on the channelized controller. Values are M23 and C-Bit.
Line Code	Line coding format on the channelized controller.
Clock Source	Clock source on the channelized controller. Values are internal and line.
Data in current interval (seconds elapsed)	Shows the current accumulation period, which rolls into the 24-hour accumulation every 15 minutes. The accumulation period is from 1 to 900 seconds. The oldest 15-minute period falls off the back of the 24-hour accumulation buffer.
Line Code Violations	Line Code Violations (LCVs) is a count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) that occur over the accumulation period. An EXZ increments the LCV by one regardless of the length of the zero string.
P-bit Coding Violation	For all DS3 applications, a P-bit coding violation (PCV) error event is a P-bit parity error event. A P-bit parity error event is the occurrence of a received P-bit code on the DS3 M-frame that is not identical to the corresponding locally calculated code.
C-bit Coding Violation	For C-bit parity and SYNTRAN DS3 applications, the C-bit coding violation (CCV) is the count of coding violations reported by the C-bits. For C-bit parity, it is the count of CP-bit parity errors that occur during the accumulation interval. For SYNTRAN, it is a count of CRC-9 errors that occur during the accumulation interval.
P-bit Err Secs	P-bit errored seconds (PES) is a second with one or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge does not increment when unavailable seconds are counted.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 73** *show controllers t3 Field Descriptions (continued)*

Field	Description
P-bit Severely Err Secs	P-bit severely errored seconds (PSES) is a second with 44 or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge does not increment when unavailable seconds are counted.
Severely Err Framing Secs	Severely errored framing seconds (SEFS) is a second with one or more out-of-frame defects or a detected incoming AIS.
Unavailable Secs	The number of unavailable seconds (UAS) is calculated by counting the number of seconds for which the interface is unavailable. For more information, see RFC 1407, <i>DS3 MIB Variables</i> .
Line Errored Secs	Line errored seconds (LES) is a second in which one or more code violations or one or more LOS defects occurred.
C-bit Errored Secs	C-bit errored seconds (CES) is a second with one or more C-bit code violations (CCV), one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.
C-bit Severely Errored Secs	C-bit severely errored seconds (CSES) is a second with 44 or more CCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.
Total Data (last 24 hours)	Shows the last 15-minute accumulation period.

Related Commands

Command	Description
controller t3	Configures a T3 controller and enters T3 configuration mode.

R3.5.0 Beta Draft—Cisco Confidential Information

shutdown (T1/E1)

To disable the T1 or E1 controller, use the **shutdown** command in T1 or E1 configuration mode. To restart a disabled T1 or E1 controller, use the **no** form of this command.

shutdown

no shutdown

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes T1 configuration
E1 configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Shutting down the T1 or E1 controller disables all functions on the interface and sends an AIS alarm to the network. The **shutdown** command marks the interface as unavailable. To check if the controller is disabled, use the **show controllers t1** or **show controllers e1** command.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples The following example shows how to bring up a controller that was previously shut down:

```
RP/0/0/CPU0:Router(config)# controller t1 0/6/0/0/10
RP/0/0/CPU0:Router(config-t1e1)# no shutdown
```

Related Commands

R3.5.0 Beta Draft—Cisco Confidential Information

Command	Description
show controllers e1	Displays information about the E1 links and hardware and software drivers for the E1 controllers.
show controllers t1	Displays information about the T1 links and hardware and software drivers for the T1 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

shutdown (T3/E3)

To disable a T3 or E3 controller, use the **shutdown** command in T3 or E3 configuration mode. To restart a disabled T3 or E3 controller, use the **no** form of this command.

shutdown

no shutdown

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes T3 configuration
E3 configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Shutting down the T3 or E3 controller disables all functions on the interface and sends an AIS alarm to the network. The **shutdown** command marks the interface as unavailable. To check if the controller is disabled, use the **show controllers t3** or **show controllers e3** command.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples The following example shows how to bring up a controller that was previously shut down:

```
RP/0/0/CPU0:Router(config)# controller t3 0/6/0/0
RP/0/0/CPU0:Router(config-t3)# no shutdown
```

Related Commands

R3.5.0 Beta Draft—Cisco Confidential Information

Command	Description
show controllers e3	Displays information about the E3 links and hardware and software drivers for the E3 controllers.
show controllers t3	Displays information about the T3 links and hardware and software drivers for the T3 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

speed (DS0)

To specify the speed of the underlying DS0s in a channel group, use the **speed** command in channel group configuration mode. To revert to the default speed, use the **no** form of this command.

speed *kbps*

no speed *kbps*

Syntax Description	<i>kbps</i>	Speed of the underlying DS0s in kilobits per second (kbps). Valid values are 56 and 64.

Defaults	The default speed is 64 kbps.

Command Modes	Channel group configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Before the channel group configuration is valid, you must define the associated DS0 time slots using the timeslots command.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples	The following example shows how to define the speed for the underlying DS0 to be 56 kbps:

```
RP/0/0/CPU0:Router(config)# controller t1 0/6/0/0/10
RP/0/0/CPU0:Router(config-t1e1)# channel-group 5
RP/0/0/CPU0:Router(config-t1e1-channel_group)# speed 56
```

Related Commands

R3.5.0 Beta Draft—Cisco Confidential Information

Command	Description
timeslots	Associates one or more DS0 time slots to the channel group.
channel-group	Configures a channel group and enters channel group configuration mode.

R3.5.0 Beta Draft—Cisco Confidential Information

timeslots

To associate one or more DS0 time slots to a channel group and create an associated serial subinterface, use the **timeslots** command in channel group configuration mode. To unassign the DS0 time slots and delete the associated serial interface, use the **no** form of this command.

timeslots *range*

no timeslots

Syntax Description	<i>range</i>	One or more DS0 time slots separated by colons, or ranges of DS0 time slots belonging to the channel group separated by a hyphen, with no spaces. For example, time slot 1, 11, 16, 17, 18 is represented by 1:11:16-18 . For T1, DS0 time slots range from 1 to 24. For E1, DS0 time slots range from 1 to 31.

Defaults	No default behavior or values

Command Modes	Channel group configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	The time slot range must match the DS0 time slots assigned to the channel group. The service provider defines the DS0 time slots that compose a channel group.
	Before the channel group configuration is valid, you must define the associated DS0 time slots using the timeslots command.

Task ID	Task ID	Operations
	sonet-sdh	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to associate DS0 time slots 1, 6, 8, 9 and 10 to channel group 5:

```
RP/0/0/CPU0:Router(config)# controller t1 0/6/0/0/10  
RP/0/0/CPU0:Router(config-t1e1)# channel-group 5  
RP/0/0/CPU0:Router(config-t1e1-channel_group)# timeslots 1:6:8-10
```

Related Commands

Command	Description
framing (E1)	Specifies the frame type for the E1 data line.
framing (T1)	Specifies the frame type for the T1 data line.
speed (DS0)	Specifies the speed of the underlying DS0s in a channel group.
channel-group	Configures a channel group and enters channel group configuration mode.

R3.5.0 Beta Draft—Cisco Confidential Information

yellow

To enable detection and generation of T1 yellow alarms, use the **yellow** command in T1 configuration mode. To disable detection and generation of T1 yellow alarms, use the **no** form of this command.

yellow {**detection** | **generation**} {**disable** | **enable**}

no yellow {**detection** | **generation**} {**disable** | **enable**}

Syntax Description

detection	Detects yellow alarms.
generation	Generates yellow alarms.
disable	Disables detection or generation of T1 yellow alarms.
enable	Enables detection or generation of T1 yellow alarms.

Defaults

Yellow alarms are detected and generated on the T1 channel.

Command Modes

T1 configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If the T1 framing type is super frame (SF), you should consider disabling yellow alarm detection because the yellow alarm can be incorrectly detected with SF framing.

The default state of the **yellow** command is enabled. If you disable yellow alarm detection and want to reenable it, you can use the **no** form of the command. Alternatively, you can use the **enable** keyword.

The **yellow** command is only applicable to T1 lines.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to disable yellow alarm generation:

```
RP/0/0/CPU0:Router(config)# controller t1 0/6/0/0/10
RP/0/0/CPU0:Router(config-t1e1)# yellow generation disable
```




Dense Wavelength Division Multiplexing Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

This module describes the commands to configure dense wavelength division multiplexing (DWDM) controller interfaces on routers supporting Cisco IOS XR software.

For information on 10-Gigabit Ethernet (GE) interface commands refer to *Ethernet Interface Commands on Cisco IOS XR Software*. For information on Packet-over-SONET/SDH (POS) interface commands, refer to *Packet-over-SONET User Interface and SONET Layer 1 Commands on Cisco IOS XR Software*.

R3.5.0 Beta Draft—Cisco Confidential Information

controller dwdm

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

controller dwdm *instance*

no controller dwdm *instance*

Syntax Description	<i>instance</i> Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. <i>port</i>: Physical port number of the interface. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults	No default behavior or values

Command Modes	Global configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	interface	read, write

Examples	The following example shows how to configure a DWDM controller in Slot 6:

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

R3.5.0 Beta Draft—Cisco Confidential Information**Related Commands**

Command	Description
show controller dwdm	Displays the optical parameters, G.709 alarms and counters, and register and module information.

R3.5.0 Beta Draft—Cisco Confidential Information

g709 bdi-to-client-gais

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

g709 bdi-to-client-gais enable

no g709 bdi-to-client-gais enable

Syntax Description	enable	Indicates that the DWDM controller will be disabled if a BDI is received on this interface.

Defaults	By default, no GAIS to client is inserted.

Command Modes	DWDM configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. The g709 bdi-to-client-gais command is available on the 10-GE DWDM PLIM only.

Task ID	Task ID	Operations
	interface	read, write

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

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

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	no g709 disable	Enables the G.709 wrapper on the controller.
	show controller dwdm	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

R3.5.0 Beta Draft—Cisco Confidential Information

g709 disable

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

g709 disable

no g709 disable

Syntax Description This command has no arguments or keywords.

Defaults The G.709 wrapper is enabled.

Command Modes DWDM configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

Task ID	Task ID	Operations
	interface	read, write

Examples The following example shows how to disable the G.709 wrapper on an interface:

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

Related Commands	Command	Description
	g709 fec	Configures FEC mode on the controller.
	show controller dwdm g709	Displays the optical parameters, G.709 alarms and counters, and register and module information.

R3.5.0 Beta Draft—Cisco Confidential Information

g709 fec

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

g709 fec {disable | standard}

no g709 fec {disable | standard}

Syntax Description

disable	Disables FEC.
standard	Enables standard FEC mode.

Defaults

Enhanced FEC mode is enabled by default.

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **g709 fec** command can be used only when the DWDM controller is in the shutdown state. The G.709 wrapper must be enabled to enable forward error correction (FEC) mode on the controller.

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



Note

The OC-768c/STM-256c DWDM PLIM supports enhanced FEC mode only. Disabling FEC or enabling standard FEC is not supported.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure standard FEC mode on a DWDM controller:

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

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	no g709 disable	Enables the G.709 wrapper on the controller.
	show controllers dwdm g709	Displays the FEC mode.

R3.5.0 Beta Draft—Cisco Confidential Information

g709 odu report

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

g709 odu report {ais | bdi | lck | oci | ptim} disable

no g709 odu report [ais | bdi | lck | oci | ptim] [disable]

Syntax Description

ais	Alarm indication signal reporting status.
bdi	Backward defect indication reporting status.
lck	Upstream connection locked reporting status.
oci	Open connection indication error reporting status.
ptim	Payload type identifier mismatch reporting status.

Defaults

Reporting is enabled for all keywords.

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to disable ODU reporting for OCI:

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

Related Commands

R3.5.0 Beta Draft—Cisco Confidential Information

Command	Description
show controller dwdm g709	Displays the G.709 alarms and counters.

R3.5.0 Beta Draft—Cisco Confidential Information

g709 otu overhead tti

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

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

no g709 otu overhead tti {expected | sent} {ascii | hex} *tti-string*

Syntax Description

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

Defaults

No TTI string is configured

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
interface	read, write

Examples

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

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

Related Commands

Command	Description
show controller dwdm g709	Displays the TTI strings.

R3.5.0 Beta Draft—Cisco Confidential Information

g709 otu report

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

g709 otu report {bdi | fecmismatch | iae | lof | lom | los | sd-ber | sf-ber} disable

no g709 otu report [bdi | iae | lof | lom | los | sd-ber | sf-ber] [disable]

Syntax Description	bdi	Backward defect indication reporting status.
	fecmismatch	FEC mismatch alarm reporting status.
	iae	Incoming alignment error reporting status.
	lof	OTU loss of frame reporting status.
	lom	Loss of multiple frame reporting status.
	los	Loss of signal reporting status.
	sd-ber	SM bit error rate (BER) is in excess of the signal degradation BER threshold.
	sf-ber	SM BER is in excess of the signal failure BER threshold.
	disable	Specifies to disable the reporting of the specified trigger.

Defaults Reporting is enabled for all keywords.

Command Modes DWDM configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	interface	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

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

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

Related Commands

Command	Description
show controller dwdm g709	Displays the G.709 alarms and counters.

R3.5.0 Beta Draft—Cisco Confidential Information

g709 odu threshold

To configure thresholds for selected optical channel data unit (ODU) bit error rate (BER) alarms, use the **g709 odu threshold** command in DWDM configuration mode. To return to the default state, use the **no** form of this command.

g709 odu threshold {**pm-tca** | **sd-ber** | **sf-ber**} *bit-error-rate*

no g709 odu threshold {**pm-tca** | **sd-ber** | **sf-ber**} *bit-error-rate*

Syntax Description	pm-tca	Path monitoring threshold crossing alert.
	sd-ber	Signal degradation bit error rate (BER).
	sf-ber	Signal failure BER above threshold.
	<i>bit-error-rate</i>	Specifies the BER threshold value in the range from 3 through 9. The threshold value is interpreted as a negative exponent of 10 when determining the bit error rate. For example, a value of 5 implies a bit error rate of 10 to the minus 5. The default BER threshold value is 6.

Defaults bit-error-rate: 6

Command Modes DWDM configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	interface	R/W

Examples The following example shows how to set the signal fail BER rate to be 5:

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

R3.5.0 Beta Draft—Cisco Confidential Information**Related Commands**

Command	Description
show controller dwdm g709	Displays the G.709 alarms and counters.

R3.5.0 Beta Draft—Cisco Confidential Information

g709 otu threshold

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

g709 otu threshold {sd-ber | sf-ber} bit-error-rate

no g709 otu threshold {sd-ber | sf-ber} bit-error-rate

Syntax Description	sd-ber	Signal degradation bit error rate (BER).
	sf-ber	Signal failure BER above threshold.
	<i>bit-error-rate</i>	Specifies the BER threshold value in the range from 3 through 9. The threshold value is interpreted as a negative exponent of 10 when determining the bit error rate. For example, a value of 5 implies a bit error rate of 10 to the minus 5. The default BER threshold value is 6.

Defaults	bit-error-rate: 6

Command Modes	DWDM configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	interface	R/W

Examples	The following example shows how to set the signal fail BER rate to be 5:

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


R3.5.0 Beta Draft—Cisco Confidential Information**Related Commands**

Command	Description
show controller dwdm g709	Displays the G.709 alarms and counters.

R3.5.0 Beta Draft—Cisco Confidential Information

laser

To turn the laser associated with the DWDM controller off, use the **laser** command in DWDM configuration mode. To turn the laser back on, use the **no** form of this command.

laser off

no laser off

Syntax Description	off Turns the laser off.

Defaults	The laser is on by default.

Command Modes	DWDM configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

The laser cannot be turned on if the controller is in the shutdown state in a non-G.709 mode or if the controller is in internal loopback mode.

Examples	In the following example, the laser is turned off:

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RP0/CPU0:router(config-dwdm)# laser off
```

R3.5.0 Beta Draft—Cisco Confidential Information

loopback (DWDM)

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

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

no loopback {**internal** | **line**}

Syntax Description

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

Defaults

This command is disabled by default.

Command Modes

DWDM configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

Examples

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

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

R3.5.0 Beta Draft—Cisco Confidential Information

pm fec report

To enable threshold crossing alert (TCA) generation on the FEC layer, use the **pm fec report** command in DWDM configuration mode. To disable TCAs, use the **no** form of this command.

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

no pm {15-min | 24-hour} fec report {ec-bits | uc-words} enable

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

Defaults TCA is not enabled.

Command Modes DWDM configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	interface	read, write

Examples The following example shows how to enable TCAs on the FEC layer reporting for uncorrectable words:

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

Related Commands

R3.5.0 Beta Draft—Cisco Confidential Information

Command	Description
show controller dwdm pm fec	Displays performance measurement information for the FEC layer.

R3.5.0 Beta Draft—Cisco Confidential Information

pm fec threshold

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

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

no pm {15-min | 24-hour} fec threshold {ec-bits | uc-words} threshold

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

Defaults No threshold is configured.

Command Modes DWDM configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	interface	read, write

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

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

Related Commands

R3.5.0 Beta Draft—Cisco Confidential Information

Command	Description
show controller dwdm pm fec	Displays performance measurement information for the FEC layer.

R3.5.0 Beta Draft—Cisco Confidential Information

pm optics report

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

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

no pm {15-min | 24-hour} optics report {lbc | opr | opt} {max-tca | min-tca} enable

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

Defaults TCA reporting is not enabled.

Command Modes DWDM configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	interface	read, write

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

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


R3.5.0 Beta Draft—Cisco Confidential Information

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

Related Commands	Command	Description
	show controller dwdm pm optics	Displays performance measurement information for the optics layer.

R3.5.0 Beta Draft—Cisco Confidential Information

pm optics threshold

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

pm {15-min | 24-hour} optics threshold {lbc | opr | opt} {max | min} threshold

no pm {15-min | 24-hour} optics threshold {lbc | opr | opt} {max | min} threshold

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

Defaults No thresholds are configured.

Command Modes DWDM configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	interface	read, write

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

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

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show controller dwdm pm optics	Displays performance measurement information for the optics layer.

R3.5.0 Beta Draft—Cisco Confidential Information

pm otn report

To enable threshold crossing alert (TCA) generation on the optical transport network (OTN) layer, use the **pm otn report** command in DWDM configuration mode. To disable TCA reporting, use the **no** form of this command.

pm {15-min | 24-hour} otn report otn-parameter enable

no pm {15-min | 24-hour} otn report otn-parameter enable

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

R3.5.0 Beta Draft—Cisco Confidential Information

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

enable	Enables TCA generation for the specified parameter on the DWDM controller.

Defaults

TCA generation is not enabled.

R3.5.0 Beta Draft—Cisco Confidential Information

Command Modes DWDM configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	interface	read, write

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

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

Related Commands	Command	Description
	show controller dwdm pm otn	Displays performance measurement information for the OTN layer.

R3.5.0 Beta Draft—Cisco Confidential Information

pm otn threshold

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

pm {15-min | 24-hour} otn threshold *otn-parameter threshold*

no pm {15-min | 24-hour} otn report *otn-parameter threshold*

Syntax Description	15-min	Configures performance monitoring thresholds for 15-minute intervals.
	24-hour	Configures performance monitoring thresholds for 24-hour intervals.
	<i>otn-parameter</i>	Specific parameter for which to configure the threshold. OTN parameters can be as described in pm otn report, page 508 .
	<i>threshold</i>	Threshold for the performance monitoring parameter.

Defaults	No thresholds are configured.

Command Modes	DWDM configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	interface	read, write

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

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

Related Commands

R3.5.0 Beta Draft—Cisco Confidential Information

Command	Description
show controller dwdm pm otn	Displays performance measurement information for the OTN layer.

R3.5.0 Beta Draft—Cisco Confidential Information

rx-los-threshold

To configure the transponder receive power threshold on a OC-768c/STM-256c DWDM controller, use the **rx-los-threshold** command in DWDM configuration mode. To return the transponder receive power threshold to its default value, use the **no** form of this command.

rx-los-threshold *power-level*

no rx-los-threshold *power-level*

Syntax Description	<i>power-level</i>	Receive power level in units of 0.1 dBm. Values can range from -200 to 0, which corresponds to a LOS threshold range of -20 dBm to 0 dBm.

Defaults	<i>power-level</i> : -18 dBm

Command Modes	DWDM configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1 and is supported only on the OC-768c/STM-256c DWDM PLIM.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	The controller must be in the shutdown state before you can use the rx-los-threshold command.
	The rx-los-threshold command is applicable only to the OC-768c/STM-256c DWDM PLIM.

Task ID	Task ID	Operations
	interface	read, write

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

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

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show controller dwdm	Displays the optical parameters, G.709 alarms and counters, and register and module information.
	transmit-power	Configures the DWDM optics transmit laser power on a DWDM controller.

R3.5.0 Beta Draft—Cisco Confidential Information

show controller dwdm

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

show controller dwdm *instance* [**g709** [**registers**] | **optics** [**registers**] | **wavelength-map**]

Syntax Description

<i>instance</i>	Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. <i>port</i>: Physical port number of the interface. For more information about the syntax for the router, use the question mark (?) online help function.
g709	Displays the G.709 OTN protocol alarms and counters for bit errors, along with the FEC statistics and threshold-based alerts.
optics	Displays optical related information about the interface, such as output power level and wavelength.
registers	For g709 , displays platform-specific OTN framer registers; for optics , displays transponder registers.
wavelength-map	Displays the wavelength information.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	The display of the TTI strings was added.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.5.0 Beta Draft—Cisco Confidential Information**Task ID****Task ID Operations**

interface	read

Examples

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

```
RP/0/RP0/CPU0:Router# show controller dwdm 0/6/0/0
Port dwdm0/1/0/0
```

```
Controller State: admin-down
```

```
Loopback: None
```

```
G709 Status
```

```
OTU
```

LOS = 1	LOF = 0	LOM = 0
BDI = 0	IAE = 0	BIP = 0
BEI = 0		

```
ODU
```

AIS = 1	BDI = 0	OCI = 0
LCK = 0	BIP = 79681	BEI = 199574
PTIM = 0		

```
FEC Mode: Standard FEC
```

```
EC(per second rate) = 0                      UC = 0
```

```
Remote FEC Mode: Standard FEC
```

```
FECMISMATCH = 0
```

```
Detected Alarms: None
```

```
Asserted Alarms: None
```

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

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

```
OTU TTI Sent        String ASCII: test OTU 5678
```

```
OTU TTI Received String ASCII: test OTU 5678
```

```
OTU TTI Expected String ASCII: test OTU 5678
```

```
Optics Status
```

```
Optics Type: 10Gb MSA WDM (65km)
```

```
Wavelength Band: C-Band, MSA ITU Channel = 10, Frequency = 195.65 THz,
```

```
Wavelength = 1532.290 nm
```

```
TX Power = 3.49 dBm
```

```
RX Power = -11.64 dBm
```

Table 74 describes selected fields from the **show controllers dwdm** command output.

Table 74 show controllers dwdm g709 Command Output Fields

Field	Description
Controller State	Status of the controller.
Loopback	Loopback status—indicates whether loopback is enable or not and which time of loopback is enabled.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 74** *show controllers dwdm g709 Command Output Fields (continued)*

Field	Description
OTU	Optical transport unit overhead alarms.
LOS	Number of OTU loss of signal (LOS) alarms. The LOS threshold is set using the rx-los-threshold command. If the receive optical power is less than or equal to this defined threshold, the optical LOS alarm is raised.
LOF	Number of OTU loss of frame (LOF) alarms.
LOM	Number of OTU loss of multiframe (LOM) alarms.
AIS	Number of alarm indication signal (AIS) alarms. AIS is a signal sent downstream as an indication that an upstream defect has been detected.
BDI	Number of backward defect indication (BDI) alarms. The BDI is a single bit that conveys information regarding signal failure in the upstream direction.
IAE	Number of incoming alignment errors (IAE).
BIP	Number of bit interleaved parity alarms. The BIP is comprised of one byte and is used for error detection. It is computed over the entire optical channel payload unit (OPU).
ODU	Optical channel data unit alarms.
OCI	Number of open connection indication alarms. OCI is a signal sent downstream as an indication that upstream the signal is not connected to a trail termination source.
LCK	Number of upstream connection locked alarms. LCK is a signal sent downstream as an indication that upstream the connection is locked, and no signal is passed through.
PTIM	Number of payload type identifier mismatch alarms. This occurs when there is a mismatch between the way the ITU-T G.709 option is configured on the PLIM at each end of the optical span.
FEC Mode	Indicates the forward error correction (FEC) mode for the controller. This can be disabled, enhanced, or standard.
EC	Corrected code words. This is the number of words corrected by the FEC and is displayed as a per second rate.
UC	Uncorrectable code words. This is a raw counter.
Detected Alarms	Alarms detected by the hardware.
Asserted Alarms	Alarms indicated to be reported by the user.
Alarm reporting enabled for	Lists the alarms that are enabled for reporting.
BER thresholds	Values of the configured bit error rate thresholds.
OTU TTI Sent	Value of the transmit trail trace identifier (TTI).
OTU TTI Received	Value of the received TTI.
OTU TTI Expected	Value of the expected TTI.

See [Table 75](#) for a description of the optics fields.

R3.5.0 Beta Draft—Cisco Confidential Information

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

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

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

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

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

Optics Status

```

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

```

[Table 75](#) describes selected fields from the **show controllers dwdm** command output with the **optics** keyword.

Table 75 show controllers dwdm optics Command Output Fields

Field	Description
Optics Type	Indicates the optics type: GE or OC-768c/STM-256c DWDM.
Clock Source	Indicates whether the clock is internal or line.
Wavelength Band	Indicates the wavelength band: C-band, L-band.
MSA ITU Channel	Multi Source Agreement (MSA) ITU channel number.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 75** *show controllers dwdm optics Command Output Fields (continued)*

Field	Description
Frequency	Frequency of the channel in terahertz.
Wavelength	Wavelength corresponding to the channel number in nanometers.
TX power	Value of the transmit power level. This is user configurable on the OC-768c/STM-256c DWDM PLIM using the transmit-power command.
RX Power	Actual optical power at the RX port.
RX LOS Threshold	Receive loss of signal threshold. This is user configurable on the OC-768c/STM-256c DWDM PLIM using the rx-los-threshold command. If the receive optical power is less than or equal to this define threshold, the optical LOS alarm is raised.

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

```
RP/0/RP0/CPU0:Router# show controller dwdm 0/0/0/0 wavelength-map
```

```
Wavelength band: C-band
```

```
MSA ITU channel range supported: 3~82
```

```
Wavelength map table
```

```
-----
channel frequency      wavelength
Num      (THz)         (nm)
-----
03        196.00        1529.55
-----
04        195.95        1529.94
-----
05        195.90        1530.33
-----
06        195.85        1530.72
-----
07        195.80        1531.12
-----
08        195.75        1531.51
-----
09        195.70        1531.90
-----
10        195.65        1532.29
.
.
.
```

[Table 76](#) describes selected fields from the **show controllers dwdm** command output with the **wavelength-map** keyword.

Table 76 *show controllers dwdm wavelength Command Output Fields*

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

■ show controller dwdm

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	rx-los-threshold	Configures the transponder receive power threshold on a DWDM controller.

R3.5.0 Beta Draft—Cisco Confidential Information

show controller dwdm pm

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

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

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

Syntax Description		
	<i>instance</i>	Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. <i>port</i>: Physical port number of the interface. For more information about the syntax for the router, use the question mark (?) online help function.
	history	Displays all performance monitoring data.
	interval	Displays specific performance monitoring data in a particular interval.
	15-min	Displays performance monitoring data in a 15-minute interval.
	24-hour	Displays performance monitoring data in a 24-hour interval.
	fec	Displays FEC performance parameters, such as bit errors corrected (BIEC) and uncorrectable words.
	optics	Displays optics performance parameters, such as optical power.
	otn	Displays OTN performance parameters, such as path monitoring failure counts (FC-PM) and section monitoring unavailable seconds (UAS-SM).
	<i>index</i>	Interval for which to display the performance monitoring information.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID**Task ID Operations**

Task ID	Operations
interface	read

Examples

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

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

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

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

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

R3.5.0 Beta Draft—Cisco Confidential Information

Table 77 describes selected fields from the **show controllers dwdm pm** command output.

Table 77 *show controllers dwdm pm Command Output Fields*

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

R3.5.0 Beta Draft—Cisco Confidential Information**Table 77** *show controllers dwdm pm Command Output Fields (continued)*

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

R3.5.0 Beta Draft—Cisco Confidential Information

shutdown (DWDM)

To disable DWDM controller processing, use the **shutdown** command in DWDM configuration mode. To bring a DWDM controller back up and enable DWDM controller processing, use the **no** form of this command.

shutdown

no shutdown

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values

Command Modes	DWDM configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

The DWDM controller is enabled by default. You must use the **shutdown** command to disable the controller and configure it in DWDM configuration mode.

Task ID	Task ID	Operations
	interface	read, write

Examples	In the following example, the DWDM controller is brought down and DWDM controller processing is disabled:

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/3/0/2
RP/0/RP0/CPU0:router(config-dwdm)# shutdown
```

R3.5.0 Beta Draft—Cisco Confidential Information

transmit-power

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

transmit-power *power-level*

no transmit-power *power-level*

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

Defaults	power-level: 0 dBm

Command Modes	DWDM configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1 and is supported only on the OC-768c/STM-256c DWDM PLIM.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	The controller must be in the shutdown state before you can use the transmit-power command. You can configure the transponder transmit power only on the OC-768c/STM-256c DWDM PLIM.

Task ID	Task ID	Operations
	interface	read, write

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

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

R3.5.0 Beta Draft—Cisco Confidential Information**Related Commands**

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

R3.5.0 Beta Draft—Cisco Confidential Information

wavelength

To configure the starting wavelength on a DWDM controller, use the **wavelength** command in DWDM configuration mode. To return the wavelength to its default value, use the **no** form of this command.

wavelength *channel-number*

no wavelength *channel-number*

Syntax Description	<i>channel-number</i>	ITU channel number that is an integer between 1 and 83 for the C-band and between 106 and 185 for the L-band.

Defaults	OC-768c/STM-256c DWDM PLIM, C-band: 1 10-GE PLIM, C-band: 3 10-GE PLIM, L-band: 106

Command Modes	DWDM configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

The wavelength should be specified. It is represented by a channel number in the Multi Source Agreement (MSA) ITU grid. The default channel number for the 10-GE PLIM, C-band is 3, which corresponds to a frequency of 196.00 THz and wavelength of 1529.553 nm. The default channel number for the 10-GE PLIM, L-band is 106, which corresponds to a frequency of 190.85 THz and wavelength of 1570.83 nm. The default channel number for the OC-768c/STM-256c DWDM PLIM, C-band is 1, which corresponds to a frequency of 196.10 and a wavelength of 1528.773.

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

The controller must be in the shutdown state before you can use the **wavelength** command.

Task ID	Task ID	Operations
	interface	read, write

R3.5.0 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to configure the starting wavelength to the tenth wavelength:

```
RP/0/RP0/CPU0:Router(config)# controller dwdm 0/0/0/0
RP/0/RP0/CPU0:Router(config-dwdm)# wavelength 10
```

Related Commands

Command	Description
show controller dwdm wavelength-map	Displays the valid channel number, frequency, and wavelength information for the controller.

■ wavelength

R3.5.0 Beta Draft—Cisco Confidential Information



10-Gigabit Ethernet WAN Physical Controller Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

This module describes the commands to configure a 10-Gigabit Ethernet WAN physical controller on Cisco CRS-1 routers supporting Cisco IOS XR software.

For information on 10-Gigabit Ethernet (GE) interface commands see the *Ethernet Interface Commands on Cisco IOS XR Software* module.

R3.5.0 Beta Draft—Cisco Confidential Information

clear controller wanphy

To clear the alarms counters for a specific 10-Gigabit Ethernet WAN physical controller, use the **clear controller wanphy** command in EXEC mode.

clear controller wanphy *interface-id* **stats**

Syntax Description	<i>interface-id</i>	Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. <i>port</i>: 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 physical controller.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the Cisco CRS-1.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	interface	read, write, execute

Examples The following example shows how to configure a 10-Gigabit Ethernet WAN physical controller in Slot 6:

```
RP/0/RP0/CPU0:Router # clear controller wanphy 0/6/0/0 stats
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show controllers wanphy	Displays alarms, registers, and module information for a 10-Gigabit Ethernet WAN physical controller.
	clear controller wanphy	

R3.5.0 Beta Draft—Cisco Confidential Information

controller wanphy

To enter WAN physical controller configuration mode in which you can configure a 10-Gigabit Ethernet WAN physical controller, use the **controller wanphy** command in global configuration mode. To return the 10-Gigabit Ethernet WAN physical controller to its default configuration, use the **no** form of this command.

controller wanphy *interface-id*

no controller wanphy *interface-id*

Syntax Description	<i>interface-id</i>	Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. <i>port</i>: Physical port number of the interface. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults	No default behavior or values

Command Modes	Global configuration

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the Cisco CRS-1.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

**Note**

After you use the **no controller wanphy** command to return a 10-Gigabit Ethernet WAN physical controller to its default configuration, you need to use the **hw-module subslot reload** command to reload the Cisco IOS XR software on the 10-Gigabit Ethernet WAN SPA for the mode configuration changes to take affect.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	interface	read, write

Examples

The following example shows how to configure a 10-Gigabit Ethernet WAN physical controller in slot 6:

```
RP/0/RP0/CPU0:Router # configure
RP/0/RP0/CPU0:Router(config)# controller wanphy 0/6/0/0
```

Related Commands	Command	Description
	lanmode on	Configures a 10-Gigabit Ethernet WAN physical controller to run in LAN mode, or returns a 10-Gigabit Ethernet WAN physical controller to run in the default WAN mode.
	show controllers wanphy	Displays alarms, registers, and module information for a 10-Gigabit Ethernet WAN physical controller.

R3.5.0 Beta Draft—Cisco Confidential Information

lanmode on

To configure a 10-Gigabit Ethernet WAN physical controller to run in LAN mode, use the **lanmode on** command in WAN physical controller configuration mode. To return the controller to its default WAN state, use the **no** form of this command.

lanmode on

no lanmode on

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes WAN physical controller configuration

Release	Modification
Release 3.5.0	This command was introduced on the Cisco CRS-1.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Operations
interface	read, write

Examples The following example shows how to enable LAN mode on a 10-Gigabit Ethernet WAN physical controller:

```
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)# RP/0/RP0/CPU0:srt-crs1(config-wanphy)# lanmode on
```

Changing Mode requires a hw-module subslot <x/y/z> reload

The following example shows how to disable LAN mode on a 10-Gigabit Ethernet WAN physical controller and return that controller to the default WAN 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)# RP/0/RP0/CPU0:srt-crs1(config-wanphy)# no lanmode on
```

Changing Mode requires a hw-module subslot <x/y/z> reload

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands ^{SR}	Command	Description
	show controllers wanphy	Displays alarms, registers, and module information for a 10-Gigabit Ethernet WAN physical controller.

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers wanphy

To display alarms, registers, and module information for a 10-Gigabit Ethernet WAN physical controller, use the **show controllers wanphy** command in EXEC mode.

show controller wanphy *interface-id* [**alarms** | **all** | **registers**]

Syntax Description	<i>interface-id</i>	Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. • <i>rack</i>: Chassis number of the rack. • <i>slot</i>: Physical slot number of the line card. • <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. • <i>port</i>: 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 physical controller.
	all	Displays registers, alarms, and module information for the specified 10-Gigabit Ethernet WAN physical controller.
	registers	Displays registers for the specified 10-Gigabit Ethernet WAN physical controller.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the Cisco CRS-1.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	interface	read

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows sample output from the **show controllers wanphy** command with the **all** keyword:

```
RP/0/RP0/CPU0:srt-crs1# 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 78 describes the significant fields shown in the display.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 78** show controllers wanphy Command Output Fields

Field	Description
Interface	Identifies the WAN physical interface, in the format <i>rack/slot/module/port</i>. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. <i>port</i>: 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.
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.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 78** *show controllers wanphy Command Output Fields (continued)*

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).
WIS ALARMS	Displays the following WAN Interconnect Sublayer (WIS) layer alarms: • SER—Number of Severely Errored Seconds (SER) errors • FELCDP—Number of FELCDP errors • FEAISP—Number of FEAISP errors • WLOS—Number of WLOS errors • PLCD—Number of PLCD errors • LFEBIP—Number of LFEBIP errors • PBEC—Number of PBEC errors
Active Alarms[All defects]	Total number of active alarms on this interface.
Active Alarms[Highest Alarms]	Total number of critical active alarms on this interface.
Rx(K1/K2)	Total number of errored K1/K2 bytes from the Line OverHead (LOH) of the SONET frame that were received by this interface.
Tx(K1/K2)	Total number of errored K1/K2 bytes from the Line OverHead (LOH) of the SONET frame that were transmitted by this interface.
S1S0	Number of errored payload pointer bytes on this interface.
C2	Number of errored STS identifier (C1) bytes on this interface.
PATH TRACE BUFFER	Current status of the path trace buffer.
Remote IP addr	IP address of the remote end of this connection.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 78** *show controllers wanphy Command Output Fields (continued)*

Field	Description
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.
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—Total number of path errors received on the path's J1 0 connector. • J1-Rx1—Total number of errors received on the J1-RX1 connector. • J1-Rx2—Total number of errors received on the J1-RX2 connector. • J1-Rx3—Total number of errors received on the J1-RX3 connector. • J1-Rx4—Total number of errors received on the J1-RX4 connector. • J1-Rx5—Total number of errors received on the J1-RX5 connector. • J1-Rx6—Total number of errors received on the J1-RX6 connector. • J1-Rx7—Total number of errors received on the J1-RX7 connector.
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—Current alarms on this controller.

R3.5.0 Beta Draft—Cisco Confidential Information

The following example shows sample output from the **show controllers wanphy** command with the **alarms** keyword:

```
RP/0/RP0/CPU0:srt-crs1# 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 78](#).

The following example shows sample output from the **show controllers wanphy** command with the **registers** keyword:

```
RP/0/RP0/CPU0:srt-crs1# 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 is described in [Table 78](#).

 show controllers wanphy***R3.5.0 Beta Draft—Cisco Confidential Information***

Related Commands	Command	Description
	clear controller wanphy	Clears the alarms counters for a specific 10-Gigabit Ethernet WAN physical controller.
	lanmode on	Configures a 10-Gigabit Ethernet WAN physical controller to run in LAN mode, or returns a 10-Gigabit Ethernet WAN physical controller to run in the default WAN mode.



Global Interface Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

This module describes the global interface commands that apply to all interface types. This command set lets you configure, monitor, and troubleshoot the interfaces.

R3.5.0 Beta Draft—Cisco Confidential Information

bandwidth (global)

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

bandwidth *rate*

Syntax Description

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

Defaults

The default bandwidth depends on the interface type.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

**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

The following 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
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	interface (global)	Configures an interface.
	show interfaces	Displays statistics for all interfaces configured on the router or on a specific node.

R3.5.0 Beta Draft—Cisco Confidential Information

clear interface

To clear interface statistics or packet counters, use the **clear interface** command in EXEC mode.

clear interface *type instance*

Syntax Description	<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
	<i>instance</i>	Either a physical interface instance or a virtual interface instance: - Physical interface instance. The naming notation is <i>rack/slot/module/port</i>, and a slash between values is required as part of the notation. <i>rack</i>—Chassis number of the rack. <i>slot</i>—Physical slot number of the line card or modular services card. <i>module</i>—Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>—Physical port number of the interface. Note In references to a Management Ethernet interface located on a route processor (RP) card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
interface	execute
basic-services	read, write

Examples

The following 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.
show interfaces	Displays statistics for all interfaces configured on the router or on a specific node.

R3.5.0 Beta Draft—Cisco Confidential Information

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		
<i>half-life</i>		(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.
<i>reuse</i>		(Optional) Penalty value below which a stable interface is unsuppressed. Range is from 1 through 20000. Default value is 750.
<i>suppress</i>		(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.
<i>max-suppress-time</i>		(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.

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

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

Command Modes Interface configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

The following 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	Displays the state of all interfaces (or caps nodes) on which dampening has been configured.

R3.5.0 Beta Draft—Cisco Confidential Information

interface (global)

To configure an interface or to create or configure a virtual interface, use the **interface** command in global configuration mode. To delete the interface configuration, use the **no** form of this command.

interface *type instance*

no interface *type instance*

Syntax Description	<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
	<i>instance</i>	Either a physical interface instance or a virtual interface instance: - Physical interface instance. The naming notation is <i>rack/slot/module/port</i>, and a slash between values is required as part of the notation. <i>rack</i>—Chassis number of the rack. <i>slot</i>—Physical slot number of the line card or modular services card. <i>module</i>—Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>—Physical port number of the interface. Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults No interfaces are configured

Command Modes Global configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

The **no** form of this command applies only to virtual interfaces or to subinterfaces (that is, interfaces that have been created in global configuration mode).

Task ID

Task ID	Operations
interface	read, write

Examples

In the following example, the **interface** command is given for the POS card in location 0/2/0/1, and interface configuration mode is entered for that interface:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/2/0/1
```

Related Commands

Command	Description
clear interface	Clears interface statistics or packet counters.
show interfaces	Displays statistics for all interfaces configured on the router or on a specific node.

R3.5.0 Beta Draft—Cisco Confidential Information**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

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

Defaults

The default MTU for each interface is as follows:

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

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

R3.5.0 Beta Draft—Cisco Confidential Information

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.

You can use the **show interfaces** command to determine if the MTU value has been changed.



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

Task ID

Task ID Operations

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 Name	Intf State	LineP State	Encap Type	MTU (byte)	BW (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/RP0/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 Name	Intf State	LineP State	Encap Type	MTU (byte)	BW (Kbps)
Nu0	up	up	Null	1500	Unknown
PO6/0/0/0	up	up	HDLC	1000	2488320
PO6/0/0/1	up	up	HDLC	4474	2488320
PO6/0/0/2	admin-down	admin-down	HDLC	4474	2488320
PO6/0/0/3	admin-down	admin-down	HDLC	4474	2488320
Mg0/RP0/CPU0/0	up	up	ARPA	1514	100000

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show interfaces	Displays statistics for all interfaces configured on the router or on a specific node.

R3.5.0 Beta Draft—Cisco Confidential Information

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 <i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
ifhandle <i>handle</i>	(Optional) Identifies the caps node whose Interface Manager (IM) dampening information you want to display.

Defaults

If you do not specify an interface, then the system displays brief details about all dampened interfaces.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If you do not specify an interface, then the system displays brief details about all dampened interfaces.

Task ID

Task ID	Operations
interface	read

R3.5.0 Beta Draft—Cisco Confidential Information

Examples

The following is sample 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

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
  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
  0 carrier transitions
```

Table 79 describes the significant fields shown in the display.

Table 79 *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	Time (in minutes) after which a penalty is decreased.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 79** *show im dampening Field Descriptions (continued)*

Field	Description
reuse	Penalty value below which a stable interface is unsuppressed.
suppress	Limit at which an unstable interface is suppressed when the penalty value exceeds the suppress value.
max-suppress-time	Maximum time (in minutes) that an interface can be suppressed.

Related Commands

Command	Description
dampening	Limits propagation of transient or frequently changing interface states on IM clients.
show interfaces	Displays statistics for all interfaces configured on the router or on a specific node.

R3.5.0 Beta Draft—Cisco Confidential Information

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 instance* | **all** | **local** | **location node-id**] [**accounting** | **brief** | **detail** | **summary**]

Syntax Description		
	<i>type</i>	(Optional) Specifies the type of interface for which you want to display statistics. For more information, use the question mark (?) online help function.
	<i>instance</i>	Specifies the number of the interface whose statistics you want to display. You can display statistics for a physical interface or a virtual interface: - Physical interface instance. The naming notation is <i>rack/slot/module/port</i>, and a slash between values is required as part of the notation. <i>rack</i>—Chassis number of the rack. <i>slot</i>—Physical slot number of the line card or modular services card. <i>module</i>—Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>—Physical port number of the interface. Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. 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 <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
	accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
	brief	(Optional) Displays brief information about each interface (one line per interface).

R3.5.0 Beta Draft—Cisco Confidential Information

detail	(Optional) Displays detailed information about each interface. This is the default.
summary	(Optional) Displays a summary of interface information by interface type.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	The show interfaces command field description table was updated with enhanced definitions for 5 minute output rate and 5 minute output rate.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 will be within 2 percent of the instantaneous rate of a uniform stream of traffic over that period.

Task ID

Task ID	Operations
interface	read

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following is sample 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
  0 carrier transitions
```

R3.5.0 Beta Draft—Cisco Confidential Information

Table 80 describes the significant fields shown in the display.

Table 80 *show interfaces Field Descriptions*

Field	Description
Interface name	Displays the name of the current interface. In the example, the interface name is POS0/1/0/1.
Interface state	Displays the state of the interface. In the example, the interface is in the administratively down state.
line protocol state	Displays the state of the Layer 2 line protocol. This field may be different from the interface state if, for example, a keepalive failure has brought down the Layer 2. Note The line protocol state is not the same as the protocol state displayed in the show ip interfaces command, because it is the state of Layer 2 (media) rather than Layer 3 (IP protocol).
Hardware	Displays the current hardware type.
Internet address is <i>n.n.n.n/n</i>	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.
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.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 80** **show interfaces Field Descriptions (continued)**

Field	Description
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 <i>keepalive</i> field may not be present if it is not applicable to the interface type.
Duplexity	Displays the duplexity of the link. Note This field is present only for shared media. Note For some interface types, you can configure the duplexity by entering the full-duplex and half-duplex commands.
Speed	Speed and bandwidth of the link in Mbps. This field is present only when other parts of the media info line are also displayed (see duplexity and media type).
Media Type	Media type of the interface.
output flow control	Whether output flow control is enabled on the interface.
input flow control	See output flow control.
ARP type	Address Resolution Protocol (ARP) type used on the interface. This value is not displayed on interface types that do not use ARP.
ARP timeout	ARP timeout in <i>hours:mins:secs</i> . 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 <i>hours:mins:secs</i> .

R3.5.0 Beta Draft—Cisco Confidential Information**Table 80** **show interfaces Field Descriptions (continued)**

Field	Description
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 five-minute input should be used only as an approximation of traffic per second during a given five-minute period. This rate is exponentially weighted average with a time constant of five minutes. A period of four time constants must pass before the average will be 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 five-minute output should be used only as an approximation of traffic per second during a given five-minute period. This rate is exponentially weighted average with a time constant of five minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Number of packets received on the interface that were successfully delivered to higher layers.
bytes input	Total number of bytes successfully received on the interface
total input drops	Total number of valid 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. 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.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 80** *show interfaces Field Descriptions (continued)*

Field	Description
giants	Number of received packets that were too large to be handled. This is a subset of the input errors count.
throttles	Number of packets dropped due to throttling (because the input queue was full).
parity	Number of packets dropped because the parity check failed.
input errors	Total number of received packets that contain errors and hence cannot be delivered. Compare this to total input drops, which counts packets that were not delivered despite containing no errors.
CRC	Number of packets that failed the CRC check.
frame	Number of packets with bad framing bytes.
overrun	Number of overrun errors experienced by the interface. Overruns represent the number of times that the receiver hardware is unable to send received data to a hardware buffer because the input rate exceeds the receiver's ability to handle the data.
ignored	Total number of ignored packet errors. Ignored packets are those that are discarded because the interface hardware does not have enough internal buffers. Broadcast storms and bursts of noise can result in an increased number of ignored packets.
abort	Total number of 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.
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-specific.
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.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 80** *show interfaces* Field Descriptions (continued)

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.

R3.5.0 Beta Draft—Cisco Confidential Information

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 arguments or keywords.

Defaults

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



Note

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

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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, encapsulations, 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.

R3.5.0 Beta Draft—Cisco Confidential Information

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

R3.5.0 Beta Draft—Cisco Confidential Information



Management Ethernet Interface Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

This module describes the Cisco IOS XR commands used to configure the Management Ethernet interfaces.

R3.5.0 Beta Draft—Cisco Confidential Information

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.

Defaults

Autonegotiates duplex operation

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The duplex command replaced the full-duplex and half-duplex commands.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure the Management Ethernet interface to operate in full duplex mode:

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

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

R3.5.0 Beta Draft—Cisco Confidential Information

The following example shows how to configure the Management Ethernet interface to operate in half duplex mode:

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

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

The following example shows how to return a Management Ethernet interface to autonegotiated duplex mode:

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

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

Related Commands

Command	Description
interface MgmtEth	Enters interface configuration mode for the Management Ethernet interface.
show interfaces	Displays statistics for all interfaces configured on the router.

R3.5.0 Beta Draft—Cisco Confidential Information

interface MgmtEth

To enter interface configuration mode for the Management Ethernet interface, use the **interface MgmtEth** command in global configuration mode. To delete a Management Ethernet interface configuration, use the **no** form of this command.

interface MgmtEth *instance*

no interface MgmtEth *instance*

Syntax Description	<i>instance</i> Physical interface instance. Naming notation is <i>rack/slot/CPU0/port</i> and a slash between values is required as part of the notation. <i>rack</i>—Chassis number of the rack. In a single-shelf system, the rack is always “0.” {RP0 RP1}—Physical slot number of the RP on which the interface is located. Can be RP0 or RP1. CPU0—Identifies the module. <i>port</i>—Physical port number of the interface. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults	No default behavior or values

Command Modes	Global configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter interface configuration mode for a Management Ethernet interface:

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

Related Commands

Command	Description
duplex (Management Ethernet)	Configures duplex mode operation on a Management Ethernet interface for a Management Ethernet interface.
mac-address (Management Ethernet)	Sets the MAC layer address of a Management Ethernet interface.
show interfaces	Displays statistics for all interfaces configured on the router.
speed (Management Ethernet)	Configures the speed for a Management Ethernet interface.

R3.5.0 Beta Draft—Cisco Confidential Information

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

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

Command Modes Interface configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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/RP0/CPU0/0:

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


R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	interface MgmtEth	Enters interface configuration mode for the Management Ethernet interface.
	show interfaces	Displays statistics for all interfaces configured on the router.

R3.5.0 Beta Draft—Cisco Confidential Information

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.
	Note	This option is available only on the Cisco CRS-1.
	1000	Configures the interface to transmit at 1000 Mbps (1 Gbps).

