Cisco ASR 14000 Series Router Interface and Hardware Component Command Reference

Cisco IOS XR Software Release 3.7.1

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-17228-01

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.

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.

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.

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 ASR 14000 Series Router Interface and Hardware Component Command Reference

Preface

The *Cisco ASR 14000 Series Router Interface and Hardware Component Command Reference* provides information about commands related to router interface and hardware configuration.

The preface contains the following sections:

- Changes to This Document, page HR-iii
- Obtaining Documentation and Submitting a Service Request, page HR-iii

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-17228-01	October 2008	Initial release of this document.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Bidirectional Forwarding Detection Commands on Cisco IOS XR Software

This module describes the commands used to configure and monitor Bidirectional Forwarding Detection (BFD).

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

address	IPv4 unicast destination address and prefix on which to enable BFD fast-detection.
nexthop	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 *interval*	(Optional) Ensures that the next hop is assigned with the same hello interval. Replace *interval* with a number that specifies the interval in milliseconds. Range is from 15 through 5000.
multiplier *multiplier*	(Optional) Ensures that the next hop is assigned with the same detect multiplier. Replace *multiplier* with a number that specifies the detect multiplier. Range is from 2 through 10.

Defaults

interval: 100

multiplier: 3

Command Modes

Static route configuration mode

Command History.

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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
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	Displays BFD 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
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	Displays BFD 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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	Displays BFD 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

milliseconds	Interval between sending BFD packets to the neighbor. The following ranges are listed: – BGP—15 to 30000 milliseconds. – IS-IS—15 to 5000 milliseconds. – MPLS-TE—15 to 200 milliseconds. – OSPF—15 to 30000 milliseconds.

Defaults

BGP *interval* = 50 milliseconds

IS-IS *interval* = 150 milliseconds

OSPF *interval* = 150 milliseconds

MPLS-TE *interval* = 15 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

Router PIM interface configuration mode

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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, 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, 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.

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
```

Related Commands

Command	Description
bfd fast-detect	Enables BFD for communication failure detection.
bfd multiplier	Sets the BFD multiplier.
show bfd	Displays BFD 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

multiplier	Number of times a packets is missed before BFD declares the neighbor down. The following ranges are listed: • BGP—2 to 16 • IS-IS—2 to 50 • MPLS-TE—2 to 10 • OSPF—2 to 50

Defaults

multiplier = 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

Router PIM interface configuration mode

Command History.

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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	Displays BFD information.

clear bfd counters

To clear Bidirectional Forwarding Detection (BFD) counters, use the **clear bfd counters** command in EXEC mode.

clear bfd counters [**ipv4** | **ipv6** | **all**] [**packet**] [**timing**] [**interface** *type interface-path-id*] **location** *node-id*

Syntax Description

ipv4	(Optional) Clears BFD over IPv4 information only.
ipv6	(Optional) Clears BFD over IPv6 information only.
all	(Optional) Clears both BFD over IPv4 and BFD over IPv6 information.
packet	(Optional) Specifies that packet counters will be cleared.
timing	(Optional) Specifies that timing counters will be cleared.
interface	(Optional) Specifies the interface from which the BFD packet counters will be cleared.
type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location *node-id*	Clears BFD counters from the specified location.

Defaults

The default is the default address family identifier (AFI) that is set by the **set default-afi** command, IPv4 or IPv6.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

Both IPv4 and IPv6 BFD sessions can run simultaneously on the same line card.

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 clear the BFD IPv6 packet counters on a Packet over SONET (POS) interface:

```
RP/0/RP0/CPU0:router# clear bfd counters packet ipv6 interface POS 0/1/0/0 location 
0/1/cpu0
```

The following example shows how to clear the BFD IPv6 timing counters:

```
RP/0/RP0/CPU0:router# clear bfd counters ipv6 timing 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	Displays BFD 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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

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	Displays BFD 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 interface-path-id*

no interface *type interface-path-id*

Syntax Description

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

Defaults

.No default behavior or values

Command Modes

BFD configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

For the bundle ID for a POS or Ethernet bundle, the range is from 1 through 65535.

If you are using BFD with Unicast Reverse Path Forwarding (uRPF) on a particular interface, 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	Displays BFD information.

show bfd

To display Bidirectional Forwarding Detection (BFD) information for a specific location, use the **show bfd** command in EXEC mode.

show bfd [**ipv4** | **ipv6** | **all**] [**location** *node-id*]

Syntax Description

ipv4	(Optional) Displays BFD over IPv4 information only.
ipv6	(Optional) Displays BFD over IPv6 information only.
all	(Optional) Displays both BFD over IPv4 and BFD over IPv6 information.
location *node-id*	Displays BFD information for the specified location.

Defaults

The default is the default address family identifier (AFI) that is set by the **set default-afi** command, IPv4 or IPv6.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
bgp	read
ospf	read
isis	read
mpls-te	read

Examples

The following example shows the output from the **show bfd** command:

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

IPV4 Sessions Up: 0, Down: 0, Total: 0
```

The following example shows the 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
```

The following example shows the output from the **show bfd ipv4** command:

```
RP/0/RP0/CPU0:router# show bfd ipv4

IPV4 Sessions Up: 0, Down: 0, Total: 0
```

The following example shows the output from the **show bfd ipv6** command:

```
RP/0/RP0/CPU0:router# show bfd ipv6

IPV4 Sessions Up: 0, Down: 0, Total: 0
```

The following example shows the output from the **show bfd ipv4 location** command:

```
RP/0/RP0/CPU0:router# show bfd ipv4 location 0/3/cpu0

IPV4 Sessions Up: 0, Down: 1, Standby: 0, Total: 1
```

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 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) Displays detailed client information including number of sessions and client reconnects.

Defaults

Use the **show bfd client** command without specifying the **detail** keyword to display summarized BFD client information.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
bgp	read
ospf	read
isis	read
mpls-te	read

Examples

The following example shows the 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
```

Table 1 describes the significant fields shown in the display.

Table 1 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	Displays BFD information.

show bfd counters

To display Bidirectional Forwarding Detection (BFD) counter information, use the **show bfd counters** command in EXEC mode.

show bfd counters [**ipv4** | **ipv6** | **all**] **packet** [**interface** *type interface-path-id*] **location** *node-id*

Syntax Description

ipv4	(Optional) Displays BFD over IPv4 information only.
ipv6	(Optional) Displays BFD over IPv6 information only.
all	(Optional) Displays both BFD over IPv4 and BFD over IPv6 information.
packet	Specifies that packet counters are displayed.
interface	(Optional) Specifies the interface for which to show counters.
type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location *node-id*	Displays BFD counters from the specified location.

Defaults

The default is the default address family identifier (AFI) that is set by the **set default-afi** command, IPv4 or IPv6.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
bgp	read
ospf	read
isis	read
mpls-te	read

Examples

The following sample output shows both IPv4 and IPv6:

```
RP/0/RP0/CPU0:router# show bfd counters packet all interface POS 0/1/0/0 location 0/1/cpu0

Mon Nov  5 08:49:51.950 UTC
IPv4:
-----
 POS 0/1/0/0             Recv       Xmit                 Recv       Xmit
      Async:             520        515       Echo:      9400       9400

IPv6:
-----
 POS 0/1/0/0             Recv       Xmit                 Recv       Xmit
      Async:             237        237       Echo:         0          0
```

Table 2 describes the significant fields shown in the display.

Table 2 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	Displays BFD information.

show bfd session

To display Bidirectional Forwarding Detection (BFD) session information, use the **show bfd session** command in EXEC mode.

show bfd session [**ipv4** | **ipv6** | **all**] [**interface** *type interface-path-id* [**destination** *ip-address*] [**detail**]] [**location** *node-id*]

Syntax Description

ipv4	(Optional) Displays BFD over IPv4 information only.
ipv6	(Optional) Displays BFD over IPv6 information only.
all	(Optional) Displays both BFD over IPv4 and BFD over IPv6 information.
interface	(Optional) Specifies an interface.
type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
destination *ip-address*	(Optional) Displays the BFD session destined for the specified IP address.
detail	(Optional) Displays detailed session information, including statistics and number of state transitions.
location *node-id*	(Optional) Displays BFD sessions hosted from the specified location.

Defaults

The default is the default address family identifier (AFI) that is set by the **set default-afi** command, IPv4 or IPv6.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
bgp	read
ospf	read

Task ID	Operations
isis	read
mpls-te	read

Examples

The following sample output is from the **show bfd session** command with the **detail** keyword and IPv4 as the default:

```
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
```

The following sample output is from the **show bfd session** command with the **all** keyword, which displays both IPv4 and IPv6 information:

```
RP/0/RP0/CPU0:router# show bfd all session location 0/1/CPU0

Mon Nov  5 08:51:50.339 UTC
IPv4:
-----
Interface            Dest Addr           Local det time(int*mult)      State
                                           Echo            Async
-------------------- --------------- ---------------- ---------------- ---------
PO0/1/0/0            10.0.0.2        300ms(100ms*3)   6s(2s*3)         UP

IPv6:
-----
Interface            Dest Addr
                     Local det time(int*mult)          State
                            Echo            Async
```

```
-------------------- -----------------------------------------------
PO0/1/0/0            abcd::2
                     0s(0s*0)          15s(5s*3)        UP
```

Table 3 describes the significant fields shown in the display.

Table 3 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 *rack/slot/module* 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	Following information is listed 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	Following information is listed 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.

Table 3 show bfd session detail command Field Descriptions (continued)

Field	Description
Timer Values	Following information is listed on the timer values used by the local and remote ends: • 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	Following information is listed about 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 two consecutive control packets – max—Maximum measured interval between two consecutive control packets – avg—Average measured interval between two 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; that is, the time between tx and rx of echo packets: – Number of packets—Number of sampled echo packets. – min—Minimum measured latency of echo packets. – max—Maximum measured latency of echo packets. – avg—Average measured latency of echo packets.
Session owner information	Following information is listed 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.

Command	Description
bfd minimum-interval	Sets the BFD interval.
bfd multiplier	Sets the BFD multiplier.

Diagnostics Commands on Cisco IOS XR Software

This module describes the commands used to manage diagnostics on a router running Cisco IOS XR software.

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.

Defaults

The default bootup diagnostics level is minimal.

Command Modes

Administration configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

Note 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.

Note To specify a physical layer interface module (PLIM) node using the *node-id* argument, use the following notation: *rack*/PL*slot-number*/SP. For example, 0/PL1/SP. PLIM diagnostic tests are supported.

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.

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 *node-id*	Loads an offline diagnostic image for a specified location. 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **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.

Note After the diagnostic image is loaded, use the **diagnostic start location** *node-id* **test** {*id* | **all** | **basic** | **non-disruptive**} command to execute the tests.

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
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/asr14k-diag-l3sp-fdiags
Downloading IDS diagnostics image /pkg/ucode/asr14k-diag-l3-fdiags
Please wait for UUT image downloading ...
diagnostic load in progress.
```

Related Commands

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

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

node-id	Location to enable diagnostic monitoring.
test {*id* | *test-name*}	Specifies diagnostic test selection. The following test selections are available: • *id*—Test ID, as shown in the **show diagnostic content** command. • *test-name*—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 may be different for each test.

Command Modes

Administration configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **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 that is enabled by default. For example, if test 1 is enabled 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 enabled.

Note To specify a physical layer interface module (PLIM) node using the *node-id* argument, use the following notation: *rack*/PL*slot-number*/SP. For example, 0/PL1/SP. PLIM diagnostic tests are supported.

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.

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 *node-id*	Specifies a location.
test {*id* | *test-name*}	Specifies diagnostic test selection. The following test selections are available: • *id*—Test ID. • *test-name*—Test name, as shown in the **show diagnostic content** command.
number-of-days hour:*minutes*:*seconds.milliseconds*	Interval between each test run. The *number-of-days* argument specifies the number of days between testing. The *hour:minutes:seconds.milliseconds* argument specifies the interval, where *hour* is a number in the range from 0 through 23, *minutes* is a number in the range from 0 through 59, *seconds* is a number in the range from 0 through 59, and *milliseconds* 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 may be different for each test.

Command Modes

Administration configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **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.

Note To specify a physical layer interface module (PLIM) node using the *node-id* argument, use the following notation: *rack*/PL*slot-number*/SP. For example, 0/PL1/SP. PLIM diagnostic tests are supported.

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 4 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.

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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **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.

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 *node-id*	Specifies a location.
test {*id* | *test-name*}	Specifies diagnostic test selection. The following test selections are available: • *id*—Test ID. • *test-name*—Test name, as shown in the **show diagnostic content** command.
failure count *failures*	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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **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*/PL*slot-number*/SP. For example, 0/PL1/SP. PLIM diagnostic tests are supported.

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
all 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.

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 *failure-count*	Specifies that test execution continue until the number of failures reaches the specified *failure-count*. Range is 0 to 65534. A *failure-count* 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

failure-count: 0

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **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
```

Related Commands

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

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

count	Number of times to repeat the specified on-demand tests. Range is 1 to 999.

Defaults

count: 1

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **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:

```
RP/0/RP0/CPU0:router(admin)# diagnostic ondemand iterations 12
```

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 for the number of iterations set by the diagnostic ondemand iterations command.

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 *node-id*	Schedules a diagnostic test for a specified location.
test	Specifies a specific diagnostic test, or all diagnostic tests.
id	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 *month day year*	Schedules an exact date.
weekly *day-of-week*	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 0 through 6.
hour:*minute*	Scheduled start time, where *hour* is a number in the range from 0 through 23, and *minute* 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **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*/PL*slot-number*/SP. For example, 0/PL1/SP. PLIM diagnostic tests are supported.

Task ID

Task ID	Operations
diag	read, write

Examples

The following example shows how to schedule a diagnostic test:

```
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.

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 *node-id*	Runs diagnostic testing for a specified location.
test	Specifies a specific diagnostic test, or all diagnostic tests.
id	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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **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*/PL*slot-number*/SP. For example, 0/PL1/SP. PLIM diagnostic tests are supported.

Task ID

Task ID	Operations
diag	execute

Examples

The following example shows how to run a suite of basic diagnostic tests 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.

diagnostic stop

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

diagnostic stop location *node-id*

Syntax Description

location *node-id*	Stops diagnostic testing for a specified location.

Defaults

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **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*/PL*slot-number*/SP. For example, 0/PL1/SP. PLIM diagnostic tests are supported.

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
```

Related Commands

Command	Description
diagnostic start	Runs specified diagnostic tests for the number of iterations set by the diagnostic ondemand iterations command.

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 *node-id*	Unloads an offline diagnostic image for a specified location. 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **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.

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

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

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 *pings*	(Optional) Configures the 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 *milliseconds*	(Optional) Hold-off time between each ping in milliseconds. Range is from 0 through 4294967295. The total test time will be as follows: (count-1) * (RTT + interval) + RTT RTT = Round Trip Time for the ping.
pattern random	(Optional) Specifies a data pattern for the ping packet payload.
retries *number*	(Optional) Configures the 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 *payload_size*	(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 *seconds*	(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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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:

```
(received_packet_count * RTT + lost_packet_count * timeout + (count-1) * 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
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
```

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 administration EXEC mode:

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

Syntax Description

node-id	(Optional) Node whose information you want to display. Follow the *node-id* 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

Administration EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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:

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

MAIN:  board type 500066
        800-27067-03 rev 14
        dev 090074
        S/N SAD11170518
 PCA:   73-10334-03 rev 14
 PID:   ASR14K-FP40
 VID:   V01
 CLEI:
 ECI:   123460
 RMA:   Test Hist: ab, RMA#: 00-00-00, RMA Hist: 00
 DIAGNOSTICS RESULTS:
   ENTRY 1: 24
     TIMESTAMP: 02/14/2008 14:00:38
     VERSION: v6.7
     PARAM1: 25      PARAM2: n/a
     TESTNUM: 0
     RESULT: 0 (PASS)
     ERRCODE: 0
   ENTRY 2: 25
     TIMESTAMP: 09/09/2008 18:25:57
     VERSION: v7.0
     PARAM1: 1      PARAM2: n/a
     TESTNUM: 0
     RESULT: 0 (PASS)
     ERRCODE: 0
   ENTRY 3: 23
     TIMESTAMP: 02/14/2008 14:00:29
     VERSION: v6.7
     PARAM1: 24      PARAM2: n/a
     TESTNUM: 0
     RESULT: 0 (PASS)
     ERRCODE: 0

PLIM 0/PL0/* : Cisco ASR14000 Series 20x1GE Flexible Interface Module
 MAIN:  board type 600116
        800-23819-05 rev A0
        dev N/A
        S/N SAD120401HC
 PCA:   73-8982-07 rev A0
 PID:   ASR14K-20XGE-FL
 VID:   V03
 CLEI:  COUIANKCAA
 ECI:   155804
 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
     VERSION: v0.0
     PARAM1: 0      PARAM2: n/a
     TESTNUM: 0
     RESULT: 0 (PASS)
     ERRCODE: 0
 Interface port config:  0 Ports
 Optical reach type:  Unknown
 Connector type:  MT-P

NODE 0/0/CPU0
 Node State : IOS XR RUN
 PLD:   Motherboard: 0x0015, Processor: 0x0015, Power: N/A
 MONLIB: QNXFFS Monlib Version 3.1
 ROMMON: Version 1.51(20080807:092259) [ASR 14000 ROMMON]
 CPU0:  ASMP,  CPU1:  N/A
 SPEED: OSC Speed:  150 Mhz, CPU Speed: 1500 Mhz
        BUS Speed:  133 Mhz, MEM Speed:  150 Mhz
 MEM Size: 2048 Mbytes

SPA 0/0/0 : 10-port 1 GbE Shared Port Adapter V2
 MAIN:  board type 0508
        68-2615-02 rev B0
        dev N/A
        S/N JAE1224L9HG
 PCA:   73-10420-02 rev B0
 PID:
 VID:   V02
 CLEI:  CNUIAWWAAA
 Node State : OK

SPA 0/0/1 : 4-port OC3/STM1 POS Shared Port Adapter
 MAIN:  board type 0440
        68-2169-01 rev J0
        dev N/A
        S/N JAE12046H52
 PCA:   73-9313-04 rev H0
 PID:   SPA-4XOC3-POS
 VID:   V01
 CLEI:  IPUIAFNRAA
 Node State : OK

SPA 0/0/2 : 10-port 1 GbE Shared Port Adapter V2
 MAIN:  board type 0508
        68-2615-02 rev B0
        dev N/A
        S/N JAE1222JPHR
 PCA:   73-10420-02 rev B0
 PID:
 VID:   V02
 CLEI:  CNUIAWWAAA
 Node State : OK

SPA 0/0/4 : 4-port OC48/STM16 POS/RPR Shared Port Adapter
 MAIN:  board type 0470
        68-2227-01 rev C0
        dev N/A
        S/N JAE1211BBEC
 PCA:   73-9090-06 rev C0
 PID:   SPA-4XOC48POS/RPR
 VID:   V01
 CLEI:  IPUIAXZRAA
 Node State : OK

CARD 0/1/* : Cisco ASR14000 Series Forwarding Processor 40G
 MAIN:  board type 500066
        800-27067-03 rev D0
        dev N/A
        S/N SAD12260391
 PCA:   73-10334-03 rev D0
 PID:   ASR14K-FP40
 VID:   V01
 CLEI:  IPUCALFBAA
 ECI:   154280
 RMA:   Test Hist: ab, RMA#: 00-00-00, RMA Hist: 00
 DIAGNOSTICS RESULTS:
   ENTRY 1: 51
     TIMESTAMP: 09/22/2008 23:31:19
     VERSION: v7.0
     PARAM1: 21      PARAM2: n/a
     TESTNUM: 0
     RESULT: 0 (PASS)
     ERRCODE: 0
   ENTRY 2: 52
     TIMESTAMP: 09/22/2008 23:34:16
     VERSION: v7.0
     PARAM1: 22      PARAM2: n/a
     TESTNUM: 0
     RESULT: 0 (PASS)
     ERRCODE: 0
   ENTRY 3: 53
     TIMESTAMP: 09/22/2008 23:34:18
     VERSION: v7.0
     PARAM1: 23      PARAM2: n/a
     TESTNUM: 0
     RESULT: 1 (FAIL)
     ERRCODE: 0
--More--
```

Table 4 describes the significant fields shown in the display.

Table 4 show diag Field Descriptions

Field	Description
MAIN	General information about the hardware is listed as follows: • Board type • Revision • Device identifier • S/N
PCA	Cisco PCA[1] hardware and revision number.
PID	PID[2] revision for the specified node.
VID	VID[3] for the specified node.
CLEI	CLEI[4] for the specified node.
ECI	ECI[5] for the specified node.

Table 4 show diag Field Descriptions (continued)

Field	Description
Board State	Current software on the board (in this case, Cisco IOS XR software) and whether or not the board is running.
PLD	Information about the following PLD[6] components on the current module: • Processor • Power • MONLIB
SPEED	Speed information for the various components of the specified node, in Mhz.
MEM Size	Memory size of the specified node, in megabytes.
RMA	RMA[7] information for the specified node.
DIAGNOSTICS RESULTS	Information about the last diagnostics test that was run on the specified node is listed as follows: • 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.

show diagnostic bootup level

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

show diagnostic bootup level location *node-id*

Syntax Description

location *node-id*	Specifies a card.

Defaults

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

Note There are no bootup diagnostic tests available. 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.

Note To specify a physical layer interface module (PLIM) node using the *node-id* argument, use the following notation: *rack*/PL*slot-number*/SP. For example, 0/PL1/SP. PLIM diagnostic tests are supported.

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

Command	Description
diagnostic bootup level	Specifies the diagnostic bootup level.

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 *node-id*	Displays the diagnostic content for a specified location.

Defaults

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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

Note To specify a physical layer interface module (PLIM) node using the *node-id* argument, use the following notation: *rack*/PL*slot-number*/SP. For example, 0/PL1/SP. PLIM diagnostic tests are supported.

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
      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

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

Table 5 describes the significant fields shown in the display.

Table 5 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.
diagnostic schedule	Schedules a diagnostic test.
diagnostic start	Runs specified diagnostic tests for the number of iterations set by the diagnostic ondemand iterations command.

show diagnostic ondemand settings

To display the current on-demand settings, use the **show diagnostic ondemand settings** command in administration EXEC mode.

show diagnostic ondemand settings

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
diag	read

Examples

The following example shows how to display the on-demand settings:

```
RP/0/RP0/CPU0:router(admin)# show diagnostic ondemand settings

Test iterations = 45
Action on test failure = continue until test failure limit reaches 25
```

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 *node-id*	Displays the diagnostic test results for a specified location.
test {*id* | **all**}	(Optional) Specifies diagnostic test selection. The following test selections are available: • *id*—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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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

Note To specify a physical layer interface module (PLIM) node using the *node-id* argument, use the following notation: *rack*/PL*slot-number*/SP. For example, 0/PL1/SP. PLIM diagnostic tests are supported.

Task ID

Task ID	Operations
diag	read

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 6 describes the significant fields shown in the display.

Table 6 show diagnostic result Field Descriptions

Field	Description
Test results:	Test result options: • .—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.
Last test failure time	Last time the test failed.
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	Runs specified diagnostic tests for the number of iterations set by the diagnostic ondemand iterations command.

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 *node-id*	Displays the diagnostic schedule for a specified location.

Defaults

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 diagnostic schedule** command to display scheduled diagnostic tasks for a specific location.

Note To specify a physical layer interface module (PLIM) node using the *node-id* argument, use the following notation: *rack*/PL*slot-number*/SP. For example, 0/PL1/SP. PLIM diagnostic tests are supported.

Task ID

Task ID	Operations
diag	read

Examples

The following example shows how to display scheduled diagnostic tasks:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# show diagnostic schedule location 0/3/CPU0

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 .
```

Table 7 describes the significant fields shown in the display.

Table 7 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.

show diagnostic status

To display the current running tests, use the **show diagnostic status** command in administration EXEC mode.

show diagnostic status

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
diag	read

Examples

The following example shows how to display the current running tests:

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

<BU> - Bootup Diagnostics, <HM> - Health Monitoring Diagnostics,
<OD> - OnDemand Diagnostics, <SCHD> - Scheduled Diagnostics

==================================== =============================== ======
Card   Description                   Current Running Test            Run by
------------------------------------ ------------------------------- ------
RP 0/RP0/CPU0                        N/A                             N/A

------------------------------------ ------------------------------- ------
FP40 0/1/CPU0                        N/A                             N/A

20-1GbE-FLX 0/PL1/SP                 N/A                             N/A

------------------------------------ ------------------------------- ------
FP40 0/6/CPU0                        N/A                             N/A

42-1GbE 0/PL6/SP                     N/A                             N/A

------------------------------------ ------------------------------- ------
```

```
FP40 0/0/CPU0                        N/A                             N/A

20-1GbE-FLX 0/PL0/SP                 N/A                             N/A

------------------------------------ ------------------------------- ------
FP40 0/5/CPU0                        N/A                             N/A

4-10GbE 0/PL5/SP                     N/A                             N/A

------------------------------------ ------------------------------- ------
FC/S 0/SM0/SP                        N/A                             N/A

------------------------------------ ------------------------------- ------
FC/S 0/SM1/SP                        N/A                             N/A

------------------------------------ ------------------------------- ------
FC/S 0/SM2/SP                        N/A                             N/A

------------------------------------ ------------------------------- ------
FC/S 0/SM3/SP                        N/A                             N/A

------------------------------------ ------------------------------- ------
FP40 0/5/SP                          N/A                             N/A

------------------------------------ ------------------------------- ------
FP40 0/0/SP                          N/A                             N/A

------------------------------------ ------------------------------- ------
FP40 0/1/SP                          N/A                             N/A

------------------------------------ ------------------------------- ------
FP40 0/6/SP                          N/A                             N/A

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

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

node-id	(Optional) Location for which to display the specified information.
device	(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.
device-index	(Optional) Index of the specific device if there are multiple devices of the same type.
device-subindex	(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

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 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/RP0/CPU0:router# show hw-module subslot brief

Subslot 0/0/0 brief info:
-----------------------
SPA inserted: YES
SPA type:     10xGE SPA
SPA operational state: READY
SPA cfg admin up: YES

Subslot 0/0/1 brief info:
-----------------------
SPA inserted: YES
SPA type:     4xOC3 POS SPA
SPA operational state: READY
SPA cfg admin up: YES

Subslot 0/0/2 brief info:
-----------------------
SPA inserted: YES
SPA type:     10xGE SPA
SPA operational state: READY
SPA cfg admin up: YES

Subslot 0/0/3 brief info:
-----------------------
SPA inserted: NO

Subslot 0/0/4 brief info:
-----------------------
SPA inserted: YES
SPA type:     4xOC48 POS/RPR
SPA operational state: READY
SPA cfg admin up: YES

Subslot 0/0/5 brief info:
-----------------------
SPA inserted: NO

Subslot 0/1/0 brief info:
-----------------------
SPA inserted: YES
SPA type:     8xGE SPA
SPA operational state: READY
SPA cfg admin up: YES

Subslot 0/1/1 brief info:
-----------------------
SPA inserted: YES
SPA type:     5xGE SPA
SPA operational state: READY
SPA cfg admin up: YES

Subslot 0/1/2 brief info:
-----------------------
SPA inserted: YES
SPA type:     8xGE SPA
SPA operational state: READY
SPA cfg admin up: YES

Subslot 0/1/3 brief info:
-----------------------
SPA inserted: YES
SPA type:     8xGE SPA
SPA operational state: READY
SPA cfg admin up: YES

Subslot 0/1/4 brief info:
-----------------------
SPA inserted: YES
SPA type:     5xGE SPA
SPA operational state: READY
SPA cfg admin up: YES

Subslot 0/1/5 brief info:
-----------------------
SPA inserted: YES
SPA type:     8xGE SPA
SPA operational state: READY
SPA cfg admin up: YES

Subslot 0/6/0 brief info:
-----------------------
SPA inserted: YES
SPA type:     8xGE SPA
SPA operational state: READY
SPA cfg admin up: YES

Subslot 0/6/1 brief info:
-----------------------
SPA inserted: YES
SPA type:     5xGE SPA
SPA operational state: READY
SPA cfg admin up: YES

Subslot 0/6/2 brief info:
-----------------------
SPA inserted: YES
SPA type:     8xGE SPA
SPA operational state: READY
SPA cfg admin up: YES

Subslot 0/6/3 brief info:
-----------------------
SPA inserted: YES
SPA type:     8xGE SPA
SPA operational state: READY
SPA cfg admin up: YES
```

```
Subslot 0/6/4 brief info:
-----------------------
SPA inserted: NO

Subslot 0/6/5 brief info:
-----------------------
SPA inserted: YES
SPA type:     8xGE SPA
SPA operational state: READY
SPA cfg admin up: YES
```

Table 8 describes the significant fields shown in the display.

Table 8 show hw-module subslot brief Field Descriptions

Field	Description
SPA inserted	SPA is currently detected in the subslot or not.
SPA type	Description of SPA including the technology type, number of ports, height of SPA (HHSPA—single height, FHSPA—double height), and optics type.
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/RP0/CPU0:router# show hw-module subslot 0/2/cpu0 brief c2w

SPA 0/0/0 device c2w 0/0 info:

C2W driver (0x50196ff4), name AUX C2W (busywait), state 4


SPA 0/0/1 device c2w 0/0 info:

C2W driver (0x50193a54), name AUX C2W (busywait), state 4


SPA 0/0/2 device c2w 0/0 info:

C2W driver (0x5019700c), name AUX C2W (busywait), state 4


SPA 0/0/4 device c2w 0/0 info:

C2W driver (0x501d7eb4), name AUX C2W (busywait), state 4


SPA 0/1/0 device c2w 0/0 info:

C2W driver (0x501969f4), name AUX C2W (busywait), state 4


SPA 0/1/1 device c2w 0/0 info:

C2W driver (0x501960f4), name AUX C2W (busywait), state 4
```

```
SPA 0/1/2 device c2w 0/0 info:

C2W driver (0x501969f8), name AUX C2W (busywait), state 4


SPA 0/1/3 device c2w 0/0 info:

C2W driver (0x501969fc), name AUX C2W (busywait), state 4


SPA 0/1/4 device c2w 0/0 info:

C2W driver (0x50196114), name AUX C2W (busywait), state 4


SPA 0/1/5 device c2w 0/0 info:

C2W driver (0x50196a18), name AUX C2W (busywait), state 4


SPA 0/6/0 device c2w 0/0 info:

C2W driver (0x50196a6c), name AUX C2W (busywait), state 4


SPA 0/6/1 device c2w 0/0 info:

C2W driver (0x50196178), name AUX C2W (busywait), state 4


SPA 0/6/2 device c2w 0/0 info:

C2W driver (0x50195060), name AUX C2W (busywait), state 4


SPA 0/6/3 device c2w 0/0 info:

C2W driver (0x50195064), name AUX C2W (busywait), state 4


SPA 0/6/5 device c2w 0/0 info:

C2W driver (0x50195068), name AUX C2W (busywait), state 4
```

Related Commands

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

Ethernet Interface Commands on Cisco IOS XR Software

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.

carrier-delay

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

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

Syntax Description

down *milliseconds*	Configures the length of time, in milliseconds, to delay the processing of hardware link down notifications. Range is from 1 through 5000.
up *milliseconds*	Configures the 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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

Task ID

Task ID	Operations
interface	read, write

Examples

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.

clear mac-accounting (Ethernet)

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

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

Syntax Description

{**GigabitEthernet** | **TenGigE**}	Clears the type of Ethernet interface for MAC accounting statistics. Use **GigabitEthernet** or **TenGigE**keyword.
interface-path-id	Interface whose MAC accounting statistics you want to clear. Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location *node-id*	(Optional) Clears MAC accounting statistics for the designated node.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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, 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.

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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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.
- The **flow-control** command is supported on Gigabit Ethernet and TenGigE interfaces only; the **flow-control** command is not supported on Management Ethernet Interfaces.
- 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 or for a specific node.

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 *interface-path-id*

no interface TenGigE *interface-path-id*

Syntax Description

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

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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, write

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 or for a specific node.

loopback (Ethernet)

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

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

no loopback

Syntax Description

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

Defaults

Loopback mode is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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

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

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

Task ID

Task ID	Operations
interface	read, write

Examples

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

```
RP/0/RP0/CPU0:router(config)# interface TenGigE 0/3/0/0
RP/0/RP0/CPU0:router(config-if)# loopback internal
```

mac-accounting

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

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

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

Syntax Description

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

Defaults

MAC accounting is disabled

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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
```

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.

mac-address (Ethernet)

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

mac-address *value1.value2.value3*

no mac-address

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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 and 10-Gigabit Ethernet) and for the Management Ethernet interface.

Task ID

Task ID	Operations
interface	read, write

Examples

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

```
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 0/1/5/0
RP/0/RP0/CPU0:router(config-if)# mac-address 0001.2468.ABCD
```

negotiation auto

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

negotiation auto

no negotiation auto

Syntax Description

This command has no arguments or keywords.