Defaults Interface speed is autonegotiated.

Command Modes Interface configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

On the Cisco CRS-1, valid interface speed options are 10 Mbps, 100 Mbps, or 1000 Mbps.

On the Cisco XR 12000 Series Router, valid interface speed options are 10 Mbps or 100 Mbps.

**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.

R3.5.0 Beta Draft—Cisco Confidential Information

Table 81 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 81 Relationship Between duplex and speed Commands

duplex Command	speed Command	Resulting System Action
no duplex	no speed	Autonegotiates both speed and duplex modes.
no duplex	speed 1000	Forces 1000 Mbps (1 Gbps) and full duplex.
no duplex	speed 100	Autonegotiates for duplex mode and forces 100 Mbps.
no duplex	speed 10	Autonegotiates for duplex mode and forces 10 Mbps.
duplex full	no speed	Forces full duplex and autonegotiates for speed.
duplex full	speed 1000	Forces 1000 Mbps (1 Gbps) and full duplex.
duplex full	speed 100	Forces 100 Mbps and full duplex.
duplex 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/RP0/CPU0/0
```

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

Related Commands

Command	Description
interface MgmtEth	Enters interface configuration mode for the Management Ethernet interface.
show interfaces	Displays statistics for all interfaces configured on the router.

R3.5.0 Beta Draft—Cisco Confidential Information



Packet-over-SONET/SDH Interface Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

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.

R3.5.0 Beta Draft—Cisco Confidential Information

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.

Defaults

The default CRC mode is 32 bits.

Command Modes

POS configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

R3.5.0 Beta Draft—Cisco Confidential Information

Examples

In the following example, the 32-bit CRC on POS interface 0/1/0/2 is enabled:

```
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)# crc 32
```

Related Commands

Command	Description
transmit-delay	Specifies a number of flag sequences to be inserted between the packets.

R3.5.0 Beta Draft—Cisco Confidential Information

encapsulation (POS)

To set the Layer 2 encapsulation of an interface, use the **encapsulation** command in interface configuration mode. To restore the system to the default encapsulation, use the **no** form of this command.

encapsulation {**hdlc** | **ppp** | **frame-relay**}

no encapsulation

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.

Defaults For Packet-over-SONET/SDH (POS) interfaces, the default encapsulation is HDLC.

Command Modes Interface configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	Frame Relay encapsulation was supported on POS interfaces.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	hdlc	read, write
	interface	read, write

Examples In the following 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
```


R3.5.0 Beta Draft—Cisco Confidential Information**Related Commands**

Command	Description
show interface	Displays statistics for all interfaces configured on the router.
show ppp interfaces	Displays PPP state information for an interface.

R3.5.0 Beta Draft—Cisco Confidential Information

interface pos

To enter interface configuration mode for a POS interface, use the **interface pos** command in global configuration mode. To delete a POS configuration, use the **no** form of this command.

interface POS *instance* [*.subinterface* [**point-to-point**]]

no interface POS *instance* [*.subinterface* [**point-to-point**]]

Syntax Description		
	<i>instance</i>	Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i>, and a slash between values is required as part of the notation. <i>rack</i>—Chassis number of the rack. <i>slot</i>—Physical slot number of the card. <i>module</i>—Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>—Physical port number of the interface. - Virtual interface instance. Range of numbers varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
	<i>.subinterface</i>	(Optional) Subinterface instance. Naming notation is <i>.subinterface</i>. The period in front of the <i>subinterface</i> value is required as part of the notation. Replace <i>subinterface</i> with the virtual interface number to be associated with the physical interface. Note For more information about the syntax for the router, use the question mark (?) online help function.
	point-to-point	(Optional) Interface functions as one endpoint of a point-to-point link.

Defaults No default behavior or values

Command Modes Global configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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/0/0/CPU0:Router(config)# interface pos 0/1/1/2.1
```

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

Related Commands

Command	Description
show interfaces pos	Displays information about a POS interface.

R3.5.0 Beta Draft—Cisco Confidential Information

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 {*seconds* | **disable**}

no keepalive

Syntax Description	<i>seconds</i>	Number of seconds that define the keepalive interval. Range is from 0 through 32767seconds. Default is 10 seconds.
	disable	Turns off the keepalive timer.

Defaults *seconds* = 10 seconds

Command Modes Interface configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following 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
```

R3.5.0 Beta Draft—Cisco Confidential Information

pos

To access the POS configuration submode, use the **pos** command in interface configuration mode.

pos

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Interface configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

R3.5.0 Beta Draft—Cisco Confidential Information

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)	Sets the length of the CRC on a POS interface.
	transmit-delay	Specifies a number of flag sequences to be inserted between the packets.

R3.5.0 Beta Draft—Cisco Confidential Information

show interfaces pos

To display information about a POS interface, use the **show interfaces pos** command in EXEC mode.

show interfaces pos [*instance*] [**accounting** [*rates*]] | **brief** | **description** | **detail** | **summary** [*location node-id*]

<i>instance</i>	(Optional) POS interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. – <i>rack</i>—Chassis number of the rack. – <i>slot</i>—Physical slot number of the modular services card or line card. – <i>module</i>—Module number. A physical layer interface module (PLIM) is always 0. – <i>port</i>—Physical port number of the interface. 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 <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
summary	(Optional) Displays summarized POS interface information.

Defaults

Enter the **show interfaces pos** command without including any of the optional keywords or arguments to display detailed information about all POS interfaces configured on the router.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was first introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information

Release	Modification
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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 82 describes the significant fields shown in the display.

Table 82 *show interfaces pos summary Field Descriptions*

Field	Description
Intf Type	Type of interface described in the display.
Total	Total number of configured interfaces of the specified type.
Up	Number of interfaces of the specified type that are in the “Up” state.
Down	Number of interfaces of the specified type that are in the “Down” state.
Admin Down	Number of interfaces of the specified type that are in the “Admin Down” state.

The following example shows how to display brief information for a specific POS interface:

```
RP/0/RP0/CPU0:router# show interfaces pos 0/2/0/0 brief
```

Intf Name	Intf State	LineP State	Encap Type	MTU (byte)	BW (Kbps)
-----	-----	-----	-----	-----	-----
PO0/2/0/0	admin-down	admin-down	HDLC	4474	2488320

```
P/0/RP1/CPU0:MiniQ#
```

R3.5.0 Beta Draft—Cisco Confidential Information

Table 83 describes the significant fields shown in the display.

Table 83 *show interfaces pos Field Descriptions*

Field	Description
Intf Name	Interface identifier, in the <i>type*rack/slot/module/port</i> 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 SONET controllers that are associated with Packet-over-SONET/SDH (POS) interfaces.
show controllers sonet	Displays information about the operational status of SONET layers.

R3.5.0 Beta Draft—Cisco Confidential Information

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

Defaults	<i>microseconds</i> = 0 (disabled)

Command Modes	POS configuration

Command History	Releases	Modifications
	Release 3.2	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	pos-dpt	read, write

Examples	In the following example, a delay of 2 microseconds is specified on POS interface 0/1/0/2:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface POS 0/1/0/2
RP/0/0/CPU0:router(config-if)# pos
RP/0/0/CPU0:router(config-if-pos)# transmit-delay 2
```

R3.5.0 Beta Draft—Cisco Confidential Information

In the following example, the transmit delay on POS interface 0/1/0/2 is disabled:

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

```
RP/0/0/CPU0:router(config)# interface POS 0/1/0/2
```

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

```
RP/0/0/CPU0:router(config-if-pos)# no transmit-delay
```

Related Commands

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



SRP Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

This module describes the commands to configure Spatial Reuse Protocol (SRP) on supported Cisco Dynamic Packet Transport (DPT) interfaces in routers running Cisco IOS XR software.

SRP is a MAC-layer protocol developed by Cisco and is used in conjunction with Cisco DPT products. DPT products deliver scalable Internet service, reliable IP-aware optical transport, and simplified network operations. These solutions allow you to scale and distribute your IP services across a reliable optical packet ring infrastructure.



Note

Throughout the remainder of this publication, the term SRP is used to describe features related to the DPT product family.

R3.5.0 Beta Draft—Cisco Confidential Information

clear srp counters

To clear the SRP counters, use the **clear srp counters** command in EXEC mode.

clear srp counters {**interface srp** *instance* | **location** *node-id*}

Syntax Description	interface srp	Specifies the SRP interface.
	<i>instance</i>	Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. <i>port</i>: Physical port number of the interface. An SRP interface is comprised of two consecutive physical ports and is named according to the first, lower-numbered port. For example, the SRP interface 0/4/0/2 is comprised of the two physical ports 0/4/0/2 and 0/4/0/3. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 3.2.2	This command was introduced on the Cisco CRS-1 and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
	Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.
	Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **clear srp counters** command clears the counters displayed in the following commands:

- **show controllers srp rac-error**
- **show srp counters**
- **show srp counters source**

R3.5.0 Beta Draft—Cisco Confidential Information

- **show srp transit**

Task ID	Task ID	Operations
	pos-dpt	read, write

Examples

The following example shows how to use the **clear srp counters** command to make the counts displayed from the **show srp source-counters** command return to zero:

```
RP/0/RP0/CPU0:Router# show srp counters interface srp 0/7/0/0
```

Data Traffic Counters for Interface SRP0/7/0/0

Side A:

Transit	Packets	Bytes
Total Low Priority:	0	0
Total High Priority:	183	768543
Total Multicast:	174	767913
Total Unicast:	9	630
Host Receive	Packets	Bytes
Unicast Low Priority:	6	648
Unicast High Priority:	0	0
Multicast Low Priority:	0	0
Multicast High Priority:	1	41
Total Receive	Packets	Bytes
Unicast Low Priority:	6	648
Unicast High Priority:	9	630
Multicast Low Priority:	3	144
Multicast High Priority:	174	767913
Host Transmit	Packets	Bytes
Unicast Low Priority:	4	480
Unicast High Priority:	0	0
Multicast Low Priority:	0	0
Multicast High Priority:	0	0
Total Transmit	Packets	Bytes
Unicast Low Priority:	4	480
Unicast High Priority:	0	0
Multicast Low Priority:	0	0
Multicast High Priority:	772	1575090
Traffic Rate (5 Minutes)	packets/sec	bits/sec
Transit Low Priority	0	0
Transit High Priority	0	0
Transit Multicast	0	0
Transit Unicast	0	0
Host Receive	0	0
Total Receive	0	0
Host Transmit	0	0
Total Transmit	0	0

Received Errors:

0 input errors, 0 CRC, 0 ignored,
0 framer runs, 0 framer giants, 0 framer aborts,
0 mac runs, 0 mac giants, 0 mac ttl strips

Side B:

Transit	Packets	Bytes
Total Low Priority:	0	0
Total High Priority:	772	1575090
Total Multicast:	772	1575090
Total Unicast:	0	0
Host Receive	Packets	Bytes
Unicast Low Priority:	6	648

```
clear srp counters
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

Unicast High Priority:                0                0
Multicast Low Priority:               0                0
Multicast High Priority:              1                41
Total Receive                        Packets           Bytes
Unicast Low Priority:                 6                648
Unicast High Priority:                0                0
Multicast Low Priority:               0                0
Multicast High Priority:              772             1575090
Host Transmit                        Packets           Bytes
Unicast Low Priority:                 6                720
Unicast High Priority:                0                0
Multicast Low Priority:               3                144
Multicast High Priority:              0                0
Total Transmit                       Packets           Bytes
Unicast Low Priority:                 6                720
Unicast High Priority:                9                630
Multicast Low Priority:               3                144
Multicast High Priority:              174             767913
Traffic Rate (5 Minutes)             packets/sec      bits/sec
Transit Low Priority                  0                0
Transit High Priority                 0                0
Transit Multicast                    0                0
Transit Unicast                      0                0
Host Receive                         0                0
Total Receive                        0                0
Host Transmit                        0                0
Total Transmit                       0                0
Received Errors:
  0 input errors, 0 CRC, 0 ignored,
  0 framer runts, 0 framer giants, 0 framer aborts,
  0 mac runts, 0 mac giants, 0 mac ttl strips

```

```
RP/0/RP0/CPU0:Router# clear srp counters interface srp 0/7/0/0
```

```
RP/0/RP0/CPU0:Router# show srp counters interface srp 0/7/0/0
```

Data Traffic Counters for Interface SRP0/7/0/0

Side A:

```

Transit                        Packets           Bytes
Total Low Priority:            0                0
Total High Priority:           0                0
Total Multicast:               0                0
Total Unicast:                 0                0
Host Receive                  Packets           Bytes
Unicast Low Priority:          0                0
Unicast High Priority:         0                0
Multicast Low Priority:        0                0
Multicast High Priority:       0                0
Total Receive                  Packets           Bytes
Unicast Low Priority:          0                0
Unicast High Priority:         0                0
Multicast Low Priority:        0                0
Multicast High Priority:       0                0
Host Transmit                  Packets           Bytes
Unicast Low Priority:          0                0
Unicast High Priority:         0                0
Multicast Low Priority:        0                0
Multicast High Priority:       0                0
Total Transmit                 Packets           Bytes
Unicast Low Priority:          0                0
Unicast High Priority:         0                0
Multicast Low Priority:        0                0
Multicast High Priority:       0                0
Traffic Rate (5 Minutes)      packets/sec      bits/sec
Transit Low Priority           0                0

```


R3.5.0 Beta Draft—Cisco Confidential Information

```

Transit High Priority                0                0
Transit Multicast                   0                0
Transit Unicast                     0                0
Host Receive                        0                0
Total Receive                       0                0
Host Transmit                       0                0
Total Transmit                      0                0
Received Errors:
  0 input errors, 0 CRC, 0 ignored,
  0 framer runts, 0 framer giants, 0 framer aborts,
  0 mac runts, 0 mac giants, 0 mac ttl strips

Side B:
Transit                             Packets           Bytes
  Total Low Priority:                0                0
  Total High Priority:               0                0
  Total Multicast:                   0                0
  Total Unicast:                     0                0
Host Receive                         Packets           Bytes
  Unicast Low Priority:              0                0
  Unicast High Priority:              0                0
  Multicast Low Priority:             0                0
  Multicast High Priority:            0                0
Total Receive                       Packets           Bytes
  Unicast Low Priority:              0                0
  Unicast High Priority:              0                0
  Multicast Low Priority:             0                0
  Multicast High Priority:            0                0
Host Transmit                       Packets           Bytes
  Unicast Low Priority:              0                0
  Unicast High Priority:              0                0
  Multicast Low Priority:             0                0
  Multicast High Priority:            0                0
Total Transmit                      Packets           Bytes
  Unicast Low Priority:              0                0
  Unicast High Priority:              0                0
  Multicast Low Priority:             0                0
  Multicast High Priority:            0                0
Traffic Rate (5 Minutes)            packets/sec      bits/sec
Transit Low Priority                 0                0
Transit High Priority                0                0
Transit Multicast                    0                0
Transit Unicast                     0                0
Host Receive                        0                0
Total Receive                       0                0
Host Transmit                       0                0
Total Transmit                      0                0
Received Errors:
  0 input errors, 0 CRC, 0 ignored,
  0 framer runts, 0 framer giants, 0 framer aborts,
  0 mac runts, 0 mac giants, 0 mac ttl strips

```

Related Commands

Command	Description
show srp	Displays information about SRP interfaces on the ring, including MAC addresses of neighboring interfaces, IPS status, source-counters, and topology map.

R3.5.0 Beta Draft—Cisco Confidential Information

hw-module port

To enable a port to be used for SRP, use the **hw-module port** command in global configuration mode. To disable SRP and enable the port for POS, use the **no** form of this command.

hw-module port *port-number* **srp** **location** *node-id*

no hw-module port *port-number* **srp** **location** *node-id*

Syntax Description

<i>port-number</i>	Number of the physical interface on the PLIM.
srp	Specifies an SRP interface.
location	Specifies the location of the module.
<i>node-id</i>	Location of the module in the <i>rack/slot/module</i> notation.

Defaults

When there is no **hw-module port** configuration, ports are enabled for POS by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2.2	This command was introduced on the Cisco CRS-1 and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

POS is the default port mode on POS/DPT PLIMs. Use the **hw-module port** command to allow the ports to be configured for SRP use.

SRP requires two consecutive physical ports for use as a single SRP interface. The first port must be even numbered and the second port must be odd numbered. No other combinations are allowed. You must use this command on both of the ports to be used as an SRP interface. SRP interfaces take the number of the lower, even-numbered port. For example, if ports 0/1/0/2 and 0/1/0/3 are enabled as an SRP interface, the interface would be referred to as SRP0/1/0/2.

On the 16-port OC-48c/STM-16c POS/DPT PLIM, groups of four consecutive ports must be configured the same. Ports 0-3 all must be configured as either SRP or POS. The same is true for ports 4-7, 8-11 and 12-15.

After using the **hw-module port** command, you must save the configuration and reload the PLIM. To disable SRP and reenable POS on the port, use the **no** form of the command.

R3.5.0 Beta Draft—Cisco Confidential Information**Note**

You must reload the PLIM to enable this configuration change and create the SRP or POS interface. Use the **hw-module location reload** command in EXEC mode.

**Note**

Internal clocking is required for SRP interfaces. Use the **clock source internal** command in SONET configuration mode to configure the clock source.

Task ID**Task ID****Operations**

root-lr

read, write

Examples

In the following example, ports 0 and 1 are enabled for SRP:

```
RP/0/RP0/CPU0:Router(config)# hw-module port 0 srp location 0/6/cpu0
RP/0/RP0/CPU0:Router(config)# hw-module port 1 srp location 0/6/cpu0
RP/0/RP0/CPU0:Router(config)# exit
```

Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: y

```
RP/0/RP0/CPU0:Sep  8 11:13:30.817 : config[65732]: %MGBL-LIBTARCFG-6-COMMIT :
Configuration committed by user 'xxx'.  Use 'show configuration commit changes
1000000646' to view the changes.
```

```
RP/0/RP0/CPU0:Sep  8 11:13:30.902 : config[65732]: %MGBL-SYS-5-CONFIG_I : Configured from
console by xxx
```

```
RP/0/RP0/CPU0:Router# hw-module location 0/6/cpu0 reload
```

```
RP/0/RP0/CPU0:Anjou#SP/0/6/SP:Sep  8 11:17:17.037 : alphadisplay[100]:
%PLATFORM-ALPHA_DISPLAY-6-CHANGE : Alpha display on node 0/6/SP changed to      in
state default
```

```
shRP/0/RP0/CPU0:Sep  8 11:17:17.865 : shelfmgr[283]: %PLATFORM-SHELFMGR-3-USER_RESET :
Node 0/6/CPU0 is reset due to user reload request
```

Related Commands**Command****Description**

clock source internal Configures SONET clocking as internal.

hw-module location reload Reloads the PLIM.

R3.5.0 Beta Draft—Cisco Confidential Information

interface srp

To configure the SRP protocol on a DPT interface and enter interface configuration mode, use the **interface srp** command in global configuration mode.

interface srp *instance*

Syntax Description

instance

Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation.

- *rack*: Chassis number of the rack.
- *slot*: Physical slot number of the modular services card or line card.
- *module*: Module number. A physical layer interface module (PLIM) is always 0.
- *port*: Physical port number of the interface. An SRP interface is comprised of two consecutive physical ports and is named according to the first, lower-numbered port. For example, the SRP interface 0/4/0/2 is comprised of the two physical ports 0/4/0/2 and 0/4/0/3.

For more information about the syntax for the router, use the question mark (?) online help function.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2.2	This command was introduced on the Cisco CRS-1 and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
interface	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to enter srp interface mode:

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

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers srp

To display information on the SRP controllers, use the **show controllers srp** command in EXEC mode.

show controllers srp *instance* **side** {**a** | **b**} [**rac-error** | **rac-reg** | **ucode-inst** | **ucode-reg**]

Syntax Description		
	<i>instance</i>	Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. <i>port</i>: Physical port number of the interface. An SRP interface is comprised of two consecutive physical ports and is named according to the first, lower-numbered port. For example, the SRP interface 0/4/0/2 is comprised of the two physical ports 0/4/0/2 and 0/4/0/3. For more information about the syntax for the router, use the question mark (?) online help function.
	side	Specify the side of the node.
	a	The side of a node that has outer ring receive fiber is identified as side A.
	b	The side of a node that has inner ring receive fiber is identified as side B.
	rac-error	Displays the error reported by the Ring Access Controller (RAC) device.
	rac-reg	Displays the value of the RAC device register set.
	ucode-inst	Displays the RAC micro-controller binary code instruction set (currently loaded or executing) in hexadecimal format. Note This is an intrusive command that will cause adjacent nodes to detect a MAC keepalive failure and then wrap.
	ucode-reg	Displays the RAC micro-controller register set.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.2.2	This command was introduced on the Cisco CRS-1 and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
	Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.
	Release 3.5.0	No modification.

R3.5.0 Beta Draft – Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
interface	read

Examples

This example shows how to display the RAC registers for a specified SRP interface:

```
RP/0/RP0/CPU0:Router# show controllers srp 0/5/0/0 side a rac-reg
```

Related Commands

Command	Description
show srp	Displays information about SRP interfaces on the ring, including MAC addresses of neighboring nodes, IPS status, source-counters, and topology map.

R3.5.0 Beta Draft—Cisco Confidential Information

show srp

To display information about an SRP interface, use the **show srp** command in EXEC mode.

```
show srp [counters [source] | failures | ips | platform | srr | topology | transit] [interface srp
instance | location node-id]
```

Syntax Description

counters	Displays counters for the packets received, transmitted, and transited on both sides of an SRP node.
source	Displays the counters for the SRP source address.
failures	Displays all SRP failures that were detected by the router.
ips	Displays the Intelligent Protection Switching (IPS) status.
platform	Displays platform-specific SRP interface details.
srr	Displays single ring recovery (SRR) information.
topology	Identifies the nodes on the ring.
transit	Displays transit delays (in nanoseconds) between the time that a packet enters the transit buffer and the time it comes back on the ring.
interface	Specifies the interface for which to display the counters.
srp	Specifies an SRP interface.
<i>instance</i>	Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. <i>port</i>: Physical port number of the interface. An SRP interface is comprised of two consecutive physical ports and is named according to the first, lower-numbered port. For example, the SRP interface 0/4/0/2 is comprised of the two physical ports 0/4/0/2 and 0/4/0/3. For more information about the syntax for the router, use the question mark (?) online help function.
location	Specifies the location of the module.
<i>node-id</i>	Location of the module in the <i>rack/slot/module</i> notation.

Defaults

No default behavior or values

Command Modes

EXEC

R3.5.0 Beta Draft—Cisco Confidential Information**Command History**

Release	Modification
Release 3.2.2	This command was introduced on the Cisco CRS-1 and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

To clear the SRP counters, use the [clear srp counters](#) command. The **show srp** command with the **counters** keyword reports the per-side counters and rates for various packet paths.

The **show srp** command with the **failures** keyword reports the SRP failures that were detected by the router. Use the **failures** keyword when an SRP interface is wrapped and you want to display information about the cause of the failure.

Use the **transit** keyword to determine the approximate latency when transmitting a packet, which due to higher latency, gives the approximation of congestion at this interface. If there is no latency, there is no congestion. Latency indicates that traffic transiting the ring and transmitted from the host are competing, meaning there is congestion.

Regarding the **topology** keyword, Address Resolution Protocol (ARP) is independent of the Layer 2 topology mapping. In other words, the absence of a MAC address in the topology map does not prevent ARP or any Layer 3 protocol from reaching the node. Alternatively, the presence of a MAC address in the topology map does not mean that it will be possible to resolve the Layer 3 address. The topology map is used to determine the most efficient side (in hops) to use to reach any given MAC address.

Task ID

Task ID	Operations
pos-dpt	read

Examples

Sample output from the **show srp** command is displayed in the following sections:

- [show srp counters Sample Output, page 609](#)
- [show srp failures Sample Output, page 613](#)
- [show srp interface Sample Output, page 614](#)
- [show srp ips Sample Output, page 615](#)
- [show srp topology Sample Output, page 617](#)
- [show srp transit Sample Output, page 617](#)

show srp counters Sample Output

In the following example, output from the **show srp** command with the **counters** keyword is displayed:

```
RP/0/RP0/CPU0:Router# show srp counters interface srp 0/7/0/0
```

```
Data Traffic Counters for Interface SRP0/7/0/0
```

```
Side A:
```

```
Transit
```

```
Packets
```

```
Bytes
```

R3.5.0 Beta Draft—Cisco Confidential Information

Total Low Priority:	0	0
Total High Priority:	183	768543
Total Multicast:	174	767913
Total Unicast:	9	630
Host Receive	Packets	Bytes
Unicast Low Priority:	6	648
Unicast High Priority:	0	0
Multicast Low Priority:	0	0
Multicast High Priority:	1	41
Total Receive	Packets	Bytes
Unicast Low Priority:	6	648
Unicast High Priority:	9	630
Multicast Low Priority:	3	144
Multicast High Priority:	174	767913
Host Transmit	Packets	Bytes
Unicast Low Priority:	4	480
Unicast High Priority:	0	0
Multicast Low Priority:	0	0
Multicast High Priority:	0	0
Total Transmit	Packets	Bytes
Unicast Low Priority:	4	480
Unicast High Priority:	0	0
Multicast Low Priority:	0	0
Multicast High Priority:	772	1575090
Traffic Rate (5 Minutes)	packets/sec	bits/sec
Transit Low Priority	0	0
Transit High Priority	0	0
Transit Multicast	0	0
Transit Unicast	0	0
Host Receive	0	0
Total Receive	0	0
Host Transmit	0	0
Total Transmit	0	0
Received Errors:		
0 input errors, 0 CRC, 0 ignored,		
0 framer runts, 0 framer giants, 0 framer aborts,		
0 mac runts, 0 mac giants, 0 mac ttl strips		

Side B:

Transit	Packets	Bytes
Total Low Priority:	0	0
Total High Priority:	772	1575090
Total Multicast:	772	1575090
Total Unicast:	0	0
Host Receive	Packets	Bytes
Unicast Low Priority:	6	648
Unicast High Priority:	0	0
Multicast Low Priority:	0	0
Multicast High Priority:	1	41
Total Receive	Packets	Bytes
Unicast Low Priority:	6	648
Unicast High Priority:	0	0
Multicast Low Priority:	0	0
Multicast High Priority:	772	1575090
Host Transmit	Packets	Bytes
Unicast Low Priority:	6	720
Unicast High Priority:	0	0
Multicast Low Priority:	3	144
Multicast High Priority:	0	0
Total Transmit	Packets	Bytes
Unicast Low Priority:	6	720
Unicast High Priority:	9	630
Multicast Low Priority:	3	144
Multicast High Priority:	174	767913

R3.5.0 Beta Draft—Cisco Confidential Information

```

Traffic Rate (5 Minutes)
Transit Low Priority          packets/sec      bits/sec
Transit High Priority         0                0
Transit Multicast             0                0
Transit Unicast               0                0
Host Receive                  0                0
Total Receive                  0                0
Host Transmit                  0                0
Total Transmit                 0                0
Received Errors:
  0 input errors, 0 CRC, 0 ignored,
  0 framer runts, 0 framer giants, 0 framer aborts,
  0 mac runts, 0 mac giants, 0 mac ttl strips

```

Table 84 describes the significant fields shown in the display.

Table 84 *show srp counters Command Output Fields*

Field	Description
Side A	Header for packets received, transmitted, and transited by the Resource Availability Confirmation (RAC) device on side A.
Side B	Header for packets received, transmitted, and transited by the RAC device on side B.
Transit Total Low Priority	Total number of unicast and multicast packets marked as SRP low priority (based on the SRP priority mapping) that transit the router and are counted in the transmit low-priority counters.
Transit Total High Priority	Total number of unicast and multicast packets marked as SRP high priority (based on the SRP priority mapping) that transit the router and are counted in the transmit high-priority counters.
Transit Total Multicast	Total number of low- and high-priority multicast packets that transit the router and are counted in the transmit multicast counters.
Transit Total Unicast	Total number of low- and high-priority unicast packets that transit the router and are counted in the transmit unicast counters.
Host Receive Unicast Low/High priority	Total number of low- and high-priority unicast packets received by the router.
Host Receive Multicast Low/High priority	Total number of low- and high-priority multicast packets received by the router.
Total Receive Unicast Low/High priority	Total number of low- and high-priority unicast packets that transit or are received by the router.
Total Receive Multicast Low/High priority	Total number of low- and high-priority multicast packets that transit or are received by the router.
Host Transmit Unicast Low/High priority	Total number of low- and high-priority unicast packets sourced onto the ring by the router.
Host Transmit Multicast Low/High priority	Total number of low- and high-priority multicast packets sourced onto the ring by the router.
Total Transmit Unicast Low/High priority	Total number of low- and high-priority unicast packets transmitted by this side and transited out of the other side of the node.
Total Transmit Multicast Low/High priority	Total number of low- and high-priority multicast packets transmitted by this side and transited out of the other side of the node.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 84** *show srp counters Command Output Fields (continued)*

Field	Description
Traffic Rate (5 Minutes)	Average number of packets and bits transmitted per second during the last 5 minutes. The 5-minute traffic rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period. The 5-minute value is the load interval, and it is configurable using the load-interval command.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of a station transmitting bad data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be increased.
framer runts	Number of packets dropped by the framer as runts, that are smaller than 16 bytes.
framer giants	Number of packets dropped by the framer as giants, whose size is greater than the MTU.
framer aborts	Number of packets dropped by the framer due to an error in packet insertion from the SONET frame. Normally a framer abort is caused by a delimiter inserted at the transmit framer that forces the receive framer to drop the packet on reception because it is bad. The delimiter is inserted by the transmit framer when it cannot transmit a packet due to a transmission error. A runt or CRC error may also result. A framer abort can be caused by any of the following: • A bad transmit framer at the neighbor node (upstream) • BIP errors in the SONET frame that cause a false abort delimiter (often due to intermediate equipment failure or clocking issues) • A bad receive framer at this node
mac runts	Packets dropped by the MAC controller as runts, that are smaller than 24 bytes.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 84** *show srp counters Command Output Fields (continued)*

Field	Description
mac giants	Packets dropped by the MAC controller as giants, whose size is greater than the MTU.
mac ttl strips	Packets stripped by the MAC controller when the SRP Time to Live value expires. (TTL value is 1 when a packet arrives.) These packets are removed from the ring because the TTL value cannot be decreased. As a result, the packet is dropped if it is not destined for the node that strips it.

show srp failures Sample Output

In the following example, self-detected failures in the SRP interface configured on slot 7, subslot 0, and port 0 are displayed:

```
RP/0/RP0/CPU0:Router# show srp failures
```

```
Self Detected Failures Information for Interface SRP0/7/0/0
```

```
Side A:
```

	Reported state	Debounce state	Current state	Stable for (sec)	Debounce delay (sec)
HW missing	IDLE	IDLE	IDLE	778	0
L1 Admin State	IDLE	IDLE	IDLE	777	0
Layer 1	IDLE	IDLE	IDLE	778	0
MAC Keepalive	IDLE	IDLE	IDLE	477	5
Link quality	IDLE	IDLE	IDLE	778	0
Mate interface	IDLE	IDLE	IDLE	778	10
Side mismatch	IDLE	IDLE	IDLE	477	5

Result Self Detect = IDLE

```
Side B:
```

	Reported state	Debounce state	Current state	Stable for (sec)	Debounce delay (sec)
HW missing	IDLE	IDLE	IDLE	778	0
L1 Admin State	IDLE	IDLE	IDLE	775	0
Layer 1	IDLE	IDLE	IDLE	778	0
MAC Keepalive	IDLE	IDLE	IDLE	477	5
Link quality	IDLE	IDLE	IDLE	778	0
Mate interface	IDLE	IDLE	IDLE	778	10
Side mismatch	IDLE	IDLE	IDLE	477	5

Result Self Detect = IDLE

Table 85 describes the significant fields shown in the display.

Table 85 *show srp failures Command Output Fields*

Field	Description
HW missing	Presence of this side's hardware port. Possible states: IDLE—No error or failure SF—Port is not installed or is still booting
L1 Admin State	Layer 1 administrative state. Possible states: IDLE—SONET controller is configured as up FS—SONET controller is configured as administratively down Note This is the only field in which the status is related to a user-configurable state.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 85** *show srp failures Command Output Fields (continued)*

Field	Description
Layer 1	Operating state of the SONET controller. Possible states: IDLE—No alarms, etc. SF—Some alarms, such as section loss of signal (SLOS), section loss of frame (SLOF), or line alarm indicator signal (LAIS) Note For detailed information about a Layer 1 failure, use the show controllers sonet command.
MAC keepalive	The MAC keepalive timer has expired.
Link quality	The SONET B3 bit error rate (BER) threshold has been crossed. To configure SRP signal degrade detection and signal fail detection, use the srp priority-threshold command.
Mate interface	The external mate cable on a line card interface is missing or malfunctioning. Note This is only applicable to one-port PLIMs or SPAs that would require a second PLIM or SPA to create an SRP interface.
Side mismatch	Side A of the node is connected to side A of the neighbor node, or side B of the node is connected to side B of the neighbor node.
Result Self Detect	IPS state requested for this side. The state will be the highest IPS request listed under “Reported state.”
Reported state	State that is reported to the IPS engine.
Debounced state	Current SF/FS state or the current IDLE state if IDLE has been stable for the amount of time of the debounce delay.
Current state	Current state as reported by the source.
Stable for (sec)	Amount of time the current state has been stable.
Debounce delay (sec)	Amount of time to wait when transitioning from SF to IDLE. The IDLE state must be stable for this amount of time before getting debounced or reported. This is to prevent flapping and is similar to higher-level WTR values.

show srp interface Sample Output

In the following example, the display from the **show srp** command with the **interface** keyword is shown:

```
RP/0/RP0/CPU0:Router# show srp interface srp 0/5/0/0
```

```
IPS Information for Interface SRP0/5/0/0
```

```
MAC Addresses
```

```
Side A (Outer ring RX) neighbor 0009.11d8.3c66
```

```
Side B (Inner ring RX) neighbor 0012.da6a.f664
```

```
Node MAC address 0800.453d.8644
```

```
IPS State
```

```
Side A not wrapped
```

```
Side B not wrapped
```

```
Side A (Inner ring TX) IPS pkt. sent every 1 sec. (next pkt. after 1 sec.)
```

```
Side B (Outer ring TX) IPS pkt. sent every 1 sec. (next pkt. after 1 sec.)
```

```
inter card bus disabled
```

```
IPS WTR period is 60 sec. (timer is inactive)
```

```
Node IPS State: idle
```

```
IPS Self Detected Requests
```

```
Side A IDLE
```

```
Side B IDLE
```

```
Side A Failures: none
```

```
IPS Remote Requests
```

```
Side A IDLE
```

```
Side B IDLE
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

Side B Failures: none
IPS messages received
Side A (Outer ring RX) { 0009.11d8.3c66,IDLE,SHORT}, TTL 255
Side B (Inner ring RX) { 0012.da6a.f664,IDLE,SHORT}, TTL 255
IPS messages transmitted
Side A (Inner ring TX) { 0800.453d.8644,IDLE,SHORT}, TTL 255
Side B (Outer ring TX) { 0800.453d.8644,IDLE,SHORT}, TTL 255
IPS delay trigger keepalive
Side A: 0 milliseconds
Side B: 0 milliseconds

Topology Map for Interface: SRP0/5/0/0
Topology pkt. sent every 5 sec. (next pkt. after 1 sec.)
Last received topology pkt. 00:00:05
Last topology change was 00:01:59 ago.
Nodes on the ring: 3
Hops (outer ring)      MAC          IP Address      Wrapped SRR      Name
0                      0800.453d.8644  0.0.0.0         No               -      ios
1                      0012.da6a.f664  0.0.0.0         No               -      gsr
2                      0009.11d8.3c66  0.0.0.0         No               -      gsre

SRR not enabled for Interface SRP0/5/0/0

Rate Limit Information for Interface SRP0/5/0/0
Minimum SRP priority value of high priority outgoing/transit traffic: 2

```

Fields from the **show srp** command output with the **interface** keyword are described in [Table 86](#) and [Table 87](#). The minimum SRP priority value for high-priority traffic is set to 2 by default.

show srp ips Sample Output

The following example shows the display from the **show srp** command with the **ips** keyword:

```

RP/0/RP0/CPU0:Router# show srp ips

IPS Information for Interface SRP0/7/0/0
MAC Addresses
Side A (Outer ring RX) neighbor 000e.3900.4800
Side B (Inner ring RX) neighbor 000a.8b08.9600
Node MAC address 0800.453c.f882
IPS State
Side A not wrapped
Side B not wrapped
Side A (Inner ring TX) IPS pkt. sent every 1 sec. (next pkt. after 1 sec.)
Side B (Outer ring TX) IPS pkt. sent every 1 sec. (next pkt. after 1 sec.)
inter card bus disabled
IPS WTR period is 60 sec. (timer is inactive)
Node IPS State: idle
IPS Self Detected Requests      IPS Remote Requests
Side A IDLE                    Side A IDLE
Side B IDLE                    Side B IDLE
Side A Failures: none
Side B Failures: none
IPS messages received
Side A (Outer ring RX) { 000e.3900.4800,IDLE,SHORT}, TTL 255
Side B (Inner ring RX) { 000a.8b08.9600,IDLE,SHORT}, TTL 255
IPS messages transmitted
Side A (Inner ring TX) { 0800.453c.f882,IDLE,SHORT}, TTL 255
Side B (Outer ring TX) { 0800.453c.f882,IDLE,SHORT}, TTL 255
IPS delay trigger keepalive
Side A: 0 milliseconds
Side B: 0 milliseconds

```

[Table 86](#) describes the significant fields shown in the display.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 86** *show srp ips Command Output Fields*

Field	Description
IPS Information for Interface	IPS (Intelligent Protection Switching) identifies the status of an SRP interface on the SRP ring.
MAC Addresses Side A (Outer ring RX) neighbor	MAC address of the next SRP node on the outer ring.
MAC Addresses Side B (Inner ring RX) neighbor	MAC address of the next SRP node on the inner ring.
Node MAC address	MAC address of this SRP node.
IPS State	Reports whether or not a wrap exists on side A or side B of the SRP ring.
IPS WTR period is 60 seconds (timer is inactive)	Displays the current WTR (Wait to Restore) timer value. If a timer is active, the time remaining before the timer expires also is given.
Node IPS State IDLE	Displays the current IPS state of the node. IDLE is the normal state. Other states are WRAPPED and UNKNOWN. Unknown means that the node is in pass-through mode.
IPS self-detected requests	Indicates any locally generated requests. Displays local IPS requests, as well as IDLE status. Possible requests include the following: FS — Forced Switch SF — Signal Fail SD — Signal Degrade MS — Manual Switch WTR — Wait to Restore
IPS remote requests	Indicates any remotely generated requests. Displays remote IPS requests, as well as IDLE status. Possible requests include the following: FS — Forced Switch SF — Signal Fail SD — Signal Degrade MS — Manual Switch WTR — Wait to Restore
IPS messages received	Provides details of the last IPS messages received. Fields within the braces ({}) are the MAC addresses of the sending node and the IPS state (IDLE, FS, and so on). It also indicates either a short or long path.
IPS messages transmitted	Provides details of the last IPS messages transmitted, in the format used for received messages.
IPS delay trigger keepalive	Configured value of the srp ips delay trigger-keepalive command. The default value is 0.

R3.5.0 Beta Draft—Cisco Confidential Information

show srp topology Sample Output

The following example shows the display from the **show srp** command with the **topology** keyword:

```
RP/0/RP0/CPU0:Router# show srp topology
```

```
Topology Map for Interface SRP0/7/0/0
Topology pkt. sent every 5 sec. (next pkt. after 5 sec.)
Last received topology pkt. 00:00:01
Last topology change was 00:09:44 ago.
Nodes on the ring: 3
Hops (outer ring)      MAC          IP Address      Wrapped SRR      Name
0                      0800.453c.f882  30.30.30.2      No               -      crs1
1                      000a.8b08.9600  30.30.30.1      No               -      gsra
2                      000e.3900.4800  30.30.30.3      No               -      gsrB
```

Table 87 describes the significant fields shown in the display.

Table 87 *show srp topology Command Output Fields*

Field	Description
Topology map for interface	Displays SRP topology information that identifies the SRP interface.
Topology packet sent every 10 seconds (next packet after 5 seconds)	Displays the interval between successive topology packets sent from this node and the time until the next one is to be sent (rounded down to the nearest second).
Last received topology packet 00:00:04	Displays the time since the last topology packet was received at this node.
Nodes on the ring: 4	Displays the number of nodes in the current ring topology.
Hops	Displays the number of hops to the destination node along the outer ring (from side B). The local node is at hop count zero.
MAC	Displays the MAC address of the node.
IP Address	Displays the IP address of the SRP interface on the node. If the address is not known, the text string “unknown” is displayed. The IP address information is gathered by the ARP table. When a ring is first established, it is normal for the IP address of a node to remain unknown until some time after the MAC address is known.
Wrapped	Uses Yes or No to indicates whether the SRP ring is wrapped at that node.
SRR	Indicates whether SRR is enabled on the node.
Name	Displays the hostname of the router. If the name is not known, this field is left blank. The hostname is obtained from information that is broadcast on the ring at a slower rate than other topology information. When a ring is first established, it is normal for the hostname of a remote node to remain unknown until some time after the MAC address is known.

show srp transit Sample Output

The following example shows the display from the **show srp** command with the **transit** keyword:

R3.5.0 Beta Draft—Cisco Confidential Information

RP/0/RP0/CPU0:Router# **show srp transit interface srp 0/7/0/0**

Transit Buffer Delay Counters for Interface SRP0/7/0/0

Side A:

Transit Delay (5 Minutes)	Nanoseconds
Low TB Min Delay:	0
Low TB Avg Delay:	0
Low TB Max Delay:	0
High TB Min Delay:	569
High TB Avg Delay:	569
High TB Max Delay:	570

Side B:

Transit Delay (5 Minutes)	Nanoseconds
Low TB Min Delay:	0
Low TB Avg Delay:	0
Low TB Max Delay:	0
High TB Min Delay:	15
High TB Avg Delay:	261
High TB Max Delay:	574

Table 88 describes the significant fields shown in the display.

Table 88 *show srp transit Command Output Fields*

Field	Description
Low TB Min Delay	Minimum value for the low transit buffer as calculated over the last load interval.
Low TB Avg Delay	Average value for the low transit buffer as calculated over the last load interval.
Low TB Max Delay	Maximum value for the low transit buffer as calculated over the last load interval.
High TB Min Delay	Minimum value for the high transit buffer as calculated over the last load interval.
High TB Avg Delay	Average value for the high transit buffer as calculated over the last load interval.
High TB Max Delay	Maximum value for the high transit buffer as calculated over the last load interval.

Related Commands

Command	Description
clear srp counters	Clears the various SRP packet counters.
load-interval	Sets the time (in seconds) used to gather data for computing load statistics.
show controllers sonet	Displays the SONET controller information for the interface.
show controllers srp	Displays the current controller configuration on an SRP interface.
show interfaces srp	Displays current IPS wrap state, along with other SRP interface information.

R3.5.0 Beta Draft—Cisco Confidential Information

srp ips delay trigger-keepalive

To specify a delay for the IPS keepalive value, use the **srp ips delay keep-alive** command in interface configuration mode. To restore the default value, use the **no** form of this command.

srp ips delay trigger-keepalive *value* {**a** | **b**}

no srp ips delay trigger-keepalive *value* {**a** | **b**}

Syntax Description

<i>value</i>	Time in milliseconds of the trigger keepalive. Values can range from 51 to 200.
a	The side of a node that has outer ring receive fiber is identified as side A.
b	The side of a node that has inner ring receive fiber is identified as side B.

Defaults

The default IPS keepalive delay value is 0.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2.2	This command was introduced on the Cisco CRS-1 and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The default keepalive value is 1 ms. Use the **srp ips delay trigger-keepalive** command to delay this 1 ms up to the configured delay value. You should use this command only if the Layer 1 (SONET) is already protected (for example, with SONET APS). This delay gives the first protection mechanism time to protect, before the Layer 2 protection is enabled. For example, if an SRP side is connected to an Add-Drop Multiplexer (ADM) that utilizes dual SONET ring and APS, you should delay the Layer 2 keepalive value using this command.

Task ID

Task ID	Operations
pos-dpt	read, write

Examples

The following example indicates how to set the trigger keepalive timer to 60 milliseconds:

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

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:Router(config)# interface srp 0/5/0/0
RP/0/RP0/CPU0:Router(config-if)# srp ips delay trigger-keepalive 60 a
```

Related Commands	Command	Description
	show srp	Displays information about SRP interfaces on the ring, including MAC addresses of neighboring nodes, IPS status, source-counters, and topology map.

R3.5.0 Beta Draft—Cisco Confidential Information

srp ips request forced-switch

To initiate a forced-switch wrap on a ring, use the **srp ips request forced-switch** command in interface configuration mode. To remove the wrap, use the **no** form of this command.

srp ips request forced-switch {a | b}

no srp ips request forced-switch {a | b}

Syntax Description

a	The side of a node that has outer ring receive fiber is identified as side A.
b	The side of a node that has inner ring receive fiber is identified as side B.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2.2	This command was introduced on the Cisco CRS-1 and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
pos-dpt	read, write

Examples

The following example shows how to insert a forced-switch wrap on side A of the interface by entering the **srp ips request forced-switch** command:

```
RP/0/RP0/CPU0:Router# configure
RP/0/RP0/CPU0:Router(config)# interface srp 0/5/0/0
RP/0/RP0/CPU0:Router(config-if)# srp ips request forced-switch a
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show interfaces srp	Displays current IPS wrap state, along with other SRP interface information.
	show srp	Displays information about SRP interfaces on the ring, including MAC addresses of neighboring nodes, IPS status, source-counters, and topology map.
	srp ips wtr-timer	Determines how long a wrap remains on the fiber after the original cause of the wrap is removed.
	srp manual-switch	Inserts a manual-switch wrap on the ring.
	srp shutdown	Provides an alternative form of the srp ips request forced-switch command.

R3.5.0 Beta Draft—Cisco Confidential Information

srp ips timer

To control the frequency of the transmission of Intelligent Protection Switching (IPS) requests, use the **srp ips timer** command in interface configuration mode. To restore the default value, use the **no** form of this command.

srp ips timer *value*

no srp ips timer *value*

Syntax Description	<i>value</i>	Amount of time in seconds between transmission of IPS requests. Values can range from 1 to 60.

Defaults	The default IPS timer value is 1 second.

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.2.2	This command was introduced on the Cisco CRS-1 and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
	Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

In general, you should not need to adjust the IPS timer value.

We recommend that you configure the same IPS timer value on all nodes on an SRP ring. This means that if you modify the IPS timer setting on one node, you must reconfigure all other nodes on the ring with the same IPS timer value.

Task ID	Task ID	Operations
	pos-dpt	read, write

Examples	The following example indicates how to change the IPS timer to 30 seconds:

```
RP/0/RP0/CPU0:Router# config
RP/0/RP0/CPU0:Router(config)# interface srp 0/5/0/0
RP/0/RP0/CPU0:Router(config-if)# srp ips timer 30
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show srp	Displays information about SRP interfaces on the ring, including MAC addresses of neighboring nodes, IPS status, source-counters, and topology map.
	srp ips wtr-timer	Determines how long a wrap remains on the fiber after the original cause of the wrap is removed.

R3.5.0 Beta Draft—Cisco Confidential Information

srp ips wtr-timer

To control the amount of time to wait before a wrap is removed after there is no more reason for the wrap, use the **srp ips wtr-timer** command in interface configuration mode. To restore the default value, use the **no** form of this command.

srp ips wtr-timer *value*

no srp ips wtr-timer *value*

Syntax Description	<i>value</i>	Amount of time in seconds for the wait-to-restore (WTR) timer. Values can range from 10 to 600.

Defaults	The default WTR timer value is 60 seconds.

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.2.2	This command was introduced on the Cisco CRS-1 and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
	Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	In general, you should not need to adjust the Intelligent Protection Switching (IPS) wait-to-restore (WTR) timer value.

Task ID	Task ID	Operations
	pos-dpt	read, write

Examples	The following example indicates how to change the IPS wait-to-restore timer to 120 seconds:

```
RP/0/RP0/CPU0:Router# config
RP/0/RP0/CPU0:Router(config)# interface srp 0/5/0/0
RP/0/RP0/CPU0:Router(config-if)# srp ips wtr-timer 120
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show srp	Displays information about SRP interfaces on the ring, including MAC addresses of neighboring nodes, IPS status, source-counters, and topology map.
	srp ips timer	Controls the frequency of the transmission of SRP IPS packets.

R3.5.0 Beta Draft—Cisco Confidential Information

srp mac-count

To keep track of the number of SRP packets from a specific source MAC address, use the **srp mac-count** command in interface configuration mode. To disable counting by MAC address, use the **no** form of this command.

srp mac-count *mac-address*

no srp mac-count *mac-address*

Syntax Description	<i>mac-address</i>	48-bit source MAC address from which to count SRP packets.

Defaults	The srp mac-count command is disabled by default.

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.2.2	This command was introduced on the Cisco CRS-1 and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
	Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	pos-dpt	read, write

Examples	The following example shows how to count SRP packets from the source with MAC address 2.2.2:

```
RP/0/RP0/CPU0:Router# config
RP/0/RP0/CPU0:Router(config)# interface srp 0/5/0/0
RP/0/RP0/CPU0:Router(config-if)# srp mac-count 2.2.2
```

Related Commands

R3.5.0 Beta Draft—Cisco Confidential Information

Command	Description
clear srp counters	Clears the various SRP packet counters.
show srp	Displays information about SRP interfaces on the ring, including MAC addresses of neighboring nodes, IPS status, source-counters, and topology map.

R3.5.0 Beta Draft—Cisco Confidential Information

srp mac-reject

To reject SRP packets from a specific source MAC address, use the **srp mac-reject** command in interface configuration mode. To disable rejection by MAC address, use the **no** form of this command.

srp mac-reject *mac-address*

no srp mac-reject *mac-address*

Syntax Description	<i>mac-address</i>	48-bit source MAC address from which to reject SRP packets.

Defaults	The srp mac-reject command is disabled by default.

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.2.2	This command was introduced on the Cisco CRS-1 and is supported on the 4-port OC-192c/STM-64c POS/DPT PLIM.
	Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Use srp mac-reject command to control a node that cannot be fixed because it is owned or administered by someone else. For example, if such a node is flooding your node with packets, you can use this command to limit the amount of traffic that is processed.

Task ID	Task ID	Operations
	pos-dpt	read, write

Examples	The following example shows how to reject SRP packets from the source with MAC address 2.2.2:

```
RP/0/RP0/CPU0:Router# config
RP/0/RP0/CPU0:Router(config)# interface srp 0/5/0/0
RP/0/RP0/CPU0:Router(config-if)# srp mac-reject 2.2.2
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	clear srp counters	Clears the various SRP packet counters.
	show srp	Displays information about SRP interfaces on the ring, including MAC addresses of neighboring nodes, IPS status, source-counters, and topology map.