Defaults

Link autonegotiation is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

The **negotiation auto** command is available on Gigabit 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 GigabitEthernet 0/1/5/0
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 GigabitEthernet 0/1/5/0
RP/0/RP0/CPU0:router(config-if)# no negotiation auto
```

packet-gap non-standard

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

packet-gap non-standard

no packet-gap non-standard

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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

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

Task ID

Task ID	Operations
interface	read, write

Examples

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

```
RP/0/RP0/CPU0:router(config)# interface TenGigE 0/3/0/0
RP/0/RP0/CPU0:router(config-if)# packet-gap non-standard
```

show controllers (Ethernet)

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

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

Syntax Description

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

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 sample output is from the **show controllers** command with the **gigabitEthernet** keyword:

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

port:0
   good_octets_received: 6008282
   bad_octets_received: 0
   good_frames_received: 65020
   bad_frames_received: 0
   broadcast_frames_received: 11
   multicast_frames_received: 49985
   good_octets_sent: 4483774
   good_frames_sent: 45648
   broadcast_frames_sent: 0
   multicast_frames_sent: 0
   mac_transfer_error: 0
   excessive_collision: 0
   unrecog_mac_control_received: 0
   fc_sent: 0
   good_fc_received: 0
   rx_over_flow_events: 0
   undersize: 0
   fragments: 0
   oversize: 0
   jabber: 0
   mac_rcv_error: 0
   bad_crc: 0
   collisions: 0
   late_collision: 0
   rate_limit_dropped: 0
   spi4_rx_frames: 0
   spi4_tx_frames: 0
   DeviceID: 0x211911ab
   RevisionID: 0x00000003
   SideBandFC: 0xc0000000
   SERDESGlbCntl: 0x80000800
   GlblEPDCntlCfg: 0x0000a033
   TxFIFOUrecECCErrCtr: 0x00000000
   RxFIFOUrecECCErrCtr: 0x00000000
   DeviceGlobalRst: 0x00000000
   GlobalCfg: 0xb480d000
   PortTest: 0x00000000
   PL4IOGlblStat: 0x00000002
   DeviceTest: 0x00000000
   MACStatus Port0: 0x0000801f
   MACControl0 Port0: 0x000c0000
   MACControl1 Port0: 0xb1240151
   MACControl2 Port0: 0x0d805f60
   SERDESCntl Port0: 0x0000501a
   RateLimCntl Port0: 0x00000001
   SysIntMask: 0x000000f0
   SysIntCause: 0x00000000

   GOPIntMask0: 0x801ffffe
   GOPIntCause0: 0x40000000
   GOPIntMask1: 0x00000000
   GOPIntCause1: 0x00000000
   GOPIntMask2: 0xffdfb800
   GOPIntCause2: 0x00000000
   GOPIntMask3: 0x00000000
   GOPIntCause3: 0x00000000
   CalendarParam: 0x00040004
   SPI4SrcDPDeskew: 0x000f2710
   SrcClndrCmd: 0x00100404
```

```
SnkCalSeqPrgm: 0x00100404
SinkControl: 0x00000000
SPI4SrcMaxBrst: 0x00040004
SPI4IntfBrstLen: 0x0007000f
TxPacketSize: 0xc0280011
RxFullWatermarks: 0x01f000c0
RxFIFOXOnOffFCWtrmrk: 0x05000300
```

Table 9 describes the significant fields shown in the display.

Table 9 show controllers Field Descriptions

Field	Description
port	Ethernet port in which information is displayed in the show controllers command output.
good_octets_received	Count of received octets that had no errors.
bad_octets_received	Count of received octets that had errors.
good_frames_received	Count of received frames that had no errors.
bad_frames_received	Count of received frames that had errors.
broadcast_frames_received	Total number of well-formed broadcast packets received by the port. It excludes packets received with errors or with multicast destination addresses.
multicast_frames_received	Total number of well-formed multicast packets received by the port. It excludes packets received with errors or with broadcast destination addresses.
good_octets_sent	Count of transmitted octets that had no errors.
good_frames_sent	Count of transmitted frames that had no errors.
broadcast_frames_sent	Total number of well-formed broadcast packets transmitted by the port. It excludes packets received with errors or with multicast destination addresses.
multicast_frames_sent	Total number of well-formed multicast packets transmitted by the port. It excludes packets received with errors or with multicast destination addresses.
mac_transfer_error	Register that tracks all MAC transfer errors on the interface.
excessive_collision	Total number of packets that failed to be sent after 16 collisions. It includes packets of all destination address types.
unrecog_mac_control_received	Number of received MAC control frames that have an opcode different than 00-01.
fc_sent	Number of flow control frames sent undersize.
good_fc_received	Number of good flow control messages received.
rx_over_flow_events	Number of times the port RxFifo has reached full level and at least one packet was dropped.
undersize	Number of undersize frames received (valid packet with length less than 64 bytes).
fragments	Number of fragments received on this interface.
oversize	Number of oversized frames received on this interface.
jabber	Number of jabber packets received (packet length is greater than the MRU, and there is an invalid CRC, and no Rx Error event).

Table 9 show controllers Field Descriptions (continued)

Field	Description
mac_rcv_error	Number of Rx Error events seen by the receive side of the MAC (the Rx Error signal/symbol was asserted while the frame is being received).
bad_crc	Number of frames received with bad CRC. **Note** Collisions and late collisions apply to only half duplex mode.
collisions	Total number of packets sent without error after having 1 to 15 collisions. It includes packets of all destination address types and excludes packets discarded because of insufficient resources or late collisions.
late_collision	Total number of packets discarded because of late collisions detected during transmission. It includes all transmit packets that had a collision after the transmission of the packet's 64th byte. The preamble and SFD are not included in the frame's byte count.
rate_limit_dropped	Number of frames dropped due to the broadcast/multicast rate limit.
spi4_rx_frames	SPI-4/1 receive frame count. This counter increments once for every Start of Packet (SOP) delineation marker sent on the SPI-4.2 receive interface. **Note** Packets that come from the CPU are not counted.
spi4_tx_frames:	SPI-4/1 transmit frame count. This counter increments once for every packet arriving on the SPI-4.2 receive interface. **Note** Packets that contain certain types of errors and packets sent to the CPU are not counted.
DeviceID	Unique number identifying the device.
RevisionID	Revision of the device.
SideBandFC	Serial sideband flow control is enabled on this port or not, and the status of ports in which flow control is currently active.
SERDESGlbCntl	Information about SERDES speed and receive (Rx) Gain on this port.
GlblEPDCntlCfg	Register specific to Cisco that shows whether Ethernet Packet Decoding is enabled.
TxFIFOUrecECCErrCtr	Transmit (Tx) FIFO unrecoverable ECC errors counter. This counter increments once per each ECC unrecoverable error. A masked interrupt is optionally generated.
RxFIFOUrecECCErrCtr	Receive (Rx) FIFO unrecoverable ECC errors counter. This counter increments once per each ECC unrecoverable error. A masked interrupt is optionally generated.
DeviceGlobalRst	Global register that controls device reset state.
GlobalCfg	Global register that controls enable, clock modes, and Rx Interface behavior.
PortTest	Port diagnostics register.
PL4IOGlblStat	Register used during SPI4.2 initialization.
DeviceTest	Diagnostic loopback register.

Table 9 show controllers Field Descriptions (continued)

Field	Description
MACStatus Port0	MAC control port register.
MACControl0 Port0	MAC control port register. Indicates whether the port is enabled on this port, and the status of flow control on this port.
MACControl1 Port0	MAC control port1 register. Indicates whether the port is enabled on this port, and the status of flow control on this port.
MACControl2 Port0	MAC control port2 register. Indicates whether the port is enabled on this port, and the status of flow control on this port.
SERDESCntl Port0	SERDES control port register. The following information is displayed: • 0 = 50 Ohm • 1 = 75 Ohm
RateLimCntl Port0	Rate Limit control port 10 register.
SysIntMask	When the matching bit in the mask register is reset, the matching interrupt in the cause register is not included in the sum.
SysIntCause	Register that tracks the causes of system interrupts.
GOPIntMask0	GOP interrupt Mask0. When the matching bit in the mask register is reset, the matching cause in the GOP register is not included in the sum.
GOPIntCause0	Register that tracks all GOP interrupts and matches them with the GOP0 register.
GOPIntMask1	GOP interrupt Mask1. When the matching bit in the mask register is reset, the matching cause in the GOP register is not included in the sum.
GOPIntCause1	Register that tracks all GOP interrupts and matches them with the Mask1 register.
GOPIntMask2	GOP interrupt Mask2. When the matching bit in the mask register is reset, the matching cause in the GOP register is not included in the sum.
GOPIntCause2	Register that tracks all GOP interrupts and matches them with the Mask2 register.
GOPIntMask3	GOP interrupt Mask3. When the matching bit in the mask register is reset, the matching cause in the GOP register is not included in the sum.
GOPIntCause3	Register that tracks all GOP interrupts and matches them with the Mask3 register.
CalendarParam	Register that determines the value of Calendar_LEN and Calendar M for the sink and source side.
SPI4SrcDPDeskew	Register used to control the training pattern generation on the source side.
SrcClndrCmd	Register used to program the CALENDAR slots in the calendar report generated by the device.
SnkCalSeqPrgm	Register used to program the CALENDAR slots in the calendar report generated by the device.

Table 9 show controllers Field Descriptions (continued)

Field	Description
SinkControl	Register used to control the operation of the SPI-4.2 SINK section.
SPI4SrcMaxBrst	Register used to determine the system parameters MaxBurst1 and MaxBurst2 on the source side. These values are used by the internal packet scheduler to initiate bursts on the SP-4.2 Rx interface.
SPI4IntfBrstLen	Register used to determine the actual length of the data bursts on the SP-4.2 physical interfaces. These values are different than the system parameters MaxBurts1/2, which corresponds to SP-4.2 flow control.
TxPacketSize	Maximum transmit packet size for the port, in hexadecimal format.
RxFullWatermarks	Internal RxFIFO full thresholds.
RxFIFOXOnOffFCWtrmrk	Generation of 802.3x PAUSE frames based on RxFIFO data fill thresholds.

The following sample output is from the **show controllers** command with the **tenGigE** keyword:

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

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

Vendor Name: CISCO-AGILENT
Vendor PN: QFCT-7088
Vendor Rev: 02
Vendor SN: AGS08170SJZ
Package OUI: 0041f420
Vendor OUI: 00332c00
Vendor Date Code: 2004042301

Center Wavelength:
chan0 = 1310.00 nm
chan1 =    0.00 nm
chan2 =    0.00 nm
chan3 =    0.00 nm

Digital Optical Monitoring:
Transceiver Temp: 33.895 C
Laser Bias Current:   0.0000 mA
Laser Output Power: 0.0087 mW, -20.6 dBm
Receive Optical Power: 0.0190 mW, -17.2 dBm

Previous Alarm Status:
 Rx Xenpak Fault:
   Xenpak Phy XS Rx Local Fault
   Xenpak PCS Rx Local Fault
   Xenpak PMA PMD Rx Local Fault
 Tx Xenpak Fault:
   Xenpak PCS Tx Local Fault
 Lasi Faults:
   Xenpak Rx Alarm
   Xenpak Tx LS Alarm
Current Alarm Status:
 Rx Xenpak Fault:
   Xenpak PCS Rx Local Fault
   Xenpak PMA PMD Rx Local Fault
 No Tx Xenpak Faults
 Lasi Faults:
   Xenpak Rx Alarm

10GE PMA/PMD Registers:
  Previous Alarm Status:
    PMA/PMD NOT Locked to Local Signal
    PMA/PMD Local Fault
    LR Ability
    Loopback Ability
    Rx Local Fault
  Current Alarm Status:
    PMA/PMD NOT Locked to Local Signal
    PMA/PMD Local Fault
    LR Ability
    Loopback Ability
    Rx Local Fault

10GE PCS Registers:
  Previous Alarm Status:
    PCS Rx Link DOWN
    PCS Local Fault Detected
    PCS Rx Local Fault Detected
    PCS Rx NOT Block Locked
    PCS Rx Link Status DOWN
    PCS has NO Block Lock
  Current Alarm Status:
    PCS Rx Link DOWN
    PCS Local Fault Detected
    PCS Rx Local Fault Detected
    PCS Rx NOT Block Locked
    PCS Rx Link Status DOWN
    PCS has NO Block Lock

10GE XS/XS Registers:
  Previous Alarm Status:
    PHY XS Rx Lanes Synchronized
    PHY XS Tx Lanes Synchronized
    PHY XS Loopback Capable
  Current Alarm Status:
    PHY XS Rx Lanes Synchronized
    PHY XS Tx Lanes Synchronized
    PHY XS Loopback Capable

DTE XGXS (BCM8011):
  Previous Alarm Status:
    XGXS Lanes All Synchronized
    XGXS Lane Status Valid
  Current Alarm Status:
    XGXS Lanes All Synchronized
    XGXS Lane Status Valid
```

show mac-accounting (Ethernet)

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

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

Syntax Description

{**GigabitEthernet** | **TenGigE**}	Displays the type of Ethernet interface for the MAC accounting statistics. Enter **GigabitEthernet** or **TenGigE**.
interface-path-id	Detailed MAC accounting information for the specified interface. Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location *node-id*	(Optional) Displays detailed MAC accounting information for the specified interface on the specified node.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 sample output is 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 10 describes the significant fields shown in the display.

Table 10 show mac-accounting Field Descriptions

Field	Description
Interface	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.

Global Interface Commands on Cisco IOS XR Software

This module describes the global interface commands that apply to all interface types. This command set lets you configure, monitor, and troubleshoot the interfaces.

bandwidth (global)

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

bandwidth *rate*

Syntax Description

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

Defaults

The default bandwidth depends on the interface type.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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(config)# interface GigabitEthernet 0/4/1/0
RP/0/RP0/CPU0:router(config-if)# bandwidth 4000000
```

Related Commands

Command	Description
interface (global)	Configures an interface.
show interfaces	Displays statistics for all interfaces configured on the router or for a specific node.

clear interface

To clear interface statistics or packet counters, use the **clear interface** command in EXEC mode.

clear interface *type interface-path-id*

Syntax Description

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

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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	execute
basic-services	read, write

Examples

The following example shows how 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 for a specific node.

dampening

To limit propagation of transient or frequently changing interface states on Interface Manager (IM) clients, turn on event dampening by using the **dampening** command in interface configuration mode. To turn dampening off, use the **no** form of this command.

dampening [*half-life* [*reuse suppress max-suppress-time*]]

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

Syntax Description

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

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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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.

interface (global)

To configure an interface or to create or configure a virtual interface, use the **interface** command in global configuration mode. To delete the interface configuration, use the **no** form of this command.

interface *type interface-path-id*

no interface *type interface-path-id*

Syntax Description

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

Defaults

No interfaces are configured

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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 for a specific node.

mtu

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

mtu *bytes*

no mtu

Syntax Description

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

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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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

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

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

Note

- The MTU size, which is displayed, includes the Layer 2 header bytes used for each encapsulation type.
- Changing the MTU on an interface triggers a change on the protocols and capsulations configured on that interface, although some protocol-specific configurations can override the interface MTU. For example, specifically changing the interface MTU configuration does not affect the IP MTU configuration, but may affect the resulting MTU on that node.

Task ID

Task ID	Operations
interface	read, write

Examples

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

```
RP/0/RP0/CPU0:router# show interfaces all brief

                Intf        Intf         LineP              Encap  MTU       BW
                Name        State        State               Type (byte)   (Kbps)
--------------------------------------------------------------------------------
                 Nu0           up           up               Null  1500   Unknown
           PO6/0/0/0           up           up               HDLC  4474   2488320
           PO6/0/0/1           up           up               HDLC  4474   2488320
           PO6/0/0/2   admin-down   admin-down               HDLC  4474   2488320
           PO6/0/0/3   admin-down   admin-down               HDLC  4474   2488320
      Mg0/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        Intf         LineP              Encap  MTU       BW
                Name        State        State               Type (byte)   (Kbps)
--------------------------------------------------------------------------------
                 Nu0           up           up               Null  1500   Unknown
           PO6/0/0/0           up           up               HDLC  1000   2488320
           PO6/0/0/1           up           up               HDLC  4474   2488320
           PO6/0/0/2   admin-down   admin-down               HDLC  4474   2488320
           PO6/0/0/3   admin-down   admin-down               HDLC  4474   2488320
      Mg0/RP0/CPU0/0           up           up               ARPA  1514    100000
```

Related Commands

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

show im dampening

To display the state of all interfaces on which dampening has been configured, use the **show im dampening** command in EXEC mode.

show im dampening [**interface** *type* | **ifhandle** *handle*]

Syntax Description

interface *type*	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
ifhandle *handle*	(Optional) Identifies the caps node whose Interface Manager (IM) dampening information you want to display.

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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

If you do not specify an interface, then the system displays brief details about all dampened interfaces.

Task ID

Task ID	Operations
interface	read

Examples

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

```
RP/0/RP0/CPU0:router(config)# interface POS 0/4/0/3
RP/0/RP0/CPU0:router(config-if)# no shutdown
RP/0/RP0/CPU0:router(config-if)# dampening
RP/0/RP0/CPU0:router(config-if)# exit
RP/0/RP0/CPU0:router(config)# exit
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
```

Table 11 describes the significant fields shown in the display.

Table 11 show im dampening Field Descriptions

Field	Description
Dampening	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.
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 for a specific node.

show interfaces

To display statistics for all interfaces configured on the router or for a specific node, use the **show interfaces** command in EXEC mode.

show interfaces [*type interface-path-id* | **all** | **local** | **location** *node-id*] [**accounting** | **brief** | **detail** | **summary**]

Syntax Description

type	(Optional) Type of interface for which you want to display statistics. For more information, use the question mark (**?**) online help function.
interface-path-id	(Optional) Number of the interface whose statistics you want to display. Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
all	(Optional) Displays interface information for all interfaces.This is the default.
local	(Optional) Displays interface information for all interfaces in the local card.
location *node-id*	(Optional) Displays information about all interfaces on the specified node.
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

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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

Examples

The following sample output is 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
```

Table 12 describes the significant fields shown in the display.

Table 12 show interfaces Field Descriptions

Field	Description
Interface name	Name of the current interface. In the example, the interface name is POS0/1/0/1.
Interface state	State of the interface. In the example, the interface is in the administratively down state.
line protocol state	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	Current hardware type.
Internet address is *n.n.n.n/n*	Layer 2 address (MAC address for Ethernet interfaces). **Note** Use the **mac-address** command to configure the hardware address.
bia	Burned-in address (BIA) for the interface. The BIA is the default Layer 2 (MAC) address for the interface. **Note** The BIA is not configurable.
description	User-defined string that is associated with the interface. **Note** Use the **description** command to configure the description associated with the interface.
Internet Address	Layer 3 (IP) address for the interface. **Note** Use the **ipv4 address** command to configure the Internet address for the interface.

Table 12 show interfaces Field Descriptions (continued)

Field	Description
MTU	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. Use the **mtu** command to configure a lower MTU value at the Layer 3 level.
BW	Bandwidth of the interface in kbps.
reliability	Proportion of packets that are not dropped and do not have errors. **Note** The reliability is shown as a fraction of 255.
txload	Traffic flowing out of the interface as a proportion of the bandwidth. **Note** The txload is shown as a fraction of 255.
rxload	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	Length of the cyclic redundancy check (CRC), in bytes. **Note** The CRC is not present for all interface types. **Note** Use the **pos crc** command to configure the CRC.
loopback or controller loopback	Whether the hardware has been configured to be looped back. **Note** Use the **loopback** command to configure the loopback or controller loopback.
keepalive	Keepalive value, in seconds. **Note** Use the **keepalive** command to configure the value of the keepalive field. **Note** The *keepalive* field cannot be present if it is not applicable to the interface type.
Duplexity	Duplexity of the link. **Note** This field is present only for shared media. **Note** For some interface types, you can configure the duplexity by using 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 *hours*:*mins*:*secs*. This value is configurable using the **arp timeout** command.

Table 12 show interfaces Field Descriptions (continued)

Field	Description
Last clearing of counters	Time since the following counters were last cleared using the **clear counters** exec command in *hours*:*mins*:*secs*.
5 minute input rate	Average number of bits and packets received per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic that it sends and receives (rather than all network traffic). **Note** The 5-minute period referenced in the command output is a load interval that is configurable under the interface. The default value is 5 minutes. **Note** The 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.

Table 12 show interfaces Field Descriptions (continued)

Field	Description
runts	Number of received packets that were too small to be handled. This is a subset of the input errors count.
giants	Number of received packets that were too large to be handled. This is a subset of the input errors count.
throttles	Number of packets dropped due to throttling (because the input queue was full).
parity	Number of packets dropped because the parity check failed.
input errors	Total number of received packets that contain errors and hence cannot be delivered. Compare this to total input drops, which counts packets that were not delivered despite containing no errors.
CRC	Number of packets that failed the CRC check.
frame	Number of packets with bad framing bytes.
overrun	Number of overrun errors experienced by the interface. Overruns represent the number of times that the receiver hardware is unable to send received data to a hardware buffer because the input rate exceeds the receiver's ability to handle the data.
ignored	Total number of ignored packet errors. Ignored packets are those that are discarded because the interface hardware does not have enough internal buffers. Broadcast storms and bursts of noise can result in an increased number of ignored packets.
abort	Total number of 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-specifc.
output buffer failures	Number of times that a packet was not output from the output hold queue because of a shortage of MEMD shared memory.

Table 12 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 interfaces	Displays statistics for all interfaces configured on the router or for a specific node.

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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **shutdown** command to move the state of an interface to administratively down, which stops traffic flowing through the interface. This state does not stop other action from happening on the interface such as changes in configuration, protocols, capsulations, and so forth.

The **shutdown** command also marks the interface as unavailable. To check whether the state of an interface is down, use the **show interfaces** command in EXEC mode, which displays the current state of the interface. An interface that has been shut down is shown as administratively down in the display from the **show interfaces** command.

Task ID

Task ID	Operations
interface	read, write

Examples

In the following example, POS interface 0/4/0/2 is turned off:

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

Related Commands

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

Internal Ethernet Control Network Commands on Cisco IOS XR Software

This module describes the commands used to administer and configure internal control network commands on Cisco IOS XR software.

clear controller backplane ethernet clients

To clear the client applications of traffic sent and received over the control Ethernet, use the **clear controller backplane ethernet clients** command in administration EXEC mode.

clear controller backplane ethernet clients {*client-id* {**statistics**} | **all**} **location** *node-id*

Syntax Description

client-id	Client ID. Range is from 1 to 28.
all	Clears all client applications and their IDs.
statistics	Clears a list of client statistics.
location *node-id*	Clears the node or the controller information for a specified location.

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
system	execute

Examples

The following example shows how to clear all client statistics on the node at 0/1/1:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# clear controller backplane ethernet clients all statistics
location 0/1/1
```

Related Commands

Command	Description
show controllers backplane ethernet clients	Displays information about client applications in a particular location.
show controllers backplane ethernet detail	Displays detailed information about the backplane interfaces in a particular location.

clear controller backplane ethernet statistics

To clear the aggregate statistics of traffic sent and received over the control Ethernet, use the **clear controller backplane ethernet statistics** command in administration EXEC mode.

clear controller backplane ethernet statistics location *node-id*

Syntax Description

location *node-id*	Clears the node or the controller information for a specified location.

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
system	execute

Examples

The following example shows how to clear all client statistics on the node at 0/1/1:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# clear controller backplane ethernet statistics location 0/1/1
```

Related Commands

Command	Description
show controllers backplane ethernet clients	Displays information about client applications in a particular location.
show controllers backplane ethernet detail	Displays detailed information about the backplane interfaces in a particular location.

show controllers backplane ethernet brief

To display brief information about backplane Ethernet interfaces in a particular location, use the **show controllers backplane ethernet brief** command in administration EXEC mode.

show controllers backplane ethernet brief location *node-id*

Syntax Description

location *node-id*	Displays brief backplane Ethernet information for a specified location.

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
fabric	read
system	read

Examples

The following sample output is from the **show controllers backplane ethernet brief** command:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet brief location 0/1/CPU0

FastEthernet0_1_CPU0 (local) is up, MTU 1514 bytes
    345166 packets input, 162769252 bytes
    147865 packets output, 22764013 bytes
```

Table 13 describes the significant fields shown in the display.

Table 13 show controllers backplane ethernet brief Field Descriptions

Field	Description
MTU	Maximum packet size, in bytes, that a particular interface can handle.
packets input	Total number of packets received.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets transmitted by the system.

Related Commands

Command	Description
show controllers backplane ethernet clients	Displays information about client applications in a particular location.
show controllers backplane ethernet detail	Displays detailed information about the backplane interfaces in a particular location.
show controllers backplane ethernet multicast groups	Displays information about backplane interfaces that are in multicast groups in a particular location.

show controllers backplane ethernet clients

To display information about client applications in a particular location, use the **show controllers backplane ethernet clients** command in administration EXEC mode.

show controllers backplane ethernet clients {*client-id* {**statistics**} | **all**} **location** *node-id*

Syntax Description

client-id	Client ID. Range is from 1 to 28.
statistics	Displays a list of client statistics for the specified client ID.
location *node-id*	Displays a list of all client applications and their IDs for a specified location.
all	Displays a list of all client applications and their IDs.

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
fabric	read
system	read

Examples

The following sample output shows a list of client statistics for client ID 1:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet clients 1 statistics
location 0/1/CPU0

Client QNET, ES Client Id 1, PID 24600 running on FastEthernet0_1_CPU0
   LWM calls 1 open, 0 close, 0 close callback, 0 unblocks
   107065 packets input, 126686167 bytes
   107065 packets delivered,126043777 bytes
   0 packets discarded (0 bytes) in garbage collection
   0 (0 bytes) unicast packets filtered
   0 (0 bytes) multicast packets filtered
   0 (0 bytes) buffer mgmt policy discards
   0 (0 bytes) locking error discards
   0 packets waiting for client

   26513 packets output, 4800023 bytes, 0 could not be transmitted
   Packets output at high priority : 0
   Packets output at med  priority : 0
   Packets output at low  priority : 26513
   Out-of-packet write rejects (high) : 0
   Out-of-packet write rejects (med ) : 0
   Out-of-packet write rejects (low ) : 0
   DMA write rejects (high) : 0
   DMA write rejects (med ) : 0
   DMA write rejects (low ) : 0
```

Table 14 describes the significant fields shown in the display.

Table 14 show controllers backplane ethernet clients with statistics Keyword Field Descriptions

Field	Description
Client	Client application name and ID, followed by backplane client application statistics.
PID	Process ID.

The following sample output shows detailed information about the backplane client applications:

```
RP/0/RP0/CPU0:router# show controllers backplane ethernet clients all location 0/0/CPU0

    Intf           Client ethernet         Client              Description
    Name              server id            Process Id
------------------------------------------------------------------------------
  FE0_0_CPU0               1                 24600          QNX network manager
                           2                 49215               Group services
                           3                     0          Reserved for Attach
                           4                     0            Plugin controller
                           5                     0                Designated SC
                           6                     0           Platform H/W diags
                           7                     0            IP packet handler
                           8                 32804        Redundancy controller
                           9                     0     Platform Virtual console
                          10                 24599    Platform Virtual terminal
                          11                 24598        Control ethernet echo
                          12                     0       Control eth echo reply
                          13                     0  Card Configuration Protocol
                          14                     0          Reserved for Attach
                          15                     0           Chassis controller
                          16                     0            Forwarding driver
                          17                     0                    MBI hello
                          18                 32801       MBI Boot Server Source
                          19                     0                HSR ES client
                          20                     0  Packets for ethernet server
                          21                 81989         For Diag application
                          22                 24598                 QAD echo req
                          23                 24598               QAD echo reply
                          24                     0           Test application 1
                          25                     0           Test application 2
                          26                     0           Test application 1
                          27                     0      Test client out-of-band
```

Table 15 describes the significant fields shown in the display.

Table 15 show controllers backplane ethernet clients with all Keyword Field Descriptions

Field	Description
Intf Name	Ethernet interface.
Client ethernet server id	Ethernet server for the specified interface.
Client process id	Client process running on the specified interface.
Description	Backplane client application.

Related Commands

Command	Description
show controllers backplane ethernet brief	Displays brief information about backplane Ethernet interfaces in a particular location.
show controllers backplane ethernet detail	Displays detailed information about the backplane interfaces in a particular location.
show controllers backplane ethernet multicast groups	Displays information about backplane interfaces that are in multicast groups in a particular location.

show controllers backplane ethernet detail

To display detailed information about the backplane interfaces in a particular location, use the **show controllers backplane ethernet detail** command in administration EXEC mode.

show controllers backplane ethernet detail location *node-id*

Syntax Description

location *node-id*	Displays detailed information about backplane interfaces for a specified location. **Note** Use the **show platform** command to obtain the *node-id*.

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
fabric	read
system	read

Examples

The following sample output is from the **show controllers backplane ethernet detail** command:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet detail location 0/1/CPU0

FastEthernet0_1_CPU0 is up
  Hardware is 10/100 Ethernet, H/W address is 5246.4800.0011
  Internet address is 10.0.0.17
  MTU 1514 bytes
  Encapsulation HFRIES (Platform Internal Ethernet Server)
  Mode : Full Duplex,  Rate : 100Mb/s
    167245 packets input, 136745473 bytes, 0 total input drops
    140015 driver inputs,139357 driver callbacks
    1 packets discarded (66 bytes) in garbage collection
    16 packets discarded (3752 bytes) in recv processing
    0 incomplete frames discarded
    0 packets discarded due to bad headers
    0 packets waiting for clients
    0 packets waiting on Rx
    Packets waiting at high priority : 0
    Packets waiting at med  priority : 0
    Packets waiting at low  priority : 0
    Received 5705 broadcast packets, 44702 multicast packets
```

```
Input errors: 0 CRC, 0 overrun, 0 alignment, 0 length, 0 collision
49017 packets output, 9145593 bytes, 0 total output drops
Output 1 broadcast packets, 1 multicast packets
Output errors: 0 underruns, 0 aborts, 0 loss of carrier
Write rejects : 0
Rx mem score 1000, alloc fails 0, free fails 0, retrieved buffers 0
Rx mem threshold exceeded rejects 0, mutex lock fails 0
Tx mem score 1, server held 0, alloc fails 0, free fails 0
Tx mem threshold exceeded rejects 0, mutex lock fails 0, retrieved buffers 0
Tx quota for high :  100  med  :  100  low  :  799
Tx waits for high :    0  med  :    0  low  :    0
```

Table 16 describes the significant fields shown in the display.

Table 16 show controllers backplane ethernet detail Field Descriptions

Field	Description
Hardware	Hardware type, followed by the hardware address.
Internet address	IP address of the interface.
MTU	Maximum packet size, in bytes, that a particular interface can handle.
Encapsulation	Encapsulation method assigned to the interface.
Mode	Operating mode of the interface, followed by transmission data.
packets input	Total number of packets received.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
total input drops	Total number of packets dropped from the input queue because the queue was full.
packets discarded in garbage collection	Number of packets and bytes discarded.
packets discarded in recv processing	Number of packets and bytes discarded.
Received broadcast packets and multicast packets	Total number of broadcast and multicast packets that are received by the interface.

Table 16 show controllers backplane ethernet detail Field Descriptions (continued)

Field	Description
Input errors	Number of errors that are received by the interface. Input errors occur when incoming cells are dropped or corrupted. The following input errors are listed: • CRC—Number of times that the checksum calculated from the data received did not match the checksum from the transmitted data. • overrun—Number of times that the receiver hardware was incapable of handing received data to a hardware buffer because the input rate exceeded the receiver's capability to handle the data. • alignment—Number of nonoctets received. • length—Number of times the interface prevented the ASIC from overrunning a maximum transmission unit (MTU) size. • collision—Number of messages retransmitted because of an Ethernet collision.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets transmitted by the system.
total output drops	Total number of packets dropped from the output queue because the queue was full.
Output	Total number of broadcast and multicast packets that are transmitted by the interface.
Output errors	Number of errors that are transmitted on the interface. Output errors occur when outgoing cells are dropped or corrupted. The following types of output errors are listed: • underruns—Number of times that the far-end transmitter has been running faster than the near-end receiver can handle. • aborts—Number of illegal sequences of one bits on the interface. • loss of carrier—Number of times the interface was reset because the carrier detect line of that interface was up, but the line protocol was down.

Related Commands

Command	Description
show controllers backplane ethernet brief	Displays brief information about backplane Ethernet interfaces in a particular location.
show controllers backplane ethernet clients	Displays information about client applications in a particular location.
show controllers backplane ethernet multicast groups	Displays information about backplane interfaces that are in multicast groups in a particular location.

show controllers backplane ethernet multicast groups

To display information about backplane interfaces that are in multicast groups in a particular location, use the **show controllers backplane ethernet multicast groups** command in administration EXEC mode.

show controllers backplane ethernet multicast groups location *node-id*

Syntax Description

location *node-id*	Displays backplane information for multicast groups for a specified location.

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
fabric	read
system	read

Examples

The following sample output shows detailed information about the backplane interfaces:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# show controllers backplane ethernet multicast groups location
0/1/CPU0

    Intf                    Multicast      Client registered for this address
    Name                     address               Id               Name
------------------------------------------------------------------------------
  FastEthernet0_1_CPU0    0100.0000.0064            2                 GSP
                          0100.0000.0065            2                 GSP
                          0100.0000.0066            2                 GSP
                          0100.0000.0068            2                 GSP
                          0100.0000.006a            2                 GSP
                          0100.0000.006c            2                 GSP
                          0100.0000.006e            2                 GSP
                          0100.0000.0070            2                 GSP
                          0100.0000.0073            2                 GSP
                          0100.0000.0075            2                 GSP
                          0100.0000.2774            2                 GSP
                          0100.0000.2776            2                 GSP
                          0100.0000.2777            2                 GSP
                          0100.0000.2778            2                 GSP
                          0100.0000.277a            2                 GSP
                          0100.0000.277e            2                 GSP
                          0100.0000.2782            2                 GSP
                          0100.0000.2786            2                 GSP
                          0100.0000.2790            2                 GSP
                          0100.0000.2793            2                 GSP
                          0100.0000.279c            2                 GSP
                          0100.0000.279e            2                 GSP
                          0100.0000.27a8            2                 GSP
                          0100.0000.27ab            2                 GSP
--More--
```

Table 17 describes the significant fields shown in the display.

Table 17 show controllers backplane ethernet multicast groups Field Descriptions

Field	Description
Intf Name	Interface whose multicast addresses are displayed. **Note** A multicast address is a single address that refers to multiple network devices.
Multicast address	Multicast addresses associated with the specified interface. **Note** A multicast address is a single address that refers to multiple network devices.
ID	Client identifier.
Name	Client application name.

Related Commands

Command	Description
show controllers backplane ethernet brief	Displays brief information about backplane Ethernet interfaces in a particular location.
show controllers backplane ethernet clients	Displays information about client applications in a particular location.
show controllers backplane ethernet detail	Displays detailed information about the backplane interfaces in a particular location.

show controllers switch ports

To display status on a switch port, use the **show controllers switch ports** command in administration EXEC mode.

show controllers switch {**0** | **1**} **ports** [**FE** *port number* | **GE** *port number*] **location** *node-id*

Syntax Description

0 | **1**	Displays the instance of the controller.
FE *port number*	(Optional) Displays information for the Fast Ethernet (FE) port. Range is from 0 to 15.
GE *port number*	(Optional) Displays information for the Gigabit Ethernet (GE) port. Range is from 0 to 1.
location *node-id*	Displays the status of the switch port for a specified location.

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
fabric	read
root-system	read

Examples

The following sample output shows the status about the switch controller ports on switch 0 for location 0/RP0/CPU0:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# show controllers switch 0 ports location 0/RP0/CPU0

Ports Active on Switch 0
 FE Port  2  STP State : FORWARDING  (Connected to - 0/RP1)
 FE Port  9  STP State : FORWARDING  (Connected to - 0/SM0)
 FE Port 10  STP State : FORWARDING  (Connected to - 0/SM1)
 GE Port  2  STP State : FORWARDING
```

Table 18 describes the significant fields shown in the display.