R3.5.0 Beta Draft—Cisco Confidential Information

srp manual-switch

To initiate or remove a manual switch wrap on a ring, use the **srp manual-switch** command in EXEC mode.

srp {**request** | **remove**} **manual-switch** {**a** | **b**} **interface** **srp** *instance*

Syntax Description

request	Initiate a manual switch wrap on the interface.
remove	Remove a manual switch wrap on the interface.
a	The side of a node that has outer ring receive fiber is identified as side A.
b	The side of a node that has inner ring receive fiber is identified as side B.
interface	Specifies the interface for which to display the counters.
srp	Specifies an SRP interface.
<i>instance</i>	Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. <i>port</i>: Physical port number of the interface. An SRP interface is comprised of two consecutive physical ports and is named according to the first, lower-numbered port. For example, the SRP interface 0/4/0/2 is comprised of the two physical ports 0/4/0/2 and 0/4/0/3. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2.2	This command was introduced on the Cisco CRS-1 and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.
Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
pos-dpt	read, write

Examples

The following example shows how to insert a manual switch wrap on side A of the interface:

```
RP/0/RP0/CPU0:Router# srp request manual-switch a interface srp 0/5/0/0
```

Related Commands

Command	Description
show interfaces srp	Displays current IPS wrap state, along with other SRP interface information.
show srp	Displays information about SRP interfaces on the ring, including MAC addresses of neighboring nodes, IPS status, source-counters, and topology map.
srp ips request forced-switch	Inserts a forced switch wrap on the ring; this command is an alternate form of the srp shutdown command.
srp ips wtr-timer	Determines how long a wrap remains on the fiber after the original cause of the wrap is removed.
srp shutdown	Provides an alternative form of the srp ips request forced-switch command.

R3.5.0 Beta Draft—Cisco Confidential Information

srp priority-threshold

To specify the RAC threshold for placing packets in the high-priority queue, use the **srp priority-threshold** command in Interface configuration mode. To return the priority threshold to its default value, use the **no** form of this command.

srp priority-threshold [*RAC-threshold* | **non-high**]

no srp priority-threshold [*RAC-threshold* | **non-high**]

Syntax Description

<i>RAC-threshold</i>	RAC priority slicing point threshold ranging from 1 to 7.
non-high	Specifies not to place any packets into the RAC high priority transmit queue.

Defaults

Is there a default RAC threshold?

No default behavior or values???

Command Modes

Interface configuration

Command History

Release	Modification
3.2.2	This command was introduced on the Cisco CRS-1.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Examples

The following example shows how to qualify traffic with a RAC of 5 or greater into the high-priority transmit queue:

```
RP/0/RP0/CPU0:Router# config
RP/0/RP0/CPU0:Router(config)# interface srp 0/5/0/0
RP/0/RP0/CPU0:Router(config-if)# srp priority-threshold 5
```

Related Commands

Command	Description
show srp	Displays information about SRP interfaces on the ring, including MAC addresses of neighboring nodes, IPS status, source-counters, and topology map.

R3.5.0 Beta Draft—Cisco Confidential Information

srp rate-limit

To configure the amount of high- and low-priority traffic being transmitted from the router onto the SRP ring, use the **srp rate-limit** command in Interface configuration mode. To disable rate limiting, use the **no** form of this command.

rate-limit [**high** | **low**] *limit*

no rate-limit [**high** | **low**] *limit*

Syntax Description	high	Specifies the SRP high priority transmit queue rate limit.
	low	Specifies the SRP low priority transmit queue rate limit.
	<i>limit</i>	Rate limit in Mbps. The value can range from 0 to 4,294,967,295.

Defaults	Is there a default behavior?
	No default behavior or values

Command Modes	Interface configuration

Command History	Release	Modification
	3.2.2	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Examples	The following example shows how to limit the traffic in the high and low priority traffic to the SRP ring:

```
RP/0/RP0/CPU0:Router# config
RP/0/RP0/CPU0:Router(config)# interface srp 0/5/0/0
RP/0/RP0/CPU0:Router(config-if)# srp rate-limit high 622
RP/0/RP0/CPU0:Router(config-if)# srp rate-limit low 1866
```

Related Commands	Command	Description
	show srp	Displays information about SRP interfaces on the ring, including MAC addresses of neighboring nodes, IPS status, source-counters, and topology map.

R3.5.0 Beta Draft—Cisco Confidential Information

srp shutdown

To shut down an interface by entering a forced switch, use the **srp shutdown** command in interface configuration mode. To remove the forced switch wrap near the interface, use the **no** form of this command.

srp shutdown

no srp shutdown

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Interface configuration

Command History	Release	Modification
	Release 3.2.2	This command was introduced on the Cisco CRS-1 and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
	Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	pos-dpt	read, write

Examples The following example shows how to enter a forced switch on the interface:

```
RP/0/RP0/CPU0:Router# config
RP/0/RP0/CPU0:Router(config)# interface srp 0/5/0/0
RP/0/RP0/CPU0:Router(config-if)# srp shutdown
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show interfaces srp	Displays current IPS wrap state along with other SRP interface information.
	show srp	Displays information about SRP interfaces on the ring, including MAC addresses of neighboring nodes, IPS status, source-counters, and topology map.
	srp ips request forced-switch	Inserts a forced switch wrap on the ring; this command is an alternate form of the srp shutdown command.

R3.5.0 Beta Draft—Cisco Confidential Information

srp topology-timer

To specify the frequency of the topology timer, use the **srp topology-timer** command in interface configuration mode. To restore the default value, use the **no** form of this command.

srp topology-timer *value*

no srp topology-timer *value*

Syntax Description	<i>value</i>	Value of topology timer in seconds, ranging from 1 to 600.

Defaults	The default topology timer value is 10 seconds.

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.2.2	This command was introduced on the Cisco CRS-1 and is supported only on the 4-port OC-192c/STM-64c POS/DPT PLIM.
	Release 3.4.0	This command was first supported on the 16-port OC-48c/STM-16c POS/DPT PLIM.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	The srp topology-timer interface configuration command determines how frequently topology discovery messages are sent around the ring to identify the current nodes on the SRP ring.
	In general, you should not need to adjust the topology timer value.

Task ID	Task ID	Operations
	pos-dpt	read, write

Examples	The following example indicates how to change the topology timer to 300 seconds:

```
RP/0/RP0/CPU0:Router# config
RP/0/RP0/CPU0:Router(config)# interface srp 0/5/0/0
RP/0/RP0/CPU0:Router(config-if)# srp topology-timer 1
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show srp	Displays information about SRP interfaces on the ring, including MAC addresses of neighboring nodes, IPS status, source-counters, and topology map.



Ethernet Interface Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

This module describes the Cisco IOS XR commands used to configure the Ethernet interfaces.



Note

This module does not include the commands for Management Ethernet interfaces. To configure a Management Ethernet interface for routing or modify the configuration of a Management Ethernet interface, use the commands described in the [Management Ethernet Interface Commands on Cisco IOS XR Software](#) module earlier in this document.

R3.5.0 Beta Draft—Cisco Confidential Information

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 <i>milliseconds</i>	Length of time, in milliseconds, to delay the processing of hardware link down notifications. Range is from 1 through 5000.
up <i>milliseconds</i>	Length of time, in milliseconds, to delay the processing of hardware link up notifications. Range is from 1 through 5000.

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was first introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	The msec keyword was replaced by the down keyword, and the up milliseconds keyword argument was added.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	interface	read, write

Examples

The following 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	Limits propagation of transient or frequently changing interface states on Interface Manager (IM) clients.

R3.5.0 Beta Draft—Cisco Confidential Information

clear mac-accounting (Ethernet)

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

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

Syntax Description

{ GigabitEthernet TenGigE FastEthernet }	Type of Ethernet interface whose MAC accounting statistics you want to clear. Enter GigabitEthernet , TenGigE , or FastEthernet . Note Fast Ethernet interfaces are available only on the Cisco XR 12000 Series Router.
<i>instance</i>	Interface whose MAC accounting statistics you want to clear. The naming notation is <i>rack/slot/module/port</i> , 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 or modular services card. - module—Module number. A physical layer interface module (PLIM) is always 0. - port—Physical port number of the interface. The instance argument is entered in the <i>rack/slot/module/port</i> notation. Note For more information about the syntax for the router, use the question mark (?) online help function.
location <i>node-id</i>	(Optional) Clears MAC accounting statistics for the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was first introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.5.0 Beta Draft—Cisco Confidential Information

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

Examples

The following 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	Configures MAC accounting on an interface.
show mac-accounting (Ethernet)	Displays MAC accounting statistics for an interface.

R3.5.0 Beta Draft—Cisco Confidential Information

duplex full (Fast Ethernet)

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

duplex full

no duplex full

Syntax Description This command has no arguments or keywords.

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

Command Modes Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	No modification.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

**Note**

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

Task ID

Task ID	Operations
interface	read, write

Examples

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

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

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	duplex half (Fast Ethernet)	Configures half-duplex operation on a Fast Ethernet interface.
	negotiation auto	Enables link autonegotiation on Gigabit Ethernet and Fast Ethernet interfaces.
	show interfaces	Displays statistics for all interfaces configured on the router.
	speed (Fast Ethernet)	Configures the speed for a Fast Ethernet interface.

R3.5.0 Beta Draft—Cisco Confidential Information

duplex half (Fast Ethernet)

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

duplex half

no duplex half

Syntax Description This command has no arguments or keywords.

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

Command Modes Interface configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	No modification.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

**Note**

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

Task ID	Task ID	Operations
	interface	read, write

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

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

R3.5.0 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	duplex full (Fast Ethernet)	Configures full-duplex operation on a Fast Ethernet interface.
	negotiation auto	Enables link autonegotiation on Gigabit Ethernet and Fast Ethernet interfaces.
	show interfaces	Displays statistics for all interfaces configured on the router.
	speed (Fast Ethernet)	Configures the speed for a Fast Ethernet interface.

R3.5.0 Beta Draft—Cisco Confidential Information

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	Sends flow-control pause frames for both ingress and egress traffic.
	egress	Sends flow-control pause frames for egress traffic.
	ingress	Sends flow-control pause frames for ingress traffic.

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

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.0	This command was introduced on the Cisco CRS-1.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

**Note**

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

**Note**

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

R3.5.0 Beta Draft—Cisco Confidential Information**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

The following 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](#)

Displays statistics for all interfaces configured on the router.

R3.5.0 Beta Draft—Cisco Confidential Information

interface FastEthernet

To enter interface configuration mode for a Fast Ethernet interface, use the **interface FastEthernet** command in global configuration mode. To delete a Fast Ethernet interface configuration, use the **no** form of this command.

interface FastEthernet *instance*

no interface FastEthernet *instance*

Syntax Description

<i>instance</i>	Physical interface instance. Naming notation is <i>rack/slot/module/port</i> , and a slash between values is required as part of the notation. • <i>rack</i>—Chassis number of the rack. • <i>slot</i>—Physical slot number of the card. • <i>module</i>—Module number. A physical layer interface module (PLIM) is always 0. • <i>port</i>—Physical port number of the interface. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter interface configuration mode for a Fast Ethernet interface:

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

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router.

R3.5.0 Beta Draft—Cisco Confidential Information

interface GigabitEthernet

To enter interface configuration mode for a Gigabit Ethernet interface, use the **interface GigabitEthernet** command in global configuration mode. To delete a Gigabit Ethernet interface configuration, use the **no** form of this command.

interface GigabitEthernet *instance*

no interface GigabitEthernet *instance*

Syntax Description	<i>instance</i> Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>—Chassis number of the rack. <i>slot</i>—Physical slot number of the card. <i>module</i>—Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>—Physical port number of the interface. Note For more information about the syntax for the router, use the question mark (?) online help function.

Defaults	No default behavior or values

Command Modes	Global configuration

Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>Release 3.2</td><td>This command was introduced on the Cisco XR 12000 Series Router.</td></tr> <tr> <td>Release 3.3.0</td><td>No modification.</td></tr> <tr> <td>Release 3.4.0</td><td>No modification.</td></tr> <tr> <td>Release 3.5.0</td><td>No modification.</td></tr> </table>	Release	Modification	Release 3.2	This command was introduced on the Cisco XR 12000 Series Router.	Release 3.3.0	No modification.	Release 3.4.0	No modification.	Release 3.5.0	No modification.
Release	Modification										
Release 3.2	This command was introduced on the Cisco XR 12000 Series Router.										
Release 3.3.0	No modification.										
Release 3.4.0	No modification.										
Release 3.5.0	No modification.										

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	<table> <tr> <th>Task ID</th><th>Operations</th></tr> <tr> <td>interface</td><td>read, write</td></tr> </table>	Task ID	Operations	interface	read, write
Task ID	Operations				
interface	read, write				

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

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

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

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router.

R3.5.0 Beta Draft—Cisco Confidential Information

interface TenGigE

To enter interface configuration mode for a 10-Gigabit Ethernet interface, use the **interface TenGigE** command in global configuration mode. To delete a 10-Gigabit Ethernet interface configuration, use the **no** form of this command.

interface TenGigE *instance*

no interface TenGigE *instance*

Syntax Description

<i>instance</i>	Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. – <i>rack</i>—Chassis number of the rack. – <i>slot</i>—Physical slot number of the card. – <i>module</i>—Module number. A physical layer interface module (PLIM) is always 0. – <i>port</i>—Physical port number of the interface. Note For more information about the syntax for the router, use the question mark (?) online help function.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
interface	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to enter interface configuration mode for a 10-Gigabit Ethernet interface:

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

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router.

R3.5.0 Beta Draft—Cisco Confidential Information

I2protocol (Ethernet)

To configure Layer 2 protocol tunneling and protocol data unit (PDU) filtering on an Ethernet interface, use the **I2protocol** command in Layer 2 transport configuration mode. To disable a Layer 2 protocol tunneling and Layer 2 protocol data units configuration, use the **no** form of this command.

I2protocol {**cdp** | **pvst** | **stp** | **vtp**} {[**tunnel**] **experimental bits** | **drop**}

no I2protocol

Syntax Description	cdp	Configures Cisco Discovery Protocol (CDP) tunneling and data unit parameters for the Ethernet interface.
	pvst	Configures VLAN spanning tree protocol tunneling and data unit parameters.
	stp	Configures spanning tree protocol tunneling and data unit parameters for the Ethernet interface.
	vtp	Configures VLAN trunk protocol tunneling and data unit parameters.
	tunnel	Tunnels the packets associated with the specified protocol. When you specify the tunnel keyword, the packet destination MAC address is re-written with an alternative address before that packet is sent over a pseudowire. After the packet comes through the other end of the pseudowire, the alternative address reverts to the original destination MAC address.
	experimental bits	Replaces the experimental bits in the MPLS header with the 802.1p bits from the MAC header and vice-versa.
	drop	Drops packets associated with the specified protocol.

Command Default All Layer 2 protocol data units are forwarded through the network without modification.

Command Modes Layer 2 transport configuration

Command History	Release	Modification
	Release 3.4.0	This command was first introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Note The **I2protocol** command is available only when Layer 2 transport port mode is enabled on the interface with the **I2transport** command.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	l2vpn	read, write

Examples

The following example shows how to configure an Ethernet interface to drop CDP packets:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface TenGigE 0/0/0/1
RP/0/RP0/CPU0:router(config-if)# l2transport
RP/0/RP0/CPU0:router(config-if-l2)# l2protocol cdp drop
```

Related Commands

Command	Description
l2transport (Ethernet)	Enables Layer 2 transport port mode on an Ethernet interface and enters Layer 2 transport configuration mode.
show interfaces	Displays statistics for all interfaces configured on the router or for a specific node.

R3.5.0 Beta Draft—Cisco Confidential Information

I2transport (Ethernet)

To enable Layer 2 transport port mode on an Ethernet interface and enter Layer 2 transport configuration mode, use the **I2transport** command in interface configuration mode for an Ethernet interface. To disable Layer 2 transport port mode on an Ethernet interface, use the **no** form of this command.

I2transport

no I2transport

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.4.0	This command was first introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When you issue the **I2transport** command in interface configuration mode, the CLI prompt changes to “config-if-l2,” indicating that you have entered the Layer 2 transport configuration submenu. In the following sample output, the question mark (?) online help function displays all the commands available under Layer 2 transport configuration submenu for an Ethernet interface:

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 0/1/5/0
RP/0/RP0/CPU0:router(config-if)#I2transport
RP/0/RP0/CPU0:router(config-if-l2)#?
  commit          Commit the configuration changes to running
  describe        Describe a command without taking real actions
  do              Run an exec command
  exit            Exit from this submenu
  no              Negate a command or set its defaults
  service-policy  Configure QoS Service policy
  show            Show contents of configuration
RP/0/RP0/CPU0:router(config-if-l2)#
```



Note

The **I2transport** command is mutually exclusive with any Layer 3 interface configuration.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	l2vpn	read, write

Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)#interface GigabitEthernet 0/2/0/0
RP/0/RP0/CPU0:router(config-if)#l2transport
RP/0/RP0/CPU0:router(config-if-l2)#
```

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router or for a specific node.
show l2vpn xconnect	Displays brief information on configured xconnects.

R3.5.0 Beta Draft—Cisco Confidential Information

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 will be looped back internally within the router before reaching an external cable.
	line	Incoming network packets will be looped back through the external cable.

Defaults Loopback mode is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	Release 3.0	This command was introduced on the Cisco CRS-1.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

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



Tip

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

R3.5.0 Beta Draft—Cisco Confidential Information

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
```

R3.5.0 Beta Draft—Cisco Confidential Information

mac-accounting

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

mac-accounting {egress | ingress}

Syntax Description

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

Defaults

MAC accounting is disabled

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.0	This command was first introduced on the Cisco CRS-1.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

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

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

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	clear mac-accounting (Ethernet)	Clears MAC accounting statistics for a specified interface.
	show mac-accounting (Ethernet)	Displays MAC accounting statistics for a specified interface.

R3.5.0 Beta Draft—Cisco Confidential Information

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

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

Command Modes Interface configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	No modification.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

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

Task ID	Task ID	Operations
	interface	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**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
```

R3.5.0 Beta Draft—Cisco Confidential Information

negotiation auto

To enable link autonegotiation on Gigabit Ethernet and Fast 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 arguments or keywords.

Defaults Link autonegotiation is disabled.

Command Modes Interface configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enable link autonegotiation on an interface:

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

The following example shows how to disable link autonegotiation on an interface:

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

R3.5.0 Beta Draft—Cisco Confidential Information

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 802.3ae specification, use the **no** form of this command.

packet-gap non-standard

no packet-gap non-standard

Syntax Description

This command has no arguments or keywords.

Defaults

The interface uses the standard packet interval as defined by the IEEE 802.3ae specification.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.0	This command was first introduced on the Cisco CRS-1.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 802.3ae 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

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

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(config)# interface TenGigE 0/3/0/0  
RP/0/RP0/CPU0:router(config-if)# packet-gap non-standard
```

R3.5.0 Beta Draft—Cisco Confidential Information

show mac-accounting (Ethernet)

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

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

Syntax Description	{ GigabitEthernet TenGigE FastEthernet } Indicates the type of Ethernet interface whose MAC accounting statistics you want to display. Enter GigabitEthernet, TenGigE, or FastEthernet. Note Fast Ethernet interfaces are available only on the Cisco XR 12000 Series Router. <i>instance</i> (Optional) Displays detailed MAC accounting information for the specified interface. The naming notation is <i>rack/slot/module/port</i>, and a slash between values is required as part of the notation. • <i>rack</i>—Chassis number of the rack. • <i>slot</i>—Physical slot number of the line card or modular services card. • <i>module</i>—Module number. A physical layer interface module (PLIM) is always 0. • <i>port</i>—Physical port number of the interface. The instance argument is entered in the <i>rack/slot/module/port</i> notation. Note For more information about the syntax for the router, use the question mark (?) online help function. location <i>node-id</i> (Optional) Displays detailed MAC accounting information for the specified interface on the specified node. The <i>node-id</i> argument is entered in the <i>rack/slot/module/port</i> notation.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release Modification Release 3.0 This command was first introduced on the Cisco CRS-1. Release 3.2 This command was first supported on the Cisco XR 12000 Series Router. Release 3.3.0 No modification. Release 3.4.0 No modification. Release 3.5.0 No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID

Task ID	Operations
interface	read

Examples

The following is sample output from the **show mac-accounting** command, which displays MAC accounting statistics on the specified interface:

```
RP/0/RP0/CPU0:router# show mac-accounting TenGigE 0/2/0/4 location 0/1/CPU0

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

[Table 89](#) describes the significant fields shown in the display.

Table 89 *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.

Related Commands

Command	Description
clear mac-accounting (Ethernet)	Clears MAC accounting statistics.
mac-accounting	Generates MAC accounting statistics.

R3.5.0 Beta Draft—Cisco Confidential Information

speed (Fast Ethernet)

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

speed {10 | 100 | 1000}

no speed

Syntax Description

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

Defaults

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

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

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.



Note

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



Note

Keep in mind that both ends of a link must have the same interface speed. A manually configured interface speed 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.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	interface	read, write

Examples

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

```
RP/0/RP0/CPU0:router(config)# interface FastEthernet 0/0/2/0
RP/0/RP0/CPU0:router(config-if)# speed 1000
```




802.1Q VLAN Subinterface Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

This module contains commands for configuring and monitoring 802.1Q VLAN commands on Cisco IOS XR software.

R3.5.0 Beta Draft—Cisco Confidential Information

dot1q native vlan

To assign the native VLAN ID of a physical interface trunking 802.1Q VLAN traffic, use the **dot1q native vlan** command in interface configuration mode. To remove the VLAN ID assignment, use the **no** form of this command.

dot1q native vlan *vlan-id*

no dot1q native vlan *vlan-id*

Syntax Description	<i>vlan-id</i> Trunk interface ID. Range is from 1 to 4094 inclusive (0 and 4095 are reserved).

Defaults	No default behavior or values

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.0	This command was introduced on the Cisco CRS-1.
	Release 3.2	No modification.
	Release 3.3.0	Support was added for this command on Cisco CRS-1 shared port adapters (SPAs).
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

The **dot1q native vlan** command defines the default, or native VLAN, associated with a 802.1Q trunk interface. The native VLAN of a trunk interface is the VLAN to which all untagged VLAN packets are logically assigned.



Note

The native VLAN cannot be configured on a subinterface of the trunk interface. The native VLAN must be configured with the same value at both ends of the link, or traffic can be lost or sent to the wrong VLAN.

Task ID	Task ID	Operations
	vlan	read, write

R3.5.0 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to configure the native VLAN of a TenGigE0/2/0/4 trunk interface as 1. Packets received on this interface that are untagged, or that have an 802.1Q tag with VLAN ID 1, are received on the main interface. Packets sent from the main interface are transmitted without an 802.1Q tag.

```
RP/0/RP0/CPU0:router(config)# interface TenGigE 0/2/0/4
RP/0/RP0/CPU0:router(config-if)# dot1q native vlan 1
```

Related Commands

Command	Description
dot1q vlan	Assigns a VLAN ID to a subinterface, or changes the VLAN ID assigned to a subinterface.

R3.5.0 Beta Draft—Cisco Confidential Information

dot1q tunneling ethertype 0x9100

To configure the Ethertype used by peer devices when implementing Q-in-Q VLAN tagging to be 0x9100, use the **dot1q tunneling ethertype** command in interface configuration mode for an Ethernet interface. To return to the default configuration of Ethertype 0x8100, use the **no** form of this command.

```
dot1q tunneling ethertype 0x9100

no dot1q tunneling ethertype 0x9100
```

Syntax Description This command has no arguments or keywords.

Defaults The Ethertype field used by peer devices when implementing Q-in-Q VLAN tagging is 0x8100.

Command Modes Interface configuration

Command History	Release	Modification
	Release 3.4.0	This command was first introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Q-in-Q tunneling uses a second ethertype and VLAN identification field that allows a service provider tag to be added to a packet that already has a customer VLAN tag.

Use the **dot1q tunneling ethertype 0x9100** command if the peer switching devices are using an Ethertype field value of 0x9100. All Cisco switching devices use the default Ethertype field value of 0x8100.

After you issue the **dot1q tunneling ethertype 0x9100** command, all peer devices will use that Ethertype when implementing Q-in-Q VLAN tagging.

Task ID	Task ID	Operations
	vlan	read, write

Examples

The following example shows how to configure the inter-packet gap for a 10-Gigabit Ethernet interface:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config-if)# interface GigabitEthernet 0/1/5/0
RP/0/0/CPU0:router(config-if)# dot1q tunneling ethertype 0x9100
```

R3.5.0 Beta Draft—Cisco Confidential Information**Related Commands**

Command	Description
dot1q vlan	Assigns a VLAN ID to a subinterface, or modifies the VLAN ID that is currently assigned to a subinterface.

R3.5.0 Beta Draft—Cisco Confidential Information

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.

On the Cisco CRS-1:

```
dot1q vlan vlan-id
```

```
no dot1q vlan vlan-id
```

On the Cisco XR 12000 Series Router.

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

```
no dot1q vlan vlan-id
```

Syntax Description	<i>vlan-id</i>	ID of the subinterface. Range is from 1 to 4094 (0 and 4095 are reserved).
	<i>vlan-id2</i>	(Optional) Identifies the host VLAN of a Q-in-Q VLAN pair. Replace <i>vlan-id2</i> with a number that specifies the host VLAN. Range is from 1 to 4094.
		Note The <i>vlan-id2</i> argument is available for Q-in-Q VLANs on a 10-Gigabit Ethernet node that is installed in a Cisco XR 12000 Series Router only.
	any	(Optional) Identifies the host VLAN of a Q-in any VLAN pair.
		Note The any keyword is available for Q-in-any VLANs on a 10-Gigabit Ethernet node that is installed in a Cisco XR 12000 Series Router only.

Defaults	No default behavior or values

Command Modes	Subinterface configuration

Command History	Release	Modification
	Release 3.0	This command was introduced on the Cisco CRS-1.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface TenGigE 0/2/0/4.1
RP/0/0/CPU0:router(config-subif)# dot1q vlan 10 20
```

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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface TenGigE 0/2/0/4.1 l2transport
RP/0/0/CPU0:router(config-subif)# dot1q vlan 10 any
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	dot1q native vlan	Defines the native VLAN ID associated with a VLAN trunk.
	show interfaces	Displays statistics for all interfaces configured on the router or for a specific node,
	show vlan interface	Displays summarized information for the VLAN subinterfaces configured on your router.
	show vlan tags	Displays VLAN tagging allocation information.

R3.5.0 Beta Draft—Cisco Confidential Information

interface (VLAN)

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

interface { **GigabitEthernet** | **TenGigE** | **FastEthernet** | **Bundle-Ether** } *instance.subinterface* [**l2transport**]

no interface { **GigabitEthernet** | **TenGigE** | **FastEthernet** | **Bundle-Ether** } *instance.subinterface* [**l2transport**]

Syntax Description	{ GigabitEthernet TenGigE FastEthernet Bundle-Ether } Type of Ethernet interface on which you want to create a VLAN. Enter GigabitEthernet, TenGigE, FastEthernet, or Bundle-Ether. Note Fast Ethernet interfaces are supported on the Cisco XR 12000 Series Router only. Note Ethernet bundles are available on the Cisco CRS-1 only. <i>instance.subinterface</i> Physical interface instance, followed by the subinterface identifier. Naming notation is <i>instance.subinterface</i>, and a period between arguments is required as part of the notation. Replace the <i>instance</i> argument with one of the following Ethernet interface identifiers: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>—Chassis number of the rack. <i>slot</i>—Physical slot number of the card. <i>module</i>—Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>—Physical port number of the interface. - Ethernet Bundle instance. Range is from 1 through 65535. Replace the <i>subinterface</i> argument with the subinterface value. Range is from 0 through 4095. Note 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.

Defaults No default behavior or values

Command Modes Global configuration

R3.5.0 Beta Draft—Cisco Confidential Information**Command History**

Release	Modification
Release 3.0	This command was introduced on the Cisco CRS-1.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

The following 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
```

The following example shows how to create a VLAN subinterface with Layer 2 transport port mode enabled, and enter Layer 2 transport configuration mode under that VLAN:

```
RP/0/0/CPU0:router(config)# interface GigabitEthernet 0/4/0/1.1
```

```
RP/0/RP0/CPU0:router(config-if-l2)#
```

Related Commands

Command	Description
dot1q native vlan	Defines the native VLAN ID associated with a VLAN trunk.
dot1q vlan	Assigns a VLAN ID to a subinterface, or changes the VLAN ID assigned to a subinterface.

R3.5.0 Beta Draft—Cisco Confidential Information

I2protocol (VLAN)

To configure Layer 2 protocol tunneling and data units parameters on an VLAN interface, use the **I2protocol** command in subinterface configuration mode. To disable a Layer 2 protocol tunneling and Layer 2 protocol data units configuration, use the **no** form of this command.

I2protocol { **cdp** | **pvst** | **stp** | **vtp** } {[**tunnel**] **experimental bits** | **drop**}

no I2protocol

Syntax Description	cdp	Configures Cisco Discovery Protocol (CDP) tunneling and data unit parameters for the Ethernet interface.
	pvst	Configures VLAN spanning tree protocol tunneling and data unit parameters.
	stp	Configures spanning tree protocol tunneling and data unit parameters for the Ethernet interface.
	vtp	Configures VLAN trunk protocol tunneling and data unit parameters.
	tunnel	Tunnels the packets associated with the specified protocol.
	experimental bits	Modifies the experimental bits for the specified protocol.
	drop	Drop packets associated with the specified protocol.

Defaults All Layer 2 protocol data units are tunneled through the network without modification.

Command Modes Subinterface configuration

Command History	Release	Modification
	Release 3.4.0	This command was first introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **I2protocol** command is accepted only when Layer 2 transport port mode is enabled on the interface.

Task ID	Task ID	Operations
	I2vpn	read, write

R3.5.0 Beta Draft—Cisco Confidential Information

Examples

The following example shows how configure a VLAN to drop CDP packets:

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

RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 0/1/5/0.1 l2transport

RP/0/RP0/CPU0:router(config-subif)# l2protocol cdp drop
```

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router or for a specific node.
show l2vpn xconnect	Displays brief information on configured xconnects.

R3.5.0 Beta Draft—Cisco Confidential Information

show vlan interface

To display summarized information about VLAN subinterfaces, use the **show vlan interface** command in EXEC mode.

show vlan interface [{ **GigabitEthernet** | **TenGigE** | **FastEthernet** | **Bundle-Ether** } *instance* | **location** *instance*]

Syntax Description	
{ GigabitEthernet TenGigE FastEthernet Bundle-Ether }	(Optional) Type of Ethernet interface whose VLAN information you want to display. Enter GigabitEthernet, TenGigE, FastEthernet, or Bundle-Ether. Note Fast Ethernet interfaces are supported on the Cisco XR 12000 Series Router only. Note Ethernet bundles are available on the Cisco CRS-1 only.
<i>instance.subinterface</i>	Physical interface instance, followed by the subinterface identifier. Naming notation is <i>instance.subinterface</i>, and a period between arguments is required as part of the notation. Replace the <i>instance</i> argument with one of the following Ethernet interface identifiers: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>—Chassis number of the rack. <i>slot</i>—Physical slot number of the card. <i>module</i>—Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>—Physical port number of the interface. - Ethernet Bundle instance. Range is from 1 through 65535. Replace the <i>subinterface</i> argument with the subinterface value. Range is from 0 through 4095. Note For more information about the syntax for the router, use the question mark (?) online help function.
location <i>instance</i>	(Optional) Displays VLAN subinterfaces on a particular port. The <i>instance</i> argument is entered in the <i>rack/slot/module/port</i> notation.

Defaults No default behavior or values

Command Modes EXEC

R3.5.0 Beta Draft—Cisco Confidential Information**Command History**

Release	Modification
Release 3.0	This command was introduced Cisco CRS-1.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Enter the **show vlan interface** command without including any of the optional parameters to display summarized information about all VLANs configured on the router.

Task ID

Task ID	Operations
vlan	read

Examples

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

```
RP/0/RP0/CPU0:router#show vlan interface
```

Interface	Encapsulation	Outer VLAN	2nd VLAN	Service	MTU	LineP State
Gi0/1/5/0.1	802.1Q	10		L3	1518	up
Gi0/1/5/0.2	None			L3	1518	down

```
RP/0/RP0/CPU0:P2_CRS-8#
```

[Table 90](#) describes the significant fields shown in the display.

Table 90 *show vlan interface Field Descriptions*

Field	Description
interface	VLAN subinterface.
encapsulation	Encapsulation of the VLAN subinterface. Currently, this is always 802.1Q.
Outer VLAN	VLAN ID currently assigned to the subinterface. Range is from 1 to 4094 (or blank if no VLAN ID has been assigned).
2nd VLAN	VLAN ID currently assigned to the second subinterface in a pair. Range is from 1 to 4094 (or blank if no VLAN ID has been assigned). For Q-in-any VLANs, this field shows “Any.”
Service	Service currently assigned to the VLAN. Possible services are L2 and L3.

R3.5.0 Beta Draft—Cisco Confidential Information

Table 90 *show vlan interface Field Descriptions (continued)*

Field	Description
MTU	Maximum transmission unit (MTU) value configured for the specified VLAN, in bytes.
LineP state	Displays the line protocol state of the VLAN interface. Possible states: up, down, admin-down. The line protocol state reflects whether a VLAN ID is configured or not.

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router. These statistics include VLAN L2 interface statistics.
show vlan trunks	Displays summary information about VLAN trunk interfaces.

R3.5.0 Beta Draft—Cisco Confidential Information

show vlan tags

To display VLAN tagging allocation information, use the **show vlan tags** command in EXEC mode.

show vlan tags [**Bundle-Ether** *instance* | **GigabitEthernet** *instance* | **TenGigE** *instance* | **location** *node-id*]

Syntax Description	Bundle-Ether <i>instance</i>	Displays VLAN tagging information for a specific Ethernet bundle. Note Use the show interfaces bundle-ether command to see a list of all Ethernet bundles currently configured on the router.
	FastEthernet <i>instance</i>	Displays VLAN tagging information for a specific Fast Ethernet interface. Note Use the show interfaces FastEthernet command to see a list of all Ethernet interfaces currently configured on the router. Note Fast Ethernet interfaces are supported on the Cisco XR 12000 Series Router only.
	GigabitEthernet <i>instance</i>	Displays VLAN tagging information for a specific Gigabit Ethernet interface. Note Use the show interfaces GigabitEthernet command to see a list of all Ethernet interfaces currently configured on the router.
	TenGigE <i>instance</i>	Displays VLAN tagging information for a specific 10-Gigabit Ethernet interface. Note Use the show interfaces TenGigE command to see a list of all 10-Gigabit Ethernet interfaces currently configured on the router.
	location <i>node-id</i>	Displays VLAN tagging information for a specific node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults Enter the command without any of the optional keywords or arguments to display tagging allocation information for all VLANs configured on the router.

Command Modes EXEC

Command History	Release	Modification
	Release 3.4.0	This command was first introduced on the Cisco CRS-1.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	vlan	read

Examples

The following example shows how to display VLAN tagging allocation information for a router:

```
RP/0/RP0/CPU0:router# show vlan tags
```

Interface	Outer VLAN	2nd VLAN	Service	MTU	LineP State
Gi0/1/5/0.1	10		L3	1518	up
Gi0/1/5/0.2	20		L3	1518	up
Gi0/1/5/0.3	30		L3	1518	up

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

Table 91 describes the significant fields shown in the display

Table 91 *show vlan tags Field Descriptions*

Field	Description
Outer Vlan	The first (outermost) 802.1Q VLAN ID. This field is empty if no VLAN ID is configured. An asterisk (*) indicate the native VLAN.
2nd Vlan	The second 802.1Q VLAN ID. This field reports “any” for a Q-in-Any service. If no VLAN ID is configured, then this field is empty.
Service	Service currently assigned to the subinterface. Can be Layer 2 (L2) or Layer 3 (L3).
MTU	Maximum transmission unit (MTU) value configured for the specified VLAN, in bytes.
LineP state	Displays the state of the VLAN interface. Possible states: up, down, admin-down.

Related Commands

Command	Description
dot1q vlan	Assigns a VLAN ID to a subinterface, or modifies the VLAN ID that is currently assigned to a subinterface.
show vlan interface	Displays summary information about each of the VLAN interfaces and subinterfaces.
show vlan trunks	Displays information about the VLAN trunks currently configured on your router.

R3.5.0 Beta Draft—Cisco Confidential Information

show vlan trunks

To display information about VLAN trunks, use the **show vlan trunks** command in EXEC mode.

show vlan trunks [**brief**] [**location** *node-id*] [*type instance*] [**summary**]

Syntax Description		
	<i>type</i>	(Optional) Type of Ethernet interface whose VLAN trunk information you want to display. Possible Ethernet types are GigabitEthernet, TenGigE, FastEthernet, or Bundle-Ether. Note Fast Ethernet interfaces are supported on the Cisco XR 12000 Series Router only. Note Ethernet bundles are available on the Cisco CRS-1 only.
	<i>instance</i>	Either a physical interface instance or an Ethernet Bundle instance. Replace the <i>instance</i> argument with one of the following Ethernet interface identifiers: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>—Chassis number of the rack. <i>slot</i>—Physical slot number of the card. <i>module</i>—Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>—Physical port number of the interface. - Ethernet Bundle instance. Range is from 1 through 65535. Note For more information about the syntax for the router, use the question mark (?) online help function.
	brief	(Optional) Displays a short summary output.
	summary	(Optional) Displays a summarize output. Note The summary option can be specified only if the trunk interface is not specified.
	location <i>node-id</i>	(Optional) Displays VLAN trunk information for a specific node. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation. Note For more information about the syntax for the router, use the question mark (?) online help function.

R3.5.0 Beta Draft—Cisco Confidential Information

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.0	This command was introducedCisco CRS-1.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **show vlan trunks** command provides summary information about VLAN trunk interfaces. It is used to determine the number of configured subinterfaces and verify the state of the subinterfaces.

Task ID	Task ID	Operations
	vlan	read

Examples The following is sample output from the **show vlan trunks** command:

```
RP/0/RP0/CPU0:router# show vlan trunks

GigabitEthernet0/4/0/0 is up
  Outer VLAN tag format is Dot1Q (0x8100)
  L3 Encapsulations: Ether, 802.1Q
    Sub-interfaces: 2
      2 are up
    Single tag sub-interfaces: 2
  No native VLAN Id
  L2 Encapsulations: 802.1Q
    VLAN ACs: 1
      1 are up
    Single tag ACs: 1
```

[Table 92](#) describes the significant fields shown in the display.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 92** *show vlan trunks summary Field Descriptions*

Field	Description
Outer VLAN tag format	The first (outermost) 802.1Q VLAN Id. - This field is empty if no VLAN ID is configured. - An asterisk (*) indicates that a native VLAN is configured.
L3 Encapsulations	VLAN encapsulations currently used for terminated Layer 3 traffic. Possible Layer 3 encapsulations are as follows: - Nat – A Native VLAN is configured. - Q – One or more sub-interfaces are configured with either 0 or 1 802.1Q VLAN tags. 2Q – One or more sub-interfaces have been configured with two 802.1Q VLAN tags.
Sub-interfaces	The number of subinterfaces configured on the main Ethernet interface, and the current state of those subinterfaces. Possible states are up, down, and admin-down. Note The number of Down and Admin-down subinterfaces is only reported only if that number is greater than 0.
Single tag sub-interfaces:	Number of sub-interfaces configured with a single 802.1Q tag. Note The number of sub-interfaces is displayed only if that number is greater than 0.
No native VLAN Id	Indicate that a native VLAN ID is not configured on this interface.
L2 Encapsulations:	VLAN encapsulations currently used for terminated L2 traffic. Possible Layer 2 encapsulations are as follows: - Q – One or more single 802.1Q tag ACs are configured. 2Q – One or more double 802.1Q tag ACs have been configured. - Qany – One or more double 802.1Q tag ACs have been configured that have a wildcard “any” innertag.
VLAN ACs	Number of ACs currently configured under the specified interface.
Single tag ACs	Note The number of sub-interfaces sub-interfaces configured with a single 802.1Q tag is displayed only if that number is greater than 0.

Related Commands

Command	Description
interface (VLAN)	Displays summary information about each of the VLAN interfaces and subinterfaces.



Serial Interface Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

This module describes the commands used to configure serial interfaces on routers supporting Cisco IOS XR software.

R3.5.0 Beta Draft—Cisco Confidential Information

crc (serial)

To set the length of the cyclic redundancy check (CRC) on a serial interface, use the **crc** command in serial configuration mode. To return the CRC setting on a serial interface to the default setting, use the **no** form of this command.

crc {16 | 32}

no crc {16 | 32}

Syntax Description	16	Sets 16-bit CRC mode.
	32	Sets 32-bit CRC mode.

Defaults	16 bits is the default for serial interfaces.

Command Modes	Serial configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.

CRC is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data. The designators 16 and 32 indicate the length (in bits) of the frame check sequence (FCS). A CRC of 32 bits provides more powerful error detection, but adds overhead. Both the sender and receiver must use the same setting.

CRC-16, the most widely used error checking method throughout the United States and Europe, is used extensively with WANs. CRC-32 is specified by IEEE standard 802 and as an option by some point-to-point transmission standards. It is often used on Switched Multimegabit Data Service (SMDS) networks and LANs.

Task ID	Task ID	Operations
	hdlc	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

In the following example, the 32-bit CRC on serial interface 0/3/0/0/0:10 is enabled:

```
RP/0/0/CPU0:Router(config)# interface serial 0/3/0/0/0:10
RP/0/0/CPU0:Router(config-if)# serial
RP/0/0/CPU0:Router(config-if-serial)# crc 32
```

Related Commands

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

R3.5.0 Beta Draft—Cisco Confidential Information

encapsulation (serial)

To set the Layer 2 encapsulation of an interface, use the **encapsulation** command in interface configuration mode. To restore the system to the default encapsulation, use the **no** form of this command.

encapsulation {**hdlc** | **ppp** | **frame-relay**}

no encapsulation

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 encapsulation on the interface.

Defaults For serial interfaces, the default encapsulation is HDLC.

Command Modes Interface configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	Frame Relay encapsulation was supported on serial interfaces.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	hdlc	read, write
	interface	read, write

Examples In the following example, PPP encapsulation is set on serial interface 0/3/0/1:

```
RP/0/RP0/CPU0:router(config)# interface serial 0/3/0/1
```

```
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
```


R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show interfaces	Displays statistics for all interfaces configured on the router.
	show ppp interfaces	Displays PPP state information for an interface.

R3.5.0 Beta Draft—Cisco Confidential Information

interface serial

To configure a serial interface and enter interface or subinterface configuration mode, use the **interface serial** command in global configuration mode.

interface serial *instance* [*.subinterface* **[point-to-point]**]

Syntax Description

<i>instance</i>	Serial interface instance. Naming notation for T3/E3 interfaces is <i>rack/slot/module/port</i> ; naming notation for T1/E1/DS0 interfaces is <i>rack/slot/module/port/t1-num:channel-group-number</i> . A slash between values is required as part of the notation. • <i>rack</i>: Chassis number of the rack. • <i>slot</i>: Physical slot number of the modular services card or line card. • <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. • <i>port</i>: Physical port number of the T3 controller. • <i>t1-num</i>: T1 or E1 channel number. T1 channels range from 0 to 23; E1 channels range from 0 to 30. • <i>channel-group-number</i>: Time slot number. T1 time slots range from 1 to 24; E1 time slots range from 1 to 31. The <i>channel-group-number</i> is preceded by a colon and not a slash. For a complete list of all valid instances, use the question mark (?) online help function.
<i>.subinterface</i>	(Optional) Subinterface instance. Naming notation is <i>.subinterface</i> . The period in front of the <i>subinterface</i> value is required as part of the notation. Replace <i>subinterface</i> with the virtual interface number to be associated with the physical interface. Note For more information about the syntax for the router, use the question mark (?) online help function.
point-to-point	(Optional) Interface functions as one endpoint of a point-to-point link.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the question mark (?) online help function following the **serial** keyword to view a list of all valid interface choices. To reference the serial interface on channel group 3 of T1 channel group 4 on port 2 of a SPA in subslot 1, use the following notation: **interface serial 0/0/1/2/4:3**.

Serial interfaces on channelized T3 can be deleted using the **no channel-group** command in T1 configuration mode. If there are nondefault serial parameters defined, you need to use the **no interface serial** command first to revert to the default configuration, and then delete the serial interface using the **no channel-group** command.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter interface configuration mode for a serial interface in slot 6, subslot 2, port 4, T1 channel number 10 and channel group 8:

```
RP/0/0/CPU0:Router(config)# interface serial 0/6/2/4/10:8
RP/0/0/CPU0:Router(config-if)#
```

The following example shows how to create a subinterface on a serial interface in slot 6, subslot 2, port 3 and enter subinterface configuration mode:

```
RP/0/0/CPU0:Router(config)# interface serial 0/6/2/3.1
RP/0/0/CPU0:Router(config-if)#
```

Related Commands

Command	Description
channel-group	Configures a T1 channel group and enter s channel group configuration mode.
show interfaces	Displays statistics for all interfaces configured on the router or on a specific node.

R3.5.0 Beta Draft—Cisco Confidential Information

keepalive (serial)

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

keepalive {*seconds* | **disable**}

no keepalive

Syntax Description

<i>seconds</i>	Number of seconds that define the keepalive interval. Default is 10 seconds.
disable	Turns off the keepalive timer.

Defaults

seconds = 10 seconds

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

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

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

Task ID

Task ID	Operations
hdlc	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to configure keepalives for 3 seconds on serial interface 0/7/0/1:

```
RP/0/0/CPU0:router(config)# interface serial 0/7/0/1
RP/0/0/CPU0:router(config-if)# keepalive 3
```

Related Commands

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

R3.5.0 Beta Draft—Cisco Confidential Information

invert

To invert the data stream on a serial interface, use the **invert** command in serial configuration mode. To disable data inversion, use the **no** form of this command.

invert

no invert

Syntax Description This command has no arguments or keywords.

Defaults Data is not inverted

Command Modes Serial configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

To verify that data inversion is configured on the interface, use the **show interfaces serial** command.

Task ID	Task ID	Operations
	hdlc	read, write

Examples In the following example, data inversion is enabled on serial interface 0/3/0/0/0:10:

```
RP/0/0/CPU0:Router(config)# interface serial 0/3/0/0/0:10
RP/0/0/CPU0:Router(config-if)# serial
RP/0/0/CPU0:Router(config-if-serial)# invert
```

Related Commands	Command	Description
	show interfaces	Displays statistics for all interfaces configured on the router or on a specific node.

R3.5.0 Beta Draft—Cisco Confidential Information

pvc (serial)

To create a Frame Relay permanent virtual circuit (PVC) under a serial subinterface and enter Frame Relay virtual circuit configuration mode, use the **pvc** command in subinterface configuration mode. To remove a PVC from a subinterface, use the **no** form of this command.

pvc *dlci*

no pvc *dlci*

Syntax Description	<i>dlci</i>	DLCI number used to identify the PVC. Range is from 16 to 1007.
Defaults	No PVC is defined.	
Command Modes	Subinterface configuration	
Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **pvc** command creates a PVC and attaches it to the specified DLCI.

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

When you issue the **pvc** command in global configuration mode, the CLI prompt changes to “config-fr-vc,” indicating that you have entered the Frame Relay virtual circuit configuration submode.

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

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface serial 0/3/2/0.1
RP/0/0/CPU0:router(config-subif)# pvc 20
RP/0/0/CPU0:router(config-fr-vc)# ?

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

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

R3.5.0 Beta Draft—Cisco Confidential Information**Task ID****Task ID****Operations**

fr

read, write

Examples

The following example shows how to create a Frame Relay PVC on a serial subinterface, and enter Frame Relay virtual circuit configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface serial 0/6/0/1.1 point-to-point
RP/0/0/CPU0:router(config-if)# pvc 16
RP/0/0/CPU0:router(config-fr-vc)#
```


R3.5.0 Beta Draft—Cisco Confidential Information

scramble

To enable payload scrambling (encryption) on a serial interface, use the **scramble** command in interface configuration mode. To disable scrambling, use the **no** form of this command.

scramble

no scramble

Syntax Description This command has no arguments or keywords.

Defaults Scrambling is disabled

Command Modes Interface configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Scrambling is used to assist clock recovery on the receiving end. Scrambling is designed to randomize the pattern of 1s and 0s carried in the physical layer frame. Randomizing the digital bits can prevent continuous, nonvariable bit patterns—in other words, long strings of all 1s or all 0s. Several physical layer protocols rely on transitions between 1s and 0s to maintain clocking.

Scrambling can prevent some bit patterns from being mistakenly interpreted as alarms by switches placed between the Data Service Units (DSUs).

The local interface configuration must match the remote interface configuration. For example, if you enable scrambling on the local port, you must also do the same on the remote port.

To verify that scrambling is configured on the interface, use the **show interfaces serial** command.