Table 18 show controllers switch ports Field Descriptions

Field	Description
Ports Active	Active switch ports on the controller.
FE Port	FE port.
GE Port	GE port.
STP State	State of the Spanning-Tree Protocol: FORWARDING or DISABLED.
Connected to	Node that owns the specified port.

Related Commands

Command	Description
show controllers switch statistics	Displays statistics on all ports on the switch controllers.

show controllers switch statistics

To display statistics on all ports on the switch controllers, use the **show controllers switch statistics** command in administration EXEC mode.

show controllers switch {**0** | **1**} **statistics** [**FE** *port number* | **GE** *port number*] **location** *node-id*

Syntax Description

0 | **1**	Displays the instance of the controller.
FE *port number*	(Optional) Displays information for the Fast Ethernet (FE) port. Range is from 0 to 15.
GE *port number*	(Optional) Displays information for the Gigabit Ethernet (GE) port. Range is from 0 to 1.
location *node-id*	Displays the status of the switch port for a specified location.

Defaults

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
fabric	read
root-system	read

Examples

The following sample output shows information about switch controller statistics on all ports for location 0/rp1/cpu0:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# show controllers switch 0 statistics location 0/rp1/cpu0

Switch Instance 0:
Port   Tx Frames   Tx Errors   Rx Frames   Rx Errors   Connects
-----------------------------------------------------------------
 0 :           0           0           0           0       0/RP0
 1 :      156117           0      329032           0       0/RP1
 2 :       62166           0       17030           2       0/SM0
 3 :       70291           0       24874           2       0/SM1
 4 :       69294           0       24495           2       0/SM2
 5 :       71515           0       25067           2       0/SM3
 6 :           0           0           0           0
 7 :           0           0           0           0
 8 :         123           0           1           1       0/LC0
 9 :           0           0           0           0       0/LC1
10 :      173553           0       56051           2       0/LC2
11 :           0           0           0           0       0/LC3
12 :           0           0           0           0       0/LC4
13 :           0           0           0           0       0/LC5
14 :           0           0           0           0       0/LC6
15 :           0           0           0           0       0/LC7
24 :           0           0           0           0        GE_0
25 :           0           0           0           0        GE_1
```

Table 19 describes the significant fields shown in the display.

Table 19 show controllers switch statistics Field Descriptions

Field	Description
Tx Frames	Number of packets transmitted from the switch port.
Tx Errors	Number of transmission errors.
Rx Frames	Number of packets received on the switch port.
Rx Errors	Number of receive errors.

Related Commands

Command	Description
show controllers switch ports	Displays status on a switch port.

show spantree

To display spantree configuration information, use the **show spantree** command in administration EXEC mode.

show spantree {**mst 1** {**brief** | **detail** | **port** {**FE** *port-id* | **GE** *port-id*} | **config**} **location** *node-id*

Syntax Description

mst 1	Displays Multiple Spanning Tree (MST) information for instance 1.
config	Displays MST configuration information.
brief	Displays a summary of the spanning tree information.
detail	Displays detailed spanning tree information.
port	Displays spanning tree information for a specific Spanning Tree Protocol (STP) port.
FE *port-id*	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 *port-id*	Displays information for the Gigabit Ethernet (GE) port. Choose one of the following values: • 0—GE port number 0. • 1—GE port number 1.
location *node-id*	Displays the spantree information for a specified location.

Defaults

No default behavior or values

Command Modes

Administration EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
system	read
root-system	read

Examples

The following sample output shows how to display Multiple Spanning Tree configuration information for location 0/rp1/cpu0:

```
RP/0/RP0/CPU0:router# show spantree mst config location 0/rp1/cpu0

Name      [STP_1]
Revision      1
Instances configured 2

--------  ---------------------------------------------------------------------
   0      2-4094
   1      1
-------------------------------------------------------------------------------
```

Table 20 describes the significant fields shown in the display.

Table 20 show spantree Field Descriptions

Field	Description
Revision	Revision of the current MST configuration.
Instances configured	MST instance.

Link Bundling Commands on Cisco IOS XR Software

This module contains commands for configuring and monitoring Link Bundling on Cisco IOS XR software.

bundle id

To add a port to an aggregated interface (or bundle), use the **bundle id** command in interface configuration mode. To disable this feature, use the **no** form of this command.

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

no bundle id *bundle-id*

Syntax Description

bundle-id	Bundle on which you want to add a port. Range is 1 through 65535.
bundle-id.vlan_id	VLAN bundle on which you want to add a port. The VLAN bundle ID is entered in the *bundle-id.vlan_id* format, and a period between the *bundle-id* and *vlan_id* arguments is required. • Replace the *bundle-id* argument with the bundle ID. Range is from 1 through 65535. • Replace the *vlan_id* argument with the VLAN trunk interface ID. Range is from 1 to 4094 inclusive (0 and 4095 are reserved). **Note** The *vlan_id* 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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, the port does not unbind, but the mode changes to the mode that 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 for a specific node.
show lacp bundle	Displays detailed information about LACP ports and their peers.
show lacp port	Displays detailed information about LACP ports.

bundle-hash

To calculate load balancing across the members of a multilink interface bundle, use the **bundle-hash** command in the EXEC mode.

bundle-hash *bundleID*

Syntax Description

bundleID	ID number of the multilink interface bundle. Range is from 1 through 1024.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

Bundle interface traffic is distributed over the various member links of a bundle according to a hash function. The **bundle-hash** command displays the load-balancing information.

This information includes such things as the member link on which the traffic for a specific source address and destination address is transmitted, or how the load balancing is distributed on member links for a specific subnet.

Task ID

Task ID	Operations
bundle	read

Examples

The following example shows how to calculate load balancing across the members of a multilink interface bundle:

```
RP/0/RP0/CPU0:router# bundle-hash bundleID 100
```

Related Commands

Command	Description
bundle id	Adds a port to an aggregated interface (or bundle).

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

links	Number of active links you want to bring up in the specified bundle. Replace the *links* with **1**. **Note** Only one active link is supported.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

Note

- The **bundle maximum-active links** command is supported only for bundles that are not running LACP.
- If the **bundle maximum-active links** command is issued, 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, you can set the required number of active links that are required to bring up POS bundle 5 to 2.

```
RP/0/RP0/CPU0:router(config)# interface Bundle-POS 5
RP/0/RP0/CPU0:router(config-if)# bundle maximum-active links 1
```

Related Commands

Command	Description
bundle minimum-active links	Sets the minimum amount of bandwidth required before a user can 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.

bundle minimum-active bandwidth

To set the minimum amount of bandwidth required before a user can bring up a specific bundle, use the **bundle minimum-active bandwidth** command in interface configuration mode.

bundle minimum-active bandwidth *kbps*

Syntax Description

kbps	Minimum bandwidth required before you can bring up a bundle. Range is from 1 through a number that is equivalent to the combined bandwidths of 32 OC768 interfaces.

Defaults

kbps = 1

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
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, you can set the minimum amount of bandwidth that is 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.

bundle minimum-active links

To set the number of active links that are required to bring up a specific bundle, use the **bundle minimum-active links** command in interface configuration mode.

bundle minimum-active links *links*

Syntax Description

links	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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
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, you can configure the POS bundle 5 so that 2 links are 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
```

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.

bundle port-priority

To configure Link Aggregation Control Protocol (LACP) priority for a port, use the **bundle port-priority** command in interface configuration mode. To return to the default LACP priority value, use the **no** form of this command.

bundle port-priority *priority*

no bundle port-priority *priority*

Syntax Description

priority	Priority for this port, where a lower value equals a higher priority. Replace the *priority* argument with a number. Range is from 0 through 65535.

Defaults

priority = 32768

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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
```

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.

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, use the **clear lacp counters** command in EXEC mode.

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

Syntax Description

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

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
bundle	execute
basic-services	read, write

Examples

The following example shows how to clear LACP counters:

```
RP/0/RP0/CPU0:router# clear lacp counters
```

Related Commands

Command	Description
show lacp counters	Displays LACP statistics.

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

bundle-id	Ethernet bundle you want to create or configure. Replace *bundle-id* 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
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.

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

bundle-id	Number of the POS bundle you want to create or configure. Replace *bundle-id* 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
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	Displays information about a specific Ethernet bundle.

lacp period short

To configure a one second interval between LACP packets that are received from the peer, use 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
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.

lacp system-priority

To configure the priority for the current system, use 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

priority	Priority for this system. Replace *priority* with a number. Range is from 0 through 65535. A lower value is higher priority.

Defaults

priority = 32768

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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.

show bundle Bundle-Ether

To display information about a specific Ethernet bundle, use the **show bundle Bundle-Ether** command in EXEC mode.

show bundle Bundle-Ether *bundle-id* [**reasons**]

Syntax Description

bundle-id	Number of the Ethernet bundle whose information you want to display. Replace *bundle-id* 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
bundle	read

Examples

The following sample output is 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 sample output is 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 21 describes the significant fields shown in the display.

Table 21 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 *rack/slot/module/port* format.
State	Current state of the specified port. The following port states are listed: • 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).

Command	Description
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.

show bundle Bundle-POS

To display information about a specific POS bundle, use the **show bundle Bundle-POS** command in EXEC mode.

show bundle Bundle-POS *bundle-id* [**reasons**]

Syntax Description

bundle-id	Number of the POS bundle whose information you want to display. Replace *bundle-id* 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
bundle	read

Examples

The following sample output is 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
                                Minimum active     Maximum active
  B/W (Kbps)   MAC address      Links  B/W (Kbps)  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
  PO0/0/0/1      0      0x8000, 0x0002       155520  N/A
  PO0/0/0/2      0      0x8000, 0x0003       155520  N/A
```

The following sample output is 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

                                Minimum active     Maximum active
  B/W (Kbps)   MAC address      Links  B/W (Kbps)  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 22 describes the significant fields shown in the display.

Table 22 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 *rack/slot/module/port* 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.

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 for a specific node.

show lacp bundle

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

show lacp bundle [**Bundle-Ether** *bundle-id* | **Bundle-POS** *bundle-id*]

Syntax Description

Bundle-Ether *bundle-id*	(Optional) Displays the number of the Ethernet bundle. Range is through 65535.
Bundle-POS *bundle-id*	(Optional) Displays the number of the POS bundle. Range is 1 through 65535.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
bundle	read

Examples

The following sample output shows LACP information for a specific Ethernet Bundle:

```
RP/0/RP0/CPU0:router# show lacp bundle Bundle-Ether 1

Flags: A - Device is in Active mode. P - Device is in Passive mode.
       S - Device sends PDUs at slow rate. F - Device sends PDUs at fast rate.
       D - Port is using default values for partner information
       E - Information about partner has expired
State: 0 - Port is Not Aggregatable. 1 - Port is Out Of Sync with peer.
       2 - Port is In Sync with peer. 3 - Port is Collecting.
       4 - Port is Collecting and Distributing.

Bundle-Ether1
                                Minimum active     Maximum active
  B/W (Kbps)   MAC address      Links  B/W (Kbps)  Links
  ----------   --------------   -----  ----------  -----
           0   0800.453a.651d       1      620000     32

  Port           State  Flags  Port ID         Key     System-ID
  ------------   -----  -----  --------------  ------  -------------------------
  Gi0/0/2/0      1      ASDE   0x8000, 0x0001  0x0001  0x8000, 08-00-45-3a-65-01
   PEER          0      PSD    0xffff, 0x0000  0x0000  0xffff, 00-00-00-00-00-00
```

Table 23 describes the significant fields shown in the display.

Table 23 show lacp bundle Field Descriptions

Field	Description
Flags	Flags that can apply to a device or port, under the “Flags” field.
State	Flags that can apply the port state, under the “State” field.
Port	Port identifier, in the *rack/slot/module/port* notation.
State	Information about the state of the specified port. The following flags are listed: • 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	Information about the state of the specified device or port. The following flags are listed: • 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 *N*x*nnnn*. *N* is the port priority, and *nnnn* 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.

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.

show lacp counters

To display Link Aggregation Control Protocol (LACP) statistics, use the **show lacp counters** command in EXEC mode.

show lacp counters [**Bundle-Ether** *bundle-id* | **Bundle-POS** *bundle-id*]

Syntax Description

Bundle-Ether *bundle-id*	(Optional) Displays the counters for the Ethernet bundle. Replace *bundle-id* with a bundle identifier. Range is from 1 through 65535.
Bundle-POS *bundle-id*	(Optional) Displays the counters for the POS bundle. Replace *bundle-id* with a bundle identifier. Range is from 1 through 65535.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
bundle	read

Examples

The following sample output shows the LACP counters on an Ethernet bundle:

```
RP/0/RP0/CPU0:router# show lacp counters bundle-ether 4

Bundle-Ether1
                    LACPDUs                  Marker
Port           Sent        Received    Received    Resp. Sent  Last Cleared
-------------  ----------------------  ----------------------  ------------
Gi0/0/2/0              12           0           0           0  never

Port           Excess                  Excess                  Pkt Errors
-------------  ----------              ----------              ----------
Gi0/0/2/0               0                       0                       0
```

Table 24 describes the significant fields shown in the display.

Table 24 show lacp counters Field Descriptions

Field	Description
LACPDUs	Link Aggregation Control Protocol data units (LACPDUs) for the following statistics: • Port • Sent • Received • Last Cleared • Excess • Pkt Errors
Marker	Marker packets for the following statistics: • 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.

show lacp port

To display detailed information about Link Aggregation Control Protocol (LACP) ports, use the **show lacp port** command in EXEC mode.

show lacp port [**GigabitEthernet** *interface-path-id* | **TenGigE** *interface-path-id* | **POS** *interface-path-id*]

Syntax Description

GigabitEthernet	(Optional) Displays the Gigabit Ethernet interface bundle for the LACP port information.
TenGigE	(Optional) Displays the TenGigE interface for the LACP port information.
POS	(Optional) Displays the Packet-over-SONET/SDH (POS) network for the LACP port information.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
bundle	read

Examples

The following sample output shows the LACP port information for all link bundles on a router:

```
RP/0/RP0/CPU0:router# show lacp port

Flags: A - Device is in Active mode. P - Device is in Passive mode.
       S - Device sends PDUs at slow rate. F - Device sends PDUs at fast rate.
       D - Port is using default values for partner information
       E - Information about partner has expired
State: 0 - Port is Not Aggregatable. 1 - Port is Out Of Sync with peer.
```

```
       2 - Port is In Sync with peer. 3 - Port is Collecting.
       4 - Port is Collecting and Distributing.

Bundle-Ether1
                                Minimum active     Maximum active
  B/W (Kbps)   MAC address      Links  B/W (Kbps)  Links
  ----------   --------------   -----  ----------  -----
           0   0800.453a.651d       1      620000     32

  Port           State  Flags  Port ID         Key     System-ID
  ------------   -----  -----  --------------  ------  -------------------------
  Gi0/0/2/0      1      ASDE   0x8000, 0x0001  0x0001  0x8000, 08-00-45-3a-65-01
   PEER          0      PSD    0xffff, 0x0000  0x0000  0xffff, 00-00-00-00-00-00
```

Table 25 describes the significant fields shown in the display.

Table 25 show lacp port Field Descriptions

Field	Description
Port	LACP port whose information is displayed. The port number is expressed in the *rack/slot/module/port* notation.
State	Information about the state of the specified device or port. The following flags are listed: • 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	Information about the state of the specified port. The following flags are listed: • 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: *Nxnnnn*. *N* is the port priority, and *nnnn* 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 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.

show lacp system-id

To display the local system ID used by the Link Aggregation Control Protocol (LACP), use 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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

Task ID

Task ID	Operations
bundle	read

Examples

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

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

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

Table 26 describes the significant fields shown in the display.

Table 26 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

Management Ethernet Interface Commands on Cisco IOS XR Software

This module describes the Cisco IOS XR commands used to configure the Management Ethernet interfaces.

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 this 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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, write

Examples

The following example shows how to configure the Management Ethernet interface to operate in full duplex mode:

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

The following example shows how to configure the Management Ethernet interface to operate in half duplex mode:

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

The following example shows how to return a Management Ethernet interface to autonegotiated duplex mode:

```
RP/0/RP0/CPU0:router(config)# interface MgmtEth 0/RP0/CPU0/0
RP/0/RP0/CPU0:router(config-if)# no duplex
```

Related Commands

Command	Description
interface MgmtEth	Enters interface configuration mode for the Management Ethernet interface.
show interfaces	Displays statistics for all interfaces configured on the router or for a specific node.

interface MgmtEth

To enter interface configuration mode for the Management Ethernet interface, use the **interface MgmtEth** command in global configuration mode. To delete a Management Ethernet interface configuration, use the **no** form of this command.

interface MgmtEth *interface-path-id*

no interface MgmtEth *interface-path-id*

Syntax Description

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

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

The naming notation for the interface path ID is *rack/slot/CPU0/port* and a slash between values is required as part of the notation. The following definitions are listed:

- rack—Chassis number of the rack. In a single-shelf system, the rack is always “0.”
- slot—Physical slot number of the RP on which the interface is located. The slot number is either RP0 or RP1.
- module—Module number. A physical layer interface module (PLIM) is always 0.
- port—Physical port number of the interface.

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 or for a specific node.
speed (Management Ethernet)	Configures the speed for a Management Ethernet interface.

mac-address (Management Ethernet)

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

mac-address *value1.value2.value3*

no mac-address

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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
```

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 or for a specific node.

speed (Management Ethernet)

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

Interface speed is autonegotiated.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

The valid interface speed options are 10 Mbps, 100 Mbps, or 1000 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.

Table 27 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 27 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.

Table 27 Relationship Between duplex and speed Commands (continued)

duplex Command	speed Command	Resulting System Action
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 or for a specific node.

NetFlow Commands on Cisco IOS XR Software

This module describes the NetFlow commands on Cisco IOS XR software.

cache entries

To configure the number of entries in the monitor map flow cache, use 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

number	Number of entries in the flow cache. Replace the *number* argument with the number of flow entries allowed in the flow cache. Range is from 4096 through 1000000.

Defaults

number = 65535

Command Modes

Flow monitor map configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
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
```

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.

Command	Description
show flow monitor	Displays flow monitor cache information.
show flow monitor-map	Displays flow monitor map information.

cache permanent

To disable the removal of entries from the monitor map flow cache, use 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
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
```

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.

Command	Description
show flow monitor	Displays flow monitor cache information.
show flow monitor-map	Displays flow monitor map information.

cache timeout

To configure the active, inactive, and update flow cache timeout, use 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.
timeout_value	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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

Note

- The **inactive** timeout value should be smaller than the **active** timeout value.
- 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.

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.

clear flow exporter

To export flow exporter templates to the collector or restart the flow exporter statistics collector, use the **clear flow exporter** command in EXEC mode.

clear flow exporter [*fem-name*] {**restart** | **statistics**} **location** *node-id*

Syntax Description

fem-name	(Optional) Flow exporter name.
restart	Exports all of the current templates to the collector.
statistics	Clears the exporter statistics.
location *node-id*	Identifies the node whose flow exporter statistics you want to clear, or whose flow exporter statistics collector you want to restart.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
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

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.

clear flow monitor

To clear the flow monitor data, use the **clear flow monitor** command in EXEC mode.

clear flow monitor [*name*] **cache** [**force-export** | **statistics**] **location** *node-id*

Syntax Description

name	(Optional) 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 *node-id*	Clears the node for the flow monitor.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
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]
```

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.

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

node-id	Node on which to clear statistics collected by the NetFlow producer. **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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
netflow	read, write

Examples

The following example shows how to clear statistics collected by the NetFlow producer:

```
RP/0/RP0/CPU0:router # clear flow platform producer statistics location 0/0/CPU0
```

destination

To configure the collector export destination, use 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.

Defaults

No default behavior or values

Command Modes

Flow exporter map configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
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
```

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.

dscp

To configure the differentiated services code point (DSCP) value for export packets, use 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

dscp_value	Specifies the DSCP value for export packets. Replace *dscp_value* 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
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
```

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.

exporter

To associate a flow exporter map with the current flow monitor map, use 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

map_name	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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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
```

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.

flow

To specify a flow monitor map and a sampler map for the packets on an interface, use the **flow** command in interface configuration mode.

flow [**ipv4** | **ipv6** | **mpls**] **monitor** *name* **sampler** *name* {**egress** | **ingress**}

Syntax Description

ipv4	(Optional) Enables IPV4 NetFlow on the specified interface.
ipv6	(Optional) Enables IPV6 NetFlow on the specified interface.
mpls	(Optional) Enables Multiprotocol Label Switching (MPLS)-aware NetFlow on the specified interface.
monitor *name*	Specifies the name of the flow monitor map you want to specify for IPv4, IPv6, or MPLS packets.
sampler *name*	Configures the name of the sampler map that 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
netflow	read, write

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 submode.
show flow monitor-map	Displays flow monitor map information.

flow exporter-map

To create a flow exporter map and enter flow exporter map configuration mode, use 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

fem-name	New exporter map name or name of an existing exporter map.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
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.

flow monitor-map

To create and configure a flow monitor map and enter flow monitor map configuration submode, use 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

map_name	New monitor map name or 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
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.

Command	Description
show flow monitor	Displays flow monitor cache information.
show flow monitor-map	Displays flow monitor map information.

options

To export the tables in the options template and specify export timeout values, use 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	Exports the interface table.
sampler-table	Exports the sampler table.
timeout *seconds*	(Optional) Specifies the export timeout value. Replace *seconds* 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
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
```

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.

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

number_of_packets	Sampling interval in units of packets. Replace the *number_of_packets* 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
netflow	read, write

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.

record ipv4

To activate an IPv4 flow record, use the **record ipv4** command in flow monitor map configuration mode. To deactivate the flow record, use the **no** form of this command.

record ipv4 [**destination**]

no record ipv4 [**destination**]

Syntax Description

destination	(Optional) Specifies the IPv4 flow record as a destination-based NetFlow accounting record.

Defaults

The default is no IPv4 flow record is enabled.

Command Modes

Flow monitor map configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
netflow	read, write

Examples

The following example shows how to configure an IPv4 flow record:

```
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
```

The following example shows how to configure an IPv4 flow record for destination-based NetFlow accounting:

```
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 destination
RP/0/RP0/CPU0:router(config-fmm)# exit
RP/0/RP0/CPU0:router(config)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# flow ipv4 monitor monitor1 ingress
```

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 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.

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

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
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
```

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 mpls	Configures the flow record map name for MPLS.
record ipv4	Configures the flow record map name for IPv4.

Command	Description
show flow monitor	Displays flow monitor cache information.
show flow monitor-map	Displays flow monitor map 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**] [**ipv6-fields**] [**ipv4-ipv6-fields**] [**labels** *number*]

no record mpls [**ipv4-fields**] [**ipv6-fields**] [**ipv4-ipv6-fields**] [**labels** *number*]

Syntax Description

ipv4-fields	(Optional) Collects IPv4 fields in the MPLS-aware Netflow when the payload of the MPLS packet has IPv4 fields. It also collects MPLS traffic with no IPv4 payload, but the IPv4 fields are set to zero.
ipv6-fields	(Optional) Collects IPv6 fields in the MPLS-aware Netflow when the payload of the MPLS packet has IPv6 fields. It also collects MPLS traffic with no IPv6 payload, but the IPv6 fields are set to zero.
ipv4-ipv6-fields	(Optional) Collects IPv4 and IPv6 fields in the MPLS-aware Netflow when the payload of the MPLS packet has either IPv4 fields or IPv6 fields. It also collects MPLS traffic with no IPv4 or IPv6 payload, but those fields are set to zero.
labels *number*	(Optional) Configures the number of labels that are used in hashing. The *number* 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

You can have only one MPLS flow monitor running on an interface at a time. If you apply an additional MPLS flow monitor to the interface, the new flow monitor overwrites the existing one.

You can configure the MPLS flow monitor to collect IPv4 fields, IPv6 fields, or both types of fields.

Task ID

Task ID	Operations
netflow	read, write

Examples

The following configuration allows you to collect only MPLS fields. No payload information is collected.

```
RP/0/RP0/CPU0:router(config)# flow monitor-map MPLS-fmm
RP/0/RP0/CPU0:router(config-fmm)# record mpls labels 3
RP/0/RP0/CPU0:router(config-fmm)# cache permanent
RP/0/RP0/CPU0:router(config)# exit
RP/0/RP0/CPU0:router(config)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# flow mpls monitor MPLS-fmm sampler fsm ingress
```

The following configuration allows you to collect MPLS traffic with IPv4 fields. It also collects MPLS traffic with no IPv4 payload, but the IPv4 fields are set to zero.

```
RP/0/RP0/CPU0:router(config)# flow monitor-map MPLS-IPv4-fmm
RP/0/RP0/CPU0:router(config-fmm)# record mpls IPv4-fields labels 3
RP/0/RP0/CPU0:router(config-fmm)# cache permanent
RP/0/RP0/CPU0:router(config-fmm)# exit
RP/0/RP0/CPU0:router(config)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# flow mpls monitor MPLS-IPv4-fmm sampler fsm ingress
```

The following configuration allows you to collect MPLS traffic with IPv6 fields. It also collects MPLS traffic with no IPv6 payload, but the IPv6 fields are set to zero.

```
RP/0/RP0/CPU0:router(config)# flow monitor-map MPLS-IPv6-fmm
RP/0/RP0/CPU0:router(config-fmm)# record mpls IPv6-fields labels 3
RP/0/RP0/CPU0:router(config-fmm)# cache permanent
RP/0/RP0/CPU0:router(config-fmm)# exit
RP/0/RP0/CPU0:router(config)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# flow mpls monitor MPLS-IPv6-fmm sampler fsm ingress
```

The following configuration allows you to collect MPLS traffic with both IPv6 and IPv4 fields. It also collects MPLS traffic with no IPv4 or IPv6 payload, but those fields are set to zero.

```
RP/0/RP0/CPU0:router(config)# flow monitor-map MPLS-IPv4-IPv6-fmm
RP/0/RP0/CPU0:router(config-fmm)# record mpls IPv4-IPv6-fields labels 3
RP/0/RP0/CPU0:router(config-fmm)# cache permanent
RP/0/RP0/CPU0:router(config-fmm)# exit
RP/0/RP0/CPU0:router(config)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# flow mpls monitor MPLS-IPv4-IPv6-fmm sampler fsm ingress
```

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.

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

map_name	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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

To prevent the NetFlow processes from using up all of the available CPU, NetFlow supports a policer rate of 35,000 packets per second per direction for each individual line card.

Task ID

Task ID	Operations
netflow	read, write

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.

show flow exporter

To display flow exporter data, use the **show flow exporter** command in EXEC mode.

show flow exporter [*exporter_name*] **location** *node-id*

Syntax Description

exporter_name	(Optional) Displays the flow exporter data.
location *node-id*	Displays the location in which the cache resides. **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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
netflow	read

Examples

The following sample output shows the flow exporter map data:

```
RP/0/RP0/CPU0:router# show flow exporter fem1 location 0/0/CPU0

Flow Exporter: NFC
Used by flow monitors: fmm4

Status: Normal
Transport   UDP
Destination 12.24.39.0      (50001)
Source      12.25.54.3      (5956)
Flows exported:                                   0 (0 bytes)
Flows dropped:                                    0 (0 bytes)

Templates exported:                               1 (88 bytes)
Templates dropped:                                0 (0 bytes)

Option data exported:                             0 (0 bytes)
Option data dropped:                              0 (0 bytes)
Option templates exported:                        2 (56 bytes)
Option templates dropped:                         0 (0 bytes)

Packets exported:                                 3 (144 bytes)
Packets dropped:                                  0 (0 bytes)

Total export over last interval of:
  1 hour:                                         0 pkts
                                                  0 bytes
                                                  0 flows
  1 minute:                                       3 pkts
                                                144 bytes
                                                  0 flows
  1 second:                                       0 pkts
                                                  0 bytes
                                                  0 flows
```

Table 28 describes the significant fields shown in the display.

Table 28 show flow exporter Field Descriptions

Field	Description
Id	ID for 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.

Related Commands

Command	Description
clear flow exporter	Clears flow exporter statistics or restarts the flow exporter statistics collector.

Command	Description
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.

show flow exporter-map

To display flow exporter map information for a specific node, use the **show flow exporter-map** command in EXEC mode.

show flow exporter-map [*name*]

Syntax Description

name	(Optional) 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
netflow	read

Examples

The following sample output shows the information for the flow exporter map:

```
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
  Data Template Timeout : 600 seconds
  Interface-Table Export Timeout : 1800 seconds
  Sampler-Table Export Timeout : 0 seconds
```

Table 29 describes the significant fields shown in the display.

Table 29 show flow exporter-map Field Descriptions

Field	Description
Id	ID of 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	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	Configured destination port for UDP packets.
Export Version	Configured export format. **Note** Cisco IOS XR software supports export format version 9 only.
Common Template Timeout	Configured common template timeout.
Options Template Timeout	Configured options template timeout. **Note** You can specify the options template timeout with the **flow exporter-map** command.
Data Template Timeout	Configured data template timeout. **Note** You can specify the data template timeout with the **flow exporter-map** command.
Interface-Table Export Timeout	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	Export timeout value for the sampler table. **Note** You can specify the export timeout for the sampler table with the **flow exporter-map** command.

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.

show flow monitor

To display flow monitor cache data in various formats, use 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**} | **ipv4** {**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:

monitor-name	Flow monitor map whose details you want to display.
cache	Displays details about the flow monitor cache.

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 *name* with the name of the access whose information you want to display.
source-address *match-options*	Specifies source IP address match options. The following match options are listed: • **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. The following match options are listed: • **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. The following match options are listed: • **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.

protocol *match-options*	Compares fields and matches them based on the **protocol** value. The following match options are listed: • **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. The following match options are listed: • **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.

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. The following match options are listed: • **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. The following match options are listed: • **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.

destination-as *match-options*	Compares and matches the BGP autonomous system number of the source address. The following match options are listed: • **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** *match-if-options* • **egress** *match-if-options*
ingress *match-if-options*	Compares ingress interface fields and matches them based on the *match-if-options* value. The following match options are listed: • **eq**—Match if equal to field value. • **neq**—Match if not equal to field value.
egress *match-if-options*	Compares egress interface fields and matches them based on the *match-options* value. The following match options are listed: • **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 *match-options*	Compares fields from the first time stamp and matches them based on the *match-options* value. The following match options are listed: • **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.

last *match-options*	Compares fields from the last time stamp and matches them based on the *match-if-options* value. The following match options are listed: • **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 *match-options*	Compares bytes counter fields and matches them based on the *match-options* value. The following match options are listed: • **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 *match-options*	Compares packets counter fields and matches them based on the *match-options* value. The following match options are listed: • **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.

forwarding-status *match-options*	Compares forwarding status fields and matches them based on the *match-options* value. The following match options are listed: • **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 *match-dir-options*	Compares information about the direction of the flow and matches it based on the *match-options* value. The following match options are listed: • **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:

monitor-name	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.

source-address	Displays IPv4 or IPv6 information for the source address according to the specified sorting criteria. The following sorting options are listed: • **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. The following sorting options are listed: • **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. The following sorting options are listed: • **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. The following sorting options are listed: • **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. The following sorting options are listed: • **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.

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. The following sorting options are listed: • **top**—Displays top cache entries. • **bottom**—Displays bottom cache entries.
label-3	Displays MPLS information for the third label in the MPLS label stack. The following sorting options are listed: • **top**—Displays top cache entries. • **bottom**—Displays bottom cache entries.
label-4	Displays MPLS information for the fourth label in the MPLS label stack. The following sorting options are listed: • **top**—Displays top cache entries. • **bottom**—Displays bottom cache entries.
label-5	Displays MPLS information for the fifth label in the MPLS label stack. The following sorting options are listed: • **top**—Displays top cache entries. • **bottom**—Displays bottom cache entries.
label-6	Displays MPLS information for the sixth label in the MPLS label stack. The following sorting options are listed: • **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. The following sorting options are listed: • **top**—Displays top cache entries. • **bottom**—Displays bottom cache entries.
prefix	Displays MPLS information for the destination address. The following sorting options are listed: • **top**—Displays top cache entries. • **bottom**—Displays bottom cache entries.

top-label	Displays MPLS information for the top label in the MPLS label stack. The following sorting options are listed: • **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. The following sorting options are listed: • **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. The following sorting options are listed: • **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. The following sorting options are listed: • **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. The following sorting options are listed: • **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.

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. The following sorting options are listed: • **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. The following sorting options are listed: • **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. The following sorting options are listed: • **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. The following sorting options are listed: • **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. The following sorting options are listed: • **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.

packets	Displays packets counter information according to the specified sorting criteria. The following sorting options are listed: • **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. The following sorting options are listed: • **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. The following sorting options are listed: • **top**—Displays top cache entries. • **bottom**—Displays bottom cache entries. **Note** Enter the **direction** keyword followed by the **?** command to see a complete list of possible match criteria.
top	Displays top cache entries. Replace *records* with the number of records you want to display. **Note** You can follow the **top** keyword with the optional *entries* argument to specify the number of records to display.
bottom	Displays bottom cache entries. Replace *records* with the number of records you want to display. **Note** You can follow the **bottom** keyword with the optional *entries* argument to specify the number of records to display.
entries	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:

monitor-name	Name of 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.

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.

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.

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 *records* with the number of records you want to display.

bottom	Includes or excludes bottom cache entries. Replace *records* with the number of records you want to display.
entries	Number of records to display. Range is from 1 through 1000.

To display summarized flow record statistics:

monitor-name	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:

monitor-name	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:

monitor-name	Flow monitor map whose details you want to display.
cache	Displays details about the flow monitor cache.
location *node-id*	Identifies the node whose flow exporter statistics you want to clear, or whose flow exporter statistics collector you want to restart. **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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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**.

Task ID

Task ID	Operations
netflow	read

Examples

The following sample output shows the 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
IPV4DstPrfxLen
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
00:02:43:797 00 00:02:49:980 34720        620          Out 0

L4SrcPort  L4DestPort BGPDstOrigAS BGPSrcOrigAS IPV4DstPrfxLen
```

Table 30 describes the significant fields shown in the display.