Task ID	Task ID	Operations
	hdlc	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

In the following example, scrambling is enabled on serial interface 0/3/0/0/0:10:

```
RP/0/0/CPU0:Router(config)# interface serial 0/3/0/0/0:10
RP/0/0/CPU0:Router(config-if)# serial
RP/0/0/CPU0:Router(config-if-serial)# scramble
```

Related Commands

Command	Description
show controllers t3	Displays information about the T3 controllers.

R3.5.0 Beta Draft—Cisco Confidential Information

serial

To configure the serial parameters and enter serial configuration mode, use the **serial** command in interface configuration mode. To return to the default state of the serial interface, use the **no** form of this command.

serial

no serial

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.

Serial interfaces are automatically created for unchannelized ports; for channelized ports, serial interfaces are created when you add T1/E1 channel groups.

Task ID	Task ID	Operations
	hdlc	read, write

Examples	The following example shows how to enter serial configuration mode:

```
RP/0/0/CPU0:Router(config-if)# serial
RP/0/0/CPU0:Router(config-if-serial)#
```

R3.5.0 Beta Draft—Cisco Confidential Information

transmit-delay (serial)

To specify a number of High-Level Data Link Control (HDLC) flag sequences to be inserted between the packets, use the **transmit-delay** command in serial configuration mode. To restore the default, use the **no** form of this command.

transmit-delay *microseconds*

no transmit-delay *microseconds*

Syntax Description	<i>microseconds</i>	Number of microseconds of minimum delay after sending a packet. Range is from 0 to 128. Default is 0 (disabled).

Defaults	<i>microseconds</i> = 0 (disabled)

Command Modes	serial configuration

Command History	Releases	Modifications
	Release 3.2	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	hdlc	read, write

Examples	In the following example, a delay of 2 microseconds is specified on serial interface 0/3/0/0/0:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface serial 0/3/0/0/0:0
RP/0/0/CPU0:router(config-if)# serial
RP/0/0/CPU0:router(config-if-serial)# transmit-delay 2
```

R3.5.0 Beta Draft—Cisco Confidential Information

In the following example, the transmit delay on serial interface 0/3/0/0:0 is disabled:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface serial 0/3/0/0:0
RP/0/0/CPU0:router(config-if)# serial
RP/0/0/CPU0:router(config-if-serial)# no transmit-delay
```

Related Commands

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

R3.5.0 Beta Draft—Cisco Confidential Information



ATM Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

This module describes the commands used to manage the ATM connections on a router running Cisco IOS XR software.

R3.5.0 Beta Draft—Cisco Confidential Information

atm address-registration

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

atm address-registration

no atm address-registration

Syntax Description This command has no arguments or keywords.

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

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

Command Modes Interface configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

**Note**

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

Task ID	Task ID	Operations
	atm	read, write

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

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


R3.5.0 Beta Draft—Cisco Confidential Information

atm ilmi-config disable

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

atm ilmi-config disable

no atm ilmi-config disable

Syntax Description This command has no arguments or keywords.

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

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

Command Modes Interface configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.



Note

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

Task ID	Task ID	Operations
	atm	read, write

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

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

R3.5.0 Beta Draft—Cisco Confidential Information

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

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

Related Commands

Command	Description
show atm ilmi-status	Displays status information that is related to ILMI.

R3.5.0 Beta Draft—Cisco Confidential Information

atm ilmi-keepalive

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

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

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

Syntax Description

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

Defaults

act-poll-freq *frequency* = 5

retries *count* = 4

inact-poll-freq *frequency* = 1

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

**Note**

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

Task ID

Task ID	Operations
atm	read, write

R3.5.0 Beta Draft—Cisco Confidential Information

Examples

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

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

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

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

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

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

Related Commands

Command	Description
show atm ilmi-status	Displays status information that is related to ILMI.

R3.5.0 Beta Draft—Cisco Confidential Information

atm maxvpi-bits 12

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

atm maxvpi-bits 12

no atm maxvpi-bits 12

Syntax Description This command has no arguments or keywords.

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

Command Modes Interface configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

**Note**

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

Task ID	Task ID	Operations
	atm	read, write

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

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

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

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

R3.5.0 Beta Draft—Cisco Confidential Information

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

Related Commands

Command	Description
show atm interface atm	Displays ATM-specific information about an ATM interface.

R3.5.0 Beta Draft—Cisco Confidential Information

atm mcpt-timers

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

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

no atm mcpt-timers

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

Defaults	<i>timer-1</i> = 50 microseconds
	<i>timer-2</i> = 50 microseconds
	<i>timer-3</i> = 50 microseconds

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.4.1	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Use the cell-packing command to attach one of the three MCPT timers to an individual L2VPN port, PVC, or PVP. If the associated MCPT timer expires before the maximum number of cells that can be packed is reached, then the packet is transmitted with the number of cells that have been packed thus far.

R3.5.0 Beta Draft—Cisco Confidential Information**Note**

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

Task ID**Task ID****Operations**

atm

read, write

Examples

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

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

Related Commands**Command****Description****cell-packing**

Configures the maximum number of cells allowed per packet, and specifies an MCPT timer for cell-packing.

show atm interface atm

Displays ATM-specific information about an ATM interface.

R3.5.0 Beta Draft—Cisco Confidential Information

atm oam flush

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

atm oam flush

no atm oam flush

Syntax Description	This command has no arguments or keywords.

Defaults	The dropping of OAM cells is disabled.

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	atm	read, write

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

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

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

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface atm 0/6/0/1
RP/0/0/CPU0:router(config-if)# no atm oam flush
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show atm interface atm	Displays ATM-specific information about an ATM interface.
	show atm class-link	Displays configuration information for the parameters on a virtual circuit (VC) class that is associated with a particular PVC.
	show atm vc-class	Displays information about all ATM virtual circuit (VC) classes on the router or for a specific ATM vc-class.
	show atm vp-tunnel	Displays virtual path (VP) tunnel information for the entire router or for a specific interface.

R3.5.0 Beta Draft—Cisco Confidential Information

cell-packing

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

cell-packing *cells timer*

no cell-packing

Syntax Description

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

Defaults

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

Command Modes

ATM layer 2 transport interface configuration
 ATM layer 2 transport PVC configuration
 ATM layer 2 transport PVP configuration

Command History

Release	Modification
Release 3.4.1	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **atm mcpt-timers** command to configure the three MCPT timers under the main ATM interface.

Task ID

Task ID	Operations
atm	read, write

Examples

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

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface ATM 0/2/0/0
RP/0/0/CPU0:router (config-if)# l2transport
RP/0/0/CPU0:router (config-if-l2)# cell-packing 6 3
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show atm cell-packing	Displays cell-packing information for the Layer 2 attachment circuits (ACs) configured on your system.
	show atm interface atm	Displays ATM-specific information about an ATM interface.
	show interfaces	Displays statistics for all interfaces configured on the router or for a specific node.
	show atm pvc	Displays ATM PVC and traffic information for the entire router, or a specific VPI/VCI or ATM interface
	show atm pvp	Displays ATM PVP and traffic information for the entire router, or a specific VPI or ATM interface.
	atm mcpt-timers	Defines the three MCPT timers under a main ATM interface.

R3.5.0 Beta Draft—Cisco Confidential Information

class-int

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

class-int *vc-class-name*

no class-int *vc-class-name*

Syntax Description

<i>vc-class-name</i>	Name of the vc-class you are assigning to your ATM main interface or subinterface.

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

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

**Note**

This command is not available for Layer 2 interfaces.

Task ID

Task ID	Operations
atm	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

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

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

Related Commands

Command	Description
show atm class-link	Displays configuration information for the parameters on a virtual circuit (VC) class that is associated with a particular PVC.
show atm vc-class	Displays information about all ATM virtual circuit (VC) classes on the router or for a specific ATM vc-class.

R3.5.0 Beta Draft—Cisco Confidential Information

class-vc

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

class-vc *vc-class-name*

no class-vc *vc-class-name*

Syntax Description

<i>vc-class-name</i>	Name of the vc-class you are assigning to your ATM PVC.

Defaults

No vc-class is assigned to an ATM PVC.

Command Modes

ATM PVC configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

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



Note

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

Task ID

Task ID	Operations
atm	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

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

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

Related Commands

Command	Description
show atm class-link	Displays configuration information for the parameters on a virtual circuit (VC) class that is associated with a particular PVC.
show atm vc-class	Displays information about all ATM virtual circuit (VC) classes on the router or for a specific ATM vc-class.

R3.5.0 Beta Draft—Cisco Confidential Information

encapsulation (ATM)

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

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

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

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

For ATM Layer 2 PVCs:

```
encapsulation {aal0 | aal5}
```

```
no encapsulation {aal0 | aal5}
```

Syntax Description.

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

R3.5.0 Beta Draft—Cisco Confidential Information

Defaults

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

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

Command Modes

ATM PVC configuration

ATM vc-class configuration

ATM Layer 2 transport PVC configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.4.1	To support Layer 2 VPN ACs, the encapsulation command was updated to include the aal0 and aal5 keywords in ATM Layer 2 transport PVC configuration mode.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

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

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

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

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

- The encapsulation assigned to the vc-class that is assigned to the PVC itself.
- The encapsulation assigned to the vc-class that is assigned to the ATM subinterface that hosts the PVC.

R3.5.0 Beta Draft—Cisco Confidential Information

- The encapsulation assigned to the vc-class that is assigned to the ATM main interface that hosts the PVC
- The default **aal5snap** encapsulation

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

- **encapsulation aal5mux ipv4**
- **encapsulation aal5snap**



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

Task ID	Task ID	Operations
	atm	read, write

Examples

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

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

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

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

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

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

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

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

Related Commands	Command	Description
	show atm pvc	Displays ATM PVC and traffic information for the entire router, or a specific VPI/VCI or ATM interface.
	show atm vc-class	Displays information about all ATM virtual circuit (VC) classes on the router or for a specific ATM vc-class.

R3.5.0 Beta Draft—Cisco Confidential Information

f4oam disable

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

f4oam disable

no f4oam disable

Syntax Description This command has no arguments or keywords.

Defaults F4 OAM is enabled by default.

Command Modes ATM Vp-tunnel configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	atm	read, write

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

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

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

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

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show atm interface atm	Displays ATM-specific information about an ATM interface.
	show atm class-link	Displays configuration information for the parameters on a virtual circuit (VC) class that is associated with a particular PVC.
	show atm vc-class	Displays information about all ATM virtual circuit (VC) classes on the router or for a specific ATM vc-class.
	show atm vp-tunnel	Displays virtual path (VP) tunnel information for the entire router or for a specific interface.

R3.5.0 Beta Draft—Cisco Confidential Information

interface atm

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

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

no interface atm *instance* [*.subinterface*]

Syntax Description	<i>instance</i>	Physical interface instance. Naming notation is <i>rack/slot/module/port</i> , and a slash between values is required as part of the notation. <i>rack</i>—Chassis number of the rack. <i>slot</i>—Physical slot number of the card. <i>module</i>—Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>—Physical port number of the interface. Note For more information about the syntax for the router, use the question mark (?) online help function.
	<i>.subinterface</i>	(Optional) Subinterface instance. Naming notation is <i>.subinterface</i> . The period in front of the <i>subinterface</i> value is required as part of the notation. Replace <i>subinterface</i> with the virtual interface number to be associated with the physical interface. Note For more information about the syntax for the router, use the question mark (?) online help function.
	point-to-point	Interface functions as one endpoint of a point-to-point link.
	l2transport	Interface functions as one endpoint on an Layer 2 link.

Defaults No interfaces are configured.

Command Modes Global configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.4.1	To support Layer 2 VPN ATM ACs, this command was updated to include the l2transport keyword.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.5.0 Beta Draft—Cisco Confidential Information

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

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



Note

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

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

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

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

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

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

affinity          Affinity to include/exclude
bandwidth         Set the bandwidth of an interface
cdp               Enable CDP on an interface
class-int         Apply a VC class
commit            Commit the configuration changes to running
crypto            Set crypto parameters
dampening         configure state dampening on the given interface
describe          Describe a command without taking real actions
description       Set description for this interface
do                Run an exec command
exit              Exit from this submode
flow              Netflow configuration
frame-relay       Frame Relay interface configuration commands
ipv4              IPv4 interface subcommands
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

ipv6          IPv6 interface subcommands
load-interval Specify interval for load calculation for an interface
logging       Per-interface logging configuration
mpls          MPLS interface subcommands
mtu           Set the MTU on an interface
no            Negate a command or set its defaults
pvc           Configure a pvc on this interface
root          Exit to the global configuration mode
show          Show contents of configuration
shutdown      shutdown the given interface
--More--

```

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

```

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

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

```

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

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



Note

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



Note

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

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	interface	read, write

Examples

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

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

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

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

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

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

Related Commands	Command	Description
	show atm interface atm	Displays ATM-specific information about an ATM interface.
	show interfaces	Displays statistics for all interfaces configured on the router or for a specific node.

R3.5.0 Beta Draft—Cisco Confidential Information

l2transport (ATM)

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

l2transport

no l2transport

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Interface configuration

Command History	Release	Modification
	Release 3.4.1	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

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

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

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

**Note**

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

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	l2vpn	read, write

Examples

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

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

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router or for a specific node.
show l2vpn xconnect	Displays brief information on configured xconnects.

R3.5.0 Beta Draft—Cisco Confidential Information

oam ais-rdi

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

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

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

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

Defaults	Down count: 1 Up count: 3

Command Modes	ATM vc-class configuration (for a vc-class) ATM PVC configuration (for an individual PVC)

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

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

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

R3.5.0 Beta Draft—Cisco Confidential Information

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

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

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

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

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

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

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

Task ID

Task ID	Operations
atm	read, write

Examples

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

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

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

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

Related Commands

Command	Description
show atm class-link	Displays configuration information for the parameters on a virtual circuit (VC) class that is associated with a particular PVC.
show atm pvc	Displays ATM PVC and traffic information for the entire router, or a specific VPI/VCI or ATM interface

R3.5.0 Beta Draft—Cisco Confidential Information

oam-pvc manage

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

In ATM PVC configuration mode:

```
oam-pvc manage [frequency] [disable] [keep-vc-up [seg-aisrdi-failure]]
```

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

In ATM vc-class configuration mode:

```
oam-pvc manage [frequency]
```

```
no oam-pvc manage [frequency]
```

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

Defaults	frequency:10 seconds.

Command Modes	ATM PVC configuration ATM vc-class configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

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

Task ID

Task ID	Operations
atm	read, write

Examples

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

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

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

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

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

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

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

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

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show atm class-link	Displays configuration information for the parameters on a virtual circuit (VC) class that is associated with a particular PVC.
	show atm pvc	Displays ATM PVC and traffic information for the entire router, or a specific VPI/VCI or ATM interface

R3.5.0 Beta Draft—Cisco Confidential Information

oam retry

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

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

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

Syntax Description

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

Defaults

up-count: 3
down-count: 5
retry-frequency: 1 second

Command Modes

ATM PVC configuration (for an individual PVC)
ATM vc-class configuration (for a vc-class)

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*. The following guidelines apply to PVCs and vc-classes.

R3.5.0 Beta Draft—Cisco Confidential Information

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

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

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

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

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

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



Note

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

Task ID

Task ID	Operations
atm	read, write

Examples

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

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

R3.5.0 Beta Draft—Cisco Confidential Information

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

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

Related Commands

Command	Description
show atm class-link	Displays configuration information for the parameters on a virtual circuit (VC) class that is associated with a particular PVC.
show atm pvc	Displays ATM PVC and traffic information for the entire router, or a specific VPI/VCI or ATM interface

R3.5.0 Beta Draft—Cisco Confidential Information

ping atm interface atm

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

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

Syntax Description		
<i>instance</i>	Physical interface instance. Naming notation is <i>rack/slot/module/port</i> , and a slash between values is required as part of the notation.	<i>rack</i>—Chassis number of the rack. <i>slot</i>—Physical slot number of the card. <i>module</i>—Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>—Physical port number of the interface. Note For more information about the syntax for the router, use the question mark (?) online help function.
<i>.subinterface</i>	(Optional) Subinterface instance. Naming notation is <i>.subinterface</i> . The period in front of the <i>subinterface</i> value is required as part of the notation. Replace <i>subinterface</i> with the virtual interface number to be associated with the physical interface.	Note For more information about the syntax for the router, use the question mark (?) online help function.
<i>vpi/vci</i>	(Optional) ATM virtual path identifier (VPI) and virtual channel identifier (VCI) numbers. The absence of the slash (/) and a <i>vpi</i> value defaults the <i>vpi</i> value to 0.	Note A VPI of 0 is not applicable to VP-tunnels or Layer 2 PVPs.
end-loopback <i>packets</i>	(Optional) Sends a specified number of end-to-end OAM loopback packets over the connection. Replace <i>packets</i> with the number of end-to-end OAM loopback packets you want to send over the ATM interface.	
seg-loopback <i>packets</i>	(Optional) Sends a specified number of segmented OAM loopback packets over the connection. Replace <i>packets</i> with the number of OAM loopback packets you want to send over the ATM interface.	
timeout <i>seconds</i>	Predetermined time during which the destination can send an OAM loopback response cell back to the source. Replace <i>seconds</i> with number of seconds to wait for an OAM loopback response before the ping times out. The default value of the timeout is 2 seconds on Cisco routers.	

Defaults **timeout** *seconds*= 2

Command Modes EXEC

R3.5.0 Beta Draft—Cisco Confidential Information**Command History**

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*. The following guidelines apply to PVCs and vc-classes.

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

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

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

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

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

**Note**

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

Task ID

Task ID	Operations
basic-services	execute
atm	read

Examples

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

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

Related Commands

show atm interface atm	Displays ATM-specific information about an ATM interface.
show interfaces	Displays statistics for all interfaces configured on the router or for a specific node.

R3.5.0 Beta Draft—Cisco Confidential Information**pvc (ATM)**

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

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

pvc vpi/vci ilmi

no pvc vpi/vci ilmi

In interface configuration mode for an ATM subinterface:

pvc vpi/vci

no pvc vpi/vci

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

Defaults

No PVC is defined.

R3.5.0 Beta Draft—Cisco Confidential Information**Command Modes**

Interface configuration
subinterface configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.4.1	This command was supported in subinterface configuration mode for ATM subinterface attachment circuits (ACs).
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

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

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

**Note**

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

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

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

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

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

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

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

R3.5.0 Beta Draft—Cisco Confidential Information

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

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

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

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

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

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

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

Task ID

Task ID

Operations

atm

read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

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

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

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

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

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

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

Related Commands

Command	Description
show atm class-link	Displays configuration information for the parameters on a virtual circuit (VC) class that is associated with a particular PVC.
show atm pvc	Displays ATM PVC and traffic information for the entire router, or a specific VPI/VCI or ATM interface.

R3.5.0 Beta Draft—Cisco Confidential Information

pvp (ATM)

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

pvp *vpi*

no pvp *vpi*

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

Defaults	No PVC is defined.

Command Modes	ATM subinterface configuration

Command History	Release	Modification
	Release 3.4.1	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.

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

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

When you issue the **pvp** command in subinterface configuration mode, the CLI prompt changes to “config-atm-l2transport-pvp,” indicating that you have entered the ATM virtual path configuration submode.

**Note**

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

R3.5.0 Beta Draft—Cisco Confidential Information



Note

PVPs do not support a VPI of 0.

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

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

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

Task ID

Task ID

Operations

atm

read, write

Examples

The following example shows how to create an ATM PVP on an ATM subinterface, and enter ATM virtual path configuration mode:

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

Related Commands

Command

Description

[show atm pvp](#)

Displays ATM PVP and traffic information for the entire router, or a specific VPI or ATM interface.

R3.5.0 Beta Draft—Cisco Confidential Information

shape

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

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

```
no shape
```

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

R3.5.0 Beta Draft—Cisco Confidential Information

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

Defaults

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

Command Modes

ATM PVC configuration
 ATM vc-class configuration
 ATM layer 2 transport PVC configuration
 ATM layer 2 transport PVP configuration
 ATM vp-tunnel configuration mode

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.4.1	This command was supported in ATM layer 2 transport PVC configuration mode and ATM layer 2 transport PVP configuration mode.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
atm	read, write

R3.5.0 Beta Draft—Cisco Confidential Information

Examples

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

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

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

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

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

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

Related Commands

Command	Description
show atm pvc	Displays ATM PVC and traffic information for the entire router, or a specific VPI/VCI or ATM interface.
show atm pvp	Displays ATM PVP and traffic information for the entire router, or a specific VPI or ATM interface.
show atm vp-tunnel	Displays virtual path (VP) tunnel information for the entire router or for a specific interface.

R3.5.0 Beta Draft—Cisco Confidential Information

show atm cell-packing

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

show atm cell-packing

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.4.1	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	atm	read

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

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

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

R3.5.0 Beta Draft—Cisco Confidential Information**Table 93** **show atm cell-packing Field Descriptions**

Field	Description
Circuit Type	AC instance and virtual channel identifier. - The AC instance is expressed in the <i>rack/slot/module/port.subinterface</i> format. - The virtual channel identifier is expressed in the <i>subinterface/vci</i> format.
Local MNCP	Maximum number of cells that can be packed on the local AC.
AVG cells/pkt rcvd	Average number of cells in a packed cell received from the peer, or the average number of cells packed by the peer.
negotiated MNCP	Negotiated maximum number of cells that can be packed on a pseudowire between PE routers.
AVG cells/pkt sent	Maximum number of cells that can be packed on the peer AC.
MCPT	Maximum number of cells allowed per packet configured on the local MCPT.

R3.5.0 Beta Draft—Cisco Confidential Information

show atm class-link

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

show atm class-link *vpi/vci*

Syntax Description

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

Defaults

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

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.4.1	The show atm class-link command output was modified to include Layer 2 VPN parameters when appropriate.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

**Note**

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

Task ID

Task ID	Operations
atm	read

Examples

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

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

```
ATM0/2/0/0.1: VPI: 10 VCI: 100
shape : cbr 100000 (VC-class configured on VC)
encapsulation : aal5snap (VC-class configured on VC)
oam-pvc : manage 300 (VC-class configured on VC)
```

R3.5.0 Beta Draft—Cisco Confidential Information

```
oam retry : 3 5 1 (Default value)
oam ais-rdi : 1 3 (Default value)
```

Table 94 describes the significant fields shown in the display.

Table 94 *show atm class-link Field Descriptions*

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

R3.5.0 Beta Draft—Cisco Confidential Information**Table 94** *show atm class-link Field Descriptions (continued)*

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

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

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

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

```
Class link for VC 0/50
```

```
ATM0/2/0/2: VPI: 0 VCI: 50
```

```
ILMI VC (VC class not supported on this VC)
```

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

Related Commands

Command	Description
class-int	Assigns a vc-class to an ATM main interface.
vc-class atm	Creates a vc-class for an ATM PVC or an ATM interface and enters vc-class configuration mode.

R3.5.0 Beta Draft—Cisco Confidential Information

show atm ilmi-status

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

show atm ilmi-status [**atm** *instance*[.*subinterface*]]

Syntax Description

atm <i>instance</i>	(Optional) Identifies a physical ATM interface whose ILMI status you want to display. Replace the <i>instance</i> argument with the number of the ATM interface whose ILMI status you want to display, in the <i>rack/slot/module/port</i> format. A slash between values is required as part of the notation. <i>rack</i>—Chassis number of the rack. <i>slot</i>—Physical slot number of the card. <i>module</i>—Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>—Physical port number of the interface. Note For more information about the syntax for the router, use the question mark (?) online help function.
<i>.subinterface</i>	(Optional) Subinterface instance. Naming notation is <i>.subinterface</i>. The period in front of the <i>subinterface</i> value is required as part of the notation. Replace <i>subinterface</i> with the virtual interface number to be associated with the physical interface. Note For more information about the syntax for the router, use the question mark (?) online help function.

Defaults

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

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	atm	read

Examples

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

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

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

RP/0/0/CPU0:router#

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

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

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

RP/0/0/CPU0:router#

Table 95 describes the significant fields shown in the display.

Table 95 *show atm ilmi-status Field Descriptions*

Field	Description
Interface	Interface type and instance. The instance is displayed in the <i>rack/slot/module/port</i> format.
Interface Type	ATM interface type (Private or Public), and the communication protocol used by this interface. Note Currently, Cisco IOS XR software supports UNI only.
ILMI VCC	The virtual channel connection associated with this interface.
ILMI Keepalive	ILMI keepalives polling frequency configured on this interface. To modify the ILMI keepalives polling frequency, use the atm ilmi-keepalive command.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 95** *show atm ilmi-status Field Descriptions (continued)*

Field	Description
ILMI State	Status of ILMI for this interface. Possible ILMI states are: • Link failing • Establishing connection • Configuring peer information • Retrieving network prefix from peer • Registering network prefix to peer • Retrieving ATM network addresses from peer • Registering ATM network addresses to peer • Verifying configuration and ATM network addresses • WaitDevType — ILMI process is initialized and in the process of sending ILMI packets to a neighbor. In this case, the ILMI PVC is not yet established. • UpAndNormal — ILMI traps are received by the neighbors, and the PVC is established.
Peer IP Addr	IP address for the remote (neighbor) end point of the connection.
Peer IF Name	Identifies the interface at the remote (neighbor) end point of the connection.
Active Prefix(s)	Network prefix that is registered from the switch side and is active and valid.

Related Commands

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

R3.5.0 Beta Draft—Cisco Confidential Information

show atm interface atm

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

show atm interface atm *instance*

Syntax Description

<i>instance</i>	ATM interface. Replace the <i>instance</i> argument with the number of the ATM interface whose information you want to display, in the <i>rack/slot/module/port</i> format.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.4.1	The show atm interface atm command output was modified to include Layer 2 VPN parameters when appropriate.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
atm	read

Examples

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

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

```
Interface                               : ATM0/3/0/0
Layer2 Transport Port Mode             : Enabled
Cell Packing Data Unavailable
Received Side Statistics:
  Received Cells                        : 0
  Received Bytes                       : 0
  Received AAL Packets                 : 0

Receive Side Cells Dropped:
  Unrecognized VPI/VCI                 : 0
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

Receive Side AAL5 Packets Dropped:
  Unavailable SAR Buffer           : 0
  Non-Resource Exhaustion         : 0
  Reassembly Timeout              : 0
  CRC-32 Errors                   : 0
  Zero Length                     : 0
  Unavailable Host Buffer          : 0
  Packet size exceeds MPS         : 0
  AAL5 Trailer Length Errors      : 0

Transmit Side Statistics:
  Transmitted Cells                : 2587327997
  Transmitted Bytes                : 0
  Transmitted AAL Packets          : 0

Transmit Side Cells Dropped:
  Unrecognized VPI/VCI            : 0

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

Cell-packing statistics:
  Average number of cells sent     : <TODO>
  Average number of cells received : <TODO>

```

Table 96 describes the significant fields shown in the display.

Table 96 *show atm interface atm Field Descriptions*

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

R3.5.0 Beta Draft—Cisco Confidential Information**Table 96** **show atm interface atm Field Descriptions (continued)**

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

R3.5.0 Beta Draft—Cisco Confidential Information**Table 96** *show atm interface atm Field Descriptions (continued)*

Field	Description
Receive side AAL5 Packets Dropped:	Displays the following information about AAL5 packets received from the remote end that were dropped by this end of the interface: • Unavailable SAR Buffer—Total number of AAL5 packets received from the remote end that were dropped because the Segmentation and Reassembly (SAR) buffer was unavailable. • Non-Resource Exhaustion—Total number of packets received from the remote end that were discarded due to events other than resource exhaustion, including raw or non AAL5 cells. • Reassembly Timeout—Number of AAL5 packets received from the remote end that were dropped because the reassembly of those packets took too long and the system timed-out. • CRC-32 Errors—Number of AAL5 packets received from the remote end that were dropped due to CRS-32 errors. • Zero Length—Number of AAL5 packets received from the remote end that were dropped due to • Unavailable Host Buffer—Number of AAL5 packets received from the remote end that were dropped because the host buffer was unavailable. • Packet size exceeds MPS—Number of AAL5 packets received from the remote end that were dropped due to a mismatch between the actual packet length and the reassembled packet length. • AAL5 Trailer Length Errors—Number of AAL5 packets received from the remote end that were dropped because their packet length was bigger than the AAL5 trailer.
Transmit Side Statistics	Displays the following statistical information for the transmit side of this interface: • Transmitted Cells—Total number of cells that were transmitted to the remote end. • Transmitted Bytes—Total number of bytes that were transmitted to the remote end. • Transmitted AAL5 Packets—Total number of AAL5 packets that were transmitted to the remote end.
Transmit side Cells Dropped	Number of VPI and VCI cells transmitted to the remote end that were dropped because they were not recognized by the remote end.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 96** *show atm interface atm Field Descriptions (continued)*

Field	Description
Transmit Side AAL5 Packets Dropped	Displays the following information about transmitted AAL5 packets that were dropped by the remote end: - Unavailable SAR Buffer—Number of transmitted AAL5 packets that were dropped by the remote end because the Segmentation and Reassembly (SAR) buffer was unavailable. - Non-Resource Exhaustion—Total number of packets dropped by the remote end due to events other than resource exhaustion, including raw or non AAL5 cells. - WRED Threshold—Number of transmitted AAL5 packets that were dropped by the remote end because their size exceeded the maximum threshold set for Weighted Random Early Discard (WRED). - WRED Random— Number of received packets that were dropped because they exceeded the maximum WRED threshold.
Cell-packing statistics	Displays the following cell-packing statistics for the specified interface: - Average number of cells sent—Average number of cells in a packed cell that were packed on this interface. - Average number of cells received—Average number of cells in a packed cell that were received by this interface.

Related Commands

Command	Description
interface atm	Configures an ATM interface and enters ATM interface configuration mode.

R3.5.0 Beta Draft—Cisco Confidential Information

show atm pvc

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

show atm pvc [*vpi/vci* | **interface atm** *instance*]

Syntax Description

<i>vpi/vci</i>	(Optional) ATM virtual path identifier (VPI) and virtual channel identifier (VCI) numbers. The absence of the slash (/) and a <i>vpi</i> value defaults the <i>vpi</i> value to 0. Note A VPI of 0 is not applicable to VP-tunnels.
interface atm <i>instance</i>	(Optional) Displays all PVCs on the specified ATM interface. To determine the appropriate form of the <i>instance</i> argument, see your ATM network module, port adapter, or router documentation.

Defaults

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

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.4.1	The show atm pvc command output was modified to include Layer 2 VPN parameters when appropriate.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
atm	read

Examples

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

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

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

R3.5.0 Beta Draft—Cisco Confidential Information

Table 97 describes the significant fields shown in the display.

Table 97 *show pvc (all PVCs) Field Descriptions*

Field	Description
Interface	Interface type and instance. The instance is displayed in the <i>rack/slot/module/port</i> format.
VPI	ATM network virtual path identifier (VPI) associated with the specified interface.
VCI	ATM network virtual channel identifier (VCI) associated with the specified interface.
Type	Type of VPI/VCI associated with the specified interface. In this release, only PVCs are supported.
Encaps	Encapsulation type that configured on the specified interface. Possible encapsulation types follow: • ILMI—Interim Local Management Interface. ILMI encapsulation is available for point-to-point PVCs only. • MUX—aal5mux ipv4; IPv4 encapsulation for multiplex (MUX)-type VCs. MUX encapsulation is available for point-to-point PVCs only. • NLPID—aal5nlpid; AAL and encapsulation type that allows ATM interfaces to interoperate with High-Speed Serial Interfaces (HSSIs), which are using an ATM data service unit (ADSU) and running ATM-Data Exchange Interface (DXI). Supported on ATM PVCs only. NLPID encapsulation is available for point-to-point PVCs only. • SNAP—aal5snap; AAL and encapsulation type that supports Inverse ARP. Logical Link Control/Subnetwork Access Protocol precedes the protocol datagram. SNAP encapsulation is available for point-to-point PVCs only. • AAL0— • AAL5— Note To disable ILMI on a point-to-point ATM interface, use the atm ilmi-config disable command in interface configuration mode for an ATM interface. To configure aal5mux, aal5nlpid, or aal5snap encapsulation on an ATM interface, use the encapsulation command in ATM vc-class configuration mode, and then assign that vc-class to the appropriate ATM main interface.
SC	Service class that is assigned to the specified ATM interface. Possible service classes follow: • cbr • ubr • vbr-nrt • vbr-rt Note To modify a configured ATM service class, use the shape command in the appropriate command mode.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 97** *show atm pvc (all PVCs) Field Descriptions (continued)*

Field	Description
Peak Kbps	Peak output rate for the bit rate in kbps. Note To modify the Peak output rate, use the shape command.
Avg/Min Kbps	Number of kilobits per second sent at the average (sustained) rate. Note To modify the average (or sustained) rate, use the shape command.
Burst cells	Identifies the burst cell size in terms of number of cells. This number is the maximum number of ATM cells the VC can send at the peak rate. Note To modify the burst cell size, use the shape command.
Sts	Status of the PVC. Can be “UP” or “DOWN.”

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

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

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

```
ATM0/2/0/0.1: VPI: 10 VCI: 100
CBR, PeakRate: 100000 Kbps
AAL5-LLC/SNAP
OAM frequency: 300 second(s), OAM retry frequency: 1 second(s),
OAM up retry count: 3, OAM down retry count: 5,
OAM Keep-vc-up: False, OAM AIS-RDI failure: None,
OAM AIS-RDI down count: 1, OAM AIS-RDI up time: 3 second(s),
OAM Loopback status: No loopback enabled,
OAM VC state: Loopback verified,
VC is managed by OAM,

OAM cells received: 12,
F5 InEndLoop: 12, F5 InSegLoop: 0,
F5 InEndAIS: 0, F5 InSegAIS: 0,
F5 InEndRDI: 0, F5 InSegRDI: 0,
OAM cells sent: 12,
F5 OutEndLoop: 12, F5 OutSegLoop: 0,
F5 OutEndAIS: 0, F5 OutSegAIS: 0,
F5 OutEndRDI: 0, F5 OutSegRDI: 0,
OAM cells drops: 0

InPkts: 12 OutPkts: 12
InBytes: 624 OutBytes: 624
WRED pkt drop: 0
Non WRED pkt drop: 0

Internal state: READY
Status: UP
```

Table 98 describes the significant fields shown in the display.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 98** **show atm pvc Field Descriptions**

Field	Description
Detailed display of VC(s) with VPI/VCI	Displays the following general information for the specified PVC: • VPI and VCI in the <i>VPI/VCI</i> format • associated interface type and instance in the <i>type rack/slot/module/port</i> format. • associated VPI • associated VCI • Service class that is assigned to the specified ATM interface. Possible service classes follow: – cbr – ubr – vbr-nrt – vbr-rt • Peak line rate (bandwidth) required for the specified ATM interface, in kilobits per second. • Whether ILMI is enabled on the interface. Note To modify a configured ATM service class, use the shape command in the appropriate command mode. Note To modify the bandwidth required for an ATM interface (peak line rate), use the shape command in interface configuration mode.
OAM frequency	Frequency (in seconds) at which end-to-end F5 OAM loopback cells are transmitted when a change in the up or down state of a PVC is being verified. Note To modify the OAM frequency, use the oam-pvc manage command in ATM virtual circuit (VC) class configuration mode.
OAM retry frequency	Frequency (in seconds) at which end-to-end F5 OAM loopback cells are transmitted when a change in the up or down state is being verified. Note To modify the OAM retry frequency, use the oam retry command in the appropriate command mode.
OAM up retry count	Number of consecutive end-to-end F5 OAM loopback cell responses that must be received in order to modify a PVC state to up.
OAM down retry count	Number of consecutive unreceived end-to-end F5 OAM loopback cell responses allowed before a PVC state changes to down.
OAM AIS-RDI down count:	Number of OAM AIS/RDI cells received on a PVC before it is brought down. Note To modify the OAM AIS-RDI down count, use the oam ais-rdi command in ATM vc-class configuration mode
OAM AIS-RDI up time	Interval after which a PVC is brought up if it has not received any OAM AIS/RDI cells. Note To modify the OAM AIS-RDI uptime, use the oam ais-rdi command in ATM vc-class configuration mode

R3.5.0 Beta Draft—Cisco Confidential Information**Table 98** *show atm pvc Field Descriptions (continued)*

Field	Description
OAM Loopback status	Status of end-to-end F5 OAM loopback cell generation for this VC. Possible value follow: - No loopback enabled—No loopback is enabled on this interface. - OAM Disabled—End-to-end F5 OAM loopback cell generation is disabled. - OAM Sent—OAM cell was sent. - OAM Received—OAM cell was received. - OAM Failed—OAM reply was not received within the frequency period or contained bad correlation tag.
OAM VC state	Current state of the specified VC. Possible VC states follow: - AIS/RDI—The VC received AIS/RDI cells. End-to-end F5 OAM loopback cells are not sent in this state. - Down Retry—An OAM loopback failed. End-to-end F5 OAM loopback cells are sent at retry frequency to verify that the VC is really down. After down-count unsuccessful retries, the VC goes to the Not Verified state. - Loopback Not Managed—VC is not being managed by OAM. - Loopback Not Verified—VC has not been verified by end-to-end F5 OAM loopback cells. AIS and RDI conditions are cleared. - Up Retry—An OAM loopback was successful. End-to-end F5 OAM loopback cells are sent at retry frequency to verify the VC is really up. After up-count successive and successful loopback retries, the VC goes to the Verified state. - Loopback Verified—Loopbacks are successful. AIS/RDI cell was not received.
OAM cells received	Number of OAM cells that have been received by this interface.
F5 InEndLoop:	Number of end-to-end F5 OAM loopback cells received by this interface.
F5 InSegLoop	Number of segment F4 OAM loopback cells received by this interface.
F5 InAIS	Number of F4 OAM AIS cells received by this interface.
F5 InRDI	Number of F4 OAM RDI cells received by this interface.
OAM cells sent	Total number of OAM cells sent on this VC.
F5 OutEndLoop	Number of end-to-end F5 OAM loopback cells sent from this interface.
F5 OutSegLoop	Number of segment F5 OAM loopback cells sent from this interface.
F5 OutAIS	Number of F5 OAM AIS cells sent from this interface.
F5 OutRDI	Number of F5 OAM RDI cells sent from this interface.
OAM cells drops	Number of OAM cells dropped (or flushed) by this interface.
InPkts	Total number of packets received on this VC. This number includes all fast-switched and process-switched packets.
OutPkts	Total number of packets sent on this VC. This number includes all fast-switched and process-switched packets.
InBytes	Total number of bytes received on this VC. This number includes all fast-switched and process-switched bytes.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 98** *show atm pvc Field Descriptions (continued)*

Field	Description
OutBytes	Total number of bytes sent on this VC. This number includes all fast-switched and process-switched bytes.
WRED pkt drop	Total number of AAL5 packets that were dropped by this interface because their size exceeded the maximum threshold set for Weighted Random Early Discard (WRED).
Non WRED pkt drop	Total number of dropped AAL5 packets that did not exceed the maximum threshold set for Weighted Random Early Discard (WRED).
Internal state	Internal PVC state.
Status	Current status of this PVC. Can be “Up” or “Down.”

Related Commands

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

R3.5.0 Beta Draft—Cisco Confidential Information

show atm pvp

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

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

Syntax Description

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

Defaults

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

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.1	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
atm	read

Examples

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

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

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

R3.5.0 Beta Draft—Cisco Confidential Information

Table 99 describes the significant fields shown in the display.

Table 99 *show pvp (all PVPs) Field Descriptions*

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

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

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

Detailed display of L2PVP(s) with VPI = 100

```
ATM0/3/0/1.100: VPI: 100
UBR, PeakRate: 155000 Kbps
AAL0
OAM frequency: 10 second(s), OAM retry frequency: 1 second(s),
OAM up retry count: 3, OAM down retry count: 5,
OAM AIS-RDI down count: 1, OAM AIS-RDI up time: 3 second(s),
OAM Loopback status: No loopback enabled,
OAM L2PVP state: Unknown,
L2PVP is not managed by OAM,

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

R3.5.0 Beta Draft—Cisco Confidential Information

```

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

Internal state: READY
Status: UP

```

Table 100 describes the significant fields shown in the display.

Table 100 *show atm pvp Field Descriptions*

Field	Description
ATM0/1/0/0.30	Associated interface type and instance in the <i>type rack/slot/module/port.subinterface</i> format. - Service class that is assigned to the specified ATM interface. Possible service classes follow: - cbr - ubr - vbr-nrt - vbr-rt - Peak line rate (bandwidth) required for the specified ATM interface, in kilobits per second. Note To modify a configured ATM service class, use the shape command in the appropriate command mode. Note To modify the bandwidth required for an ATM interface (peak line rate), use the shape command in interface configuration mode.
VPI	VPI associated with the specified PVP.
UBR	Service class that is assigned to the specified ATM interface. The example shows that vbr-rt is assigned to the interface that hosts the specified PVP. Possible service classes are: - cbr - ubr - vbr-nrt - vbr-rt
PeakRate	Peak output rate for the bit rate in kbps. Note To modify the peak output rate, use the shape command.
AAL0	ATM adaptation layer (AAL) and encapsulation type for the PVP. Currently, only AAL0 is the only supported encapsulation type for PVPs.
OAM frequency	Frequency (in seconds) at which end-to-end F5 OAM loopback cells are transmitted when a change in the up or down state of a PVC is being verified. Note To modify the OAM frequency, use the oam-pvc manage command in ATM virtual circuit (VC) class configuration mode.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 100** **show atm pvp Field Descriptions (continued)**

Field	Description
OAM retry frequency	Frequency (in seconds) at which end-to-end F5 OAM loopback cells are transmitted when a change in the up or down state is being verified. Note To modify the OAM retry frequency, use the oam retry command in the appropriate command mode.
OAM up retry count	Number of consecutive end-to-end F5 OAM loopback cell responses that must be received in order to modify a PVC state to up.
OAM down retry count	Number of consecutive unreceived end-to-end F5 OAM loopback cell responses allowed before a PVC state changes to down.
OAM AIS-RDI down count	Number of OAM AIS/RDI cells received on a PVC before it is brought down. Note To modify the OAM AIS-RDI down count, use the oam ais-rdi command in ATM vc-class configuration mode
OAM AIS-RDI up time	Interval after which a PVC is brought up if it has not received any OAM AIS/RDI cells. Note To modify the OAM AIS-RDI uptime, use the oam ais-rdi command in ATM vc-class configuration mode
OAM Loopback status	Status of end-to-end F5 OAM loopback cell generation for this VC. Possible value follow: • No loopback enabled—No loopback is enabled on this interface. • OAM Disabled—End-to-end F5 OAM loopback cell generation is disabled. • OAM Sent—OAM cell was sent. • OAM Received—OAM cell was received. • OAM Failed—OAM reply was not received within the frequency period or contained bad correlation tag.
OAM L2PVP state	Current state of the specified VC. Note OAM management is not supported on Layer 2 PVPs in the current release of Cisco IOS XR software.
OAM cells received	Number of OAM cells that have been received by this interface.
F4 InEndLoop:	Number of end-to-end F4 OAM loopback cells received by this interface.
F4 InSegLoop	Number of segment F4 OAM loopback cells received by this interface.
F4 InEndAIS	Number of F4 OAM AIS cells received by this interface.
F4 InSegAIS	Number of segment F4 OAM AIS cells received by this interface.
F4 InEndRDI	Number of F4 OAM RDI cells received by this interface.
F4 InSegRDI	Number of F4 segment OAM RDI cells received by this interface.
OAM cells drops	Number of OAM cells dropped (or flushed) by this interface.
InPkts	Total number of packets received on this VC. This number includes all fast-switched and process-switched packets.
OutPkts	Total number of packets sent on this VC. This number includes all fast-switched and process-switched packets.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 100** **show atm pvp Field Descriptions (continued)**

Field	Description
InBytes	Total number of bytes received on this VC.
OutBytes	Total number of bytes sent on this VC.
Internal state	Internal PVC state.
Status	Current status of this PVC. Can be “Up” or “Down.”

Related Commands

Command	Description
pvp (ATM)	Creates an ATM permanent virtual path (PVP) and enters ATM virtual path configuration mode.
show interfaces	Displays statistics for all interfaces configured on the router or for a specific node.

R3.5.0 Beta Draft—Cisco Confidential Information

show atm vc-class

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

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

Syntax Description

<i>vc-class-name</i>	Name of the vc-class whose information you want to display.

Defaults

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

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.4.1	The show atm vc-class command output was modified to include Layer 2 VPN parameters when appropriate.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
atm	read

Examples

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

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

```
ATM vc-class class1
```

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

```
ATM vc-class class2
```

encapsulation	-	aal5nlpid
shape	-	ubr 40000

R3.5.0 Beta Draft—Cisco Confidential Information

```

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

```

```
ATM vc-class class3
```

```

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

```

Table 101 describes the significant fields shown in the display.

Table 101 *show atm vc-class Field Descriptions*

Field	Description
encapsulation	Type of ATM adaptation layer (AAL) encapsulation type that is enabled on the specified vc-class. Possible AAL encapsulation types follow: • aal5mux ipv4—IPv4 encapsulation for multiplex (MUX)-type VCs • aal5nlpid—AAL and encapsulation type that allows ATM interfaces to interoperate with High-Speed Serial Interfaces (HSSIs), which are using an ATM data service unit (ADSU) and running ATM-Data Exchange Interface (DXI). Supported on ATM PVCs only. • aal5snap—AAL and encapsulation type that supports Inverse ARP. Logical Link Control/Subnetwork Access Protocol (LLC/SNAP) precedes the protocol datagram. Note To modify the AAL encapsulation type on an interface, use the encapsulation command in ATM vc-class configuration mode.
shape	Displays traffic shaping information for the service class that is assigned to the specified vc-class. Possible service classes follow: • cbr—command output shows the peak output rate for the bit rate in kbps. • ubr—command output shows the peak output rate for the bit rate in kbps. • vbr-nrt—command output shows the peak output rate, sustained output rate, and burst size for the bit rate in kbps. • vbr-rt—command output shows the peak output rate, sustained output rate, and burst size for the bit rate in kbps. Note To modify a configured ATM service class and peak output rate for the bit rate, use the shape command in the appropriate command mode.
oam ais-rdi	Displays the maximum number of OAM AIS/RDI cells that can be received on a PVC before it is brought down. Note Use the oam ais-rdi command in to modify the current configuration for this field.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 101** *show atm vc-class Field Descriptions (continued)*

Field	Description
oam retry	Displays the following information related to F5 OAM loopback cells, if this information was configured for the specified vc-class: - Number of consecutive end-to-end F5 OAM loopback cell responses that must be received to change a connection state to up. (Retry count) - Number of consecutive unreceived end-to-end F5 OAM loopback cells allowed on a PVC before its state changes to down. (down count) - Frequency (in seconds) at which end-to-end F5 OAM loopback cells are transmitted when a change in the up or down state is being verified. (retry frequency) Note Use the oam retry command to modify the current configuration for this field. Note If the oam retry command was not use to configure the F5 OAM loopback retry count, down count, or retry frequency, then this information is not displayed in the command output for the show atm vc-class command.
oam-pvc	Frequency (in seconds) at which end-to-end F5 OAM loopback cells are transmitted on this PVC. Range is from 0 through 600. Note Use the oam-pvc manage command to modify the current configuration for this field.