Table 30 show flow monitor Field Descriptions

Field	Description
Cache summary for Flow Monitor fmm2	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	Following ager statistics are listed: • 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.

show flow monitor-map

To display flow monitor map data, use the **show flow monitor-map** command in EXEC mode.

show flow monitor-map *map-name*

Syntax Description

map-name	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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
netflow	read

Examples

The following sample output shows the 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
CacheUpdateTout:    60 seconds
```

Table 31 describes the significant fields shown in the display.

Table 31 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. The RecordMapName can be "ipv4," "ipv6," 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

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.

Command	Description
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.

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

node-id	Location of the node whose NetFlow producer statistics you want to display. **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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
netflow	read

Examples

The following sample output shows the statistics that are 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
IPv6 Ingress Packets:                    0
IPv6 Egress Packets:                     0
MPLS Ingress Packets:                    0
MPLS Egress Packets:                     0
Drops (no space):                        0
Drops (other):                           0
Unknown Ingress Packets:                 0
Unknown Egress Packets:                  0
Worker waiting:                          0
```

Table 32 describes the significant fields shown in the display.

Table 32 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.

show sampler-map

To display sampler map information, use the **show sampler-map** command in EXEC mode.

show sampler-map [*sampler-name*]

Syntax Description

sampler-name	(Optional) Name of the sampler map whose information you want to display.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
netflow	read

Examples

The following sample output shows the 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 33 describes the significant fields shown in the display.

Table 33 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.

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 interface-path-id*

no source *type interface-path-id*

Syntax Description

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

Defaults

No default behavior or values

Command Modes

Flow exporter map configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

For T1/E1/DS0 physical interfaces, the naming notation is *rack/slot/module/port/t1-num:channel-group-number*. For all other physical interface types, the naming notation is *rack/slot/module/port.* A slash between values is required as part of the notation.

For the module, the shared port adapters (SPAs) are referenced by their subslot number.

For t1-num (T1 or E1 channel number), T1 channels range from 1 to 24; E1 channels range from 1 to 31.

For the channel-group-number (time slot number), T1 time slots range from 1 to 24; E1 time slots range from 1 to 31. The *channel-group-number* is preceded by a colon and not a slash.

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.

template

To configure the export timeout value for the data and options templates, use 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 *seconds*	Configures the timeout value for the specified template, or for both the data and options templates. Replace *seconds* 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
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
```

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.

transport udp

To configure the destination port for User Datagram Protocol (UDP) packets, use 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

port	Destination port for UDP packets. Replace *port* 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
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
```

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.

version v9

To enter flow exporter map version configuration submode so that you can configure export version parameters, use 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
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.

Command	Description
show flow exporter	Displays flow exporter data.
show flow exporter-map	Displays flow exporter map information for a specific node installed in the router.

Null Interface Commands on Cisco IOS XR Software

This module describes the Cisco IOS XR commands used to configure null interfaces.

interface null 0

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

interface null 0

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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, 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)#
```

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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
sysmgr	read

Examples

The following sample output is from the **show controllers null interface** command, which displays null interface counters:

```
RP/0/RP0/CPU0:router# show controllers null interface

Null interface:
name     : Null0
handle   : 0x00080010
rx_count : 0
tx_count : 0
drops    : 0
.
```

Table 34 describes the significant fields shown in the display.

Table 34 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.

Table 34 show controllers null interface Field Descriptions (continued)

Field	Description
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 or for a specific node.

show interfaces null0

To display null0 interfaces, use the **show interfaces null0** command in EXEC mode.

show interfaces null0 [**accounting** [**location** {*location description* | **0/1/CPU0** | **0/2/0** | **0/2/1** | **0/2/CPU0** | **0/4/0** | **0/4/1** | **0/4/CPU0** | **0/5/CPU0**} | **rates**]] [**location** {*location description* | **0/1/CPU0** | **0/2/0** | **0/2/1** | **0/2/CPU0** | **0/4/0** | **0/4/1** | **0/4/CPU0** | **0/5/CPU0**}] [**begin** *line* | **exclude** *line* | **file** *file-name* | **include** *line* | **utility** {**cut** | **egrep** | **fgrep** | **head** | **less** | **sort** | **tail** | **uniq** | **wc** | **xargs**}] [**brief** | **description** | **detail** | **location** | **summary**]

Syntax Descriptions

accounting	(Optional) Displays the interface accounting option.
rates	(Optional) Displays interface accounting (input/output) rates.
brief	(Optional) Displays interface information in condensed format.
description	(Optional) Describes an interface.
detail	(Optional) Displays interface information in detail.
location {*location description* | **0/1/CPU0** | **0/2/0** | **0/2/1** | **0/2/CPU0** | **0/4/0** | **0/4/1** | **0/4/CPU0** | **0/5/CPU0**}	(Optional) Specifies a fully qualified interface location.
summary	(Optional) Displays interface in summary format.
begin *line*	(Optional) Begins with the line that matches the regular expression *line.*
exclude *line*	(Optional) Excludes lines that match.
file *file-name*	(Optional) Saves the configuration to file.
include *line*	(Optional) Includes lines that match.
utility {cut | egrep | fgrep | head | less | sort | uniq | wc | xargs}	(Optional) Includes a set of common UNIX utilities: • **cut—**Cuts out selected fields of each line of a file. • **egrep—**Extends regular expression grep. • **fgrep—**Configures fixed string expression grep. • **head—**Shows a set of lines/characters from the top of a file. • **less—** Enables fixed string pattern matching. • **sort—**Sorts, merges, or sequence-checks text files. • **tail—**Copies the last part of files. • **uniq—** Reports or filters out repeated lines in a file. • **wc—**Counts lines/words/characters of a file. • **xargs—**Constructs argument list(s) and invokes a program.
Word	(Optional) Saves to file.
bootflash: *destination file-name*	(Optional) Saves the configuration to bootflash: file system.
compactflash: *destination file-name*	(Optional) Saves the configuration to compactflash: file system.
compactflasha: *destination file-name*	(Optional) Saves the configuration to compactflasha: file system.

disk0: *destination file-name*	(Optional) Saves the configuration to disk0: file system.
disk0a:	(Optional) Saves the configuration to disk0a: file system.
disk1: *destination file-name*	(Optional) Saves the configuration to disk1: file system.
disk1a: *destination file-name*	(Optional) Saves the configuration to disk1a: file system.
ftp: *address or name of remote host*	(Optional) Saves the configuration to ftp: file system.
harddisk: *destination file-name*	(Optional) Saves the configuration to harddisk: file system.
harddiska: *destination file-name*	(Optional) Saves the configuration to harddiska: file system.
harddiskb: *destination file-name*	(Optional) Saves the configuration to harddiskb: file system.
nvram: *destination file-name*	(Optional) Saves the configuration to NVRAM: file system.
rcp: *destination file-name*	(Optional) Saves the configuration to rcp: file system.
tcp: *destination file-name*	(Optional) Saves the configuration to tcp: file system.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

The **show interfaces null0** command displays statistics about null interfaces. When no keywords are specified, information for all null interfaces is displayed.

Task ID

Task ID	Operations
interface	read

Examples

The following sample output shows how to use the **show interfaces null0** command:

```
RP/0/RP0/CPU0:router# show interfaces null0

Null0 is up, line protocol is up
  Interface state transitions: 0
  Hardware is Null interface
  Internet address is Unknown
  MTU 1500 bytes, BW Unknown
     reliability 255/255, txload Unknown, rxload Unknown
  Encapsulation Null,  loopback not set,
  Last clearing of "show interface" counters never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 total input drops
     0 drops for unrecognized upper-level protocol
     Received 0 broadcast packets, 0 multicast packets
     0 packets output, 0 bytes, 0 total output drops
     Output 0 broadcast packets, 0 multicast packets
```

Packet-over-SONET/SDH Interface Commands on Cisco IOS XR Software

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

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

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

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

crc (POS)

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

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

no crc {**16** | **32**}

Syntax Description

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

Defaults

The default CRC mode is 32 bits.

Command Modes

POS configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

CRC is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data. The designators 16 and 32 indicate the length (in bits) of the frame check sequence (FCS). A CRC of 32 bits provides more powerful error detection, but adds overhead. Both the sender and receiver must use the same setting.

CRC-16, the most widely used error checking method throughout the United States and Europe, is used extensively with WANs. CRC-32 is specified by IEEE standard 802 and as an option by some point-to-point transmission standards. It is often used on Switched Multimegabit Data Service (SMDS) networks and LANs.

Task ID

Task ID	Operations
pos-dpt	read, write

Examples

In 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.

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 encapsulation 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
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
```

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router or for a specific node.
show ppp interfaces	Displays PPP state information for an interface.

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

no interface POS *interface-path-id*[.*subinterface*] [**point-to-point**]

Syntax Description

interface-path-id[.*subinterface*]	Physical interface or virtual interface followed by the optional subinterface path ID. Naming notation is *interface-path-id.subinterface*. The period in front of the subinterface value is required as part of the notation. For more information about the syntax for the router, use the question mark (?) online help function.
point-to-point	(Optional) Specifies that the 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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, 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)#
```

Related Commands

Command	Description
show interfaces pos	Displays information about a POS interface.

keepalive (POS)

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

keepalive {*seconds* | **disable**}

no keepalive

Syntax Description

seconds	Number of seconds that define the keepalive interval. Range is from 0 through 32767 seconds. Default is 10 seconds.
disable	Turns off the keepalive timer.

Defaults

seconds = 10 seconds

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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

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
```

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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
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.

show interfaces pos

To display information about a POS interface, use the **show interfaces pos** command in EXEC mode.

show interfaces pos [*interface-path-id*] [**accounting** [**rates**] | **brief** | **description** | **detail** | **summary**] [**location** *node-id*]

Syntax Description

interface-path-id	(Optional) POS interface path ID. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
accounting	(Optional) Displays accounting information for all POS interfaces on the router, for a specific POS interface instance, or for all POS interfaces on a specific node.
rates	(Optional) Displays interface accounting rates for all POS interfaces on the router, for a specific POS interface instance, or for all POS interfaces on a specific node.
brief	(Optional) Displays brief output for all POS interfaces on the router, for a specific POS interface instance, or for all POS interfaces on a specific node.
description	(Optional) 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.
summary	(Optional) Displays summarized POS interface information.

Defaults

Use the **show interfaces pos** command without including any of the optional keywords or arguments to display detailed information about all POS interfaces configured on the router.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 sample output shows the 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 35 describes the significant fields shown in the display.

Table 35 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 sample output shows the brief information for a specific POS interface:

```
RP/0/RP0/CPU0:router# show interfaces pos 0/2/0/0 brief

              Intf        Intf         LineP              Encap  MTU       BW
              Name        State        State               Type (byte)   (Kbps)
-------------------------------------------------------------------------------
         PO0/2/0/0    admin-down    admin-down              HDLC  4474    2488320
```

Table 36 describes the significant fields shown in the display.

Table 36 show interfaces pos Field Descriptions

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

Related Commands

Command	Description
show controllers pos	Displays information on the Packet-over-SONET/SDH (POS) controllers.
show controllers sonet	Displays information about the operational status of SONET layers.

transmit-delay

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

transmit-delay *microseconds*

no transmit-delay *microseconds*

Syntax Description

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

Defaults

microseconds = 0 (disabled)

Command Modes

POS configuration

Command History

Releases	Modifications
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
pos-dpt	read, write

Examples

In the following example, a delay of 2 microseconds is specified on POS interface 0/1/0/2:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/1/0/2
RP/0/RP0/CPU0:router(config-if)# pos
RP/0/RP0/CPU0:router(config-if-pos)# transmit-delay 2
```

In the following example, the transmit delay on POS interface 0/1/0/2 is disabled:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/1/0/2
RP/0/RP0/CPU0:router(config-if)# pos
RP/0/RP0/CPU0:router(config-if-pos)# no transmit-delay
```

Related Commands

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

PPP Commands on Cisco IOS XR Software

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/SDH (POS) and multilink 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

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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **encapsulation ppp** command to enable PPP encapsulation on an interface.

Task ID

Task ID	Operations
ppp	read, write
interface	read, write

Examples

The following example shows how to set up PPP encapsulation on interface POS 0/1/0/1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
```

Related Commands

Command	Description
show ppp interfaces	Displays PPP state information for an interface.

ppp authentication

To enable Challenge Handshake Authentication Protocol (CHAP), MS-CHAP, or Password Authentication Protocol (PAP), and to specify the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface, use the **ppp authentication** command 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

protocol	Name of the authentication protocol used for PPP authentication. See Table 37 for the appropriate keyword. You may select one, two, or all three protocols, in any order.
list-name	(Optional) Used with authentication, authorization, and accounting (AAA). Name of a list of methods of authentication to use. If no list name is specified, the system uses the default. The list is created with the **aaa authentication ppp** command.
default	(Optional) Specifies the name of the list of methods created with the **aaa authentication ppp** command.

Defaults

PPP authentication is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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

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

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

Table 37 lists the protocols used to negotiate PPP authentication.

Table 37 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

The following example shows that CHAP is enabled on POS 0/4/0/1 and uses the authentication list MIS-access:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/4/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp authentication chap MIS-access
```

Related Commands

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

ppp chap password

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

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

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

Syntax Description

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

Defaults

The password is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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

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# configure
RP/0/RP0/CPU0:router(config)# interface POS 1/0/1/0
RP/0/RP0/CPU0:router(config-if)# ppp chap password xxxx
RP/0/RP0/CPU0:router(config-if)# ppp chap password clear xxxx
RP/0/RP0/CPU0:router(config-if)# ppp chap password encrypted 1514190900
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces running PPP.
ppp authentication	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.

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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

The **ppp chap refuse** command specifies that CHAP authentication is disabled for all calls, meaning that all attempts by the peer to force the user to authenticate using CHAP are refused.

If outbound Password Authentication Protocol (PAP) has been configured (using the **ppp authentication** command), PAP is suggested as the authentication method in the refusal packet.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

The following example shows how to specify POS interface 0/3/0/1 and disable CHAP authentication from occurring if a peer calls in requesting CHAP authentication. The method of encapsulation on the interface is PPP.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp chap refuse
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces running PPP.
ppp authentication	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.

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

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

Defaults

retries = 0

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp authentication chap
RP/0/RP0/CPU0:router(config-if)# ppp max-bad-auth 3
```

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.

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

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

Defaults

retries = 10

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **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# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp max-configure 4
```

Related Commands

Command	Description
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.

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

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

Defaults

retries = 5

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
ppp	read, write

Examples

The following example specifies that no more than three CONFNAKs are permitted before terminating the negotiation:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp max-failure 3
```

Related Commands

Command	Description
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.

ppp max-terminate

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

ppp max-terminate *number*

no ppp max-terminate

Syntax Description

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

Defaults

number = 2 retries

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
ppp	read, write

Examples

In the following example, a maximum of five TermReqs are specified to be sent before terminating and closing LCP or NCP:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp max-terminate 5
```

Related Commands

Command	Description
ppp max-configure	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.

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	Configures the UNENCRYPTED (cleartext) default password.
password	Cleartext or already-encrypted password.

Defaults

The password is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp ms-chap password clear line xxxx
```

ppp ms-chap refuse

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

ppp ms-chap refuse

no ppp ms-chap refuse

Syntax Description

This command has no arguments or keywords.

Defaults

MS-CHAP authentication is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp ms-chap refuse
```

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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

The **ppp pap refuse** command specifies that PAP authentication is disabled for all calls, meaning that all attempts by the peer to force the user to authenticate using PAP are refused.

If outbound Challenge Handshake Authentication Protocol (CHAP) has been configured (using the **ppp authentication** command), CHAP is suggested as the authentication method in the refusal packet.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

The following example shows how to specify POS 0/3/0/1 using PPP encapsulation on the interface. This example shows PAP authentication being specified as disabled if a peer calls in requesting PAP authentication.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp pap refuse
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces running PPP.
ppp authentication	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.

ppp pap sent-username password

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

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

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

Syntax Description

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

Defaults

Remote PAP support is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **ppp pap sent-username password** command to enable remote PAP support (for example, to respond to the peer’s request to authenticate with PAP) and to specify the parameters to be used when sending the PAP authentication request.