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

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

```
ATM vc-class class1
```

```

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

Table 101 describes the significant fields shown in the display.

Related Commands	Command	Description
	class-vc	Attaches a vc-class to an ATM permanent virtual circuit (PVC).
	vc-class atm	Creates a vc-class for an ATM PVC or an ATM interface and enters vc-class configuration mode.

R3.5.0 Beta Draft—Cisco Confidential Information

show atm vp-tunnel

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

show atm vp-tunnel [**interface atm** *instance*]

Syntax Description

interface atm <i>instance</i>	(Optional) ATM interface whose vp-tunnel information you want to display. Replace the <i>instance</i> argument with the number of the ATM interface whose information you want to display, in the <i>rack/slot/module/port</i> format

Defaults

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

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
atm	read

Examples

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

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

Interface	VPI	SC	Data VCs	Peak Kbps	Avg/Min Kbps	Burst Cells	Status
ATM0/6/0/0	10	CBR	0	155000	N/A	N/A	DOWN
ATM0/6/0/0	20	CBR	0	155000	N/A	N/A	DOWN
ATM0/6/0/0	30	CBR	0	155000	N/A	N/A	DOWN
ATM0/6/0/0	40	CBR	0	155000	N/A	N/A	DOWN
ATM0/6/0/1	10	VBR_NRT	0	155000	155000	800	DOWN
ATM0/6/0/1	20	VBR_NRT	0	155000	155000	800	DOWN

[Table 102](#) describes the significant fields shown in the display.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 102** **Field Descriptions**

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

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

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

Data Interface	Peak VPI	Avg/Min SC	Burst VCs	Kbps	Kbps	Cells	Status
ATM0/6/0/1	10	VBR_NRT	0	155000	155000	800	DOWN
ATM0/6/0/1	20	VBR_NRT	0	155000	155000	800	DOWN

Table 102 describes the significant fields shown in the display.

Related Commands

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

R3.5.0 Beta Draft—Cisco Confidential Information

show controllers atm

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

show controllers atm *instance* [**all** | **traffic** {**f4oam** | **port** | **vc** *vpi/vci* | **vp** *vpi*]

Syntax Description

<i>instance</i>	ATM interface whose controller status and configuration information you want to display. Replace the <i>instance</i> argument with the number of the ATM interface whose information you want to display, in the <i>rack/slot/module/port</i> format.
f4oam	Displays information about the ATM layer f4oam traffic that is transmitted and received on the specified interface.
port	(Optional) Displays information about the ATM layer traffic that is transmitted and received by the ports associated with the specified interface.
vc <i>vpi/vci</i>	(Optional) Displays information about the ATM layer traffic carried by specific ATM VC (virtual channel). Replace <i>vpi/vci</i> with the ATM virtual path identifier (VPI) and virtual channel identifier (VCI) of the VC whose information you want to display.
vp <i>vpi</i>	(Optional) Displays information about the ATM layer traffic carried by specific ATM virtual path. Replace <i>vpi</i> with the ATM virtual path identifier (VPI) whose information you want to display.

Defaults

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

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
interface	read

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

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

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

```
SAR Counters:
  tx_packets           :4085                tx_bytes           :212420
  tx_total_resource_errs:0                  tx_total_other_errs :0
  tx_wred_thresh_drops :0                  tx_wred_random_drops :0
  rx_packets           :0                  rx_bytes           :0
  rx_total_resource_errs:0                  rx_total_other_errs :0
  rx_buffer_exhaust_errs:0                  rx_CRC32_errors     :0
  rx_packet_abort_errs :0                  rx_trailer_len_errs :0
  rx_mps_errors        :0                  rx_reassembly_timeout:0

The following are per-SAR counters:
Reassembly SAR:
  sys_rx_unopen_vc_cls :0                  sys_tx_unopen_vc_cls :0
  sys_ecc_errors        :0                  sys_ecc_and_addr     :      0xf
ffffff
  sys_ecc_or_addr       :      0x0
Segmentation SAR:
  sys_rx_unopen_vc_cls :0                  sys_tx_unopen_vc_cls:0
  sys_ecc_errors        :0                  sys_ecc_and_addr     :      0xf
ffffff
  sys_ecc_or_addr       :      0x0
RSAR 0: (6.0.2.1c)
RSAR Build ID= E7EE
SSAR 0: (6.0.2.1c)
SSAR Build ID= 570

--More--
```

Table 103 describes the significant fields shown in the display.

Table 103 *show controllers atm Field Descriptions*

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

R3.5.0 Beta Draft—Cisco Confidential Information**Table 103** *show controllers atm Field Descriptions (continued)*

Field	Description
tx_total_resource_errs	Total number of packets that were not transmitted because of any resource exhaustion error. This does not necessarily imply an error, because this counter includes tx_wred_thresh_drops and tx_wred_random_drops, as well as packet drops due to complete buffer exhaustion on the SAR. This should be equal to the sum of the number of resource errors that occur on all the VCs.
tx_total_other_errs	Total number of packets that were not transmitted because of any error other than resource exhaustion, but not including no-vc drops. This includes malformed packets, CRC errors, and so on. This should be approximately the total number of tx_other_errors that occur on all the VCs on this interface.
tx_wred_thresh_drops	Total number of WRED maximum threshold drops on this interface. This counter is included in the tx_total_resource_errs counter.
tx_wred_random_drops	Total number of WRED random drops on this interface. This counter is included in the tx_total_resource_errs counter.
rx_packets	Total number of packets reassembled on this interface by the SAR, including OAM cells.
rx_bytes	Number of AAL5 packets received on this interface.
rx_total_resource_errs	Total number of packet reassemblies that failed due to resource exhaustion. This error should not occur if the queue thresholds are not oversubscribed. This error includes rx_buffer_exhaust_errs.
rx_total_other_errs	Total number of packet reassemblies that failed due to errors besides resource exhaustion (not including “no-vc” cells), including rx_crc32_errors, rx_packet_abort_errs, rx_trailer_len_errs, rx_mps_errors, and rx_reassembly_timeout.
rx_buffer_exhaust_errs	Total number of packet reassemblies that failed due to complete buffer exhaustion on the SAR. This error should not occur if the queue thresholds are not oversubscribed. This is included in rx_total_resource_errs.
sys_tx_unopen_vc_cls	Total number of packets transmitted by this endpoint that failed due to an error other than those listed in the show controllers atm command output.
Reassembly SAR	Counters that provide information specific to the reassembly chip.
sys_ecc_and_addr	Total number of single bit end and addressing errors detected on the reassembly SAR.
sys_ecc_errors	Total number of single bit errors detected on the reassembly SAR.
sys_ecc_or_addr	Total number of single bit end or addressing errors detected on the reassembly SAR.
Segmentation SAR	Counters that provide information specific to the segmentation chip.
sys_tx_unopen_vc_cls	Total number of packet reassemblies transmitted by this endpoint that failed due to errors other than those listed in the show controllers atm command output.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 103** *show controllers atm Field Descriptions (continued)*

Field	Description
sys_rx_unopen_vc_cls	Total number of packet reassemblies received by this endpoint that failed due to errors other than those listed in the show controllers atm command output.
rx_CRC32_errors	Total number of packet reassemblies that failed due to an invalid AAL5 CRC32 trailer. This is included in rx_total_other_errs.
rx_packet_abort_errs	Total number of packet reassemblies that failed due to receiving a trailer length of 0. This is included in rx_total_other_errs.
rx_trailer_len_errs	Total number of packet reassemblies that failed due to a packet whose AAL5 trailer had an invalid trailer length. This is included in rx_total_other_errs.
rx_mps_errors	Total number of packet reassemblies that failed due to a packet size greater than the maximum allowed packet size. This is included in rx_total_other_errs.
rx_reassembly_timeout	Total number of packet reassemblies that failed due to timing out before receiving the last cell of a packet. This is included in rx_total_other_errs.
sys_rx_unopen_vc_cls	Packets received on nonexistent VC.
RSAR 0	RSAR ID.
RSAR Build ID	Unique number that identifies the RSAR build.
SSAR 0	SSAR ID.
SSAR Build ID	Unique number that identifies the SAR build.

Related Commands

Command	Description
show atm interface atm	Displays ATM-specific information about an ATM interface.

R3.5.0 Beta Draft—Cisco Confidential Information

shutdown (ATM)

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

shutdown

no shutdown

Syntax Description	This command has no arguments or keywords

Defaults	The ATM interface is up.

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Use the show interface atm command in EXEC mode to verify that the ATM interface is administratively up or down.

Task ID	Task ID	Operations
	interface	read, write

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

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

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

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

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

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


R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show atm interface atm	Displays ATM-specific information about an ATM interface.

R3.5.0 Beta Draft—Cisco Confidential Information

vc-class atm

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

vc-class atm *name*

no vc-class atm *name*

Syntax Description	<i>name</i> Name of your vc-class.						
Defaults	No vc-class is defined.						
Command Modes	Global configuration						
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>Release 3.4.0</td><td>This command was introduced on the Cisco XR 12000 Series Router.</td></tr> <tr> <td>Release 3.5.0</td><td>No modification.</td></tr> </table>	Release	Modification	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.	Release 3.5.0	No modification.
Release	Modification						
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.						
Release 3.5.0	No modification.						

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

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

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

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

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	atm	read, write

Examples

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

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

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

Related Commands	Command	Description
	class-vc	Attaches a vc-class to an ATM PVC.
	show atm vc-class	Displays information about all ATM virtual circuit (VC) classes on the router or for a specific ATM VC class.

R3.5.0 Beta Draft—Cisco Confidential Information

vp-tunnel

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

vp-tunnel *vpi*

Syntax Description

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

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

- 4-port OC12
- 4-port OC3

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

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

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

```

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

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

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	atm	read, write

Examples	The following example shows how to configure a virtual path (VP) tunnel on an interface and enter ATM vp-tunnel configuration mode: <pre>RP/0/0/CPU0:router# vp-tunnel 10</pre>

Related Commands	Command	Description
	show atm vp-tunnel	Displays vp-tunnel information for the entire router or for a specific interface.

R3.5.0 Beta Draft—Cisco Confidential Information



Null Interface Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

This module describes the Cisco IOS XR commands used to configure null interfaces.

R3.5.0 Beta Draft—Cisco Confidential Information

interface null 0

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

interface null 0

no null 0

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When you issue the **interface null 0** command in global configuration mode, the CLI prompt changes to “config-null0,” indicating that you have entered interface configuration mode for the null interface. In the following sample output, the question mark (?) online help function displays all the commands available under the interface configuration mode for the null interface:

```
RP/0/RP0/CPU0:router(config)# interface null 0
RP/0/RP0/CPU0:router(config-null0)#?

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

RP/0/RP0/CPU0:CRS-8_P1(config-null0)#
```


R3.5.0 Beta Draft – Cisco Confidential Information

Task ID	Task ID	Operations
	interface	read, write

Examples

The following 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)#
```

R3.5.0 Beta Draft—Cisco Confidential Information

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 arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.0	This command was first introduced on the Cisco CRS-1.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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
.
```

R3.5.0 Beta Draft—Cisco Confidential Information

Table 104 describes the significant fields shown in the display.

Table 104 *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	Displays statistics for all interfaces configured on the router.

R3.5.0 Beta Draft—Cisco Confidential Information



Link Bundling Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

This module contains commands for configuring and monitoring Link Bundling on Cisco IOS XR software.

R3.5.0 Beta Draft—Cisco Confidential Information

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	
<i>bundle-id</i>	Bundle on which you want to add a port. Range is 1 through 65535.
<i>bundle-id.vlan_id</i>	VLAN bundle on which you want to add a port. The VLAN bundle ID is entered in the <i>bundle-id.vlan_id</i> format, and a period between the <i>bundle-id</i> and <i>vlan_id</i> arguments is required. - Replace the <i>bundle-id</i> argument with the bundle ID. Range is from 1 through 65535. - Replace the <i>vlan_id</i> argument with the VLAN trunk interface ID. Range is from 1 to 4094 inclusive (0 and 4095 are reserved). Note The <i>vlan_id</i> argument is available only for Ethernet bundles. You can not add a VLAN subinterface on a POS bundle.
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 add the link to a bundle without running LACP 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.

Defaults **mode = on**

Command Modes Interface configuration

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	The bundle id command syntax was changed from bundle-id .
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

The following example shows how to add a port onto a bundle:

```
RP/0/RP0/CPU0:router(config-if)# bundle id 1
```

The following example shows how to add an active LACP port onto an aggregated interface (or bundle):

```
RP/0/RP0/CPU0:router(config-if)# bundle id 5 mode active
```

Related Commands

Command	Description
show bundle Bundle-Ether	Displays information about a specific Ethernet bundle.
show bundle Bundle-POS	Displays information about a specific POS bundle.
show interfaces	Displays statistics for all interfaces configured on the router or on a specific node.
show lacp bundle	Displays detailed information about LACP ports and their peers.
show lacp port	Displays detailed information about LACP ports.

R3.5.0 Beta Draft—Cisco Confidential Information

bundle maximum-active links

To limit the number of links that can be actively carrying traffic in a specific bundle, use the **bundle maximum-active links** command in interface configuration mode.

bundle maximum-active links *links*

Syntax Description

<i>links</i>	Number of active links you want to bring up in the specified bundle. Replace the <i>links</i> with 1 .
Note	In Release 3.3.0, only one active link is supported.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.



Note

The **bundle maximum-active links** command is supported only for bundles that are not running LACP.



Note

If the **bundle maximum-active links** command is issued, then only the highest-priority link within the bundle is active. The priority is based on the value from the **bundle port-priority** command, where a lower value is a higher priority. Therefore, we recommend that you configure a higher priority on the link that you want to be the active link.

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 sets the required number of active links required to bring up POS bundle 5 to 2:

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(config)# interface Bundle-POS 5  
RP/0/RP0/CPU0:router(config-if)# bundle maximum-active links 1
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	<code>bundle minimum-active links</code>	Sets the minimum amount of bandwidth required before a user can bring up a specific bundle.
	<code>show bundle Bundle-Ether</code>	Displays information about a specific Ethernet bundle.
	<code>show bundle Bundle-POS</code>	Displays information about a specific POS bundle.

R3.5.0 Beta Draft—Cisco Confidential Information

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	<i>kbps</i> Minimum bandwidth required before you can bring up a bundle. Range is from 1 through a number that is equivalent to the combined bandwidths of 32 OC768 interfaces.

Defaults	<i>kbps</i> = 1

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	bundle	read, write

Examples	The following 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 Bundle-Ether	Displays information about a specific Ethernet bundle.
	show bundle Bundle-POS	Displays information about a specific POS bundle.

R3.5.0 Beta Draft—Cisco Confidential Information

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

<i>links</i>	Number of active links you want to bring up in the specified bundle. Range is from 1 through 32.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 POS bundle 5 so that 2 links must be active before the bundle can be brought up:

```
RP/0/RP0/CPU0:router(config)# interface Bundle-POS 5
RP/0/RP0/CPU0:router(config-if)# bundle minimum-active links 2
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	bundle maximum-active links	Sets the active links required to bring up a specific bundle.
	show bundle Bundle-Ether	Displays information about a specific Ethernet bundle.
	show bundle Bundle-POS	Displays information about a specific POS bundle.

R3.5.0 Beta Draft—Cisco Confidential Information

bundle port-priority

To configure LACP priority for a port, enter the **bundle port-priority** command in interface configuration mode. To return to the default Link Aggregation Control Protocol (LACP) priority value, use the **no** form of this command.

bundle port-priority *priority*

no bundle port-priority *priority*

Syntax Description

<i>priority</i>	Priority for this port, where a lower value equals a higher priority. Replace the <i>priority</i> argument with a number. Range is from 0 through 65535.

Defaults

priority = 32768

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	The command name was changed from lacp port-priority to bundle port-priority .
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The LACP priority value forms part of the port ID, which is transmitted within the LACP packets that are exchanged with the peer. The peer uses the LACP packets to determine whether a given port should carry traffic for the bundle.



Note

A lower LACP value is a higher LACP priority for the port.

Task ID

Task ID	Operations
bundle	read, write

Examples

The following example shows how to configure LACP priority on a port:

```
RP/0/RP0/CPU0router(config-if)# bundle port-priority 1
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	bundle id	Adds a port to an aggregated interface (or bundle).
	show lacp bundle	Displays detailed information about LACP ports and their peers.
	show lacp port	Displays detailed information about LACP ports.
	show lacp system-id	Displays the local system ID used by LACP.

R3.5.0 Beta Draft—Cisco Confidential Information

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_instance | TenGigE interface_instance | POS
                     interface_instance}]
```

Syntax Description		
bundle		Clears LACP counters for all members of a bundle.
Bundle-Ether <i>node-id</i>		Specifies the Ethernet bundle whose LACP counters you want to clear. Replace <i>node-id</i> with a number. Range is from 1 through 65535.
Bundle-POS <i>bundle-id</i>		Specifies the POS bundle whose LACP counters you want to clear. Replace <i>bundle-id</i> with a bundle identifier. Range is from 1 through 65535.
port		Clears all LACP counters on the specified bundle or interface.
GigabitEthernet <i>interface_instance</i>		Specifies the Gigabit Ethernet interface whose LACP counters you want to clear. Replace <i>bundle-id</i> with the number of the bundle you want to clear.
TenGigE <i>interface_instance</i>		TenGigE interface whose LACP counters you want to clear. The <i>interface_instance</i> is expressed in the <i>rack/slot/module/port</i> notation.
POS <i>interface_instance</i>		Specifies the Packet-over-SONET/SDH (POS) interface whose LACP port counters you want to clear. The <i>interface_instance</i> is expressed in the <i>rack/slot/module/port</i> notation.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	bundle	execute
	basic-services	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**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	Displays LACP statistics.

R3.5.0 Beta Draft—Cisco Confidential Information

interface Bundle-Ether

To create a new Ethernet bundle and enter interface configuration mode for that bundle, use the **interface Bundle-Ether** command in global configuration mode. To delete an Ethernet bundle, use the **no** form of this command.

interface Bundle-Ether *bundle-id*

no interface Bundle-Ether *bundle-id*

Syntax Description

<i>bundle-id</i>	Ethernet bundle you want to create or configure. Replace <i>bundle-id</i> with a bundle identifier. Range is from 1 through 65535.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
bundle	read, write

Examples

The following example shows how to create a new Ethernet bundle and enter interface configuration mode for that bundle.:

```
RP/0/RP0/CPU0:router(config)# interface Bundle-Ether 3
RP/0/RP0/CPU0:router(config-if)#
```

Related Commands

Command	Description
show bundle Bundle-Ether	Displays information about a specific Ethernet bundle.

R3.5.0 Beta Draft—Cisco Confidential Information

interface Bundle-POS

To create a new Packet-over-SONET/SDH (POS) bundle and enter interface configuration mode for that bundle, use the **interface Bundle-POS** command in global configuration mode. To delete a POS bundle, use the **no** form of this command.

interface Bundle-POS *bundle-id*

no interface Bundle-POS *bundle-id*

Syntax Description

<i>bundle-id</i>	Number of the POS bundle you want to create or configure. Replace <i>bundle-id</i> with a bundle identifier. Range is from 1 through 65535.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
bundle	read, write

Examples

The following example shows how to create a new POS bundle and enter interface configuration mode for that bundle.:

```
RP/0/RP0/CPU0:router(config)# interface Bundle-POS 10
RP/0/RP0/CPU0:router(config-if)#
```

Related Commands

Command	Description
show bundle Bundle-POS	Display information about a specific Ethernet bundle

R3.5.0 Beta Draft—Cisco Confidential Information

lacp period short

To configure a one second interval between LACP packets that are received from the peer, enter the **lacp period** command in interface configuration mode. To return to the default LACP period, use the **no** form of this command.

lacp period short

no lacp period

Syntax Description

This command has no arguments or keywords.

Defaults

If you do not enter the **lacp period short** command, then the peer transmits LACP packets every 30 seconds

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
bundle	read, write

Examples

The following example shows how to configure a one-second interval between LACP packets that are received from the peer:

```
RP/0/RP0/CPU0:router(config-if)# lacp period short
```

Related Commands

Command	Description
bundle id	Adds a port to an aggregated interface (or bundle).
show lacp port	Displays detailed information about LACP ports.
show lacp bundle	Displays detailed information about LACP ports and their peers.

R3.5.0 Beta Draft—Cisco Confidential Information

lACP system-priority

To configure the priority for the current system, enter the **lACP system-priority** command in global configuration mode. To return to the default LACP system-priority value, use the **no** form of this command.

lACP system-priority *priority*

Syntax Description	<i>priority</i>	Priority for this system. Replace <i>priority</i> with a number. Range is from 0 through 65535. A lower value is higher priority.

Defaults	<i>priority</i> = 32768

Command Modes	Global configuration

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

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/CPU0router(config)# lACP system-priority 100
```

Related Commands	Command	Description
	show lACP system-id	Displays the local system ID used by LACP.
	show lACP bundle	Displays detailed information about LACP ports and their peers.
	show lACP port	Displays detailed information about LACP ports.

R3.5.0 Beta Draft—Cisco Confidential Information

show bundle Bundle-Ether

To display information about a specific Ethernet bundle, enter the **show bundle Bundle-Ether** command in EXEC mode.

show bundle Bundle-Ether *bundle-id* [**reasons**]

Syntax Description

<i>bundle-id</i>	Number of the Ethernet bundle whose information you want to display. Replace <i>bundle-id</i> with a bundle identifier. Range is from 1 through 65535.
reasons	(Optional) Displays the “Mux Reason”, which is the reason why each link is in its state.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	- The output for this command was modified. - The reasons keyword was added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
bundle	read

R3.5.0 Beta Draft—Cisco Confidential Information

Examples

The following is sample output from the **show bundle Bundle-Ether** command:

```
RP/0/RP0/CPU0:router# show bundle Bundle-Ether 1
```

```
State: 0 - Port is Detached. 1 - Port is Waiting.
       2 - Port is Attached. 3 - Port is Collecting.
       4 - Port is 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  Port ID          B/W (Kbps)  MAC address
-----
Gi0/0/2/0     0      0x8000, 0x0001    1000000     0800.453a.651d*
```

The following is sample output from the **show bundle Bundle-Ether** command with the **reasons** keyword included in the command string:

```
RP/0/RP0/CPU0:router# show bundle Bundle-Ether 1 reasons
```

```
State: 0 - Port is Detached. 1 - Port is Waiting.
       2 - Port is Attached. 3 - Port is Collecting.
       4 - Port is 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  Port ID          B/W (Kbps)  MAC address
-----
Gi0/0/2/0     0      0x8000, 0x0001    1000000     0800.453a.651d*
Link is marked individual by partner
```

Table 105 describes the significant fields shown in the display.

Table 105 show bundle Bundle-Ether Field Descriptions

Field	Description
B/W (Kbps)	Bundled interface bandwidth, in kilobits per second.
MAC address	MAC address of the bundle.
Minimum links	Minimum number of active links required before the specified bundle can be activated.
active B/W (Kbps)	Minimum amount of bandwidth required before a user can bring up the specified bundle.
Maximum active links	Maximum number of links that can be actively carrying traffic in the specified bundle.
Port ID	Port identifier, in the <i>rack/slot/module/port</i> format.

R3.5.0 Beta Draft—Cisco Confidential Information

Table 105 *show bundle Bundle-Ether Field Descriptions*

Field	Description
B/W (Kbps)	Bundled interface bandwidth, in kilobits per second.
State	Current state of the specified port. Possible port states are as follows: • 0—Port is Detached • 1—Port is Waiting • 2—Port is Attached • 3—Port is Collecting • 4—Port is Distributing
Port ID	Port identifier in hexadecimal format
B/W (Kbps)	Port bandwidth, in kilobits per second.
MAC address	MAC address associated with the specified port.

Related Commands

Command	Description
bundle id	Adds a port to an aggregated interface (or bundle).
show lacp bundle	Displays detailed information about LACP ports and their peers.
show interfaces	Displays statistics for all interfaces configured on the router or on a specific node.

R3.5.0 Beta Draft—Cisco Confidential Information

show bundle Bundle-POS

To display information about a specific POS bundle, enter the **show bundle Bundle-POS** command in EXEC mode.

show bundle Bundle-POS *bundle-id* [**reasons**]

Syntax Description	<i>bundle-id</i>	Number of the POS bundle whose information you want to display. Replace <i>bundle-id</i> with a bundle identifier. Range is from 1 through 65535.
	reasons	(Optional) Displays the “Mux Reason”, which is the reason why each link is in its state.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	- The output for this command was modified. - The reasons keyword was added.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	bundle	read

Examples	The following is sample output from the show bundle Bundle-POS command:

```
RP/0/RP0/CPU0:router# show bundle Bundle-POS 5
```

```
State: 0 - Port is Detached. 1 - Port is Waiting.
       2 - Port is Attached. 3 - Port is Collecting.
       4 - Port is Distributing.
```

```
Bundle-POS5
B/W (Kbps)  MAC address  Minimum active  Maximum active
Links  B/W (Kbps)  Links
```

R3.5.0 Beta Draft—Cisco Confidential Information

0	N/A	1	1	32
Port	State	Port ID	B/W (Kbps)	MAC address
PO0/0/0/0	0	0x8000, 0x0001	155520	N/A
PO0/0/0/1	0	0x8000, 0x0002	155520	N/A
PO0/0/0/2	0	0x8000, 0x0003	155520	N/A

The following is sample output from the **show bundle Bundle-POS** command with the **reasons** keyword included in the command string:

RP/0/RP0/CPU0:router# **show bundle Bundle-POS 5 reasons**
 Bundle-POS5

B/W (Kbps)	MAC address	Minimum active Links	B/W (Kbps)	Maximum active Links
0	N/A	1	1	32
Port	State	Port ID	B/W (Kbps)	MAC address
PO0/0/0/0	0	0x8000, 0x0001	155520	N/A
Link is down				
PO0/0/0/1	0	0x8000, 0x0002	155520	N/A
Link is down				
PO0/0/0/2	0	0x8000, 0x0003	155520	N/A
Link is down				

Table 106 describes the significant fields shown in the display.

Table 106 show bundle Bundle-POS Field Descriptions

Field	Description
B/W (Kbps)	Bundled interface bandwidth, in kilobits.
MAC address	MAC address of the bundle.
Minimum links	Minimum number of active links required before the specified bundle can be activated.
active B/W (Kbps)	Minimum amount of bandwidth required before a user can bring up the specified bundle.
Maximum active links	Maximum number of links that can be actively carrying traffic in the specified bundle.
Port	Port identifier, in the <i>rack/slot/module/port</i> format.
State	Current state of the specified port.
Port ID	Port identifier, in hexadecimal format.
B/W (Kbps)	Individual interface bandwidth, in kilobits.
MAC address	Mac address for the specified interface.

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	bundle id	Adds a port to an aggregated interface (or bundle).
	show lacp bundle	Displays detailed information about LACP ports and their peers.
	show interfaces	Displays statistics for all interfaces configured on the router or on a specific node.

R3.5.0 Beta Draft—Cisco Confidential Information

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-id* | **Bundle-POS** *bundle-id*]

Syntax Description

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

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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
```

R3.5.0 Beta Draft—Cisco Confidential Information

B/W (Kbps)	MAC address	Minimum active Links	B/W (Kbps)	Maximum active 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 107 describes the significant fields shown in the display.

Table 107 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 <i>rack/slot/module/port</i> 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 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
Port ID	Port identifier, expressed in the format <i>Nxnnnn</i> . <i>N</i> is the port priority, and <i>nnnn</i> is the port number assigned by the sending router.
Key	2-byte number associated with the specified link and aggregator. Each port 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.

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	bundle id	Adds a port to an aggregated interface (or bundle).
	show bundle Bundle-Ether	Displays information for a specific Ethernet bundle.
	show bundle Bundle-POS	Displays information for a specific POS bundle.

R3.5.0 Beta Draft—Cisco Confidential Information

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-id* | **Bundle-POS** *bundle-id*]

Syntax Description	Bundle-Ether <i>bundle-id</i>	Specifies the Ethernet bundle whose counters you want to display. Replace <i>bundle-id</i> with a bundle identifier. Range is from 1 through 65535.
	Bundle-POS <i>bundle-id</i>	Specifies the POS bundle whose counters you want to display. Replace <i>bundle-id</i> with a bundle identifier. Range is from 1 through 65535.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	bundle	read

R3.5.0 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to display LACP counters on an Ethernet bundle:

```
RP/0/RP0/CPU0:router# show lacp counters bundle-ether 4
```

Bundle-Ether1

Port	LACPDUs		Marker		Last Cleared
	Sent	Received	Received	Resp. Sent	
Gi0/0/2/0	12	0	0	0	never

Port	Excess	Excess	Pkt Errors
Gi0/0/2/0	0	0	0

[Table 108](#) describes the significant fields shown in the display.

Table 108 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 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	Clears LACP counters for all members of all bundles, all members of a specific bundle, or for a specific port.

R3.5.0 Beta Draft—Cisco Confidential Information

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 interface_instance | TenGigE interface_instance | POS  
                interface_instance]
```

Syntax Description	GigabitEthernet <i>interface_instance</i>	Specifies the Gigabit Ethernet interface bundle whose LACP port information you want to display. The <i>interface_instance</i> is expressed in the <i>rack/slot/module/port</i> notation.
	TenGigE <i>interface_instance</i>	Specifies the TenGigE interface whose LACP port information you want to display. The <i>interface_instance</i> is expressed in the <i>rack/slot/module/port</i> notation.
	POS <i>interface_instance</i>	Specifies the Packet-over-SONET/SDH (POS) network whose LACP port information you want to display. The <i>interface_instance</i> is expressed in the <i>rack/slot/module/port</i> notation.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	bundle	read

R3.5.0 Beta Draft—Cisco Confidential Information

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

  B/W (Kbps)   MAC address      Minimum active   Maximum active
  -----
             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 109 describes the significant fields shown in the display.

Table 109 show lacp port Field Descriptions

Field	Description
Port	Identifies the LACP port whose information is displayed. The port number is expressed in the <i>rack/slot/module/port</i> notation.
State	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 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
Flags	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
Port ID	Port identifier, expressed in the following format: <i>Nxnnnn</i> . <i>N</i> is the port priority, and <i>nnnn</i> is the port number assigned by the sending router.

R3.5.0 Beta Draft—Cisco Confidential Information

Table 109 *show lacp port Field Descriptions (continued)*

Field	Description
Key	2-byte number associated with the specified link and aggregator. Each port 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	Adds a port to an aggregated interface (or bundle).
show bundle Bundle-Ether	Displays information about a specific Ethernet bundle.
show bundle Bundle-POS	Displays information about a specific POS bundle.

R3.5.0 Beta Draft—Cisco Confidential Information

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 arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.



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
```

R3.5.0 Beta Draft—Cisco Confidential Information

Table 110 describes the significant fields shown in the display.

Table 110 *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	Adds a port to an aggregated interface (or bundle).
show bundle Bundle-Ether	Displays information about a specific Ethernet bundle.
show bundle Bundle-POS	Displays information about a specific POS bundle.
show lacp bundle	Displays detailed information about LACP ports and their peers.
show lacp port	Displays detailed information about LACP ports

■ show lacp system-id

R3.5.0 Beta Draft—Cisco Confidential Information



PPP Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

This module describes the commands used to configure the Point-to-Point Protocol (PPP), an encapsulation scheme that can be used on Packet-over-SONET (POS) and serial interfaces on the Cisco IOS XR software.

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

R3.5.0 Beta Draft—Cisco Confidential Information

bundle

To create a multilink interface bundle, use the **bundle** command in the interface configuration mode. To remove a multilink interface bundle, use the **no** form of this command.

bundle *bundleID*

Syntax Description	<i>bundleID</i>	ID number of the multilink interface bundle. Range is from 1 through 1024.

Defaults	No default behavior or values

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.4.1	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

The **bundle** command is used in the mgmtmultilink controller mode to dynamically create a multilink interface. This command is similar to the **channel-group** command on the T1 controller, which dynamically creates a serial interface.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples	The following example shows how to create a multilink interface with a bundle ID of 1:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# controller mgmtmultilink 0/1/0/0
RP/0/0/CPU0:router(config-mgmtmultilink)# bundle 1
RP/0/0/CPU0:router(config-mgmtmultilink)# commit
```

Related Commands	Command	Description
	multilink fragment-size	Sets the fragment size to be used on the multilink interface.
	multilink group	Adds the serial interface to the multilink interface.

R3.5.0 Beta Draft—Cisco Confidential Information

Command	Description
multilink	Enters the config-if-multilink submode.
ppp multilink minimum-active links	Sets the minimum number of active links required before the multilink interface line can be brought to the up state.

R3.5.0 Beta Draft—Cisco Confidential Information

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 arguments or keywords.

Defaults PPP encapsulation is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	Release 2.0	This command was first introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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# configuration
RP/0/RP0/CPU0:router(config)# interface POS 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show ppp interfaces	Displays PPP state information for an interface.

R3.5.0 Beta Draft—Cisco Confidential Information

multilink

To enter the config-if-multilink submode, use the **multilink** command in the interface configuration mode.

multilink

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Interface configuration

Command History	Release	Modification
	Release 3.4.1	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

For multilink interfaces, the **multilink** command provides access to the config-if-multilink submode to use the **multilink fragment-size** command. For serial interfaces, this command provides access to the config-if-multilink submode to use the **group** command.

**Note**

This command behaves similarly to the **timeslots** command. It is not possible to enter this command or remove the multilink interface after the channel-group configuration is committed.

Task ID	Task ID	Operations
	hdlc	read, write

Examples The following example shows how to enter the config-if-multilink submode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface serial 0/1/0/0/1:0
RP/0/0/CPU0:router(config-if)# multilink
RP/0/0/CPU0:router(config-if-multilink)# group 1
RP/0/0/CPU0:router(config-if-multilink)# commit
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	bundle	Creates the bundle ID for a multilink interface.
	multilink fragment-size	Sets the fragment size to be used on the multilink interface.
	multilink group	Adds the serial interface to the multilink interface.
	ppp multilink minimum-active links	Sets the minimum number of active links required before the multilink interface line can be brought to the up state.

R3.5.0 Beta Draft—Cisco Confidential Information

multilink fragment-size

To set the Layer 2 fragmentation size for a multilink interface as opposed to the Layer 3 fragment size, which is controlled by the **mtu** command, use the **multilink fragment-size** command in interface configuration mode. To set the fragment size back to the default, no fragment size, use the **no** form of this command.

multilink fragment-size *value*

no multilink fragment-size *value*

Syntax Description	<i>value</i>	Value of the fragment size. The allowed values are determined by the hardware. In the current release, the allowed values are 128, 256 and 512. The value 64 also appears in the CLI help for this parameter. However, 64 is not allowed in this release and will cause configuration problems in the system if used.

Defaults	The default is no multilink fragment-size, which means no fragmentation at Layer 2.

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.4.1	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	hdlc	read, write

Examples	The following example shows how to set the fragment size to 128:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface multilink 0/1/0/0/1
RP/0/0/CPU0:router(config-if)# multilink fragmentation-size 128
RP/0/0/CPU0:router(config-if)# commit
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	bundle	Creates the bundle ID for a multilink interface.
	multilink group	Adds the serial interface to the multilink interface.
	multilink	Enters the config-if-multilink submode.
	ppp multilink minimum-active links	Sets the minimum number of active links required before the multilink interface line can be brought to the up state.

R3.5.0 Beta Draft—Cisco Confidential Information

multilink group

To attach a serial interface to a multilink interface bundle, use the **multilink group** command in interface configuration mode. To remove a serial interface from a multilink interface bundle, use the **no** form of this command.

multilink group *bundleID*

no multilink group *bundleID*

Syntax Description	<i>bundleID</i>	The bundle ID number of the multilink interface, in the format <i>rack/slot/bay/controllerID/bundleID</i>

Defaults	No default behavior or values

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.4.1	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	hdlc	read, write

Examples	The following examples show how to attach a serial interface to a multilink interface bundle:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface serial 0/1/0/0/1:0
RP/0/0/CPU0:router(config-if)# multilink group 1
RP/0/0/CPU0:router(config-if)# commit
```

or

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface serial 0/1/0/0/1:0
RP/0/0/CPU0:router(config-if)# multilink
RP/0/0/CPU0:router(config-if-multilink)# group 1
RP/0/0/CPU0:router(config-if-multilink)# commit
```


R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	bundle	Creates the bundle ID for a multilink interface.
	multilink fragment-size	Sets the fragment size to be used on the multilink interface.
	multilink	Enters the config-if-multilink submode.
	ppp multilink minimum-active links	Sets the minimum number of active links required before the multilink interface line can be brought to the up state.

R3.5.0 Beta Draft—Cisco Confidential Information

ppp authentication

To enable Challenge Handshake Authentication Protocol (CHAP), MS-CHAP, or Password Authentication Protocol (PAP), and to specify the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface, use the **ppp authentication** command in interface 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	<i>protocol</i>	Name of the authentication protocol used for PPP authentication. See Table 111 for the appropriate keyword. You may select one, two, or all three protocols, in any order.
	<i>list-name</i>	(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.

Defaults PPP authentication is not enabled.

Command Modes Interface configuration

Command History	Release	Modification
	Release 2.0	This command was first introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router. This command was corrected to include the possibility of specifying three protocols simultaneously.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

R3.5.0 Beta Draft—Cisco Confidential Information

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 111 lists the protocols used to negotiate PPP authentication.

Table 111 *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 the following example, CHAP is enabled on POS 0/4/0/1 and uses the authentication list MIS-access:

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

```
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
```

R3.5.0 Beta Draft—Cisco Confidential Information

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.

R3.5.0 Beta Draft—Cisco Confidential Information

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.
<i>password</i>	Cleartext or already-encrypted password.

Defaults

The password is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was first introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 software 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

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

In the following 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_CRS-8 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# configuration
```

```
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	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	Refuses CHAP authentication from peers requesting it.
ppp max-bad-auth	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.

R3.5.0 Beta Draft—Cisco Confidential 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 arguments or keywords.

Defaults CHAP authentication is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	Release 2.0	This command was first introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router# configuration
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	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	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	Enables remote PAP support for an interface, and includes the sent-username and password commands in the PAP authentication request packet to the peer.

R3.5.0 Beta Draft—Cisco Confidential Information

ppp max-bad-auth

To configure a PPP interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries, use the **ppp max-bad-auth** command in interface 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	<i>retries</i>	Number of retries after which the interface is to reset itself. Range is from 0 to 10. Default is 0 retries.

Defaults	<i>retries</i> = 0

Command Modes	Interface configuration

Command History	Release	Modification
	Release 2.0	This command was first introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

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 the following 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# configuration
```

```
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
```

R3.5.0 Beta Draft—Cisco Confidential Information

```
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
```

Related Commands	Command	Description
	ppp authentication	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 password	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS XR software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.
	ppp chap refuse	Refuses CHAP authentication from peers requesting it.
	ppp pap refuse	Refuses PAP authentication from peers requesting it.
	ppp pap sent-username password	Enables remote PAP support for an interface and includes the sent-username and password commands in the PAP authentication request packet to the peer.

R3.5.0 Beta Draft—Cisco Confidential Information

ppp max-configure

To specify the maximum number of configure requests to attempt (without response) before stopping the requests, use the **ppp max-configure** command in interface 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

<i>retries</i>	Maximum number of retries. Range is 4 through 20. Default is 10.

Defaults

retries = 10

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was first introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

Examples

In the following example, a limit of four configure requests is specified:

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

```
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
```

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
```

```
RP/0/RP0/CPU0:router(config-if)# ppp max-configure 4
```

Related Commands	Command	Description
	encapsulation ppp	Enables encapsulation for communication with routers or bridges using PPP.
	ppp max-failure	Configures the maximum number of CONFNAKs to permit before terminating a negotiation.
	ppp max-terminate	Configures the maximum number of terminate requests to send without reply before closing down the LCP or NCP.

R3.5.0 Beta Draft—Cisco Confidential Information

ppp max-failure

To configure the maximum number of consecutive Configure Negative Acknowledgments (CONFNAKs) to permit before terminating a negotiation, use the **ppp max-failure** command in interface 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	<i>retries</i>	Maximum number of CONFNAKs to permit before terminating a negotiation. Range is from 2 to 10. Default is 5.

Defaults	<i>retries</i> = 5

Command Modes	Interface configuration

Command History	Release	Modification
	Release 2.0	This command was first introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	ppp	read, write

Examples	The following ppp max-failure command specifies that no more than three CONFNAKs are permitted before terminating the negotiation:

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

```
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
```

```
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
```

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(config-if)# ppp max-failure 3
```

Related Commands

Command	Description
encapsulation ppp	Enables encapsulation for communication with routers or bridges using PPP.
ppp max-configure	Specifies the maximum number of configure requests to attempt (without response) before stopping the requests.
ppp max-terminate	Configures the maximum number of terminate requests to send without reply before closing down the LCP or NCP.

R3.5.0 Beta Draft—Cisco Confidential Information

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

Defaults	<i>number</i> = 2 retries

Command Modes	Interface configuration

Command History	Release	Modification
	Release 2.0	This command was first introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

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# configuration
```

```
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
```

```
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
```

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(config-if)# ppp max-terminate 5
```

Related Commands

Command	Description
ppp max-configure	Specifies the maximum number of configure requests to attempt (without response) before stopping the requests.
ppp max-failure	Configures the maximum number of CONFNAKs to permit before terminating a negotiation.

R3.5.0 Beta Draft—Cisco Confidential Information

ppp ms-chap password

To enable a router calling a collection of routers 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**] **line** *password*

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

Syntax Description	clear	(Optional) Specifies the cleartext encryption parameter for the password.
	encrypted	(Optional) Indicates that the password is already encrypted.
	line	The UNENCRYPTED (cleartext) default password
	<i>password</i>	Cleartext or already-encrypted password.

Defaults	The password is disabled.

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.

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 Cisco IOS XR 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:

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router# configuration
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 line xxxx
```

R3.5.0 Beta Draft—Cisco Confidential Information

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 arguments or keywords.

Defaults MS-CHAP authentication is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 The following 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# configuration
```

```
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
```

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
```

```
RP/0/RP0/CPU0:router(config-if)# ppp ms-chap refuse
```

R3.5.0 Beta Draft—Cisco Confidential Information

ppp multilink minimum-active links

To set the minimum number of active links required before the multilink interface line can be brought to the up state, use the **ppp multilink minimum-active links** command in global configuration mode.

ppp multilink minimum-active links *value*

Syntax Description	<i>value</i>	Number of active links. The range is 1 through 12.

Defaults	The default value is 1 active link.

Command Modes	Global configuration

Command History	Release	Modification
	Release 3.4.1	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	When multiple links are active and one link goes down, the whole bundle goes down.

Task ID	Task ID	Operations
	ppp	read, write

Examples	The following example shows how to set the minimum number of active links to 6:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface Multilink 0/1/0/0/1
RP/0/0/CPU0:router(config-if)# ppp multilink minimum-active links 6
RP/0/0/CPU0:router(config-if)# commit
```

Related Commands	Command	Description
	bundle	Creates the bundle ID for a multilink interface.
	multilink fragment-size	Sets the fragment size to be used on the multilink interface.
	multilink group	Adds the serial interface to the multilink interface.
	multilink	Enters the config-if-multilink submode.

R3.5.0 Beta Draft—Cisco Confidential Information

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 arguments or keywords.

Defaults PAP authentication is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	Release 2.0	This command was first introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router# configuration
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	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	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	Enables remote PAP support for an interface, and includes the sent-username and password commands in the PAP authentication request packet to the peer.

R3.5.0 Beta Draft—Cisco Confidential Information

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

<i>username</i>	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.
<i>password</i>	Cleartext or already-encrypted password.

Defaults

Remote PAP support is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was first introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

R3.5.0 Beta Draft—Cisco Confidential Information**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_CRS-8 POS 0/1/4/2
ipv4 address 10.12.32.2 255.255.255.0
encapsulation ppp
ppp pap sent-username P2_CRS-8 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# configuration

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	Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.
ppp pap refuse	Refuses PAP authentication from peers requesting it
ppp timeout authentication	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.

R3.5.0 Beta Draft—Cisco Confidential 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	<i>seconds</i>	Maximum time, in seconds, to wait for a response to an authentication packet. Range is from 3 to 30 seconds. Default is 10 seconds.

Defaults	<i>seconds</i> = 10

Command Modes	Interface configuration

Command History	Release	Modification
	Release 2.0	This command was first introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

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.

R3.5.0 Beta Draft—Cisco Confidential Information

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# configuration
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	Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.

R3.5.0 Beta Draft—Cisco Confidential Information

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

Defaults	<i>seconds</i> = 3

Command Modes	Interface configuration

Command History	Release	Modification
	Release 2.0	This command was first introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

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# configuration
```

```
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
```

```
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
```

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(config-if)# ppp timeout retry 8
```

Related Commands	Command	Description
	keepalive	Controls how often LCP EchoRequest packets are sent after LCP has been negotiated.
	ppp timeout authentication	Sets PPP authentication timeout parameters.

R3.5.0 Beta Draft—Cisco Confidential Information

show ppp interfaces

To display PPP state information for an interface, use the **show ppp interfaces** command in EXEC mode.

show ppp interfaces {*type instance* | **all** | **brief** {*type interface_instance* | **all** | **location node-id**} | **detail** {*type interface_instance* | **all** | **location node-id**} | **location node-id**}

Syntax Description	<i>type</i>	Specifies the interface type as Packet-over-SONET/SDH (POS) or serial. Replace <i>type</i> with pos or serial .
	<i>instance</i>	Either a physical interface instance or a virtual interface instance as follows: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. 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.
	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.
	location node-id	(Optional) Displays detailed PPP information for the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was first introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.0	No modification.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

There are seven possible PPP states applicable for either the Link Control Protocol (LCP) or the Network Control Protocol (NCP).

Task ID	Task ID	Operations
	ppp	read

Examples

The following example shows how to display PPP state information for POS interface 0/2/0/0:

```
RP/0/RP0/CPU0:router# show ppp interfaces POS 0/2/0/0
```

```
RP/0/RP0/CPU0:P2_CRS-8#show ppp interfaces
```

```
POS0/2/0/0 is up, line protocol is up
  LCP: Open
    Keepalives enabled (10 sec)
    Local MRU: 4470 bytes
    Peer MRU: 4470 bytes
  Authentication
    Of Peer: CHAP (Completed as P1_CRS-8)
    Of Us: CHAP (Completed as P2_CRS-8)
  IPCP: Open
    Local IPv4 address: 10.12.32.2
    Peer IPv4 address: 10.12.32.1
  OSICP: Open
```

```
POS0/2/4/3 is down, line protocol is down
  LCP: Starting
    Keepalives enabled (10 sec)
    Local MRU: 4470 bytes
    Peer MRU: 4470 bytes
  IPCP: Starting
    Local IPv4 address: 10.12.32.2
    Peer IPv4 address: 10.12.32.1
  OSICP: Open
```

[Table 112](#) describes the significant fields shown in the display.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 112** *show ppp interfaces Field Descriptions*

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
Keepalive	Keepalive setting and interval in seconds for echo request packets.
Local MRU	Maximum receive unit. The maximum size of the information transported, in bytes, in the PPP packet received by the local equipment.
Peer MRU	Maximum receive unit. The maximum size of the information transported, in bytes, in the PPP packet received by the peer equipment.
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).

R3.5.0 Beta Draft—Cisco Confidential Information**Table 112** *show ppp interfaces Field Descriptions (continued)*

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.
Local IPv4 address	IPv4 address for the local interface.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 112** *show ppp interfaces Field Descriptions (continued)*

Field	Description
Peer IPv4 address	IPv4 address for the peer equipment.
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.

**Note**

In this example, only IPCP and OSICP are running. If other NCPs are running, they will be displayed in the **show ppp interfaces** command output. Possible NCPs are IPCP, OSICP, IPv6CP, MPLSCP and CDPCP.

Related Commands

Command	Description
encapsulation ppp	Enables encapsulation for communication with routers or bridges using PPP.
ipv4 address	Specifies an IPv4 family address.
ipv6 address	Specifies an IPv6 family address.
keepalive	Controls how often LCP EchoRequest packets are sent after LCP has been negotiated.
mtu	Specifies the MTU to be used.



Frame Relay Service Configuration Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

This chapter describes the commands used to configure Frame Relay service on Packet-over-SONET/SDH (POS) and serial interfaces for the Cisco XR 12000 Series Router running Cisco IOS XR software.

R3.5.0 Beta Draft—Cisco Confidential Information

encap (PVC)

To change the encapsulation for a Frame Relay permanent virtual circuit (PVC), use the **encap** command in PVC configuration mode. To restore default encapsulation from the Frame Relay main interface, use the **no** form of this command.

encap [**cisco** | **ietf**]

no encap [**cisco** | **ietf**]

Syntax Description	<table> <tr> <td data-bbox="342 573 625 680">cisco</td><td data-bbox="625 573 1502 680">(Optional) Uses Cisco encapsulation, which is a 4-byte header, with 2 bytes to identify the data-link connection identifier (DLCI) and 2 bytes to identify the packet type.</td></tr> <tr> <td data-bbox="342 680 625 821">ietf</td><td data-bbox="625 680 1502 821">(Optional) Sets the encapsulation method to comply with the Internet Engineering Task Force (IETF) standard (RFC 1490). Use this keyword when connecting to equipment that belongs to a vendor other than Cisco across a Frame Relay network.</td></tr> </table>	cisco	(Optional) Uses Cisco encapsulation, which is a 4-byte header, with 2 bytes to identify the data-link connection identifier (DLCI) and 2 bytes to identify the packet type.	ietf	(Optional) Sets the encapsulation method to comply with the Internet Engineering Task Force (IETF) standard (RFC 1490). Use this keyword when connecting to equipment that belongs to a vendor other than Cisco across a Frame Relay network.		
cisco	(Optional) Uses Cisco encapsulation, which is a 4-byte header, with 2 bytes to identify the data-link connection identifier (DLCI) and 2 bytes to identify the packet type.						
ietf	(Optional) Sets the encapsulation method to comply with the Internet Engineering Task Force (IETF) standard (RFC 1490). Use this keyword when connecting to equipment that belongs to a vendor other than Cisco across a Frame Relay network.						
Defaults	The default encapsulation keyword is Cisco. When this command is not configured, encapsulation is inherited from the Frame Relay main interface.						
Command Modes	PVC configuration						
Command History	<table> <tr> <th data-bbox="342 1146 625 1184">Release</th><th data-bbox="625 1146 1502 1184">Modification</th></tr> <tr> <td data-bbox="342 1184 625 1222">Release 3.4.0</td><td data-bbox="625 1184 1502 1222">This command was introduced on the Cisco XR 12000 Series Router.</td></tr> <tr> <td data-bbox="342 1222 625 1272">Release 3.5.0</td><td data-bbox="625 1222 1502 1272">No modification.</td></tr> </table>	Release	Modification	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.	Release 3.5.0	No modification.
Release	Modification						
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.						
Release 3.5.0	No modification.						
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the encap command to configure encapsulation for a Frame Relay PVC. If this command is not configured, encapsulation is inherited from the Frame Relay subinterface. This command is available on Packet-over-SONET/SDH (POS) and serial interfaces for this Cisco IOS XR software release.						
Task ID	<table> <tr> <th data-bbox="342 1671 625 1709">Task ID</th><th data-bbox="625 1671 1502 1709">Operations</th></tr> <tr> <td data-bbox="342 1709 625 1755">fr</td><td data-bbox="625 1709 1502 1755">read, write</td></tr> </table>	Task ID	Operations	fr	read, write		
Task ID	Operations						
fr	read, write						

R3.5.0 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to set encapsulation on PVC data-link connection identifier (DLCI) 16 for Packet-over-SONET/SDH (POS) subinterface 0/4/0/1.1:

```
RP/0/0/CPU0:router(config)# interface POS 0/4/0/1.1
RP/0/0/CPU0:router(config-subif)# pvc 16
RP/0/0/CPU0:router(config-fr-vc)# encap
```

Related Commands

Command	Description
encapsulation frame-relay	Enables Frame Relay encapsulation.

R3.5.0 Beta Draft—Cisco Confidential Information

encapsulation frame-relay

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

encapsulation frame-relay [ietf]

no encapsulation frame-relay [ietf]

Syntax Description	ietf	(Optional) Sets the encapsulation method to comply with the Internet Engineering Task Force (IETF) standard (RFC 1490). Use this keyword when connecting to another vendor's equipment across a Frame Relay network.

Defaults	The default encapsulation method is Cisco.

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **encapsulation frame-relay** command to connect an interface to a Frame Relay network. When this command is configured, incoming packets to the interface are encapsulated and outgoing packets are encapsulated with a Frame Relay header.

A Cisco or IETF encapsulation method controls the Network Layer Protocol Identifier (NLPID) that is added to outgoing packets on the interface. The encapsulation method enabled for an outgoing packet can be changed for each data-link connection identifier (DLCI) per subinterface by using the **encap (PVC)** command in PVC configuration mode.

When the **encapsulation frame-relay** command is configured, LMI is enabled by default. To disable LMI use the **frame-relay lmi disable** command.

The following restrictions apply to the **encapsulation frame-relay** command upon configuration or removal of the command on an interface:

- When configuring this command, Layer 3 and Layer 2 configurations are not allowed on the interface.
- Before removing this command, all Frame Relay subinterfaces and LMI configuration should be deleted from the interface.

R3.5.0 Beta Draft—Cisco Confidential Information

The **encapsulation frame-relay** command is available on Packet-over-SONET/SDH (POS) and serial interfaces for this Cisco IOS XR software release.

Task ID	Task ID	Operations
	interface	read, write
	fr	read, write

Examples

The following example shows Frame Relay encapsulation configured on Packet-over-SONET/SDH (POS) 0/3/0/1:

```
RP/0/0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/0/CPU0:router(config-if)# encapsulation frame-relay ietf
```

Related Commands	Command	Description
	encap (PVC)	Configures encapsulation for an FR PVC.
	frame-relay lmi disable	Disables the LMI.

R3.5.0 Beta Draft—Cisco Confidential Information

frame-relay intf-type

To configure the interface type of the User-Network Interface (UNI), use the **frame-relay intf-type** command in interface configuration mode. To change the configuration, use the **no** form of this command.

frame-relay intf-type [dce | dte]

no frame-relay intf-type [dce | dte]

Syntax Description	dce	(Optional) Router functions as a switch connected to a router.
	dte	(Optional) Router is connected to a Frame Relay network.

Defaults	DTE

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	The frame-relay intf-type command is available on Packet-over-SONET/SDH (POS) and serial interfaces for this Cisco IOS XR software release.

Task ID	Task ID	Operations
	fr	read, write

Examples	The following example shows how to configure a DCE switch type on the interface:

```
RP/0/0/CPU0:router(config)# interface pos 0/4/0/0
RP/0/0/CPU0:router(config-if)# frame-relay intf-type dce
```


R3.5.0 Beta Draft—Cisco Confidential Information

frame-relay lmi disable

To disable the Frame Relay Local Management Interface (LMI), use the **frame-relay lmi disable** command in interface configuration mode. To reenble LMI, use the **no** form of this command.

frame-relay lmi disable

no frame-relay lmi disable

Syntax Description No default behavior or values

Defaults LMI is enabled.

Command Modes Interface configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **frame-relay lmi disable** command is available on Packet-over-SONET/SDH (POS) and serial interfaces for this Cisco IOS XR software release.

Task ID	Task ID	Operations
	fr	read, write

Examples The following example shows how to configure a DCE switch type on the interface:

```
RP/0/0/CPU0:router(config)# interface pos 0/4/0/0
RP/0/0/CPU0:router(config-if)# frame-relay lmi disable
```

R3.5.0 Beta Draft—Cisco Confidential Information

frame-relay lmi-n391dte

To set the full status polling interval, use the **frame-relay lmi-n391dte** command in interface configuration mode. To restore the default interval value, use the **no** form of this command.

frame-relay lmi-n391dte *polling-cycles*

no frame-relay lmi-n391dte *polling-cycles*

Syntax Description	<i>polling-cycles</i>	Number of Line Integrity Verification (LIV) exchanges performed before requesting a full status message. Range is from 1 to 255.

Defaults	<i>polling-cycles</i> : 6

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **frame-relay lmi-n391dte** command as a means of setting the full status message polling interval. This command is relevant only when the interface type is data terminal equipment (DTE).

Two message types are supported: status inquiry and status. Status inquiry messages are sent from DTE to DCE. Status messages are sent from DCE to DTE (in response to a status inquiry). The Status (Full) and LIV report types are contained within these messages, and typically there is one status transaction for every five LIV transactions.

This command is available on Packet-over-SONET/SDH (POS) and serial interfaces for this Cisco IOS XR software release.

Task ID	Task ID	Operations
	fr	read, write

Examples

The following example shows that one out of every four status inquiries generated requests a full status response from the DCE on the interface:

```
RP/0/0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/0/CPU0:router(config-if)# frame-relay intf-type dte
RP/0/0/CPU0:router(config-if)# frame-relay lmi-n391dte 4
```

R3.5.0 Beta Draft—Cisco Confidential Information

frame-relay lmi-n392dce

To set the error threshold on a DCE interface, use the **frame-relay lmi-n392dce** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

frame-relay lmi-n392dce threshold

no frame-relay lmi-n392dce threshold

Syntax Description	<i>threshold</i>	Error threshold value. Range is from 1 to 10.

Defaults	<i>errors: 3</i>

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

N392 errors must occur within the number defined by the N393 event count for the link to be declared down. Therefore, the threshold value for this command must be less than the count value defined in the **frame-relay lmi-n393dce** command.

The **frame-relay lmi-n392dce** command is relevant only when the interface type is data computer equipment (DCE).

This command is available on Packet-over-SONET/SDH (POS) and serial interfaces for this Cisco IOS XR software release.

Task ID	Task ID	Operations
	fr	read, write

Examples	The following example shows how to set the Local Management Interface (LMI) failure threshold to 4. The router acts as a Frame Relay DCE switch.

```
RP/0/0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/0/CPU0:router(config-if)# frame-relay intf-type dce
RP/0/0/CPU0:router(config-if)# frame-relay lmi-n392dce 4
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	frame-relay lmi-n393dce	Sets the DCE monitored events count.

R3.5.0 Beta Draft—Cisco Confidential Information

frame-relay lmi-n392dte

To set the error threshold on a DTE interface, use the **frame-relay lmi-n392dte** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

frame-relay lmi-n392dte *threshold*

no frame-relay lmi-n392dte *threshold*

Syntax Description	<i>threshold</i>	Error threshold value. Range is from 1 to 10.

Defaults	<i>errors: 3</i>

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **frame-relay lmi-n392dte** command is relevant only when the interface type is data terminal equipment (DTE).

This command is available on Packet-over-SONET/SDH (POS) and serial interfaces for this Cisco IOS XR software release.

Task ID	Task ID	Operations
	fr	read, write

Examples

The following example shows how to set the Local Management Interface (LMI) failure threshold to 4. The router acts as a Frame Relay DTE switch.

```
RP/0/0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/0/CPU0:router(config-if)# frame-relay intf-type dte
RP/0/0/CPU0:router(config-if)# frame-relay lmi-n392dte 4
```

R3.5.0 Beta Draft—Cisco Confidential Information

frame-relay lmi-n393dce

To set the DCE monitored events count, use the **frame-relay lmi-n393dce** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

frame-relay lmi-n393dce *events*

no frame-relay lmi-n393dce *events*

Syntax Description	<i>events</i>	Monitored events count. Range is from 1 to 10.

Defaults	<i>events</i> : 4

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **frame-relay lmi-n393dce** command is used along with the **frame-relay lmi-n392dce** command to define the condition that causes the link to be declared down.

N392 errors must occur within the *events* argument count in order for the link to be declared down. Therefore, the events value defined in this command must be greater than the threshold value defined in the **frame-relay lmi-n392 dce** command.

The **frame-relay lmi-n393dce** command is relevant only when the interface type is data computer equipment (DCE).

This **frame-relay lmi-n393dce** command is available on Packet-over-SONET/SDH (POS) and serial interfaces for this Cisco IOS XR software release.

Task ID	Task ID	Operations
	fr	read, write

Examples

The following example shows how to set the Local Management Interface (LMI) monitored events count to 5.

```
RP/0/0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/0/CPU0:router(config-if)# frame-relay intf-type dce
```

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/0/CPU0:router(config-if)# frame-relay lmi-n393dce 5
```

Related Commands	Command	Description
	frame-relay lmi-n392dce	Sets the error threshold on a DCE interface.

R3.5.0 Beta Draft—Cisco Confidential Information

frame-relay lmi-n393dte

To set the monitored event count on a DTE interface, use the **frame-relay lmi-n393dte** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

frame-relay lmi-n393dte *events*

no frame-relay lmi-n393dte *events*

Syntax Description	<i>events</i>	Monitored events count. Range is from 1 to 10.

Defaults	<i>events</i> : 4

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **frame-relay lmi-n393dte** command is relevant only when the interface type is data terminal equipment (DTE).

This **frame-relay lmi-n393dte** command is available on Packet-over-SONET/SDH (POS) and serial interfaces for this Cisco IOS XR software release.

Task ID	Task ID	Operations
	fr	read, write

Examples

The following example shows how to set the Local Management Interface (LMI) monitored events count to 5.

```
RP/0/0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/0/CPU0:router(config-if)# frame-relay intf-type dte
RP/0/0/CPU0:router(config-if)# frame-relay lmi-n393dte 5
```


R3.5.0 Beta Draft—Cisco Confidential Information

frame-relay lmi-t391dte

To set the Local Management Interface (LMI) polling interval, use the **frame-relay lmi-t391dte** command in interface configuration mode. To restore the default interval value, use the **no** form of this command.

frame-relay lmi-t391dte *seconds*

no frame-relay lmi-t391dte *seconds*

Syntax Description	<i>seconds</i>	Polling interval (in seconds) between each status inquiry from the DTE end. Range is from 5 to 30.

Defaults	10 seconds

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

This **frame-relay lmi-t391dte** command is available on Packet-over-SONET/SDH (POS) and serial interfaces for this Cisco IOS XR software release.

The *seconds* value defined in this command must be less than the polling verification timer defined in the **frame-relay lmi-t392 dce** command.

The **frame-relay lmi-t391dte** command is relevant only when the interface type is data terminal equipment (DCE).

Task ID	Task ID	Operations
	fr	read, write

Examples

The following example shows how to set the LMI polling timer interval to 15 seconds.

```
RP/0/0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/0/CPU0:router(config-if)# frame-relay intf-type dte
RP/0/0/CPU0:router(config-if)# frame-relay lmi-t391dte 15
```

R3.5.0 Beta Draft—Cisco Confidential Information

frame-relay lmi-t392dce

To set the Local Management Interface (LMI) polling verification timer on the DCE, use the **frame-relay lmi-t392dce** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

frame-relay lmi-t392dce *seconds*

no frame-relay lmi-t392dce *seconds*

Syntax Description	<i>seconds</i>	Polling verification timer in seconds. Range is from 5 to 30.

Defaults	<i>seconds:15</i>

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **frame-relay lmi-t392dce** command is used along with the **frame-relay lmi-t391dte** command to define the condition that causes the link to be declared down.

The *seconds* value defined in this command must be greater than the polling verification timer defined in the **frame-relay lmi-t391 dte** command.

This **frame-relay lmi-n392dce** command is available on Packet-over-SONET/SDH (POS) and serial interfaces for this Cisco IOS XR software release.

Task ID	Task ID	Operations
	fr	read, write

Examples

The following example shows how to set the Local Management Interface (LMI) polling timer interval to 30 seconds.

```
RP/0/0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/0/CPU0:router(config-if)# frame-relay intf-type dce
RP/0/0/CPU0:router(config-if)# frame-relay lmi-t392dce 30
```

R3.5.0 Beta Draft—Cisco Confidential Information

frame-relay lmi-type

To select the Local Management Interface (LMI) type, use the **frame-relay lmi-type** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

frame-relay lmi-type {ansi | cisco | q933a}

no frame-relay lmi-type {ansi | cisco | q933a}

Syntax Description	ansi	Uses LMI as defined by ANSI T1.617a-1994 Annex D.
	cisco	Uses LMI as defined by Cisco (not standard).
	q933a	Uses LMI as defined by ITU-T Q.933 (02/2003) Annex A.

Defaults	Cisco

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	The ccitt keyword was replaced with the q933a keyword.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	If the DTE is not explicitly configured or the no form is not used after explicit configuration, then the DTE automatically senses the LMI type of the DCE and use that type of LMI.
	This frame-relay lmi-type command is available on Packet-over-SONET/SDH (POS) and serial interfaces for this Cisco IOS XR software release.

Task ID	Task ID	Operations
	fr	read, write

Examples	The following example shows how to set the Local Management Interface (LMI) type to Q.933, Annex A.

```
RP/0/0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/0/CPU0:router(config-if)# frame-relay lmi-type q933a
```

R3.5.0 Beta Draft—Cisco Confidential Information

match frame-relay dlci

To specify the Frame Relay data-link connection identifier (DLCI) number or number range as a match criterion in a class map, use the **match frame-relay dlci** command in class-map configuration mode. To remove a previously specified DLCI number as a match criterion, use the **no** form of this command.

match frame-relay dlci [*Dlci* | *StartDlci-EndDlci*]

no match frame-relay dlci [*Dlci* | *StartDlci-EndDlci*]

Syntax Description	<i>Dlci</i>	A DLCI number associated with the packet. Range is from 16 to 1007.
	<i>StartDlci-EndDlci</i>	A DLCI number range from 16 to 1007. Numbers are separated by a hyphen.

Defaults No DLCI number is specified.

Command Modes Class-map configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The match criterion for the **match frame-relay dlci** command can be used only on hierarchical policy maps.

Task ID	Task ID	Operations
	qos	read, write

Examples

The following example shows how to create the fr-dlci class map, and the Frame Relay DLCI number range 100-200 is specified as a match criterion. Packets matching this criterion are placed in fr-dlci:

```
RP/0/0/CPU0:router(config)# class-map fr-dlci
RP/0/0/CPU0:router(config-cmap)# match frame relay dlci 100-200
RP/0/0/CPU0:router(config-cmap)# end
```

R3.5.0 Beta Draft—Cisco Confidential Information

pvc (frame relay)

To associate a data-link connection identifier (DLCI) number to a permanent virtual circuit (PVC), and to enter PVC configuration mode, use the **pvc** command in subinterface configuration mode. To delete the PVC, use the **no** form of this command.

pvc *dlci-number*

no pvc *dlci-number*

Syntax Description	<i>dlci-number</i>	DLCI number used to identify the PVC. Range is from 16 to 1007.

Defaults	No PVC is defined.

Command Modes	Subinterface configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Commands available in PVC configuration mode are:

RP/0/0/CPU0:router(config-fr-vc)#?

```

commit      Commit the configuration changes to running
describe    Describe a command without taking real actions
do          Run an exec command
encap       Set the Encapsulation of this PVC
exit        Exit from this submode
no          Negate a command or set its defaults
show        Show contents of configuration

```

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

The **pvc** command is available on Packet-over-SONET/SDH (POS) and serial interfaces for this Cisco IOS XR software release.

Task ID	Task ID	Operations
	fr	read, write

R3.5.0 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to create a PVC with DLCI 16:

```
RP/0/0/CPU0:router(config)# interface pos 0/4/0/0.1  
RP/0/0/CPU0:router(config-subif)# pvc 16  
RP/0/0/CPU0:router(config-fr-vc)#
```

R3.5.0 Beta Draft—Cisco Confidential Information

show frame-relay lmi

To display Frame Relay statistics about the Local Management Interface (LMI), use the **show frame-relay lmi** EXEC command.

show frame-relay lmi [**interface** *type instance* | **location** *node-id*]

Syntax Description	interface <i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
	<i>instance</i>	(Optional) Either a physical interface instance or a virtual interface instance as follows: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
	location <i>node-id</i>	(Optional) Clears hardware resource counters from the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.5.0 Beta Draft—Cisco Confidential Information

This command is available on Packet-over-SONET/SDH (POS) and serial interfaces for this Cisco IOS XR software release.

This command is used to check the status enquiry and status message between DCE and DTE.

Task ID	Task ID	Operations
	fr	read, write

Examples

The following is sample output from the **show frame-relay lmi** command:

```
RP/0/0/CPU0:router# show frame-relay lmi
```

```
LMI Statistics for interface POS0/1/0/0/ (Frame Relay DCE) LMI TYPE = ANSI
  Invalid Unnumbered Info 0          Invalid Prot Disc 0
  Invalid Dummy Call Ref 0          Invalid Msg Type 0
  Invalid Status Message 0          Invalid Lock Shift 9
  Invalid Information ID 0          Invalid Report IE Len 0
  Invalid Report Request 0          Invalid Keep IE Len 0
  Num Status Enq. Rcvd 9444          Num Status Msgs Sent 9444
  Num Full Status Sent 1578          Num St Enq. Timeouts 41
  Num Link Timeouts 7
```

```
LMI Statistics for interface POS0/1/0/1/ (Frame Relay DCE) LMI TYPE = CISCO
  Invalid Unnumbered Info 0          Invalid Prot Disc 0
  Invalid Dummy Call Ref 0          Invalid Msg Type 0
  Invalid Status Message 0          Invalid Lock Shift 0
  Invalid Information ID 0          Invalid Report IE Len 0
  Invalid Report Request 0          Invalid Keep IE Len 0
  Num Status Enq. Rcvd 9481          Num Status Msgs Sent 9481
  Num Full Status Sent 1588          Num St Enq. Timeouts 16
  Num Link Timeouts 4
```

Table 113 describes the significant fields shown in the display.

Table 113 *show frame-relay lmi* Field Descriptions

Field	Description
LMI Statistics	Signaling or LMI specification: CISCO, ANSI, or CCITT. Note CCITT is LMI as defined by ITU-T Q.933 (02/2003) Annex A.
Invalid Unnumbered Info	Number of received LMI messages with invalid unnumbered information field.
Invalid Dummy Call	Number of received LMI messages with invalid dummy calls.
Invalid Status Message	Number of received LMI messages with invalid status message.
Invalid Information ID	Number of received LMI messages with invalid information identifier.
Invalid Report Request	Number of received LMI messages with invalid Report Request.

R3.5.0 Beta Draft—Cisco Confidential Information

Table 113 **show frame-relay lmi Field Descriptions**

Field	Description
Num Status Enq. Rcvd	Number of LMI status enquiry messages received.
Num Link Timeouts	Number of link timeouts.
Invalid Prot Disc	Number of received LMI messages with invalid protocol discriminator.
Invalid Msg Type	Number of received LMI messages with invalid message type.
Invalid Lock Shift	Number of received LMI messages with invalid lock shift type.
Invalid Report IE Len	Number of received LMI messages with invalid Report IE Length.
Invalid Keep IE Len	Number of received LMI messages with invalid Report Request.
Num Status Msgs Sent	Number of LMI status enquiry messages sent.
Num St Enq. Timeouts	Number of times the status enquiry message was not received within the T392 DCE timer value.

R3.5.0 Beta Draft—Cisco Confidential Information

show frame-relay pvc

To display statistics about Frame Relay permanent virtual circuits (PVCs), use the **show frame-relay pvc** command in EXEC mode.

show frame-relay pvc [**interface** *instance* | **location** *node-id*] [*dlci-number*]

Syntax Description

interface <i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>instance</i>	(Optional) Either a physical interface instance or a virtual interface instance as follows: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
location <i>node-id</i>	(Optional) Clears hardware resource counters from the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<i>dlci-number</i>	(Optional) DLCI number used to identify the PVC. Range is from 16 to 1007.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

This command is available on Packet-over-SONET/SDH (POS) and serial interfaces for this Cisco IOS XR software release.

This command is used to check the status of PVCs on interfaces.

Task ID

Task ID	Operations
fr	read, write

Examples

The following is sample output from the **show frame-relay pvc** command:

```
RP/0/0/CPU0:router# show frame-relay pvc
```

PVC Statistics for interface Serial0/3/2/0 (Frame Relay DCE)

	Active	Inactive	Deleted	Static
Local	4	0	0	0
Switched	0	0	0	0
Dynamic	0	0	0	0

DLCI = 612, DLCI USAGE = LOCAL, ENCAP = CISCO, INHERIT = TRUE, PVC STATUS = ACTIVE, INTERFACE = Serial0/3/2/0.1

```
input pkts 0          output pkts 0          in bytes 0
out bytes 0           dropped pkts 0        in FECN packets 0
in BECN pkts 0        out FECN pkts 0        out BECN pkts 0
in DE pkts 0          out DE pkts 0
out bcast pkts 0      out bcast bytes 0
pvc create time 00:00:00    last time pvc status changed 00:00:00
```

DLCI = 613, DLCI USAGE = LOCAL, ENCAP = CISCO, INHERIT = TRUE, PVC STATUS = ACTIVE, INTERFACE = Serial0/3/2/0.2

```
input pkts 0          output pkts 0          in bytes 0
out bytes 0           dropped pkts 0        in FECN packets 0
in BECN pkts 0        out FECN pkts 0        out BECN pkts 0
in DE pkts 0          out DE pkts 0
out bcast pkts 0      out bcast bytes 0
pvc create time 00:00:00    last time pvc status changed 00:00:00
```

DLCI = 614, DLCI USAGE = LOCAL, ENCAP = CISCO, INHERIT = TRUE, PVC STATUS = ACTIVE, INTERFACE = Serial0/3/2/0.3

```
input pkts 0          output pkts 0          in bytes 0
out bytes 0           dropped pkts 0        in FECN packets 0
in BECN pkts 0        out FECN pkts 0        out BECN pkts 0
in DE pkts 0          out DE pkts 0
out bcast pkts 0      out bcast bytes 0
pvc create time 00:00:00    last time pvc status changed 00:00:00
```

DLCI = 615, DLCI USAGE = LOCAL, ENCAP = CISCO, INHERIT = TRUE, PVC STATUS = ACTIVE, INTERFACE = Serial0/3/2/0.4

```
input pkts 0          output pkts 0          in bytes 0
out bytes 0           dropped pkts 0        in FECN packets 0
in BECN pkts 0        out FECN pkts 0        out BECN pkts 0
in DE pkts 0          out DE pkts 0
out bcast pkts 0      out bcast bytes 0
```

```
show frame-relay pvc
```

R3.5.0 Beta Draft—Cisco Confidential Information

```
pvc create time 00:00:00      last time pvc status changed 00:00:00
RP/0/0/CPU0:router#
```

The following is sample output for a specific frame-relay PVC:

```
RP/0/0/CPU0:router# show frame-relay pvc 613
```

```
DLCI = 613, DLCI USAGE = LOCAL, ENCAP = CISCO, INHERIT = TRUE, PVC STATUS = ACTI
VE, INTERFACE = Serial0/3/2/0.2
  input pkts 0      output pkts 0      in bytes 0
  out bytes 0      dropped pkts 0      in FECN packets 0
  in BECN pkts 0    out FECN pkts 0      out BECN pkts 0
  in DE pkts 0      out DE pkts 0
  out bcast pkts 0  out bcast bytes 0
pvc create time 00:00:00      last time pvc status changed 00:00:00
```

Table 114 describes the significant fields shown in the displays.

Table 114 *show frame-relay pvc Field Descriptions*

Field	Description
DLCI	One of the DLCI numbers for the PVC.
DLCI USAGE	Lists SWITCHED when the router or access server is used as a switch, or LOCAL when the router or access server is used as a DTE device.
ENCAP	Type of encapsulation.
INHERIT	Encapsulation type for the PVC is inherited from the main interface.
PVC STATUS	Status of the PVC: ACTIVE, INACTIVE, or DELETED.
INTERFACE	Specific subinterface associated with this DLCI.
input pkts	Number of packets received on this PVC.
output pkts	Number of packets sent on this PVC.
in bytes	Number of bytes received on this PVC.
out bytes	Number of bytes sent on this PVC.
dropped pkts	Number of incoming and outgoing packets dropped by the router at the Frame Relay level.
in FECN pkts	Number of packets received with the FECN bit set.
in BECN pkts	Number of packets received with the BECN bit set.
out FECN pkts	Number of packets sent with the FECN bit set.
out BECN pkts	Number of packets sent with the BECN bit set.
in DE pkts	Number of DE packets received.
out DE pkts	Number of DE packets sent.
out bcast pkts	Number of output broadcast packets.
out bcast bytes	Number of output broadcast bytes.
pvc create time	Time at which the PVC was created.
last time pvc status changed	Time at which the PVC changed status.
shaping drops	Number of packets dropped by the traffic-shaping process.

R3.5.0 Beta Draft—Cisco Confidential Information

show interfaces (frame relay)

To display statistics about Frame Relay interfaces, use the **show interfaces** command in EXEC mode.

show interfaces [*type instance* | **all** | **local** | **location** *node-id*] [**accounting** | **brief** | **detail** | **summary**]

Syntax Description	
<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>instance</i>	(Optional) Either a physical interface instance or a virtual interface instance as follows: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. 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 <i>node-id</i>	(Optional) Clears hardware resource counters from the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
brief	(Optional) Displays brief information about 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.

Defaults No default behavior or values

Command Modes EXEC

R3.5.0 Beta Draft—Cisco Confidential Information**Command History**

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

This command is available on Packet-over-SONET/SDH (POS) and serial interfaces for this Cisco IOS XR software release.

Task ID

Task ID	Operations
fr	read, write

Examples

The following is sample output from the **show interfaces** command when the interface is configured with Frame Relay encapsulation:

```
RP/0/0/CPU0:router# show interfaces pos 0/1/0/0
```

```
POS0/1/0/0 is up, line protocol is up
  Hardware is Packet over SONET/SDH
  Internet address is Unknown
  MTU 4474 bytes, BW 622080 Kbit
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, crc 32, controller loopback not set,
  LMI enq sent 0, LMI stat recvd 0, LMI upd recvd 0
  LMI enq recvd 9463, LMI stat sent 9463, LMI upd sent 0, DCE LMI up
  LMI DLCI 0 LMI type is ANSI Annex D frame relay DCE
  Last clearing of "show interface" counters never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    20934 packets input, 1508069 bytes, 1151 total input drops
      0 drops for unrecognized upper-level protocol
    Received 0 broadcast packets, 0 multicast packets
      0 runs, 0 giants, 0 throttles, 0 parity
    1151 input errors, 1058 CRC, 0 frame, 0 overrun, 93 ignored, 0 abort
  19590 packets output, 990924 bytes, 0 total output drops
  Output 0 broadcast packets, 0 multicast packets
  0 output errors, 0 underruns, 0 applique, 0 resets
  0 output buffer failures, 0 output buffers swapped out
  0 carrier transitions
```

Table 115 describes the significant fields shown in the display.

Table 115 *show interfaces Field Descriptions*

Field	Description
Interface name	Displays the name of the current interface. In the example, the interface name is POS0/1/0/0.
Interface state	Displays the state of the interface. In the example, the interface is in the administratively up state.

R3.5.0 Beta Draft—Cisco Confidential Information

Table 115 *show interfaces* Field Descriptions

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 <i>n.n.n.n/n</i>	Displays the Layer 2 address (MAC address for Ethernet interfaces). Note Enter the mac-address command to configure the hardware address.
MTU	Displays the maximum transmission unit (MTU) for the interface. The MTU is the maximum packet size that can be transmitted over the interface. Note The MTU field indicates the interface MTU. Enter the mtu command to configure a lower MTU value at the layer 3 level.
BW	Displays the bandwidth of the interface in kbps.
reliability	Displays the proportion of packets that are not dropped and do not have errors. Note The reliability is shown as a fraction of 255.
txload	Indicates the traffic flowing out of the interface as a proportion of the bandwidth. Note The txload is shown as a fraction of 255.
rxload	Indicates the traffic flowing into the interface as a proportion of the bandwidth. Note The rxload is shown as a fraction of 255.
Encapsulation	Layer 2 encapsulation installed on the interface.
CRC	Indicates the length of the cyclic redundancy check (CRC), in bytes. Note Enter the pos crc command to configure the CRC.
controller loopback	Indicates that the hardware was configured as controller loopback.
LMI enq sent	Number of LMI enquiry messages sent.
LMI stat recvd	Number of LMI status messages received.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 115** **show interfaces Field Descriptions**

Field	Description
LMI upd rcvd	Number of LMI updated messages received.
LMI enq rcvd	Number of LMI enquiry messages received.
LMI stat sent	Number of LMI status messages sent.
LMI upd sent	Number of LMI updated messages sent.
DCE LMI	Displays the state of the DCE LMI.
LMI DLCI	Displays the LMI DLCI identifier.
LMI type	Displays the LMI type.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing for example, load and reliability) are not cleared when the counters are cleared.
5 minute input rate 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
Received...broadcasts	Total number of broadcast or multicast packets received by the interface
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.

R3.5.0 Beta Draft—Cisco Confidential Information

Table 115 **show interfaces Field Descriptions**

Field	Description
CRC	Cyclic redundancy checksum generated by the originating station or far-end device does not match the checksum calculated from the data received. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
abort	Illegal sequence of one bits on a serial interface. This usually indicates a clocking problem between the serial interface and the data link equipment.
carrier transitions	Number of times the carrier detect signal of a serial interface has changed state. For example, if data carrier detect (DCD) goes down and comes up, the carrier transition counter will increment two times. Indicates modem or line problems if the carrier detect line is changing state often.

R3.5.0 Beta Draft—Cisco Confidential Information

snmp-server traps frame-relay pvc

To enable Simple Network Management Protocol (SNMP) trap notifications for a Frame Relay permanent virtual circuit (PVC), use the **snmp-server traps frame-relay pvc** command in global configuration mode. To disable SNMP notifications for a FR PVC, use the **no** form of this command.

snmp-server traps frame-relay pvc [*interval seconds*]

no snmp-server traps frame-relay pvc [*interval seconds*]

Syntax Description	interval seconds	(Optional) Minimum period between successive traps. Range is from 0 to 3600.

Defaults	<i>seconds</i> : 30

Command Modes	Global configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Use the snmp-server traps frame-relay pvc command to enable trap requests for a Frame Relay PVC. This command is used with the snmp-server host command. Use the snmp-server host command to specify which host or hosts receive SNMP notifications.
	See <i>Implementing SNMP on Cisco IOS XR Software</i> for detailed information about SNMP configuration tasks and commands.

Task ID	Task ID	Operations
	snmp	read, write

Examples	The following example shows how to configure the router to send SNMP trap notifications for a Frame Relay PVC:

```
RP/0/0/CPU0:router(config)# snmp-server host 12.26.25.61 traps public udp-port 5000
RP/0/0/CPU0:router(config)# snmp-server community public RW
RP/0/0/CPU0:router(config)# snmp-server traps frame-relay pvc interval 50
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	snmp-server host	Specifies the recipient of an SNMP notification operation.
	snmp-server community	Configures the community access string to permit access to the SNMP.

R3.5.0 Beta Draft—Cisco Confidential Information



Bidirectional Forwarding Detection Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

This chapter describes the commands used to configure and monitor Bidirectional Forwarding Detection (BFD).

R3.5.0 Beta Draft—Cisco Confidential Information

address-family ipv4 unicast (BFD)

To enable bidirectional forwarding detection (BFD) fast-detection on a specific IPV4 unicast destination address prefix and on the forwarding next-hop address, use the **address-family ipv4 unicast** command in static route configuration mode. To return the router to the default setting, use the **no** form of this command.

address-family ipv4 unicast *address nexthop* **bfd fast-detect** [**minimum interval** *interval*]
[**multiplier** *multiplier*]

no address-family ipv4 unicast *address nexthop* **bfd fast-detect** [**minimum interval** *interval*]
[**multiplier** *multiplier*]

Syntax Description	<i>address</i>	Specifies the IPv4 unicast destination address and prefix on which to enable BFD fast-detection.
	<i>nexthop</i>	Specifies the next-hop address on which to enable BFD fast-detection.
	bfd fast-detect	Enables BFD fast-detection on the specified IPV4 unicast destination address prefix and on the forwarding next-hop address.
	minimum interval <i>interval</i>	(Optional) Ensures that the next hop is assigned with the same hello interval. Replace <i>interval</i> with a number that specifies the interval in milliseconds. Range is from 15 through 5000.
	multiplier <i>multiplier</i>	(Optional) Ensures that the next hop is assigned with the same detect multiplier. Replace <i>multiplier</i> with a number that specifies the detect multiplier. Range is from 2 through 10.

Defaults	<i>interval</i> =15
	<i>multiplier</i> = 3

Command Modes	Static route configuration mode

Command History.	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	This command was first support the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

If the multiplier is changed using the **bfd multiplier** command, the new parameter is used to update all existing BFD sessions for the protocol (BGP, IS-IS, MPLS-TE, or OSPF).

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	static	read, write

Examples

The following example shows how to enable BFD on a static route. In this example, BFD sessions are established with the next-hop 3.3.3.3 when it becomes reachable.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router static
RP/0/RP0/CPU0:router (config-static)# address-family ipv4 unicast 2.2.2.0/24 3.3.3.3 bfd
fast-detection
```

Related Commands	Command	Description
	bfd fast-detect	Enables BFD for communication failure detection.
	show bfd all	Displays BFD information.

R3.5.0 Beta Draft—Cisco Confidential Information**bfd**

To enter Bidirectional Forwarding Detection (BFD) configuration mode, use the **bfd** command in global configuration mode. To exit BFD configuration mode and return to the global configuration mode, use the **no** form of this command.

bfd

no bfd

Syntax Description This command has no arguments or keywords.

Defaults .No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

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

```
RP/0/RP0/CPU0:router(config-bfd)#?
```

```
commit      Commit the configuration changes to running
describe    Describe a command without taking real actions
do          Run an exec command
echo        Configure BFD echo parameters
exit        Exit from this submode
interface    Configure BFD on an interface
no          Negate a command or set its defaults
root        Exit to the global configuration mode
show        Show contents of configuration
```


R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	bgp	read, write
	ospf	read, write
	isis	read, write
	mpls-te	read, write

Examples

The following example shows how to enter BFD configuration mode:

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

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

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

Related Commands

Command	Description
echo disable	Disables echo mode on an individual interface or on the entire router.
interface (BFD)	Enters BFD interface configuration mode.
show bfd all	Displays BFD information.

R3.5.0 Beta Draft—Cisco Confidential Information

bfd fast-detect

To enable bidirectional forwarding detection (BFD) to detect failures in the path between adjacent forwarding engines, use the **bfd fast-detect** command in the appropriate configuration mode. To return the software to the default state in which BFD is not enabled, use the **no** form of this command.

bfd fast-detect [**disable** | **ipv4**]

no bfd fast-detect

Syntax Description	disable	Prevents BFD settings from being inherited from the parent.
	Note	The disable keyword is available in BGP configuration mode and OSPF router configuration mode only.
	ipv4	Enables Intermediate System-to-Intermediate System (IS-IS) BFD detection of failures in the path between adjacent forwarding engines.
	Note	The ipv4 keyword is available in IS-IS router configuration mode only.

Defaults BFD is not enabled.

Command Modes

- BGP configuration mode**
 - Neighbor configuration
 - Session group configuration
 - Neighbor group configuration
- IS-IS router configuration mode**
 - Interface configuration
- MPLS-TE configuration mode**
 - Interface configuration
- OSPF router configuration mode**
 - Router configuration
 - Area configuration
 - Area Interface configuration
- Router PIM interface configuration mode**

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	This command was first support the Cisco XR 12000 Series Router.
	Release 3.4.0	The bfd fast-detect command was supported in router PIM interface configuration mode.
	Release 3.5.0	modification

R3.5.0 Beta Draft—Cisco Confidential Information**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

**Note**

BFD is supported on IPv4 directly connected external BGP peers.

Use the **bfd fast-detect** command to provide protocol- and media-independent BFD for short duration detection of failures in the path between adjacent forwarding engines, including the interfaces and data links.

BFD must be configured on directly connected neighbors for a BFD session to be established between the neighbors.

When MPLS-TE tunnels are protected by backup tunnels, BFD failure triggers fast reroute on affected tunnels.

The **disable** keyword is available in BGP configuration mode and OSPF router configuration mode only. To disable BFD or return the software to the default state in which BFD is not enabled in IS-IS router configuration mode and MPLS-TE configuration mode, you must enter the **no bfd fast-detect** command.

**Note**

The purpose of the **disable** option is to override inherited configuration. For example, if you enable BFD under an OSPF area, then BFD is enabled for all interfaces in that area. If you do not want BFD running on one of the interfaces in that OSPF area, then you need to configure the **disable** option under that interface only.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to configure BFD on a BGP router:

```
RP/0/RP0/CPU0:router # configure
RP/0/RP0/CPU0:router(config)# router bgp 65000
RP/0/RP0/CPU0:router(config-bgp)# neighbor 192.168.70.24
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 2
RP/0/RP0/CPU0:router(config-bgp-nbr)# bfd fast-detect
```

Related Commands

Command	Description
bfd minimum-interval	Sets the BFD interval.
bfd multiplier	Sets the BFD multiplier.
show bfd all	Displays BFD information.

R3.5.0 Beta Draft—Cisco Confidential Information

bfd minimum-interval

To set the bidirectional forwarding detection (BFD) interval, use the **bfd minimum-interval** command in the appropriate configuration mode. To return the router to the default setting, use the **no** form of this command.

bfd minimum-interval *milliseconds*

no bfd minimum-interval

Syntax Description	<i>milliseconds</i>	Interval between sending BFD packets to the neighbor. The ranges are:
		- On the Cisco CRS-1 - BGP—15 to 30000 milliseconds. - IS-IS—15 to 5000 milliseconds. - MPLS-TE—15 to 200 milliseconds. - OSPF—15 to 30000 milliseconds. - On the Cisco XR 12000 Series Router - BGP—50 to 30000 milliseconds - IS-IS—50 to 5000 milliseconds. - MPLS-TE—50 to 200 milliseconds. - OSPF—50 to 30000 milliseconds.

Defaults	BGP <i>interval</i> = 50 milliseconds IS-IS <i>interval</i> = 150 milliseconds OSPF <i>interval</i> = 150 milliseconds MPLS-TE <i>interval</i> on the Cisco CRS-1=15 milliseconds MPLS-TE <i>interval</i> on the Cisco XR 12000 Series Router=50 milliseconds

Command Modes	BGP configuration mode Router configuration IS-IS configuration mode Interface configuration MPLS-TE configuration mode MPLS-TE configuration OSPF router configuration mode Router configuration Interface configuration Area configuration

R3.5.0 Beta Draft—Cisco Confidential Information**Router PIM interface configuration mode****Command History**

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	This command was first support the Cisco XR 12000 Series Router.
Release 3.4.0	The bfd minimum-interval command was supported in router PIM interface configuration mode.
Release 3.5.0	modification

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If the minimum interval is changed using the **bfd minimum-interval** command, the new parameter updates all affected BFD sessions under the command mode in which the minimum interval was changed. For example, if you change the minimum interval in interface configuration mode for one OSPF interface, only the session for that specific interface is affected. If you change the minimum interval in OSPF area configuration mode, only the sessions under that area will be affection. However, if you change the minimum interval in router configuration mode, then the configuration will take place in all OSPF sessions under the interface configuration mode and the area configuration mode.

**Note**

BFD sessions must be configured with a minimum interval of 50 milliseconds or more when echo-mode is available, and 250 milliseconds or more when only asynchronous mode is available.

Keep the following router-specific rules in mind when configuring the minimum BFD interval:

- When asynchronous mode is available on the Cisco CRS-1, the minimum interval must be less than or equal to 50 milliseconds for up to 100 sessions on the line card. If you are running the maximum of 1024 sessions, the failure detection interval must be less than or equal to 500 milliseconds.
- When asynchronous mode is available on the Cisco XR 12000 Series Router, the minimum interval must be greater than or equal to 50 milliseconds, with a multiplier of 3 for up to 50 sessions per line card.
- When echo mode is available on the Cisco CRS-1, the minimum interval must be less than or equal to 50 milliseconds for up to 100 sessions on the line card. If you are running the maximum of 1024 sessions, the failure detection interval must be less than or equal to 500 milliseconds.
- When echo mode is available on the Cisco XR 12000 Series Router, the minimum interval must be 250 milliseconds with a multiplier of 3.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to set the BFD minimum interval:

```
RP/0/RP0/CPU0:router(config)# router bgp 6500
```

```
RP/0/RP0/CPU0:router(config-bgp)# bfd minimum-interval 275
```

R3.5.0 Beta Draft—Cisco Confidential Information**Related Commands**

Command	Description
bfd fast-detect	Enables BFD for communication failure detection.
bfd multiplier	Sets the BFD multiplier.
show bfd all	Displays BFD information.

R3.5.0 Beta Draft—Cisco Confidential Information

bfd multiplier

To set the bidirectional forwarding detection (BFD) multiplier, use the **bfd multiplier** command in the appropriate configuration mode. To return the router to the default setting, use the **no** form of this command.

bfd multiplier *multiplier*

no bfd multiplier

Syntax Description	<i>multiplier</i>	Number of times a packets is missed before BFD declares the neighbor down. On the Cisco CRS-1, the ranges are: - BGP—2 to 16 - IS-IS—2 to 50 - MPLS-TE—2 to 10 - OSPF—2 to 50 One the Cisco XR 12000 Series Router, the ranges are - BGP—3 to 16 - IS-IS—3 to 50 - MPLS-TE—3 to 10 - OSPF—3 to 50

Defaults	<i>multiplier</i> = 3

Command Modes	BGP configuration mode Router configuration IS-IS configuration mode Interface configuration MPLS-TE configuration mode MPLS-TE configuration OSPF router configuration mode Router configuration Interface configuration Area configuration

R3.5.0 Beta Draft—Cisco Confidential Information**Router PIM interface configuration mode**

Command History.	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	This command was first support the Cisco XR 12000 Series Router.
	Release 3.4.0	The bfd multiplier command was supported in router PIM interface configuration mode.
	Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If the multiplier is changed using the **bfd multiplier** command, the new parameter is used to update all existing BFD sessions for the protocol (BGP, IS-IS, MPLS-TE, or OSPF).

Task ID	Task ID	Operations
	bgp	read, write

Examples

The following example shows how to set the BFD multiplier:

```
RP/0/RP0/CPU0:router(config)# router bgp 65000
```

```
RP/0/RP0/CPU0:router(config-bgp)# bfd multiplier 2
```

Related Commands	Command	Description
	bfd fast-detect	Enables BFD for communication failure detection.
	bfd minimum-interval	Sets the BFD interval.
	show bfd all	Displays BFD information.

R3.5.0 Beta Draft—Cisco Confidential Information

clear bfd counters

To clear Bidirectional Forwarding Detection (BFD) counters, use the **clear bfd counters** command in EXEC mode.

clear bfd counters packet [*interface type instance*] **location** *node-id*

Syntax Description	
packet	Clears BFD packets counters.
interface	(Optional) Clears BFD counters from the specified interface.
<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>instance</i>	Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>—Chassis number of the rack. <i>slot</i>—Physical slot number of the card. <i>module</i>—Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>—Physical port number of the interface. Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
location <i>node-id</i>	Clears BFD counters from the specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	This command was first support the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	bgp	read, write
	ospf	read, write
	isis	read, write
	mpls-te	read, write

Examples

The following is sample output from the **clear bfd counters** command.

```
RP/0/RP0/CPU0:router# clear bfd counters packet interface POS 0/5/0/1 location 0/5/cpu0
```

Related Commands

Command	Description
bfd fast-detect	Enables BFD for communication failure detection.
bfd minimum-interval	Sets the BFD interval.
bfd multiplier	Sets the BFD multiplier.
show bfd all	Displays BFD information.

R3.5.0 Beta Draft—Cisco Confidential Information

echo disable

To disable echo mode on a router or on an individual interface or bundle, use the **echo disable** command in Bidirectional Forwarding Detection (BFD) configuration mode. To return the router to the default configuration where echo mode is enabled, use the **no** form of this command.

echo disable

no echo disable

Syntax Description This command has no arguments or keywords.

Defaults .No default behavior or values

Command Modes BFD configuration
BFD interface configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If you are using BFD with Unicast Reverse Path Forwarding (uRPF), you need to use the **echo disable** command to disable echo mode; otherwise, echo packets will be rejected.

**Note**

To enable or disable IPv4 uRPF checking on an IPv4 interface, use the **[no] ipv4 verify unicast source reachable-via** command in interface configuration mode. To enable or disable loose IPv6 uRPF checking on an IPv6 interface, use the **[no] ipv6 verify unicast source reachable-via any** command in interface configuration mode.

Task ID	Task ID	Operations
	bgp	read, write
	ospf	read, write
	isis	read, write
	mpls-te	read, write

R3.5.0 Beta Draft—Cisco Confidential Information**Examples**

The following example shows how to disable echo mode on a router:

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

RP/0/RP0/CPU0:router(config) # bfd

RP/0/RP0/CPU0:router(config-bfd) # echo disable
```

The following example shows how to disable echo mode on an individual interface:

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

RP/0/RP0/CPU0:router(config) # bfd

RP/0/RP0/CPU0:router(config-bfd) # interface pos 0/1/0/0

RP/0/RP0/CPU0:router(config-bfd-if) # echo disable
```

Related Commands

Command	Description
bfd	Enters BFD configuration mode.
interface (BFD)	Enters BFD interface configuration mode.
ipv4 verify unicast source reachable-via	Enables and disables IPv4 uRPF checking on an IPv4 interface.
ipv6 verify unicast source reachable-via any	Enables and disables loose IPv6 uRPF checking on an IPv6 interface.
show bfd all	Displays BFD information.

R3.5.0 Beta Draft—Cisco Confidential Information

interface (BFD)

To enter Bidirectional Forwarding Detection (BFD) interface configuration mode, where you can disable echo mode on an interface, use the **interface** command in BFD configuration mode. To return to BFD configuration mode, use the **no** form of this command.

interface *type instance*

no interface *type instance*

Syntax Description	<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
	<i>instance</i>	Either a physical interface instance, virtual interface instance, or bundle: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i>, and a slash between values is required as part of the notation. <i>rack</i>—Chassis number of the rack. <i>slot</i>—Physical slot number of the card. <i>module</i>—Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>—Physical port number of the interface. - Virtual interface instance. Range of numbers varies depending on interface type. - Bundle ID for a POS or Ethernet bundle. Range is from 1 through 65535. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults	.No default behavior or values

Command Modes	BFD configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

R3.5.0 Beta Draft—Cisco Confidential Information

If you are using BFD with Unicast Reverse Path Forwarding (uRPF) on a particular interface, then you need to use the **echo disable** command in BFD interface configuration mode to disable echo mode on that interface; otherwise, echo packets will be rejected by the interface.

**Note**

To enable or disable IPv4 uRPF checking on an IPv4 interface, use the **[no] ipv4 verify unicast source reachable-via** command in interface configuration mode. To enable or disable loose IPv6 uRPF checking on an IPv6 interface, use the **[no] ipv6 verify unicast source reachable-via any** command in interface configuration mode.

Task ID

Task ID	Operations
bgp	read, write
ospf	read, write
isis	read, write
mpls-te	read, write

Examples

The following example shows how to enter BFD interface configuration mode for a Packet-over-SONET/SDH (POS) interface:

```
RP/0/RP0/CPU0:router # configure
RP/0/RP0/CPU0:router(config)# bfd
RP/0/RP0/CPU0:router(config-bfd)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-bfd-if)#
```

Related Commands

Command	Description
bfd	Enters BFD configuration mode.
echo disable	Disables echo mode on an individual interface or on the entire router.
ipv4 verify unicast source reachable-via	Enables and disables IPv4 uRPF checking on an IPv4 interface.
ipv6 verify unicast source reachable-via any	Enables and disables loose IPv6 uRPF checking on an IPv6 interface.
show bfd all	Displays BFD information.

R3.5.0 Beta Draft—Cisco Confidential Information

show bfd

To display summarized information about all Bidirectional Forwarding Detection (BFD) sessions on the current router, use the **show bfd** command in EXEC mode.

show bfd

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	This command was first support the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	bgp	read
	ospf	read
	isis	read
	mpls-te	read

Examples	The following is sample output from the show bfd command:

```
RP/0/RP0/CPU0:router# show bfd
```

```
IPv4 Sessions Up: 0, Down: 0, Total: 0
```

R3.5.0 Beta Draft—Cisco Confidential Information

Table 116 describes the significant fields shown in the display.

Table 116 **show bfd Field Descriptions**

Field	Description
IPv4 Sessions Up	Number of active BFD sessions.
Down	Number of down BFD sessions.
Total	Total number of BFD sessions.

Related Commands

Command	Description
bfd fast-detect	Enables BFD for communication failure detection.
bfd minimum-interval	Sets the BFD interval.
bfd multiplier	Sets the BFD multiplier.

R3.5.0 Beta Draft—Cisco Confidential Information

show bfd all

To display Bidirectional Forwarding Detection (BFD) information, use the **show bfd** command in EXEC mode.

```
show bfd all [session [interface type instance [destination ip-address]] [detail]] [location
node-id]
```

Syntax Description	
session	(Optional) Specifies BFD sessions.
interface <i>type instance</i>	(Optional) Specifies an interface. Replace the <i>type</i> argument with the Interface type.
Note	For more information, use the question mark (?) online help function.
	Replace the <i>instance</i> argument with a physical interface instance or a virtual interface instance.
	- Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>—Chassis number of the rack. <i>slot</i>—Physical slot number of the card. <i>module</i>—Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>—Physical port number of the interface.
Note	In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0.
	Virtual interface instance. Number range varies depending on interface type.
	For more information about the syntax for the router, use the question mark (?) online help function.
destination <i>ip-address</i>	(Optional) Displays the BFD session destined for the specified IP address.
detail	(Optional) Specifies detailed session information, including statistics and number of state transitions.
location <i>node-id</i>	(Optional) Displays BFD sessions hosted from the specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults

Enter the **show bfd all** command without specifying any of the optional keywords or arguments to display summarized information about all BFD sessions on the router.

Command Modes

EXEC

R3.5.0 Beta Draft—Cisco Confidential Information**Command History**

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	This command was first support the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
bgp	read
ospf	read
isis	read
mpls-te	read

Examples

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

```
RP/0/RP0/CPU0:router# show bfd all
```

```
IIPV4 Sessions Up: 0, Down: 1, Standby: 0, Total: 1
```

[Table 117](#) describes the significant fields shown in the display.

Table 117 *show bfd all Field Descriptions*

Field	Description
IPV4 Sessions Up	Number of active BFD sessions.
Down	Number of down BFD sessions.
Total	Total number of BFD sessions.

R3.5.0 Beta Draft—Cisco Confidential Information

show bfd client

To display Bidirectional Forwarding Detection (BFD) client information, use the **show bfd client** command in EXEC mode.

show bfd client [detail]

Syntax Description

detail	(Optional) Specifies detailed client information including number of sessions and client reconnects.

Defaults

Enter the **show bfd client** command without specifying the **detail** keyword to display summarized BFD client information.

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	This command was first support the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
bgp	read
ospf	read
isis	read
mpls-te	read

Examples

The following is sample output from the **show bfd client** command:

```
RP/0/RP0/CPU0:router# show bfd client
```

Name	Node	Num sessions
-----	-----	-----
bgp	0/RP1/CPU0	0
isis	0/RP1/CPU0	0
isis	0/RP1/CPU0	0

R3.5.0 Beta Draft—Cisco Confidential Information

Table 118 describes the significant fields shown in the display.

Table 118 **show bfd client Field Descriptions**

Field	Description
Name	Name of the BFD client.
Node	Location of the BFD client.
Num sessions	Number of active sessions for the BFD client.

Related Commands

Command	Description
bfd fast-detect	Enables BFD for communication failure detection.
bfd minimum-interval	Sets the BFD interval.
bfd multiplier	Sets the BFD multiplier.
show bfd all	Displays BFD information.

R3.5.0 Beta Draft—Cisco Confidential Information

show bfd counters packet

To display Bidirectional Forwarding Detection (BFD) counter information, use the **show bfd counters packet** command in EXEC mode.

show bfd counters packet [*interface type instance*] **location** *node-id*

Syntax Description	
packet	Displays BFD packets counters.
interface	(Optional) Specifies BFD counters from the specified interface.
<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>instance</i>	Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>—Chassis number of the rack. <i>slot</i>—Physical slot number of the card. <i>module</i>—Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>—Physical port number of the interface. Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
location <i>node-id</i>	Displays BFD counters from the specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	This command was first support the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

R3.5.0 Beta Draft—Cisco Confidential Information**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
bgp	read
ospf	read
isis	read
mpls-te	read

Examples

The following is sample output from the **show bfd counters packet** command:

```
RP/0/RP0/CPU0:router# show bfd counters packet location 0/3/cpu0
```

```

POS 0/3/0/0      Recv  Xmit      Recv  Xmit
  Async:      2341  2311  Echo:    0    0
POS 0/3/0/1      Recv  Xmit      Recv  Xmit
  Async:         0   451  Echo:    0    0

```

[Table 119](#) describes the significant fields shown in the display.

Table 119 **show bfd counters packet Field Descriptions**

Field	Description
Async	Number of asynchronous mode (control) packets that were received or transmitted on the specified interface.
Echo	Number of echo packets that were received or transmitted on the specified interface.

Related Commands

Command	Description
bfd fast-detect	Enables BFD for communication failure detection.
bfd minimum-interval	Sets the BFD interval.
bfd multiplier	Sets the BFD multiplier.
show bfd all	Displays BFD information.

R3.5.0 Beta Draft—Cisco Confidential Information

show bfd ipv4

To display Bidirectional Forwarding Detection (BFD) information related to IPv4 address families, use the **show bfd ipv4** command in EXEC mode.

```
show bfd ipv4 [session [interface type instance [destination ip-address]] [detail]] [location
node-id]
```

Syntax Description	
session	(Optional) Specifies BFD sessions.
interface <i>type instance</i>	(Optional) Specifies an interface. Replace the <i>type</i> argument with the Interface type. Replace the <i>instance</i> argument with a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>—Chassis number of the rack. <i>slot</i>—Physical slot number of the card. <i>module</i>—Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>—Physical port number of the interface. Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
destination <i>ip-address</i>	(Optional) Displays the BFD session destined for the specified IP address.
detail	(Optional) Specifies detailed session information, including statistics and number of state transitions.
location <i>node-id</i>	(Optional) Displays BFD sessions hosted from the specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults

Enter the **show bfd ipv4** command without any of the optional parameters to display information about all BFD IPv4 sessions on the router.

Command Modes

EXEC

R3.5.0 Beta Draft—Cisco Confidential Information**Command History**

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	This command was first support the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
bgp	read
ospf	read
isis	read
mpls-te	read

Examples

The following is sample output from the **show bfd ipv4** command:

```
RP/0/RP0/CPU0:router# show bfd ipv4
```

```
IPV4 Sessions Up: 0, Down: 0, Total: 0
```

[Table 120](#) describes the significant fields shown in the display.

Table 120 *show bfd ipv4 Field Descriptions*

Field	Description
IPV4 Sessions Up	Number of active BFD sessions.
Down	Number of down BFD sessions.
Total	Total number of BFD sessions.

Related Commands

Command	Description
bfd fast-detect	Enables BFD for communication failure detection.
bfd minimum-interval	Sets the BFD interval.
bfd multiplier	Sets the BFD multiplier.

R3.5.0 Beta Draft—Cisco Confidential Information

show bfd location

To display Bidirectional Forwarding Detection (BFD) IPv4 session information for a specific location, use the **show bfd location** command in EXEC mode.

show bfd location *node-id*

Syntax Description	location <i>node-id</i>	Displays BFD information for the specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults	No default behavior or values.

Command Modes	EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	This command was first support the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	bgp	read
	ospf	read
	isis	read
	mpls-te	read

Examples	The following is sample output from the show bfd counters packet command:

```
RP/0/RP0/CPU0:router# show bfd location 0/3/cpu0
```

```
IPv4 Sessions Up: 0, Down: 1, Standby: 0, Total: 1
```

R3.5.0 Beta Draft—Cisco Confidential Information

show bfd session

To display Bidirectional Forwarding Detection (BFD) session information, use the **show bfd session** command in EXEC mode.

show bfd session [**interface** *type instance* [**destination** *ip-address*] [**detail**]] [**location** *node-id*]

Syntax Description

interface <i>type instance</i>	(Optional) Specifies an interface. Replace the <i>type</i> argument with the Interface type. Note For more information, use the question mark (?) online help function. Replace the <i>instance</i> argument with a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>—Chassis number of the rack. <i>slot</i>—Physical slot number of the card. <i>module</i>—Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>—Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
destination <i>ip-address</i>	(Optional) Displays the BFD session destined for the specified IP address.
detail	(Optional) Specifies detailed session information, including statistics and number of state transitions.
location <i>node-id</i>	(Optional) Displays BFD sessions hosted from the specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults

Enter the **show bfd session** command without any of the optional parameters to display information about all BFD sessions on the router.

Command Modes

EXEC

R3.5.0 Beta Draft—Cisco Confidential Information**Command History**

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	This command was first support the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
bgp	read
ospf	read
isis	read
mpls-te	read

Examples

The following is sample output from the **show bfd session** command with the **detail** keyword:

```
RP/0/RP0/CPU0:router# show bfd session detail

I/F:TenGigE0/2/0/0.6, Location:0/2/CPU0, dest:10.0.6.2, src:10.0.6.1
State:UP for 0d:0h:3m:4s, number of times UP:1
Received parameters:
  Version:1, desired tx interval:2 s, required rx interval:2 s
  Required echo rx interval:1 ms, multiplier:3, diag:None
  My discr:589830, your discr:590028, state UP, D/F/P/C/A:0/0/0/1/0
Transmitted parameters:
  Version:1, desired tx interval:2 s, required rx interval:2 s
  Required echo rx interval:1 ms, multiplier:3, diag:None
  My discr:590028, your discr:589830, state UP, D/F/P/C/A:0/0/0/1/0
Timer Values:
  Local negotiated async tx interval:2 s
  Remote negotiated async tx interval:2 s
  Desired echo tx interval:250 ms, local negotiated echo tx interval:250 ms
  Echo detection time:750 ms(250 ms*3), async detection time:6 s(2 s*3)
Local Stats:
  Intervals between async packets:
    Tx:Number of intervals=100, min=952 ms, max=2001 ms, avg=1835 ms
      Last packet transmitted 606 ms ago
    Rx:Number of intervals=100, min=1665 ms, max=2001 ms, avg=1828 ms
      Last packet received 1302 ms ago
  Intervals between echo packets:
    Tx:Number of intervals=100, min=250 ms, max=252 ms, avg=250 ms
      Last packet transmitted 188 ms ago
    Rx:Number of intervals=100, min=250 ms, max=252 ms, avg=250 ms
      Last packet received 187 ms ago
  Latency of echo packets (time between tx and rx):
    Number of packets:100, min=1 ms, max=2 ms, avg=1 ms
Session owner information:
  Client          Desired interval      Multiplier
  -----
  bgp-            250 ms                3
```

R3.5.0 Beta Draft—Cisco Confidential Information

R3.5.0 Beta Draft—Cisco Confidential Information

Table 121 describes the significant fields shown in the display.

Table 121 *show bfd session detail command Field Descriptions*

Field	Description
I/f	Interface type.
Location	Location of the node that hosts the local endpoint of the connection, in the <i>rack/slot/module</i> notation
dest	IP address of the destination endpoint.
src	IP address of the source endpoint.
State	Current state of the connection, and the number of days, hours, minutes, and seconds that this connection has been active.
number of times UP	Number of times this connection has been brought up.
Received parameters	Provides information on the last transmitted control packet for the session: • Version—Version number of the BFD protocol. • desired tx interval—Desired transmit interval. • required rx interval—Required receive interval. • Required echo rx interval—Required echo receive interval. • multiplier— Number of times a packets is missed before BFD declares the neighbor down. • diag—diagnostic code specifying the peer system's reason for the last transition of the session from Up to some other state. • My discr —unique, nonzero discriminator value generated by the transmitting system, used to demultiplex multiple BFD sessions between the same pair of systems. • your discr— discriminator received from the corresponding remote system. This field reflects back the received value of My discr, or is zero if that value is unknown.
Transmitted parameters	Provides information on the last transmitted control packet for the session: • Version—Version number of the BFD protocol. • desired tx interval—Desired transmit interval. • required rx interval—Required receive interval • Required echo rx interval—Required echo receive interval • multiplier— Number of times a packets is missed before BFD declares the neighbor down. • diag—diagnostic code specifying the local system's reason for the last transition of the session from Up to some other state. • My discr —unique, nonzero discriminator value generated by the transmitting system, used to demultiplex multiple BFD sessions between the same pair of systems. • your discr— discriminator received from the corresponding remote system. This field reflects back the received value of My discr, or is zero if that value is unknown.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 121** *show bfd session detail command Field Descriptions (continued)*

Field	Description
Timer Values	Provides information on the timer values used by the local and remote ends, as follows: - Local negotiated async tx interval—interval at which control packets are being transmitted by the local end. - Remote negotiated async tx interval—interval at which control packets should be transmitted by the remote end. - Desired echo tx interval—interval at which the local end would like to transmit echo packets. - local negotiated echo tx interval—interval at which echo packets are being transmitted by the local end. - Echo detection time—local failure detection time of echo packets. It is the product of the local negotiated echo tx interval and the local multiplier. - async detection time—local failure detection time of the asynchronous mode (control packets). It is the product of the remote negotiated async tx interval and the remote multiplier.
Local Stats	Displays the local transmit and receive statistics, - Intervals between async packets—provides measurements on intervals between control packets (tx and rx): - Number of intervals—number of sampled intervals between control packets - min—minimum measured interval between 2 consecutive control packets - max—maximum measured interval between 2 consecutive control packets - avg—average measured interval between 2 consecutive control packets - Last packet received/transmitted—indicates how long ago the last control packet was received/transmitted. - Intervals between echo packets—provides measurements on intervals between echo packets (tx and rx). The measurements have the same meaning as for async packets. - Latency of echo packets (time between tx and rx)—provides measurements on latency of echo packets, i.e. the time between tx and rx of echo packets: - Number of packets—number of sampled echo packets. - min—minimum measured latency for echo packets. - max—maximum measured latency of echo packets. - avg—average measured latency of echo packets.
Session owner information	Provides the following information about the session owner. - Client—name of the client application process. - Desired interval—desired interval provided by the client, in milliseconds. - Multiplier—multiplier value provided by the client.

Related Commands	Command	Description
	bfd fast-detect	Enables BFD for communication failure detection.
	bfd minimum-interval	Sets the BFD interval.
	bfd multiplier	Sets the BFD multiplier.



NetFlow Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

This module describes the NetFlow commands on Cisco IOS XR software.

R3.5.0 Beta Draft—Cisco Confidential Information

cache entries

To configure the number of entries in the monitor map flow cache, enter the **cache entries** command in flow monitor map configuration mode. To remove a configured number of entries and return the cache to the default configuration, use the **no** form of this command.

cache entries *number*

no command *number*

Syntax Description	<i>number</i>	Number of entries in the flow cache. Replace the <i>number</i> argument with the number of flow entries allowed in the flow cache. Range is from 4096 through 1000000.

Defaults	<i>number</i> = 65535

Command Modes	Flow monitor map configuration

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	netflow	read, write

Examples	The following example shows how to configure the number of entries in the monitor map flow cache to be 10000:

```
RP/0/RP0/CPU0:router # configure
RP/0/RP0/CPU0:router(config)# flow monitor-map map1
RP/0/RP0/CPU0:router(config-fmm)# cache entries 10000
```


R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	clear flow monitor	Clears the flow monitor data.
	flow monitor-map	Creates and configures a flow monitor map and enters flow monitor map configuration submode.
	show flow monitor	Displays flow monitor cache information.
	show flow monitor-map	Displays flow monitor map information.

R3.5.0 Beta Draft—Cisco Confidential Information

cache permanent

To disable the removal of entries from the monitor map flow cache, enter the **cache permanent** command in flow monitor map configuration mode. To re-enable the removal of entries from the flow cache, use the **no** form of this command.

cache permanent

no cache permanent

Syntax Description This command has no arguments or keywords.

Defaults The removal of entries from the monitor map flow cache is enabled.

Command Modes Flow monitor map configuration

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	netflow	read, write

Examples The following example shows how to disable the removal of entries from the monitor map flow cache:

```
RP/0/RP0/CPU0:router # configure
RP/0/RP0/CPU0:router(config)# flow monitor-map map1
RP/0/RP0/CPU0:router(config-fmm)# cache permanent
```

The following example shows how to re-enable the removal of entries from the monitor map flow cache:

```
RP/0/RP0/CPU0:router # configure
RP/0/RP0/CPU0:router(config)# flow monitor-map map1
RP/0/RP0/CPU0:router(config-fmm)# no cache permanent
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	clear flow monitor	Clears the flow monitor data.
	flow monitor-map	Creates and configures a flow monitor map and enters flow monitor map configuration submode.
	show flow monitor	Displays flow monitor cache information.
	show flow monitor-map	Displays flow monitor map information.

R3.5.0 Beta Draft—Cisco Confidential Information

cache timeout

To configure the active, inactive, and update flow cache timeout, enter the **cache timeout** command in flow monitor map configuration mode. To remove the configured timeout value and return the cache to its default timeout value, use the **no** form of this command.

cache timeout {**active** | **inactive** | **update**} *timeout_value*

no cache timeout {**active** | **inactive** | **update**} *timeout_value*

Syntax Description

active	Specifies the active flow timeout.
inactive	Specifies the inactive flow timeout.
update	Specifies the update timeout.
<i>timeout_value</i>	Timeout value for the specified keyword (active , inactive , or update), in seconds. Range is from 1 through 604800.

Defaults

For active timeout, the default value is 1800 seconds.

For inactive timeout, the default value is 15 seconds.

For update timeout, the default value is 1800 seconds.

Command Modes

Flow monitor map configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

**Note**

The **inactive** timeout value should be smaller than the **active** timeout value.

**Note**

The **update** keyword is used for permanent caches only. It specifies the timeout value that is used to export entries from permanent caches. In this case, the entries are exported but remain the cache.

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	netflow	read, write

Examples

The following example shows how to set the active timeout for the monitor map cache to 200,000 seconds:

```
RP/0/RP0/CPU0:router # configure
RP/0/RP0/CPU0:router(config)# flow monitor-map map1
RP/0/RP0/CPU0:router(config-fmm)# cache timeout active 200000
```

Related Commands

Command	Description
clear flow monitor	Clears the flow monitor data.
flow monitor-map	Creates and configures a flow monitor map and enters flow monitor map configuration submode.
show flow monitor	Displays flow monitor cache information.
show flow monitor-map	Displays flow monitor map information.

R3.5.0 Beta Draft—Cisco Confidential Information

clear flow exporter

To export flow exporter templates to the collector or restart the flow exporter statistics collector, enter the **clear flow exporter** command in EXEC mode.

clear flow exporter [*fem-name*] {**restart** | **statistics**} **location** *node-id*

Syntax Description

<i>fem-name</i>	(Optional) Flow exporter name.
restart	Exports all of the current templates to the collector.
statistics	Clears the exporter statistics.
location <i>node-id</i>	Identifies the node whose flow exporter statistics you want to clear, or whose flow exporter statistics collector you want to restart. The <i>node-id</i> argument is expressed in the <i>rack/slot/module</i> notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

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

Examples

The following example exports all templates to the collector:

```
RP/0/RP0/CPU0:router# clear flow exporter restart location 0/0/SP
```

```
Restart exporter all locations. Continue? [confirm]
```

The following example shows how to clear flow exporter statistics on a specific node.

```
RP/0/RP0/CPU0:router# clear flow exporter statistics location 0/0/CPU0
```

R3.5.0 Beta Draft—Cisco Confidential Information

Clear statistics for all exporters on the location. Continue? [confirm]

Related Commands	Command	Description
	flow exporter-map	Configures a flow exporter map.
	show flow exporter	Displays flow exporter data.
	show flow exporter-map	Displays flow exporter map information for a specific node.

R3.5.0 Beta Draft—Cisco Confidential Information

clear flow monitor

To clear the flow monitor data, enter the **clear flow monitor** command in EXEC mode.

clear flow monitor [*name*] **cache** [**force-export** | **statistics**] **location** *node-id*

Syntax Description	<i>name</i>	(Optional) Identifies a specific cache you want to clear.
	cache	Clears all cache related information.
	force-export	(Optional) Forces the export of flow records on flushing the cache on the specified node.
	statistics	(Optional) Clears cache statistics on a specific node.
	location <i>node-id</i>	Node whose flow monitor you want to clear. The <i>node-id</i> argument is expressed in the <i>rack/slot/module</i> notation.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	netflow	read, write

Examples The following example shows how to clear the cache-related flow records on a specific node:

```
RP/0/RP0/CPU0:router# clear flow monitor cache force-export location 0/0/CPU0
```

```
Clear cache entries for this monitor on this location. Continue? [confirm]
```


R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	flow monitor-map	Configures a flow monitor map.
	show flow monitor-map	Displays flow monitor map information for a specific node that is installed in the router.

R3.5.0 Beta Draft—Cisco Confidential Information

clear flow platform producer statistics location

To clear statistics collected by the NetFlow producer, use the **clear flow platform producer statistics location** command in EXEC mode.

clear flow platform producer statistics location *node-id*

Syntax Description	<i>node-id</i>	Node on which to clear statistics collected by the NetFlow producer. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.
	Note	Enter the show platform command to see the location of all nodes installed in the router.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	netflow	read, write

Examples	The following example shows how to clear statistics collected by the NetFlow producer: <pre>RP/0/RP0/CPU0:router # clear flow platform producer statistics location 0/0/CPU0</pre>

R3.5.0 Beta Draft—Cisco Confidential Information

destination

To configure the collector export destination, enter the **destination** command in flow exporter map configuration mode. To remove a configured export destination, use the **no** form of this command.

destination *hostname_or_IP_address*

no destination *hostname_or_IP_address*

Syntax Description

hostname_or_IP_address Export destination for the current flow exporter map. Enter the hostname or destination IP address in the A.B.C.D format.

Note We recommend that you do not use the management interface to export NetFlow packets.

Defaults

No default behavior or values

Command Modes

Flow exporter map configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.4.0	This command was moved to the flow exporter map configuration mode.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
netflow	read, write

Examples

The following example shows how to configure the flow exporter map export destination to be a specific IP address:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# flow exporter-map map1
RP/0/RP0/CPU0:router(config-fem)# destination 172.18.189.38
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	flow exporter-map	Creates and configures a flow exporter map.
	flow monitor-map	Configures a flow monitor map and associates an exporter map with a monitor map.
	show flow exporter	Displays flow exporter data.
	show flow exporter-map	Displays flow exporter map information for a specific node installed in the router.

R3.5.0 Beta Draft—Cisco Confidential Information

dscp

To configure the differentiated services codepoint (DSCP) value for export packets, enter the **dscp** command in flow exporter map configuration mode. To remove a configured DSCP value, use the **no** form of this command.

dscp *dscp_value*

no dscp *dscp_value*

Syntax Description

<i>dscp_value</i>	Specifies the DSCP value for export packets. Replace <i>dscp_value</i> with a number. Range is from 0 through 63.

Defaults

No default behavior or values

Command Modes

Flow exporter map configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
Release 3.4.0	This command was moved to the flow exporter map configuration mode.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
netflow	read, write

Examples

The following example shows how to configure the DSCP value for export packets to be 30:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# flow exporter-map map1
RP/0/RP0/CPU0:router(config-fem)# dscp 30
```

R3.5.0 Beta Draft—Cisco Confidential Information**Related Commands**

Command	Description
flow exporter-map	Creates and configures a flow exporter map.
flow monitor-map	Configures a flow monitor map and associates an exporter map with a monitor map.
show flow exporter	Displays flow exporter data.
show flow exporter-map	Displays flow exporter map information for a specific node installed in the router.

R3.5.0 Beta Draft—Cisco Confidential Information

exporter

To associate a flow exporter map with the current flow monitor map, enter the **exporter** command in flow monitor map configuration mode. To remove an associated flow exporter map from a flow monitor map, use the **no** form of this command.

exporter *map_name*

no exporter *map_name*

Syntax Description

<i>map_name</i>	Name of the flow exporter map you want to associate with the current flow monitor map. The exporter map name can be a maximum of 32 characters.

Defaults

No default behavior or values

Command Modes

Flow monitor map configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
Release 3.4.0	NetFlow was updated so that a single flow monitor map supports up to 8 exporters.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

**Note**

A single flow monitor map can support up to eight flow exporter maps.

Task ID

Task ID	Operations
netflow	read, write

Examples

The following example shows how to associate a flow exporter map called “fem_1” with the current flow monitor map:

```
RP/0/RP0/CPU0:router # configure
RP/0/RP0/CPU0:router(config)# flow monitor-map map1
RP/0/RP0/CPU0:router(config-fmm)# exporter fem_1
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	clear flow monitor	Clears the flow monitor data.
	flow monitor-map	Creates and configures a flow monitor map and enters flow monitor map configuration submode.
	show flow monitor	Displays flow monitor cache information.
	show flow monitor-map	Displays flow monitor map information.

R3.5.0 Beta Draft—Cisco Confidential Information

flow

To specify a flow monitor map and a sampler map for the packets on an interface, enter the **flow** command in interface configuration mode.

flow [ipv4 | ipv6 | mpls] **monitor** *name* **sampler** *name* {egress | ingress}

Syntax Description

ipv4	Enables IPV4 NetFlow on the specified interface.
ipv6	Enables IPV6 NetFlow on the specified interface.
mpls	Enables Multiprotocol Label Switching (MPLS) aware NetFlow on the specified interface.
monitor <i>name</i>	Specifies the name of the flow monitor map you want to specify for IPv4, IPv6, or MPLS packets.
sampler <i>name</i>	Name of the sampler map you want to apply to the flow monitor map.
egress	Applies the flow monitor map on outgoing packets.
ingress	Applies the flow monitor map on incoming packets.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
Release 3.3.1	On the Cisco CRS-1, the mpls keyword was added to the flow command to support MPLS aware NetFlow.
Release 3.4.0	No modification.
Release 3.5.0	On the Cisco CRS-1, the ipv6 keyword was added to the flow command to support IPv6 NetFlow.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
netflow	read, write

R3.5.0 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to enable IPV4 NetFlow on a Packet-over-SONET/SDH (POS) interface, and then apply the flow monitor map, named “map1,” on outgoing IPv4 packets:

```
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)# flow ipv4 monitor map1 sampler map1 egress
```

The following example shows how to enable MPLS NetFlow on a Packet-over-SONET/SDH (POS) interface, and apply the flow monitor map, named “map_mpls1,” on outgoing MPLS packets:

```
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)# flow mpls monitor map_mpls1 sampler map1 egress
```

Related Commands

Command	Description
flow monitor-map	Creates and configures a flow monitor map, and enters flow monitor map configuration submenu.
show flow monitor-map	Displays flow monitor map information.

R3.5.0 Beta Draft—Cisco Confidential Information

flow exporter-map

To create a flow exporter map and enter flow exporter map configuration mode, enter the **flow exporter-map** command in global configuration mode. To remove a configured flow exporter map, use the **no** form of this command.

flow exporter-map *fem-name*

no flow exporter-map *fem-name*

Syntax Description	<i>fem-name</i>	Creates a new exporter map name, or specifies the name of an existing exporter map.

Defaults	No default behavior or values

Command Modes	Global configuration

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

When you issue the **flow exporter-map** *fem-name* command in global configuration mode, the CLI prompt changes to “config-fem,” indicating that you have entered the flow exporter map configuration submode. In the following sample output, the question mark (?) online help function displays all the commands available under flow exporter map configuration submode:

```
RP/0/RP0/CPU0:router(config)# flow exporter-map map1
```

```
RP/0/RP0/CPU0:router(config-fem)# ?
```

```

commit      Commit the configuration changes to running
describe    Describe a command without taking real actions
destination Export destination configuration
do          Run an exec command
dscp        Specify DSCP value for export packets
exit        Exit from this submode
no          Negate a command or set its defaults
root        Exit to the global configuration mode
show        Show contents of configuration
source      Source interface
transport    Specify the transport protocol for export packets
version     Specify export version parameters
```

R3.5.0 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	netflow	read, write

Examples

The following example shows how to create a flow exporter map called “map1,” and then enter the flow exporter map configuration submode for that map:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# flow exporter-map map1
RP/0/RP0/CPU0:router(config-fem)#
```

Related Commands	Command	Description
	flow monitor-map	Configures a flow monitor map and associates an exporter map with a monitor map.
	show flow exporter	Displays flow exporter data.
	show flow exporter-map	Displays flow exporter map information for a specific node installed in the router.

R3.5.0 Beta Draft—Cisco Confidential Information

flow monitor-map

To create and configure a flow monitor map and enter flow monitor map configuration submode, enter the **flow monitor-map** command in global configuration mode. To remove a configured flow monitor map, use the **no** form of this command:

flow monitor-map *map_name*

no flow monitor-map *map_name*

Syntax Description

<i>map_name</i>	New monitor map name, or specifies the name of an existing monitor map. The monitor map name can be a maximum 32 characters.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
Release 3.4.0	NetFlow was updated so that a single flow monitor map supports up to 8 exporters.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When you issue the **flow monitor-map** *map_name* command in global configuration mode, the CLI prompt changes to “config-fmm,” indicating that you have entered the flow monitor map configuration submode. In the following sample output, the question mark (?) online help function displays all the commands available under flow monitor map configuration submode:

```
RP/0/RP0/CPU0:router(config)# flow monitor-map map1
RP/0/RP0/CPU0:router(config-fmm)# ?

cache      Specify flow cache attributes
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
exporter   Specify flow exporter map name
no         Negate a command or set its defaults
record     Specify a flow record map name
show       Show contents of configuration
```

R3.5.0 Beta Draft—Cisco Confidential Information**Task ID**

Task ID	Operations
netflow	read, write

Examples

The following example shows how to enter flow monitor map configuration mode for a monitor map called “map1:”

```
RP/0/RP0/CPU0:router # configure
RP/0/RP0/CPU0router(config)# flow monitor-map map1
RP/0/RP0/CPU0router(config-fmm)#
```

Related Commands

Command	Description
clear flow monitor	Clears the flow monitor data.
flow	Specifies a flow monitor map and a sampler map for IPv4, IPv6, or MPLS packets.
show flow monitor	Displays flow monitor cache information.
show flow monitor-map	Displays flow monitor map information.

R3.5.0 Beta Draft—Cisco Confidential Information

options

To export the tables in the options template and specify export timeout values, enter the **options** command in flow exporter map version configuration mode. To return the options template to its default configuration values, use the **no** form of this command.

options {**interface-table** | **sampler-table**} [**timeout** *seconds*]

no options {**interface-table** | **sampler-table**} [**timeout** *seconds*]

Syntax Description

interface-table	Export the interface table.
sampler-table	Exports the sampler table.
timeout <i>seconds</i>	Specifies the export timeout value. Replace <i>seconds</i> with the export timeout value. Range is from 1 through 604800 seconds.

Defaults

The default value for timeout is 0 seconds, which means that the template options are not exported by default.

Command Modes

Flow exporter map version configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
netflow	read, write

Examples

The following example shows how to export the interface table and configure the export timeout value to be 300 seconds:

```
RP/0/RP0/CPU0:router # configure
RP/0/RP0/CPU0:router(config)# flow exporter-map fem1
RP/0/RP0/CPU0:router(config-fem)# version v9
RP/0/RP0/CPU0:router(config-fem-ver)# options interface-table timeout 300
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	flow exporter-map	Creates and configures a flow exporter map.
	flow monitor-map	Configures a flow monitor map and associates an exporter map with a monitor map.
	show flow exporter	Displays flow exporter data.
	show flow exporter-map	Displays flow exporter map information for a specific node installed in the router.

R3.5.0 Beta Draft—Cisco Confidential Information

random 1 out-of

To configure the packet sampling interval for a monitor map, use the **random 1 out-of** command in sampler map configuration submode. To remove a configured sampling interval and return to the default sampling interval, use the **no** form of this command.

random 1 out-of *number_of_packets*

no random 1 out-of *number_of_packets*

Syntax Description

<i>number_of_packets</i>	Sampling interval in units of packets. Replace the <i>number_of_packets</i> argument with a number. Range is from 1 through 65535 units.

Defaults

number_of_packets = 10000

Command Modes

Sampler map configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Keep the following in mind when configuring the sampling rate with the **options** command:

- On the Cisco CRS-1, NetFlow supports sampling at a rate of 35,000 packets per second per direction for each individual line card.
- On the Cisco XR 12000 Series Router, NetFlow supports 50,000 packets per second per direction for each individual line card if Sampled NetFlow (SNF) is enabled in one direction (ingress or egress). Note that this limit does not apply if SNF is enabled in both directions. If SNF is enabled in both directions, then NetFlow supports 25,000 packets per second per direction for each individual line card.

Task ID

Task ID	Operations
netflow	read, write

R3.5.0 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to configure the sampler map to randomly sample 1 out of every 10 packets:

```
RP/0/RP0/CPU0:router # configure
RP/0/RP0/CPU0:router(config)# sampler map1
RP/0/RP0/CPU0:router(config-sm)# random 1 out-of 10
```

Related Commands

Command	Description
sampler-map	Enters sampler map configuration submode for a specific monitor map.
show sampler-map	Displays sampler map information.

R3.5.0 Beta Draft—Cisco Confidential Information

record ipv4

To configure the flow record map name for IPv4, use the **record ipv4** command in flow monitor map configuration mode. To remove the configured name from a flow record, use the **no** form of this command.

record ipv4

no record ipv4

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Flow monitor map configuration

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	netflow	read, write

Examples The following example shows how to configure the flow record map name for IPv4:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# flow monitor-map map1
RP/0/RP0/CPU0:router(config-fmm)# record ipv4
```

Related Commands	Command	Description
	clear flow monitor	Clears the flow monitor data.
	flow monitor-map	Creates and configures a flow monitor map and enters flow monitor map configuration submode.

R3.5.0 Beta Draft—Cisco Confidential Information

Command	Description
record mpls	Configures the flow record map name for MPLS.
record ipv6	Configures the flow record map name for IPv6.
show flow monitor	Displays flow monitor cache information.
show flow monitor-map	Displays flow monitor map information.

R3.5.0 Beta Draft—Cisco Confidential Information

record ipv6

To configure the flow record map name for IPv6, use the **record ipv6** command in flow monitor map configuration mode. To remove the configured name from a flow record, use the **no** form of this command.

record ipv6

no record ipv6

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Flow monitor map configuration

Release	Modification
Release 3.5.0	This command was introduced on the Cisco CRS-1.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Operations
netflow	read, write

Examples The following example shows how to configure the flow record map name for IPv6:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# flow monitor-map map1
RP/0/RP0/CPU0:router(config-fmm)# record ipv6
```

Command	Description
clear flow monitor	Clears the flow monitor data.
flow monitor-map	Creates and configures a flow monitor map and enters flow monitor map configuration submode.
record mpls	Configures the flow record map name for MPLS.
record ipv4	Configures the flow record map name for IPv4.

R3.5.0 Beta Draft—Cisco Confidential Information

Command	Description
show flow monitor	Displays flow monitor cache information.
show flow monitor-map	Displays flow monitor map information.

R3.5.0 Beta Draft—Cisco Confidential Information

record mpls

To configure the flow record map name for MPLS, use the **record mpls** command in flow monitor map configuration mode. To remove the configured name from a flow record, use the **no** form of this command.

record mpls [**ipv4-fields**] [**labels** *number*]

no record mpls [**ipv4-fields**] [**labels** *number*]

Syntax Description	ipv4-fields	(Optional) Collects IPv4 fields in the MPLS aware Netflow if the payload of the MPLS packet is IPv4.
	labels <i>number</i>	(Optional) Configures the number of labels that are used in hashing. The <i>number</i> argument is the number of labels that are used in hashing. The range is from 1 to 6.

Defaults	The default is no ipv4 fields and six labels.

Command Modes	Flow monitor map configuration

Command History	Release	Modification
	Release 3.4.1	This command was introduced on the Cisco CRS-1.
	Release 3.5.0	

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	netflow	read, write

Examples	The following example shows how to configure the flow record map name for MPLS:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# flow monitor-map map1
RP/0/RP0/CPU0:router(config-fmm)# record mpls
```

The following example shows how to collect IPv4 fields in the MPLS aware Netflow if the payload of the MPLS packet is IPv4 by using the **ipv4-fields** keyword:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# flow monitor-map map1
```

R3.5.0 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(config-fmm)# record mpls ipv4-fields
```

The following example shows how to configure three labels for hashing:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# flow monitor-map map1
RP/0/RP0/CPU0:router(config-fmm)# record mpls labels 3
```

Related Commands

Command	Description
clear flow monitor	Clears the flow monitor data.
flow monitor-map	Creates and configures a flow monitor map and enters flow monitor map configuration submode.
record ipv4	Configures the flow record map name for IPv4.
show flow monitor	Displays flow monitor cache information.
show flow monitor-map	Displays flow monitor map information.

R3.5.0 Beta Draft—Cisco Confidential Information

sampler-map

To enter sampler map configuration submode for a specific monitor map, use the **sampler-map** command in global configuration mode.

sampler-map *map_name*

Syntax Description	<i>map_name</i>	Name of the monitor map whose sampler map you want to configure. The monitor map name can be a maximum 32 characters.

Defaults	No default behavior or values

Command Modes	Global configuration

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

When you issue the **sampler-map** *map_name* command in global configuration mode, the CLI prompt changes to “config-sm,” indicating that you have entered the sampler map configuration submode. In the following sample output, the question mark (?) online help function displays all the commands available under sampler map configuration submode:

```
RP/0/RP0/CPU0:router(config)# sampler-map map1
RP/0/RP0/CPU0:router(config-sm)# ?

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
random      Use random mode for sampling packets
root        Exit to the global configuration mode
show        Show contents of configuration
```

Task ID	Task ID	Operations
	netflow	read, write

R3.5.0 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to use the **sampler-map** command to enter sampler map configuration submode for the monitor map called “map1:”

```
RP/0/RP0/CPU0:router # configure  
RP/0/RP0/CPU0:router(config) # sampler-map map1  
RP/0/RP0/CPU0:router(config-sm) #
```

Related Commands

Command	Description
flow	Specifies a flow monitor map and a sampler map for IPv4, IPv6, or MPLS packets.
show sampler-map	Displays sampler map information.

R3.5.0 Beta Draft—Cisco Confidential Information

show flow exporter

To display flow exporter data, enter the **show flow exporter** command in EXEC mode.

show flow exporter [*exporter_name*] **location** *node-id*

Syntax Description	<i>exporter_name</i>	Identifies the flow exporter whose data you want to display.
	location <i>node-id</i>	Location where the cache resides. The <i>node-id</i> argument is expressed in the <i>rack/slot/module</i> notation.
	Note	Enter the show platform command to see the location of all nodes installed in the router.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	netflow	read

Examples	The following example shows how to display flow exporter map data: <pre>RP/0/RP0/CPU0:router# show flow exporter fem1 location 0/0/CPU0</pre> Flow Exporter: fem1 Used by flow monitors: fmm1 Status: Normal Destination 10.1.1.1 (UDP 1024) Flows exported: 0 (0 bytes) Flows dropped: 0 (0 bytes) Templates exported: 3 (264 bytes)

R3.5.0 Beta Draft—Cisco Confidential Information

```

Templates dropped:                                0 (0 bytes)

Option data exported:                            1 (76 bytes)
Option data dropped:                             0 (0 bytes)

Option templates exported:                       2 (56 bytes)
Option templates dropped:                       0 (0 bytes)

Packets exported:                               6 (396 bytes)
Packets dropped:                                0 (0 bytes)

Average export rate over interval of last:
  1 hour:                                       0 pkts/sec
                                              0 bytes/sec
                                              0 flows/sec
  1 minute:                                   0 pkts/sec
                                              0 bytes/sec
                                              0 flows/sec
  1 second:                                  0 pkts/sec
                                              0 bytes/sec
                                              0 flows/sec

```

Table 122 describes the significant fields shown in the display.

Table 122 **show flow exporter Field Descriptions**

Field	Description
Id	Identifies the flow exporter map.
Used by flow monitors	Name of the flow monitors associated with the specified flow exporter map.
Status	Status of the exporter. - Normal—Exporter is active and can export packets. - Disabled—Exporter cannot send out packets because the collector is unreachable or the configuration is incomplete.
Destination	Export destination address the current flow exporter map.
Flows exported	Flows exported, in bytes.
Flows dropped	Flows dropped, in bytes.
Templates exported	Templates exported, in bytes.
Templates dropped	Templates dropped, in bytes.
Option data exported	Option data exported, in bytes.
Option data dropped	Option data dropped, in bytes.
Option templates exported	Option templates exported, in bytes.
Option templates dropped	Option templates dropped, in bytes.
Packets exported:	Packets exported, in bytes.
Packets dropped	Packets dropped, in bytes.
Average export rate over interval of last:	Average export rate, in bytes. Information is displayed for intervals of the last hour, minute, and second.

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	clear flow exporter	Clears flow exporter statistics or restarts the flow exporter statistics collector.
	flow exporter-map	Configures a flow exporter map.
	show flow exporter-map	Displays flow monitor map information for a specific node that is installed in the router.

R3.5.0 Beta Draft—Cisco Confidential Information

show flow exporter-map

To display flow exporter map information for a specific node, enter the **show flow exporter-map** command in EXEC mode.

show flow exporter-map [*name*]

Syntax Description

<i>name</i>	Name of the exporter map whose information you want to display.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
netflow	read

Examples

The following example shows how to display flow exporter map information:

```
RP/0/RP0/CPU0:router# show flow exporter-map map1
```

```
Flow Exporter Map : map1
```

```
-----
Id                : 2
DestinationIpAddr : 10.1.1.1
SourceIfName      : Loopback0
SourceIpAddr      : 10.1.1.1
DSCP              : 10
TransportProtocol : UDP
TransportDestPort : 1024
```

```
Export Version: 9
  Common Template Timeout : 1800 seconds
  Options Template Timeout : 1800 seconds
```

R3.5.0 Beta Draft—Cisco Confidential Information

Data Template Timeout : 600 seconds
 Interface-Table Export Timeout : 1800 seconds
 Sampler-Table Export Timeout : 0 seconds

Table 123 describes the significant fields shown in the display.

Table 123 *show flow exporter-map Field Descriptions*

Field	Description
Id	Identifies the flow exporter map.
DestinationIpAddr	Exports destination configuration.
SourceIfName	Source interface for this exporter map. You can specify the source interface with the flow exporter-map command.
SourceIpAddr	IP address of the source interface (SourceIfName).
DSCP	Differentiated services codepoint (DSCP) value for export packets. Note You can specify the DSCP with the flow exporter-map command.
TransportProtocol	Displays the configured transport protocol. Note Cisco IOS XR software supports the UDP transport protocol only. Note You can specify the transport protocol with the flow exporter-map command.
TransportDestPort	Displays the configured destination port for UDP packets.
Export Version	Displays the configured export format. Note Cisco IOS XR software supports export format version 9 only.
Common Template Timeout	Displays the configured common template timeout.
Options Template Timeout	Displays the configured options template timeout. Note You can specify the options template timeout with the flow exporter-map command.
Data Template Timeout	Displays the configured data template timeout. Note You can specify the data template timeout with the flow exporter-map command.
Interface-Table Export Timeout	Displays the export timeout value for the interface table. Note You can specify the export timeout for the interface table with the flow exporter-map command.
Sampler-Table Export Timeout	Displays the export timeout value for the sampler table. Note You can specify the export timeout for the sampler table with the flow exporter-map command.

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	clear flow exporter	Clears flow exporter statistics or restarts the flow exporter statistics collector.
	flow exporter-map	Configures a flow exporter map.
	show flow exporter	Displays flow exporter data.

R3.5.0 Beta Draft—Cisco Confidential Information

show flow monitor

To display flow monitor cache data in various formats, enter the **show flow monitor** command in EXEC mode.

To match on Access Control Lists (ACLs) and one or more fields:

```
show flow monitor monitor-name cache match {ipv4 {acl name | source-address match-options | destination-address match-options | protocol match-options | tos match-options} | ipv6 {acl name | source-address match-options | destination-address match-options | protocol match-options | tc match-options} | layer4 {source-port-overloaded match-options | destination-port-overloaded match-options | tcp-flags match-flags-options} | bgp {source-as match-options | destination-as match-options} | interface {ingress match-if-options | egress match-if-options} | timestamp {first match-options | last match-options} | counters {byte match-options | packets match-options} | misc {forwarding-status match-options | direction match-dir-options}}
```

To sort flow record information according to a particular field:

```
show flow monitor monitor-name cache sort {ipv4 {source-address | destination-address | tos | protocol} | ipv6 {source-address | destination-address | tc | protocol} | mpls {label-2 | label-3 | label-4 | label-5 | label-6 | label-type | prefix | top-label} | layer4 {source-port-overloaded | destination-port-overloaded} | bgp {source-as | destination-as} | interface {ingress | egress} | timestamp {first | last} | counters {bytes | packets} | misc {forwarding-status | direction} {top | bottom} [entries]
```

To include or exclude one or more fields in the **show flow monitor** command output:

```
show flow monitor monitor-name cache {include | exclude} {ipv4 {source-address | destination-address | tos | protocol} | {ipv6 {source-address | destination-address | tc | flow-label | option-headers | protocol} | mpls {label-2 | label-3 | label-4 | label-5 | label-6 | top-label} | layer4 {source-port-overloaded | destination-port-overloaded} | bgp {source-as | destination-as} | interface {ingress | egress} | timestamp {first | last} | counters {bytes | packets} | misc {forwarding-status match-options | direction match-dir-options}}
```

To display summarized flow record statistics:

```
show flow monitor monitor-name cache summary
```

To display only key field, packet, and byte information for the flow records:

```
show flow monitor monitor-name cache brief
```

To display flow record information for a particular node only:

```
show flow monitor monitor-name cache location node-id
```

Syntax Description

If you specified the **show flow monitor** *monitor-name* **cache match** command to match on ACL and one or more fields:

<i>monitor-name</i>	Flow monitor map whose details you want to display.
cache	Displays details about the flow monitor cache.

R3.5.0 Beta Draft—Cisco Confidential Information

match	Specifies match criteria for the display. Enter the match keyword followed by the ? command to see a complete list of possible match criteria.
ipv4	Specifies IPv4 fields.
ipv6	Specifies IPv6 fields.
acl name	Specifies an access list. Replace <i>name</i> with the name of the access whose information you want to display.
source-address match-options	Specifies source IP address match options. Possible match options are: • eq—Match if equal to field value. • gt—Match if greater than field value. • lt—Match if less than field value. • neq—Match if not equal to field value. • range—Match if within the range of field values. Note Enter the source-address keyword followed by the ? command to see a complete list of possible match criteria.
destination-address	Specifies IPV4 or IPv6 destination address match options. Possible match options are: • eq—Match if equal to field value. • gt—Match if greater than field value. • lt—Match if less than field value. • neq—Match if not equal to field value. • range—Match if within the range of field values. Note Enter the destination-address keyword followed by the ? command to see a complete list of possible match criteria.
tos match-options	Compares fields and matches them based on the type of service value. Range is from 0 through 255. Possible match options are: • eq—Match if equal to field value. • gt—Match if greater than field value. • lt—Match if less than field value. • neq—Match if not equal to field value. • range—Match if within the range of field values. Note Enter the tos keyword followed by the ? command to see a complete list of possible match criteria.

R3.5.0 Beta Draft—Cisco Confidential Information

protocol match-options	Compares fields and matches them based on the protocol value. Possible match options are: • eq—Match if equal to field value. • gt—Match if greater than field value. • lt—Match if less than field value. • neq—Match if not equal to field value. • range—Match if within the range of field values. Note Enter the protocol keyword followed by the ? command to see a complete list of possible match criteria.
layer4	Compares Layer 4 fields and matches them based on specific criteria. You can specify match criteria for any of the following Layer 4 fields: • destination-port-overloaded • source-port-overloaded • tcp-flags Note Enter the layer4 keyword followed by the ? command to see a complete list of possible Layer 4 fields to compare and match.
destination-port-overloaded	Compares fields and matches them based on the destination-port-overloaded value. The destination port is matched if the protocol specified for that port is TCP or UDP. Possible match options are: • eq—Match if equal to field value. • gt—Match if greater than field value. • lt—Match if less than field value. • neq—Match if not equal to field value. • range—Match if within the range of field values. Note Enter the destination-port-overloaded keyword followed by the ? command to see a complete list of possible match criteria.

R3.5.0 Beta Draft—Cisco Confidential Information

source-port-overloaded	Compares fields and matches them based on the source-port-overloaded value. The source port is matched if the protocol specified for that port is one of the following: • TCP—Range is from 0 through 65535. • UDP—Range is from 0 through 65535. • ICMP—Type or code is in range from 0 through 255. • IGMP—Type is in range from 0 through 255. Possible match options are: • eq—Match if equal to field value. • gt—Match if greater than field value. • lt—Match if less than field value. • neq—Match if not equal to field value. • range—Match if within the range of field values. Note Enter the source-port-overloaded keyword followed by the ? command to see a complete list of possible match criteria.
tcp-flags match-flags-options	Specifies TCP flags, as follows: • all—Match all of the fields • any—Match any of the fields • none—Match none of the fields. Note Enter the tcp-flags keyword followed by the ? command to see a complete list of possible match criteria.
bgp	Compares BGP fields and matches them based on specific criteria. You can specify match criteria for any of the following BGP fields: • destination-as—Destination as. • source-as—Source as.
source-as match-options	Compares and matches the BGP autonomous system number of the destination address. Possible match options are: • eq—Match if equal to field value. • gt—Match if greater than field value. • lt—Match if less than field value. • neq—Match if not equal to field value. • range—Match if within the range of field values. Note Enter the source-as keyword followed by the ? command to see a complete list of possible match criteria.

R3.5.0 Beta Draft—Cisco Confidential Information

destination-as <i>match-options</i>	Compares and matches the BGP autonomous system number of the source address. Possible match options are: • eq—Match if equal to field value. • gt—Match if greater than field value. • lt—Match if less than field value. • neq—Match if not equal to field value. • range—Match if within the range of field values. Note Enter the destination-as keyword followed by the ? command to see a complete list of possible match criteria.
interface	Compares ingress or egress interface fields and matches them based on specific criteria. Follow interface with one of the following keyword arguments: • ingress <i>match-if-options</i> • egress <i>match-if-options</i>
ingress <i>match-if-options</i>	Compares ingress interface fields and matches them based on the <i>match-if-options</i> value. Possible match options are: • eq—Match if equal to field value. • neq—Match if not equal to field value.
egress <i>match-if-options</i>	Compares egress interface fields and matches them based on the <i>match-options</i> value. Possible match options are: • eq—Match if equal to field value. • neq—Match if not equal to field value.
timestamp	Specifies the time stamp for which to compare and match the specified criteria. Enter the first keyword or the last keyword to specify the time stamp whose criteria you want to compare.
first <i>match-options</i>	Compares fields from the first time stamp and matches them based on the <i>match-options</i> value. Possible match options are: • eq—Match if equal to field value. • gt—Match if greater than field value. • lt—Match if less than field value. • neq—Match if not equal to field value. • range—Match if within the range of field values. Note Enter the first keyword followed by the ? command to see a complete list of possible match criteria.

R3.5.0 Beta Draft—Cisco Confidential Information

last <i>match-options</i>	Compares fields from the last time stamp and matches them based on the <i>match-if-options</i> value. Possible match options are: • eq—Match if equal to field value. • gt—Match if greater than field value. • lt—Match if less than field value. • neq—Match if not equal to field value. • range—Match if within the range of field values. Note Enter the last keyword followed by the ? command to see a complete list of possible match criteria.
counters	Specifies the counters for which to compare and match the specified criteria. Enter the byte keyword or the packets keyword to specify the counters whose criteria you want to compare.
byte <i>match-options</i>	Compares bytes counter fields and matches them based on the <i>match-options</i> value. Possible match options are: • eq—Match if equal to field value. • gt—Match if greater than field value. • lt—Match if less than field value. • neq—Match if not equal to field value. • range—Match if within the range of field values. Note Enter the byte keyword followed by the ? command to see a complete list of possible match criteria.
packets <i>match-options</i>	Compares packets counter fields and matches them based on the <i>match-options</i> value. Possible match options are: • eq—Match if equal to field value. • gt—Match if greater than field value. • lt—Match if less than field value. • neq—Match if not equal to field value. • range—Match if within the range of field values. Note Enter the byte keyword followed by the ? command to see a complete list of possible match criteria.
misc	Specifies miscellaneous fields for which to compare and match the specified criteria. Enter the forwarding-status keyword or the direction keyword to specify the field whose criteria you want to compare.

R3.5.0 Beta Draft—Cisco Confidential Information

forwarding-status <i>match-options</i>	Compares forwarding status fields and matches them based on the <i>match-options</i> value. Possible match options are: • eq—Match if equal to field value. • gt—Match if greater than field value. • lt—Match if less than field value. • neq—Match if not equal to field value. • range—Match if within the range of field values. Note Enter the forwarding-status keyword followed by the ? command to see a complete list of possible match criteria.
direction <i>match-dir-options</i>	Compares information about the direction of the flow and matches it based on the <i>match-options</i> value. Possible match options are: • eq—Match if equal to field value. • neq—Match if not equal to field value. Note Enter the direction keyword followed by the ? command to see a complete list of possible match criteria.

To sort flow record information according to a particular field:

<i>monitor-name</i>	Flow monitor map whose details you want to display.
cache	Displays details about the flow monitor cache.
sort	Determines sorting criteria for the show flow monitor command display.
ipv4	Specifies sorting criteria for one of the following IPv4 fields: • destination-address • source-address • protocol • tos Note Enter the ipv4 keyword followed by the ? command to see a complete list of possible sorting criteria.
ipv6	Specifies sorting criteria for one of the following IPv6 fields: • destination-address • source-address • protocol • tc Note Enter the ipv6 keyword followed by the ? command to see a complete list of possible sorting criteria.

R3.5.0 Beta Draft—Cisco Confidential Information

source-address	Displays IPv4 or IPv6 information for the source address according to the specified sorting criteria. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries. Note Enter the source-address keyword followed by the ? command to see a complete list of possible sorting criteria.
destination-address	Displays IPv4 or IPv6 information for the destination address according to the specified sorting criteria. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries. Note Enter the destination-address keyword followed by the ? command to see a complete list of possible sorting criteria.
tos	Displays IPv4 type of service information according to the specified sorting criteria. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries. Note Enter the tos keyword followed by the ? command to see a complete list of possible sorting criteria.
tc	Displays IPv6 traffic class information according to the specified sorting criteria. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries. Note Enter the tc keyword followed by the ? command to see a complete list of possible sorting criteria.
protocol	Displays IPv4 or IPv6 protocol information according to the specified sorting criteria. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries. Note Enter the tos keyword followed by the ? command to see a complete list of possible sorting criteria.

R3.5.0 Beta Draft—Cisco Confidential Information

mpls	Specifies sorting criteria for one of the following MPLS fields: • label-2 • label-3 • label-4 • label-5 • label-6 • label-type • prefix • top-label Note Enter the mpls keyword followed by the ? command to see a complete list of possible sorting criteria.
label-2	Displays MPLS information for the second label in the MPLS label stack. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries.
label-3	Displays MPLS information for the third label in the MPLS label stack. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries.
label-4	Displays MPLS information for the fourth label in the MPLS label stack. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries.
label-5	Displays MPLS information for the fifth label in the MPLS label stack. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries.
label-6	Displays MPLS information for the sixth label in the MPLS label stack. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries.
label-type	Displays MPLS information for the specified type of label in the MPLS label stack. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries.
prefix	Displays MPLS information for the destination address. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries.

R3.5.0 Beta Draft—Cisco Confidential Information

top-label	Displays MPLS information for the top label in the MPLS label stack. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries.
layer4	Specifies sorting criteria for one of the following Layer 4 fields: • source-port-overloaded • destination-port-overloaded Note Enter the layer4 keyword followed by the ? command to see a complete list of possible sorting criteria.
source-port-overloaded	Displays source port overload information according to the specified sorting criteria. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries. Note Enter the source-port-overloaded keyword followed by the ? command to see a complete list of possible sorting criteria.
destination-port-overloaded	Displays destination port overload information according to the specified sorting criteria. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries. Note Enter the destination-port-overloaded keyword followed by the ? command to see a complete list of possible sorting criteria.
bgp	Specifies sorting criteria for one of the following BGP fields: • source-as • destination-as Note Enter the layer4 keyword followed by the ? command to see a complete list of possible sorting criteria.
source-as	Displays information about the BGP source address autonomous system number according to the specified sorting criteria. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries. Note Enter the source-as keyword followed by the ? command to see a complete list of possible sorting criteria.
destination-as	Displays information about the BGP destination address autonomous system number according to the specified sorting criteria. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries. Note Enter the destination-as keyword followed by the ? command to see a complete list of possible sorting criteria.

R3.5.0 Beta Draft—Cisco Confidential Information

interface	Specifies sorting criteria for egress or ingress interface information. Enter the ingress keyword or the egress keyword to specify the interface whose criteria you want to specify. Note Enter the interface keyword followed by the ? command to see a complete list of possible sorting criteria.
ingress	Displays ingress information for an interface according to the specified sorting criteria. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries. Note Enter the ingress keyword followed by the ? command to see a complete list of possible sorting criteria.
egress	Displays egress information for an interface according to the specified sorting criteria. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries. Note Enter the egress keyword followed by the ? command to see a complete list of possible sorting criteria.
timestamp	Specifies sorting criteria for the first or last time stamp. Enter the first keyword or the last keyword to specify the time stamp whose criteria you want to specify. Note Enter the timestamp keyword followed by the ? command to see a complete list of possible sorting criteria.
first	Displays information for the first time stamp according to the specified sorting criteria. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries. Note Enter the first keyword followed by the ? command to see a complete list of possible sorting criteria.
last	Displays information for the last time stamp according to the specified sorting criteria. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries. Note Enter the last keyword followed by the ? command to see a complete list of possible sorting criteria.
counters	Specifies sorting criteria for the bytes or packets counters. Follow the counters keyword with the byte keyword or the packets keyword to specify the counters whose criteria you want to compare.
bytes	Displays bytes counter information according to the specified sorting criteria. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries. Note Enter the bytes keyword followed by the ? command to see a complete list of possible match criteria.

R3.5.0 Beta Draft—Cisco Confidential Information

packets	Displays packets counter information according to the specified sorting criteria. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries. Note Enter the packets keyword followed by the ? command to see a complete list of possible match criteria.
misc	Specifies sorting criteria for miscellaneous fields. Follow the misc keyword with the forwarding-status keyword or the direction keyword to specify the counters whose criteria you want to compare.
forwarding-status	Displays forwarding status information according to the specified sorting criteria. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries. Note Enter the forwarding-status keyword followed by the ? command to see a complete list of possible match criteria.
direction	Displays information about the direction of the flow according to the specified sorting criteria. Possible sorting options are: • top—Displays top cache entries. • bottom—Displays bottom cache entries. Enter the direction keyword followed by the ? command to see a complete list of possible match criteria.
top	Displays top cache entries. Replace <i>records</i> with the number of records you want to display. Note You can follow the top keyword with the optional <i>entries</i> argument to specify the number of records to display.
bottom	Displays bottom cache entries. Replace <i>records</i> with the number of records you want to display. Note You can follow the bottom keyword with the optional <i>entries</i> argument to specify the number of records to display.
<i>entries</i>	Number of records to display. Range is from 1 through 1000.

To include or exclude one or more fields in the **show flow monitor** command output:

<i>monitor-name</i>	Identifies the flow monitor map whose details you want to display.
cache	Displays details about the flow monitor cache.
include	Includes the specified fields in the display output. Enter the include keyword, followed by the keyword or keywords that specify the fields to include. Note To see a list of fields that can be included, enter the include keyword, followed by the ? command.

R3.5.0 Beta Draft—Cisco Confidential Information

exclude	Excludes the specified fields in the display output. Enter the exclude keyword, followed by the keyword or keywords that specify the fields to exclude. Note To see a list of fields that can be excluded, enter the exclude keyword, followed by the ? command.
ipv4	Includes or excludes one of the following IPv4 fields in the command output: • destination-address • source-address • protocol • tos Note Enter the ipv4 keyword followed by the ? command to see a complete list of fields you can include or exclude.
ipv6	Includes or excludes one of the following IPv6 fields in the command output: • destination-address • flow-label • option-headers • source-address • protocol • tc Note Enter the ipv6 keyword followed by the ? command to see a complete list of fields you can include or exclude.
source-address	Includes or excludes IPV4 or IPV6 information for the source address in the command output.
destination-address	Includes or excludes IPV4 or IPV6 information for the destination address in the command output.
flow-label	Includes or excludes information about the IPv6 flow label in the command output. The flow-label is the 20-bit flow label id present in every IPv6 packet header.
option-headers	Includes or excludes IPV6 information for the option headers in the command output. The option header is a bit mask that indicates which options headers are present in the IPv6 header.
tos	Includes or excludes IPV4 type of service information in the command output.
tc	Includes or excludes IPV6 traffic class information in the command output.
protocol	Includes or excludes IPV4 or IPV6 protocol information in the command output.

R3.5.0 Beta Draft—Cisco Confidential Information

mpls	Includes or excludes one of the following MPLS fields in the command output: • label-2 • label-3 • label-4 • label-5 • label-6 • top-label Note Enter the mpls keyword followed by the ? command to see a complete list of possible sorting criteria.
label-2	Includes or excludes MPLS information for the second label in the MPLS label stack.
label-3	Includes or excludes MPLS information for the third label in the MPLS label stack.
label-4	Includes or excludes MPLS information for the fourth label in the MPLS label stack.
label-5	Includes or excludes MPLS information for the fifth label in the MPLS label stack.
label-6	Includes or excludes MPLS information for the sixth label in the MPLS label stack.
top-label	Includes or excludes MPLS information for the top label in the MPLS label stack.
layer4	Includes or excludes one of the following the following Layer 4 fields in the command output: • source-port-overloaded • destination-port-overloaded Note Enter the layer4 keyword followed by the ? command to see a complete list of fields you can include or exclude.
source-port-overloaded	Includes or excludes source port overload information in the command output.
destination-port-overloaded	Includes or excludes destination port overload information in the command output. • top—Displays top cache entries. • bottom—Displays bottom cache entries.
bgp	Includes or excludes the following BGP fields in the command output: • source-as • destination-as Note Enter the bgp keyword followed by the ? command to see a complete list of fields you can include or exclude.
source-as	Includes or excludes information about the BGP source address autonomous system number in the command output.

R3.5.0 Beta Draft—Cisco Confidential Information

destination-as	Includes or excludes information about the BGP destination address autonomous system number in the command output.
interface	Includes or excludes egress or ingress interface information in the command output. Enter the ingress keyword or the egress keyword to specify the interface information you want to include or exclude in the output. Note Enter the interface keyword followed by the ? command to see a complete list of fields you can include or exclude.
ingress	Includes or excludes ingress interface information in the command output.
egress	Includes or excludes egress interface information in the command output.
timestamp	Includes or excludes information from the first or last time stamp in the command output. Enter the first keyword or the last keyword to include or exclude information about a specific time stamp. Note Enter the timestamp keyword followed by the ? command to see a complete list of the time stamps you can include or exclude.
first	Includes or excludes information for the first time stamp in the command output.
last	Includes or excludes information for the last time stamp in the command output.
counters	Includes or excludes bytes or packets counters in the command output. Follow the counters keyword with the byte keyword or the packets keyword to include or exclude particular counters. Note Enter the counters keyword followed by the ? command to see a complete list of the counters you can include or exclude.
bytes	Includes or excludes bytes counter information in the command output.
packets	Includes or excludes packets counter information in the command output.
misc	Includes or excludes information for miscellaneous fields in the command output. Follow the misc keyword with the forwarding-status keyword or the direction keyword to specify the field you want to include or exclude. Note Enter the misc keyword followed by the ? command to see a complete list of the miscellaneous fields you can include or exclude.
forwarding-status	Includes or excludes forwarding status information in the command output.
direction	Includes or excludes information about the direction of the flow in the command output.
top	Includes or excludes top cache entries in the command output. Replace <i>records</i> with the number of records you want to display.

R3.5.0 Beta Draft—Cisco Confidential Information

bottom	Includes or excludes bottom cache entries. Replace <i>records</i> with the number of records you want to display.
<i>entries</i>	Number of records to display. Range is from 1 through 1000.

To display summarized flow record statistics:

<i>monitor-name</i>	Flow monitor map whose details you want to display.
cache	Displays details about the flow monitor cache.
summary	Displays summarized flow monitor information only.

To display only key field, packet and byte information for the flow records:

<i>monitor-name</i>	Flow monitor map whose details you want to display.
cache	Displays details about the flow monitor cache.
brief	Abbreviates the show flow monitor command output.

To display flow record information for a particular node only:

<i>monitor-name</i>	Flow monitor map whose details you want to display.
cache	Displays details about the flow monitor cache.
location <i>node-id</i>	Identifies the node whose flow exporter statistics you want to clear, or whose flow exporter statistics collector you want to restart. The <i>node-id</i> argument is expressed in the <i>rack/slot/module</i> notation.
Note Enter the location keyword followed by the ? command to see a complete list of nodes whose flow monitor information can be display.	

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.

R3.5.0 Beta Draft—Cisco Confidential Information

Release	Modification
Release 3.3.1	- On the Cisco CRS-1, the following keywords were added to the show flow monitor command sort option: mpls {label-2 label-3 label-4 label-5 label-6 label-type prefix top-label} - On the Cisco CRS-1, the following keywords were added to the show flow monitor command include and exclude options: mpls {label-2 label-3 label-4 label-5 label-6 top-label} - On the Cisco CRS-1, the show flow monitor command output was updated to include MPLS information for MPLS aware NetFlow.
Release 3.4.0	No modification.
Release 3.5.0	On the Cisco CRS-1, the following keywords were added to the show flow monitor command to support IPv6: ipv6 tc option-headers flow-label

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

**Note**

To collect source and destination AS information, you must enable BGP on the relevant BGP AFI/SAFI. Unless this is done, all AS numbers in the flow records will be displayed as 0.

Keep the following information in mind when using the **show flow monitor** command:

- The **show flow monitor** command can include combinations of the following options:
 - format**
 - match**
 - include**
 - exclude**
 - sort**
 - summary**
 - location**
- We do not recommend including the **summary** option with the **sort** and **format** options.
- The mutually exclusive options are **summary**, **brief**, **include**, and **exclude**.
- To see a list of fields that can be included after a keyword, enter the **?** command, as shown in the following example:

```
RP/0/RP0/CPU0:router# show flow monitor map1 cache summary ?
brief      Show just the key fields
```

R3.5.0 Beta Draft—Cisco Confidential Information

exclude	Exclude field
format	Display format
include	Include field
location	Specify a location
match	Match criteria
sort	Sorting criteria

Task ID**Task ID****Operations**

netflow

read

Examples

The following example shows how to display flow monitor data for a specific monitor map cache in the location 0/0/CPU0:

```
RP/0/RP0/CPU0:router# show flow monitor fmm2 cache loc 0/0/CPU0
```

Cache summary for Flow Monitor fmm2:

```
Cache size: 65535
Current entries: 4
High Watermark: 62258
Flows added: 4
Flows not added: 0
Ager Polls: 60
- Active timeout 0
- Inactive timeout 0
- TCP FIN flag 0
- Watermark aged 0
- Emergency aged 0
- Counter wrap aged 0
- Total 0
Periodic export:
- Counter wrap 0
- TCP FIN flag 0
Flows exported 0
Matching entries: 4
```

IPV4SrcAddr	IPV4DstAddr	L4SrcPort	L4DestPort	BGPDstOrigAS	BGPSrcOrigAS		
IPV4SrcPrfxLen							
IPV4SrcPrfxLen	IPV4Prot	IPV4TOS	InputInterface	OutputInterface	L4TCPFlags		
ForwardStatus							
ForwardReason	FirstSwitched	LastSwitched	ByteCount	PacketCount	Dir	Sampler	ID
17.17.17.2	18.18.18.2	0	0	0	0	24	
24	\$						
61	normal	PO0/0/0/8	PO0/0/0/12	0	Fwd	0	
00							
00:02:43:800 00	00:02:49:980	37200	620		In 0		
18.18.18.2	17.17.17.2	0	0	0	0	24	
24	\$						
61	normal	PO0/0/0/12	PO0/0/0/8	0	Fwd	0	
00							
00:02:43:791 00	00:02:49:980	37200	620		In 0		
17.17.17.2	18.18.18.2	0	0	0	0	24	
0	\$						
61	normal	PO0/0/0/8	PO0/0/0/12	0	Fwd	0	
00							
00:02:43:798 00	00:02:49:980	34720	620		Out 0		
18.18.18.2	17.17.17.2	0	0	0	0	24	
0	\$						
61	normal	PO0/0/0/12	PO0/0/0/8	0	Fwd	0	
00							

R3.5.0 Beta Draft—Cisco Confidential Information

```
00:02:43:797 00 00:02:49:980 34720          620          Out 0
L4SrcPort  L4DestPort BGPDstOrigAS BGPSrcOrigAS IPV4DstPrfxLen
```

Table 124 describes the significant fields shown in the display.

Table 124 *show flow monitor Field Descriptions*

Field	Description
Cache summary for Flow Monitor fmm2	Display general cache information for the specified flow monitor. The following information is displayed • Cache size for the specified flow monitor map • Current number of entries in the cache • High watermark for this cache • Number of flows added to the cache • Number of flows not added to the cache
Ager Polls	Displays the following ager statistics: • Active timeout • Inactive timeout • TCP FIN flag • Watermark aged • Emergency aged • Counter wrap aged • Total
Periodic export	• Counter wrap • TCP FIN flag
Matching entries	Status of various matching criteria for traffic in the flows.

R3.5.0 Beta Draft—Cisco Confidential Information

show flow monitor-map

To display flow monitor map data, enter the **show flow monitor-map** command in EXEC mode.

show flow monitor-map *map-name*

Syntax Description	<i>map-name</i>	Name of the monitor map whose data you want to display.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
	Release 3.3.1	On the Cisco CRS-1, the show flow monitor-map command output was modified to include MPLS information.
	Release 3.4.0	No modification.
	Release 3.4.1	The ipv4-raw record map name was replaced with ipv4.
	Release 3.5.0	On the Cisco CRS-1, the record map name field was updated to include ipv6 when relevant.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	netflow	read

Examples	The following example shows how to display monitor-map data for a specific flow:

```
RP/0/RP0/CPU0:router# show flow monitor-map fmm1
```

```
Flow Monitor Map : fmm1
```

```
-----
```

```
Id: 1
RecordMapName: ipv4
ExportMapName: NFC
CacheAgingMode: Permanent
CacheMaxEntries: 10000
CacheActiveTout: N/A
CacheInactiveTout: N/A
```

R3.5.0 Beta Draft—Cisco Confidential Information

CacheUpdateTout: 60 seconds

Table 125 describes the significant fields shown in the display.

Table 125 *show flow monitor-map Field Descriptions*

Field	Description
Flow Monitor Map	Name of the flow monitor map whose information is display in the show flow monitor-map command output.
Id	Number that identifies the flow monitor map.
RecordMapName	Name of the flow record map that is associated with this monitor map. The RecordMapName indicates the type of packets NetFlow captures as they leave the router. On the Cisco CRS-1, the RecordMapName can be “ipv4,” “ipv6,” or “mpls.” On the Cisco XR 12000 Series Router, the RecordMapName can be “ipv4” or “mpls.”
ExportMapName	Name of the export map that is associated with this monitor map.
CacheAgingMode	Current aging mode configured on this cache. “Permanent” indicates that the removal of entries from the monitor map flow cache is disabled. Note To configure the number of entries allowed in the monitor map flow cache, enter the cache entries command in flow monitor map configuration mode. To disable the removal of entries from the monitor map flow cache, enter the cache permanent command in flow monitor map configuration mode.
CacheMaxEntries	Number of flow entries currently allowed in the flow cache before the oldest entry is removed. Note To modify the number of entries in the monitor map flow cache, enter the cache entries command in flow monitor map configuration mode
CacheActiveTout	Active flow timeout configured for this cache, in seconds. Note To modify the configured active flow timeout, use the cache timeout command in flow monitor map configuration mode.
CacheInactiveTout	Inactive flow timeout configured for this cache, in seconds. Note To modify the configured inactive flow timeout, use the cache timeout command in flow monitor map configuration mode.
CacheUpdateTout	Update timeout configured for this cache, in seconds. Note To modify the configured update timeout, use the cache timeout command in flow monitor map configuration mode.

Related Commands

R3.5.0 Beta Draft—Cisco Confidential Information

Command	Description
clear flow monitor	Clears the flow monitor data.
flow monitor-map	Configures a flow monitor map.
flow	Specifies a flow monitor map and a sampler map for IPv4, IPv6, or MPLS packets.
record ipv4	Configures the flow record map name for IPv4.
record ipv6	Configures the flow record map name for IPv6.
record mpls	Configures the flow record map name for MPLS.

R3.5.0 Beta Draft—Cisco Confidential Information

show flow platform producer statistics location

To display statistics collected by the NetFlow producer, use the **show flow platform producer statistics location** command in EXEC mode.

show flow platform producer statistics location *node-id*

Syntax Description	<i>node-id</i>	Location of the node whose NetFlow producer statistics you want to display. The <i>node-id</i> is expressed in the <i>rack/slot/module</i> notation.
	Note	Enter the show platform command to see the location of all nodes installed in the router.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 3.3.0	This command was introduced on the Cisco CRS-1.
	Release 3.3.1	The show flow platform producer statistics location command output was updated to include Multiprotocol Label Switching (MPLS) statistics.
	Release 3.4.0	No modification.
	Release 3.5.0	The show flow platform producer statistics location command output was updated to include IPv6 statistics.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	netflow	read

Examples	The following example shows how to display statistics collected by the NetFlow producer for the CPU card in slot 0:

```
RP/0/RP0/CPU0:router# show flow platform producer statistics location 0/0/CPU0
```

```
Netflow Platform Producer Counters:
IPv4 Ingress Packets:                0
IPv4 Egress Packets:                 0
MPLS Ingress Packets:                0
MPLS Egress Packets:                 0
Drops (no space):                    0
```

R3.5.0 Beta Draft—Cisco Confidential Information

```

Drops (other):                0
Unknown Ingress Packets:      0
Unknown Egress Packets:       0
Worker waiting:               0

```

Table 126 describes the significant fields shown in the display.

Table 126 *show flow platform producer statistics Field Descriptions*

Field	Description
IPv4 Ingress Packets	Number of IPV4 packets that were received from the remote end.
IPv4 Egress Packets	Number of transmitted IPV4 packets.
MPLS Ingress Packets	Number of MPLS packets that were received from the remote end.
MPLS Egress Packets	Number of transmitted MPLS packets.
Drops (no space)	Number of packets that the producer could not enqueue to the NetFlow server because the server input ring was full.
Drops (other)	Number of packets that the producer could not enqueue to the NetFlow server due to errors other than the server input ring being full.
Unknown Ingress Packets	Number of unrecognized packets received from the remote end that were dropped.
Unknown Egress Packets	Number of packets transmitted to the remote end that were dropped because they were not recognized by the remote end.
Worker waiting	Number of times that the producer needed to use the server. Note This field is strictly informational and does not indicate any error.

R3.5.0 Beta Draft—Cisco Confidential Information

show sampler-map

To display sampler map information, enter the **show sampler-map** command in EXEC mode.

show sampler-map [*sampler-name*]

Syntax Description	<i>sampler-name</i>	Identifies the sampler map whose information you want to display.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	netflow	read

Examples	The following example shows how to display sampler map information for a router:

```
RP/0/RP0/CPU0:router# show sampler-map map1
```

```
Sampler Map : map1
```

```
-----  
Id:      1  
Mode:    Random (1 out of 100 Pkts)
```

[Table 127](#) describes the significant fields shown in the display.

R3.5.0 Beta Draft—Cisco Confidential Information**Table 127** **show sampler-map Field Descriptions**

Field	Description
Id	Flow sampler map identifier.
Mode	Sampling interval in units of packet. “Random” mode is any mode that was configured with the flow monitor-map command. Note Currently, Cisco IOS XR software supports “Random” mode only.

Related Commands

Command	Description
sampler-map	Configures the sampler map.
flow	Specifies a flow monitor map and a sampler map for IPv4, IPv6, or MPLS packets.

R3.5.0 Beta Draft—Cisco Confidential Information

source (NetFlow)

To configure a source interface for the current collector, use the **source** command in flow exporter map configuration mode. To remove a configured source interface, use the **no** form of this command.

source *type instance*

no source *type instance*

Syntax Description		
	<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
	<i>instance</i>	Physical interface instance. Replace the <i>instance</i> argument with one of the following interface identifiers: - For T1/E1/DS0 physical interfaces, the naming notation is <i>rack/slot/module/port/t1-num:channel-group-number</i>. For all other physical interface types, the naming notation is <i>rack/slot/module/port</i>. A slash between values is required as part of the notation. The values for the <i>rack</i>, <i>slot</i>, <i>module</i>, <i>port</i>, and <i>t1-num:channel-group-number</i> arguments are as follows: – <i>rack</i>: Chassis number of the rack. – <i>slot</i>: Physical slot number of the modular services card or line card. – <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. – <i>port</i>: Physical port number of the T3 controller. – <i>t1-num</i>: T1 or E1 channel number. T1 channels range from 0 to 23; E1 channels range from 0 to 30. – <i>channel-group-number</i>: Time slot number. T1 time slots range from 1 to 24; E1 time slots range from 1 to 31. The <i>channel-group-number</i> is preceded by a colon and not a slash. - For a virtual interface instance, the number range varies depending on interface type. For a complete list of all valid instances, use the question mark (?) online help function.

Defaults	No default behavior or values

Command Modes	Flow exporter map configuration

R3.5.0 Beta Draft—Cisco Confidential Information**Command History**

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
Release 3.4.0	This command was moved to the flow exporter map configuration mode.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
netflow	read, write

Examples

The following example shows how to configure a physical interface as a source for the current collector. In this example, the source is a POS interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# flow exporter-map map1
RP/0/RP0/CPU0:router(config-fem)# source pos 0/1/0/0
```

The following example shows how to configure a virtual interface as a source for the current collector. In this example, the source is an Ethernet bundle:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# flow exporter-map map1
RP/0/RP0/CPU0:router(config-fem)# source Bundle-Ether 1
```

Related Commands

Command	Description
flow exporter-map	Creates and configures a flow exporter map.
flow monitor-map	Configures a flow monitor map and associates an exporter map with a monitor map.
show flow exporter	Displays flow exporter data.
show flow exporter-map	Displays flow exporter map information for a specific node installed in the router.

R3.5.0 Beta Draft—Cisco Confidential Information

template

To configure the export timeout value for the data and options templates, enter the **template** command in flow exporter map version configuration mode. To remove a configured template export timeout value, use the **no** form of this command.

template [**data** | **options**] **timeout** *seconds*

no template [**data** | **options**] **timeout** *seconds*

Syntax Description

data	(Optional) Specifies the data template.
options	(Optional) Specifies the options template.
timeout <i>seconds</i>	Configures the timeout value for the specified template, or for both the data and options templates. Replace <i>seconds</i> with the export timeout value. Range is from 1 through 604800 seconds.

Defaults

No default behavior or values

Command Modes

Flow exporter map version configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
netflow	read, write

Examples

The following example shows how to configure the export timeout value for the data template to be 300 seconds:

```
RP/0/RP0/CPU0:router # configure
RP/0/RP0/CPU0:router(config)# flow exporter-map fem1
RP/0/RP0/CPU0:router(config-fem)# version v9
RP/0/RP0/CPU0:router(config-fem-ver)# template data timeout 300
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	flow exporter-map	Creates and configures a flow exporter map.
	flow monitor-map	Configures a flow monitor map and associates an exporter map with a monitor map.
	show flow exporter	Displays flow exporter data.
	show flow exporter-map	Displays flow exporter map information for a specific node installed in the router.

R3.5.0 Beta Draft—Cisco Confidential Information

transport udp

To configure the destination port for User Datagram Protocol (UDP) packets, enter the **transport udp** command in flow exporter map configuration mode. To remove a configured destination port, use the **no** form of this command.

transport udp *port*

no transport udp *port*

Syntax Description	<i>port</i>	Destination port for UDP packets. Replace <i>port</i> with the destination port value. Range is from 1024 through 65535.

Defaults	No default behavior or values

Command Modes	Flow exporter map configuration

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
	Release 3.4.0	This command was moved to the flow exporter map configuration mode.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	netflow	read, write

Examples	The following example shows how to configure the destination port for UDP packets:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# flow exporter-map map1
RP/0/RP0/CPU0:router(config-fem)# transport udp 1030
```

R3.5.0 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	flow exporter-map	Creates and configures a flow exporter map.
	flow monitor-map	Configures a flow monitor map and associates an exporter map with a monitor map.
	show flow exporter	Displays flow exporter data.
	show flow exporter-map	Displays flow exporter map information for a specific node installed in the router.

R3.5.0 Beta Draft—Cisco Confidential Information

version v9

To enter flow exporter map version configuration submode so that you can configure export version parameters, enter the **version v9** command in flow exporter map configuration mode. To remove the current export version configuration and return to the default configuration, use the **no** form of this command.

version v9

no version v9

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values

Command Modes	Flow exporter map configuration

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1.
	Release 3.3.0	This feature was first supported on the Cisco XR 12000 Series Router.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.

When you issue the **version v9** command, the CLI prompt changes to “config-fem-ver,” indicating that you have entered flow exporter map version configuration submode. In the following sample output, the question mark (?) online help function displays all the commands available under flow exporter map version configuration submode:

```
RP/0/RP0/CPU0:router(config-fem)# version v9
```

```
RP/0/RP0/CPU0:router(config-fem-ver)#?
```

```
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
options     Specify export of options template
show        Show contents of configuration
template    Specify template export parameters
```

R3.5.0 Beta Draft—Cisco Confidential Information**Task ID**

Task ID	Operations
netflow	read, write

Examples

The following example shows how to enter flow exporter map version configuration submode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# flow exporter-map map1
RP/0/RP0/CPU0:router(config-fem)# version v9
RP/0/RP0/CPU0:router(config-fem-ver)#
```

Related Commands

Command	Description
flow exporter-map	Creates and configures a flow exporter map.
flow monitor-map	Configures a flow monitor map and associates an exporter map with a monitor map.
show flow exporter	Displays flow exporter data.
show flow exporter-map	Displays flow exporter map information for a specific node installed in the router.



INDEX

HR	Cisco IOS XR Interface and Hardware Component Command Reference
IR	Cisco IOS XR IP Addresses and Services Command Reference
MCR	Cisco IOS XR Multicast Command Reference
MNR	Cisco IOS XR System Monitoring Command Reference
MPR	Cisco IOS XR MPLS Command Reference
QR	Cisco IOS XR Modular Quality of Service Command Reference
RR	Cisco IOS XR Routing Command Reference
SBR	Cisco IOS XR Session Border Controller Command Reference
SMR	Cisco IOS XR System Management Command Reference
SR	Cisco IOS XR System Security Command Reference

A

address-family ipv4 unicast (BFD) command [HR-918](#)
ais-shut (SONET) command [HR-322](#)
ais-shut (SONET path) command [HR-324](#)
aps group command [HR-326](#)
asic-scan pse command [HR-244](#)
atm address-registration command [HR-712](#)
atm ilmi-config disable command [HR-713](#)
atm ilmi-keepalive command [HR-715](#)
atm maxvpi-bits 12 command [HR-717](#)
atm oam flush command [HR-721](#)
authenticate (PGP) command [HR-328](#)

B

bandwidth (global) command [HR-546](#)
bert e1 command [HR-398](#)
bert e3 command [HR-400](#)
bert error command [HR-402](#)
bert interval command [HR-404](#)
bert pattern command [HR-406](#)
bert t1 command [HR-408](#)
bert t3 command [HR-410](#)

bfd command [HR-920](#)
bfd fast-detect (BGP) command [HR-922](#)
bfd minimum-interval command [HR-924](#)
bfd multiplier command [HR-927](#)
bundle command [HR-840](#)
bundle id command [HR-806](#)
bundle maximum-active links command [HR-808](#)
bundle minimum-active bandwidth command [HR-811](#)
bundle minimum-active links command [HR-812](#)
bundle port-priority command [HR-814](#)

C

cablelength command [HR-412](#)
cache entries command [HR-952](#)
cache permanent command [HR-954](#)
cache timeout command [HR-956](#)
carrier-delay command [HR-640](#)
ce tftp server command [HR-10](#), [HR-12](#)
channel-group command [HR-414](#)
channel local command [HR-330](#)
channel remote command [HR-332](#)
class-int command [HR-725](#)
class-vc command [HR-727](#)
clear bfd counters command [HR-929](#)
clear controller egressq queue all command [HR-248](#)
clear controller egressq queue command [HR-246](#)
clear controller egressq statistics command [HR-250](#)
clear controller fabricq statistics command [HR-157](#)
clear controller fabric statistics command [HR-156](#)
clear controller ingressq command [HR-159](#)
clear controller pse statistics command [HR-251](#)
clear controller switch command [HR-161](#)
clear controller switch errdisable command [HR-162](#)
clear controller switch inter-rack command [HR-163](#)

R3.5.0 Beta Draft—Cisco Confidential Information

clear counters sonet command [HR-334](#)
clear fabricq counters command [HR-165](#)
clear flow exporter command [HR-958](#)
clear flow monitor command [HR-960](#)
clear flow platform producer statistics location command [HR-962](#)
clear interface command [HR-548](#)
clear lacp counters command [HR-816](#)
clear mac-accounting command [HR-642](#)
clear mbus-statistics location command [HR-11](#)
clear srp counters command [HR-598](#)
clock source (SONET) command [HR-336](#)
clock source (T1/E1 controller) command [HR-416](#)
clock source (T3/E3 controller) command [HR-418](#)
controller (SONET) command [HR-338](#)
controller dwdm command [HR-482, 532, 534](#)
controller e1 command [HR-420](#)
controller e3 command [HR-422](#)
controllers fabric plane command [HR-167](#)
controllers fabric plane shutdown command [HR-169](#)
controllers fabric rack command [HR-170](#)
controllers fabric statistics collection command [HR-171](#)
controller t1 command [HR-424](#)
controller t3 command [HR-426](#)
crc (serial) command [HR-694](#)
crc command (POS) [HR-582](#)

D

dampening command [HR-550](#)
delay trigger command [HR-340](#)
destination command [HR-963](#)
diagnostic bootup level command [HR-12](#)
diagnostic load command [HR-14](#)
diagnostic monitor command [HR-16](#)
diagnostic monitor interval command [HR-18](#)
diagnostic monitor syslog command [HR-20](#)
diagnostic monitor threshold command [HR-21](#)
diagnostic ondemand action-on-failure command [HR-23](#)

diagnostic ondemand iterations command [HR-25](#)
diagnostic schedule command [HR-26](#)
diagnostic start command [HR-28](#)
diagnostic stop command [HR-30](#)
diagnostic unload command [HR-32](#)
dot1q native vlan command [HR-674](#)
dot1q tunneling ethertype 0x9100 command [HR-676](#)
dot1q vlan command [HR-678](#)
dscp command [HR-965](#)
dsc serial command [HR-34](#)
dsu bandwidth command [HR-428](#)
dsu mode command [HR-430](#)
dsu remote command [HR-432](#)
duplex (Management Ethernet) command [HR-572](#)
duplex full (Fast Ethernet) command [HR-644](#)
duplex half (Fast Ethernet) command [HR-646](#)

E

echo disable command [HR-931](#)
encap (PVC) command [HR-884](#)
encapsulation (ATM) command [HR-729](#)
encapsulation command (POS) [HR-584](#)
encapsulation command (serial) [HR-696](#)
encapsulation frame-relay command [HR-886](#)
encapsulation ppp command [HR-842](#)
env disable command [HR-36](#)
env power-supply command [HR-38](#)
exporter command [HR-967](#)

F

f4oam disable command [HR-732](#)
facility-alarm contacts command [HR-40](#)
fdl ansi command [HR-434](#)
flow command [HR-969](#)
flow-control command [HR-648](#)
flow exporter-map command [HR-971](#)

R3.5.0 Beta Draft—Cisco Confidential Information

[flow monitor-map command](#) [HR-973](#)
[force command](#) [HR-341](#)
[frame-relay intf-type command](#) [HR-888](#)
[frame-relay lmi disable command](#) [HR-889](#)
[frame-relay lmi-n391dte command](#) [HR-890](#)
[frame-relay lmi-n392dce command](#) [HR-891](#)
[frame-relay lmi-n392dte command](#) [HR-893](#)
[frame-relay lmi-n393dce command](#) [HR-894](#)
[frame-relay lmi-n393dte command](#) [HR-896](#)
[frame-relay lmi-t391dte command](#) [HR-897](#)
[frame-relay lmi-t392dce command](#) [HR-898](#)
[frame-relay lmi-type command](#) [HR-899](#)
[framing \(E1\) command](#) [HR-436](#)
[framing \(E3\) command](#) [HR-438](#)
[framing \(SONET\) command](#) [HR-343](#)
[framing \(T1\) command](#) [HR-440](#)
[framing \(T3\) command](#) [HR-442](#)

G

[g709 bdi-to-client-gais command](#) [HR-484](#)
[g709 disable command](#) [HR-486](#)
[g709 fec command](#) [HR-487](#)
[g709 odu report command](#) [HR-489](#)
[g709 odu threshold command](#) [HR-494](#)
[g709 otu report command](#) [HR-491, HR-492](#)
[g709 otu threshold command](#) [HR-496](#)

H

[hw-module boot override command](#) [HR-42](#)
[hw-module location command](#) [HR-44](#)
[hw-module port command](#) [HR-47, HR-602](#)
[hw-module power command](#) [HR-49](#)
[hw-module power disable command](#) [HR-51](#)
[hw-module reset auto command](#) [HR-53](#)
[hw-module reset auto disable command](#) [HR-56](#)
[hw-module shutdown command](#) [HR-58](#)

[hw-module subslot cardtype command](#) [HR-443](#)
[hw-module subslot reload command](#) [HR-60](#)
[hw-module subslot shutdown command](#) [HR-61](#)

[interface \(BFD\) command](#) [HR-933](#)
[interface \(global\) command](#) [HR-552](#)
[interface \(VLAN\) command](#) [HR-681](#)
[interface atm command](#) [HR-734](#)
[interface Bundle-Ether command](#) [HR-818](#)
[interface Bundle-POS command](#) [HR-819](#)
[interface FastEthernet command](#) [HR-650](#)
[interface GigabitEthernet command](#) [HR-652](#)
[interface MgmtEth command](#) [HR-574](#)
[interface null 0 command](#) [HR-800](#)
[interface pos command](#) [HR-586](#)
[interface serial command](#) [HR-698](#)
[interface srp command](#) [HR-604](#)
[interface TenGigE command](#) [HR-654](#)
[invert command](#) [HR-702](#)

K

[keepalive command \(POS\)](#) [HR-588](#)
[keepalive command \(serial\)](#) [HR-700](#)

L

[l2protocol \(Ethernet\) command](#) [HR-656](#)
[l2protocol \(VLAN\) command](#) [HR-683](#)
[l2transport \(Ethernet\) command](#) [HR-658](#)
[lacp period short command](#) [HR-820](#)
[lacp system-priority command](#) [HR-821](#)
[laser command](#) [HR-498](#)
[led mode command](#) [HR-63](#)
[lockout command](#) [HR-345](#)
[loopback \(DWDM\) command](#) [HR-499](#)

R3.5.0 Beta Draft—Cisco Confidential Information

loopback (Ethernet) command [HR-660](#)
 loopback (SONET) command [HR-347](#)
 loopback (T1/E1) command [HR-446](#)
 loopback (T3/E3) command [HR-448](#)

M

mac-accounting command [HR-662](#)
 mac-address (Ethernet) command [HR-664](#)
 mac-address (Management Ethernet) command [HR-576](#)
 manual command [HR-349](#)
 match frame-relay dlci command [HR-900](#)
 mdl command [HR-450](#)
 mode command [HR-452](#)
 mtu command [HR-554](#)
 multilink command [HR-844](#)
 multilink fragment-size command [HR-846](#)
 multilink group command [HR-848](#)

N

national bits (E1) command [HR-454](#)
 national bits (E3) command [HR-455](#)
 negotiation auto command [HR-666](#)

O

oam ais-rdi command [HR-740](#)
 oam-pvc manage command [HR-742](#)
 oam retry command [HR-745](#)
 options command [HR-975](#)
 overhead (SONET) command [HR-351](#)
 overhead (SONET path) command [HR-353](#)

P

packet-gap non-standard command [HR-667](#)
 path (SONET) command [HR-355](#)

ping (administration EXEC) command [HR-65](#)
 ping atm interface atm command [HR-748](#)
 pm fec report command [HR-500](#)
 pm fec threshold command [HR-502](#)
 pm optics report command [HR-504](#)
 pm optics threshold command [HR-506](#)
 pm otn report command [HR-508](#)
 pm otn threshold command [HR-511](#)
 pos command [HR-590](#)
 ppp authentication command [HR-850](#)
 ppp chap password command [HR-853](#)
 ppp chap refuse command [HR-855](#)
 ppp max-bad-auth command [HR-857](#)
 ppp max-configure command [HR-859](#)
 ppp max-failure command [HR-861](#)
 ppp max-terminate command [HR-863](#)
 ppp ms-chap password command [HR-865](#)
 ppp ms-chap refuse command [HR-867](#)
 ppp multilink minimum-active links command [HR-869](#)
 ppp pap refuse command [HR-870](#)
 ppp pap sent-username password command [HR-872](#)
 ppp timeout authentication command [HR-874](#)
 ppp timeout retry command [HR-876](#)
 pvc (ATM) command [HR-703](#), [HR-750](#)
 pvc (Frame Relay) command [HR-901](#)

R

random 1 out-of command [HR-977](#)
 record ipv4 command [HR-979](#), [HR-981](#)
 record mpls command [HR-983](#)
 redundancy reddrv command [HR-68](#)
 redundancy switchover command [HR-70](#)
 report (SONET) command [HR-357](#)
 report (SONET path) command [HR-359](#)
 revert command [HR-361](#)
 RFC 1406, Definitions of Managed Objects for DS1 and E1 Interface Types [HR-466](#)
 rx-los-threshold command [HR-513](#)

R3.5.0 Beta Draft—Cisco Confidential Information

S

- sampler-map command [HR-985](#)
- scramble command [HR-705](#)
- scrambling disable (SONET path) command [HR-363](#)
- serial command [HR-707](#)
- shape command [HR-756](#)
- show aps agents command [HR-368](#)
- show aps command [HR-365](#)
- show aps group command [HR-370](#)
- show atm class-link command [HR-761](#)
- show atm ilmi-status command [HR-764](#)
- show atm interface atm command [HR-767](#)
- show atm pvc command [HR-772](#)
- show atm vc-class command [HR-783](#)
- show atm vp-tunnel command [HR-786](#)
- show bfd all command [HR-937](#)
- show bfd client command [HR-939](#)
- show bfd command [HR-935](#)
- show bfd counters packet command [HR-941](#)
- show bfd ipv4 command [HR-943](#)
- show bfd location command [HR-945](#)
- show bfd session command [HR-946](#)
- show bundle Bundle-Ether command [HR-822](#)
- show bundle Bundle-POS command [HR-825](#)
- show controller dwdm command [HR-515, 538](#)
- show controller dwdm pm command [HR-521](#)
- show controllers atm command [HR-788](#)
- show controllers cpuctrl cdma command [HR-253](#)
- show controllers cpuctrl clients command [HR-256](#)
- show controllers cpuctrl devices command [HR-259](#)
- show controllers cpuctrl internal command [HR-263](#)
- show controllers cpuctrl ports command [HR-266](#)
- show controllers cpuctrl summary command [HR-269](#)
- show controllers e1 command [HR-456](#)
- show controllers e3 command [HR-459](#)
- show controllers egressq eio links command [HR-272](#)
- show controllers egressq group command [HR-274](#)
- show controllers egressq interface command [HR-277](#)
- show controllers egressq port command [HR-281](#)
- show controllers egressq queue command [HR-283](#)
- show controllers egressq statistics command [HR-286](#)
- show controllers fabric bundle command [HR-174](#)
- show controllers fabric command [HR-172](#)
- show controllers fabric connectivity command [HR-176](#)
- show controllers fabric fgid resource command [HR-178](#)
- show controllers fabric fgid statistics command [HR-180](#)
- show controllers fabric fsdb-pla all command [HR-183](#)
- show controllers fabric link port command [HR-185](#)
- show controllers fabric plane command [HR-188](#)
- show controllers fabricq drop command [HR-195](#)
- show controllers fabricq errors command [HR-199](#)
- show controllers fabricq fabric-backpressure command [HR-201](#)
- show controllers fabricq frfab command [HR-204](#)
- show controllers fabricq output command [HR-207](#)
- show controllers fabricq queue command [HR-212](#)
- show controllers fabricq registers command [HR-215](#)
- show controllers fabricq statistics command [HR-210](#)
- show controllers fabricq tofab command [HR-218](#)
- show controllers fabric rack all command [HR-192](#)
- show controllers fabric sfe command [HR-193](#)
- show controllers ingressq statistics command [HR-220, HR-289](#)
- show controllers null interface command [HR-802](#)
- show controllers plim asic command [HR-291](#)
- show controllers pos command [HR-372](#)
- show controllers pse eio links command [HR-296](#)
- show controllers pse ipc command [HR-299](#)
- show controllers pse mp command [HR-304](#)
- show controllers pse statistics command [HR-309](#)
- show controllers pse summary command [HR-315](#)
- show controllers sonet command [HR-378](#)
- show controllers srp command [HR-606](#)
- show controllers switch command [HR-222](#)
- show controllers switch inter-rack ports command [HR-224](#)
- show controllers switch inter-rack statistics command [HR-226](#)
- show controllers switch inter-rack stp command [HR-229](#)

R3.5.0 Beta Draft—Cisco Confidential Information

- show controllers switch inter-rack uddl command [HR-231](#)
- show controllers switch stp location command [HR-233](#)
- show controllers switch stp ports command [HR-236](#)
- show controllers switch stp region command [HR-238](#)
- show controllers switch uddl location command [HR-239](#)
- show controllers switch uddl ports command [HR-241](#)
- show controllers t1 command [HR-463](#)
- show controllers t3 command [HR-467](#)
- show diag command [HR-73](#)
- show diagnostic bootup level command [HR-80](#)
- show diagnostic content command [HR-82](#)
- show diagnostic result command [HR-85](#)
- show diagnostic schedule command [HR-87](#)
- show diags command [HR-77](#)
- show dsc command [HR-89](#)
- show environment command [HR-91](#)
- show facility-alarm contacts command [HR-94](#)
- show flow exporter command [HR-987](#)
- show flow exporter-map command [HR-990](#)
- show flow monitor command [HR-993](#)
- show flow monitor-map command [HR-1012](#)
- show flow platform producer statistics location command [HR-1015](#)
- show fmgr interface command [HR-96](#)
- show fpd package command [HR-99](#)
- show frame-relay lmi command [HR-903](#)
- show frame-relay pvc command [HR-906](#)
- show hw-module fpd command [HR-103](#)
- show hw-module subslot brief command [HR-106](#)
- show hw-module subslot config command [HR-109](#)
- show hw-module subslot counters command [HR-112](#)
- show hw-module subslot errors command [HR-115](#)
- show hw-module subslot registers command [HR-117](#)
- show hw-module subslot status command [HR-119](#)
- show im dampening command [HR-557](#)
- show interfaces (frame relay) command [HR-909](#)
- show interfaces command [HR-560](#)
- show interfaces pos command [HR-592](#)
- show inventory command [HR-121](#)
- show lacp bundle command [HR-828](#)
- show lacp counters command [HR-831](#)
- show lacp port command [HR-833](#)
- show lacp system-id command [HR-836](#)
- show led command [HR-124](#)
- show mac-accounting (Ethernet) command [HR-669](#)
- show mbus command [HR-126](#)
- show packet-memory command [HR-318](#)
- show platform command [HR-129](#)
- show ppp interfaces command [HR-878](#)
- show redundancy command [HR-131](#)
- show sampler-map command [HR-1017](#)
- show screddrv command [HR-134](#)
- show srp command [HR-608](#)
- show srp counters [HR-608](#)
- show srp source-counters [HR-608](#)
- show version command [HR-136](#)
- show vlan interface command [HR-685](#)
- show vlan tags command [HR-688](#)
- show vlan trunks command [HR-690](#)
- shutdown (DWDM) command [HR-525](#)
- shutdown (global) command [HR-568](#)
- shutdown (SONET) command [HR-384](#)
- shutdown (T1/E1) command [HR-472](#)
- shutdown (T3/E3) command [HR-474](#)
- shutdown command [HR-792](#)
- signalling command [HR-386](#)
- snmp-server traps frame-relay pvc command [HR-914](#)
- source (NetFlow) command [HR-1019](#)
- speed (DS0) command [HR-476](#)
- speed (Fast Ethernet) command [HR-671](#)
- speed (Management Ethernet) command [HR-578](#)
- srp ips delay trigger-keepalive command [HR-619](#)
- srp ips request [HR-621, HR-631](#)
- srp ips request forced-switch [HR-621, HR-631](#)
- srp ips request forced-switch command [HR-621](#)
- srp ips timer command [HR-623](#)
- srp ips wtr-timer command [HR-625](#)
- srp mac-count command [HR-627](#)

R3.5.0 Beta Draft—Cisco Confidential Information

srp mac-reject command [HR-629](#)
srp manual-switch command [HR-631](#)
srp shutdown command [HR-635](#)
srp topology-timer command [HR-637](#)

Y

yellow command [HR-480](#)

T

template command [HR-1021](#)
threshold (SONET) command [HR-390](#)
threshold (SONET path) command [HR-392](#)
timers (APS) command [HR-388](#)
timeslots command [HR-478](#)
transmit-delay (POS) command [HR-595](#)
transmit-delay (serial) command [HR-708](#)
transmit-power command [HR-526](#)
transport udp command [HR-1023](#)

U

uneq-shut (SONET path) command [HR-394](#)
unidirectional command [HR-395](#)
upgrade all command [HR-140](#)
upgrade cpuctrlbits command [HR-142](#)
upgrade fabric-downloader command [HR-144](#)
upgrade hw-module fpd command [HR-146](#)
upgrade mbus command [HR-149](#)
upgrade rommon (Cisco CRS-1) command [HR-151](#)
upgrade rommon (Cisco XR 12000 Series Router)
command [HR-153](#)

V

vc-class atm command [HR-794](#)
version v9 command [HR-1025](#)
vp-tunnel command [HR-796](#)

W

wavelength command [HR-528](#)