You must configure the **ppp pap sent-username password** command for each interface.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

In the following example, a password is entered as a cleartext password, xxxx:

```
RP/0/RP0/CPU0:router(config-if)# ppp pap sent-username xxxx password notified
```

When the password is displayed (as shown in the following example, using the **show running-config** command), the password notified appears as 05080F1C2243:

```
RP/0/RP0/CPU0:router(config-if)# show running-config

interface POS0/1/0/0
description Connected to P1_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# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ppp pap sent-username xxxx password notified
RP/0/RP0/CPU0:router(config-if)# ppp pap sent-username xxxx password clear notified
RP/0/RP0/CPU0:router(config-if)# ppp pap sent-username xxxx encrypted 1514190900
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces running PPP.
ppp authentication	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.

ppp timeout authentication

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

ppp timeout authentication *seconds*

no ppp timeout authentication

Syntax Description

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

Defaults

seconds = 10

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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.
- Although lowering the authentication timeout is beneficial if packets are lost, sending authentication requests faster than the peer can handle them results in churn and a slower connection time.

Task ID

Task ID	Operations
ppp	read, write

Examples

In the following example, PPP timeout authentication is set to 20 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp timeout authentication 20
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces running PPP.
ppp authentication	Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.

ppp timeout retry

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

ppp timeout retry *seconds*

no ppp timeout retry

Syntax Description

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

Defaults

seconds = 3

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

The **ppp timeout retry** command is useful for setting a maximum amount of time PPP should wait for a response to any control packet it sends.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows the retry timer being set to 8 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp timeout retry 8
```

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.

show ppp interfaces

To display PPP state information for an interface, use the **show ppp interfaces** command in EXEC mode.

show ppp interfaces {*type interface-path-id* | **all** | **brief** {*type interface-path-id* | **all** | **location** *node-id*} | **detail** {*type interface-path-id* | **all** | **location** *node-id*} | **location** *node-id*}

Syntax Description

type	Interface type as Packet-over-SONET/SDH (POS) or serial. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
all	(Optional) Displays detailed PPP information for all nodes.
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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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 sample output shows the 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:router# 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_platform)
     Of Us:   CHAP (Completed as P2_platform)
  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 38 describes the significant fields shown in the display.

Table 38 show ppp interfaces Field Descriptions

Field	Description
LCP	Current state of LCP. The state of the LCP reports 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).

Table 38 show ppp interfaces Field Descriptions (continued)

Field	Description
IPCP	IP Control Protocol (IPCP) state. The following seven states can be displayed: • 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.

Table 38 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 following seven states can be displayed: • 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	Adjusts the maximum transmission unit (MTU) value for packets on the interface.

SONET Controller Commands on Cisco IOS XR Software

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.

ais-shut (SONET)

To enable automatic insertion of a line alarm indication signal (LAIS) in the sent SONET signal whenever the SONET port enters the administrative shutdown state, use the **ais-shut** command in SONET/SDH configuration mode. To disable automatic insertion of an 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/SDH configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

When the line is placed in administrative shutdown state, use the **ais-shut** command to send a signal to downstream equipment that indicates that there is a problem with the line.

The **ais-shut** command is ignored if automatic protection switching (APS) is running for the corresponding port, because the setting must be enabled for proper APS operation.

For SONET ports that do not have hardware support for LAIS insertion, the **ais-shut** command is disabled.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

In the following example, the alarm indication is forced on the SONET OC-3 controller:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/RP0/CPU0:router(config-sonet)# ais-shut
```

Related Commands

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

ais-shut (SONET path)

To enable automatic insertion of path alarm indication signal (PAIS) in the sent SONET signal whenever the SONET path enters the administratively down state, use the **ais-shut** command in SONET/SDH path configuration mode. To disable automatic insertion of a 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/SDH path configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **ais-shut** command to enable automatic insertion of PAIS in the appropriate sent SONET path overhead whenever the corresponding SONET path enters the administratively down state.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows the alarm indication being enabled on all paths:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RP0/CPU0:router(config-sonet)# path
RP/0/RP0/CPU0:router(config-sonet-path)# ais-shut
```

Related Commands

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

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

number	Number of the group. Range is from 1 through 255.

Defaults

No groups exist.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **aps group** command to enter APS group configuration mode and configure APS connections with other SONET equipment.

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

Related Commands

Command	Description
authenticate (PGP)	Configures the authentication string for the Protect Group Protocol (PGP) message exchange between the protect and working routers.
channel local	Assigns local SONET physical ports as SONET automatic protection switching (APS) channels in the current APS group.
channel remote	Assigns a port and interface that is physically located in a remote router as a SONET automatic protection switching (APS) channel (working or protect).
lockout	Initiates a forced automatic protection switching (APS) request at the local end of the SONET link.
revert	Enables automatic switchover from the protect interface to the working interface after the working interface becomes available.
show aps	Displays the operational status for all configured SONET automatic protection switching (APS) groups.
signalling	Configures the K1K2 overhead byte signaling protocol used for automatic protection switching (APS).
timers (APS)	Changes the time between hello packets and the time before the protect interface process declares a working interface router to be down.
unidirectional	Configures a protect interface for unidirectional mode.

authenticate (PGP)

To configure the authentication string for the Protect Group Protocol (PGP) message exchange between the protect and working routers, use the **authenticate** command in APS group configuration mode. To revert to the default authentication string, use the **no** form of this command.

authenticate *string*

no authenticate *string*

Syntax Description

string	Authentication string that the router uses to authenticate PGP message exchange between protect or working routers. The maximum length of the string is eight alphanumeric characters. Spaces are not accepted.

Defaults

Authentication is always disabled by using the string “cisco.”

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

The **authenticate** command applies only in multirouter automatic protection switching (APS) group configurations.

In multirouter APS topologies, the protect and working routers communicate with each other through the User Datagram Protocol (UDP)-based Pretty Good Privacy protocol. Each Pretty Good Privacy packet contains an authentication string used for packet validation. The authentication string on all routers involved in the same APS group operation must match for proper APS operation.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to enable 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 local SONET physical ports as SONET automatic protection switching (APS) channels in the current APS group.
channel remote	Assigns a port and interface that is physically located in a remote router as a SONET automatic protection switching (APS) channel (working or protect).
show aps	Displays the operational status for all configured SONET automatic protection switching (APS) groups.

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** *interface-path-id*

no channel {**0** | **1**} **local** {**sonet** | **preconfigure**} **sonet** *interface-path-id*

Syntax Description

0 | **1**	Assigns the 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 card or line card is not physically installed in a slot.
sonet	Specifies a SONET interface type.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Defaults

A SONET APS local channel is not assigned.

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **channel remote** command to assign channels that are physically located in a different router.

Preconfigured interfaces are supported.

If the protect channel is local, it must be assigned using a **channel** command *before* any of the working channels are assigned. The reason is that having only a working channel assigned is a valid configuration for a working router in a multirouter APS topology, and further attempts to configure a local protect channel are rejected.

The interface type must be a SONET controller.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to configure SONET 0/2/0/2 as a local protect channel:

```
RP/0/RP0/CPU0:router(config)# aps group 1
RP/0/RP0/CPU0:router(config-aps)# channel 0 local SONET 0/2/0/2
```

Related Commands

Command	Description
channel remote	Assigns a port and interface that is physically located in a remote router as a SONET automatic protection switching (APS) channel (working or protect).
show aps	Displays the operational status for all configured SONET automatic protection switching (APS) groups.

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**	Assigns the channel number. Replace the *channel-number* 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.
ip-address	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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **channel remote** command to assign working or protect channels that are physically located in a different router.

Use the **channel local** command to assign channels in the local router.

Note The **channel remote** command should not be used in single-router APS topologies.

The IP address of the remote router is required only if a working channel configured as the protect router contacts all working routers.

Specifying a remote protect channel is optional. If you do not specify a remote protect channel, the default value of 0.0.0.0 is used. The protect router is always the one that contacts the working router. The working router replies to the protect router using the source address extracted from the incoming messages as the destination address. If an address other than 0.0.0.0 (the default value) is specified, the working router always uses that address when sending messages to the protect router.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

In the following examples, a remote channel with IP address 192.168.1.1 is assigned as the working channel:

```
RP/0/RP0/CPU0:router(config)# aps group 1
RP/0/RP0/CPU0:router(config-aps)# channel 1 remote 192.168.1.1
```

Related Commands

Command	Description
channel local	Assigns local SONET physical ports as SONET automatic protection switching (APS) channels in the current APS group.
show aps	Displays the operational status for all configured SONET automatic protection switching (APS) groups.

clear counters sonet

To clear SONET counters for a specific SONET controller, use the **clear counters sonet** command in EXEC mode.

clear counters sonet *interface-path-id*

Syntax Description

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

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
sonet-sdh	read, write
basic-services	read, write

Examples

The following example shows how to clear the SONET counters 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.

clock source (SONET)

To set the clock source of the sent signal on SONET ports, use the **clock source** command in SONET/SDH configuration mode. To cancel a clock source setting, use the **no** form of this command.

clock source {**internal** | **line**}

no clock source {**internal** | **line**}

Syntax Description

internal	Specifies that the controller will clock its sent data from its internal clock.
line	Specifies that the controller will clock its sent data from a clock recovered from the receive data stream of the line. This is the default value.

Defaults

The clock source for the controller is **line**.

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **clock source** command to configure which reference clock is used by the sender.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to configure the SONET controller to clock its sent data from its internal clock:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RP0/CPU0:router(config-sonet)# clock source internal
```

Related Commands

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

controller (SONET)

To enter SONET/SDH configuration mode so that you can configure a specific SONET controller, use the **controller** command in global configuration mode. To return to the default state, use the **no** form of this command.

controller [**preconfigure**] **sonet** *interface-path-id*

no controller [**preconfigure**] **sonet** *interface-path-id*

Syntax Description

preconfigure	(Optional) Specifies a SONET preconfiguration. Use the **preconfigure** keyword only when a modular services card in not physically installed in a slot.
sonet	Configures SONET port controllers.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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, write

Examples

The following example shows how to enter SONET/SDH configuration mode for the SONET controller in slot number 2:

```
RP/0/RP0/CPU0:router(config)# controller SONET 0/2/0/1
RP/0/RP0/CPU0:router(config-sonet)#
```

Related Commands

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

delay trigger

To configure SONET line delay trigger values, use the **delay trigger** command in SONET/SDH 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/SDH configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
sonet-sdh	read, write

Examples

The following example shows how to configure the SONET line delay trigger value 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.

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**	Assigns the channel number. **0** = protect, **1** = working.

Defaults

No default behavior or values

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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 (using the **lockout** command) overrides a force request.

In a multirouter APS topology, a force request is allowed only on the protect router.

This command remains in effect until it is unconfigured by using the **no** form of the command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to move traffic from the working channel back to the protect channel:

```
RP/0/RP0/CPU0:router(config)# aps group 1
RP/0/RP0/CPU0:router(config-aps)# force 1
```

Related Commands

Command	Description
lockout	Initiates a forced automatic protection switching (APS) request at the local end of the SONET link.
overhead (SONET)	Initiates the SONET overhead bytes in the frame header to conform to a specific standards requirement or to ensure interoperability with equipment from another vendor.

framing (SONET)

To specify the framing used on the SONET controller, use the **framing** command in SONET/SDH configuration mode. To disable framing on the SONET controller, use the **no** form of this command.

framing {**sdh** | **sonet**}

no framing {**sdh** | **sonet**}

Syntax Description

sdh	Selects Synchronous Digital Hierarchy (SDH) framing. This framing mode is typically used in Europe.
sonet	Selects SONET framing. This is the default.

Defaults

The default framing on SONET controllers is **sonet**.

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **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

The following example shows how to configure the SONET controller for SDH framing:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/2/0/2
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.

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**]

no lockout [**0**]

Syntax Description

0	(Optional) Assigns the channel number to the value of 0 that is defined as protect. Default is **0**.

Defaults

The default is **0**.

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

The optional **0** keyword (by default **0**) identifies the channel from which the traffic should not be moved on the protect channel. The **lockout 0** command keeps traffic away from the protect router.

A lockout switch request can be used to override a forced, an automatic (Signal Failed or Signal Degraded), or a manual switch request. No other request can override a lockout request; it has the highest possible priority.

In a multirouter APS topology, a **lockout** request is allowed only on the protect router.

This command remains in effect until it is unconfigured by using the **no** form of the command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to lock out or prevent the 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 a forced automatic protection switching (APS) request at the local end of the SONET link.
overhead (SONET)	Initiates the SONET overhead bytes in the frame header to conform to a specific standards requirement or to ensure interoperability with equipment from another vendor.

loopback (SONET)

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

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

no loopback {**internal** | **line**}

Syntax Description

internal	Specifies that all the packets be looped back from the source.
line	Specifies that the incoming network packets be looped back to the SONET network.

Defaults

This command is disabled by default.

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

The SONET and Synchronous Digital Hierarchy (SDH) transport layers support two loopback operation modes for diagnostic purposes: internal and line. In the terminal (internal) loopback, the sent signal is looped back to the receiver. In the facility (line) loopback, the signal received from the far end is looped back and sent on the line. The two loopback modes cannot be active at the same time. In normal operation mode, neither of the two loopback modes is enabled.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to configure all packets to be 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.

overhead (SONET)

To set the SONET overhead bytes in the frame header to a specific standards requirement, or to ensure interoperability with equipment from another vendor, use the **overhead** command in SONET/SDH configuration mode. To remove the setting of the SONET overhead bytes from the configuration file and restore the default condition, use the **no** form of this command.

overhead {**j0** | **s1s0**} *byte-value*

no overhead {**j0** | **s1s0**} *byte-value*

Syntax Description

j0	Sets the J0/C1 byte value in the SONET section overhead. For interoperability with Synchronous Digital Hierarchy (SDH) equipment in Japan, use the value 0x1. Default is 0xcc.
s1s0	Sets the SS bits value of the H1 byte in the SONET line overhead. Use the following values to tell the SONET transmission equipment the 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.
byte-value	Byte value to which the **j1** or **s1s0** keyword should be set. Range is from 0 to 255.

Defaults

jo *byte-value*: 0x01

sls0 *byte-value*: 0

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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
```

overhead (SONET path)

To set the SONET path overhead bytes in the frame header to conform to a specific standards requirement or to ensure interoperability with equipment from another vendor, use the **overhead** command in SONET/SDH path configuration mode. To remove the setting of the SONET path overhead bytes from the configuration file and restore the system to its default condition, use the **no** form of this command.

overhead {**c2** *byte-value* | **j1** *ascii-value*}

no overhead {**c2** *byte-value* | **j1** *ascii-value*}

Syntax Description

c2 *byte-value*	Specifies Synchronous Transport Signal (STS) synchronous payload envelope (SPE) content (C2) byte. The transmitted **c2** value is automatically set to 0xCF for unscrambled payload and 0x16 for scrambled payload. If c2 is configured to a user-specified value, the user-specified value is always applied regardless of scrambling. Replace the *byte-value* argument with the byte value to which the **c2** keyword should be set. Range is from 0 to 255. Default value is 0.
j1 *ascii-value*	Configures the SONET path trace (j1) buffer. Replace the *ascii-value* argument with a text string that describes the SONET path trace buffer. Default is a 64-byte path trace ASCII message, which includes default information such as router name, (Layer 2—POS) interface name, and IP address, if applicable.

Defaults

byte-value = 0xCF

ascii-value = 0

Command Modes

SONET/SDH path configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

The SONET standards permit or require user access for configuration of some bytes or bits in the SONET path overhead.

Use the **c2** keyword to configure the desired C2 byte value in the SONET path overhead.

Use the **j1** keyword to configure a user-defined path trace message in the j1 bytes of the SONET path overhead. For the **j1** keyword, use the default message or insert your own message that has a maximum of 62 characters. If no user-defined message is configured, a default message is automatically generated, containing the router name, the controller name, its IP address, and the values of the sent and received K1 and K2 bytes in the SONET line overhead.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to set the STS SPE C2 byte in the SONET path frame header:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RP0/CPU0:router(config-sonet)# path
RP/0/RP0/CPU0:router(config-sonet-path)# overhead c2 0x13
```

Related Commands

Command	Description
scrambling disable (SONET path)	Disables payload scrambling on a SONET path.

path (SONET)

To enter the SONET/SDH 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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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
sonet-sdh	read, write

Examples

The following example shows how to enter SONET path configuration mode from SONET controller configuration mode:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/RP0/CPU0:router(config-sonet)# path
```

Related Commands

Command	Description
ais-shut (SONET path)	Enables automatic insertion of path alarm indication signal (PAIS) in the sent SONET signal whenever the SONET path enters the administratively down state.
overhead (SONET path)	Sets the SONET path overhead bytes in the frame header to conform to a specific standards requirement or to ensure interoperability with equipment from another vendor.
report (SONET path)	Configures whether or not selected SONET alarms are logged to the console for a SONET path controller.

Command	Description
scrambling disable (SONET path)	Disables payload scrambling on a SONET path.
threshold (SONET path)	Sets the bit error rate (BER) threshold values of the specified alarms for a SONET path.
uneq-shut (SONET path)	Enables automatic insertion of P-UNEQ code (0x00) in the sent SONET path overhead C2 byte.

report (SONET)

To permit selected SONET alarms to be logged to the console for a SONET controller, use the **report** command in SONET/SDH configuration mode. To disable logging of select SONET alarms, use the **no form of this command.**

report [**b1-tca** | **b2-tca** | **lais** | **lrdi** | **sd-ber** | **sf-ber** | **slof** | **slos**]

no report [**b1-tca** | **b2-tca** | **lais** | **lrdi** | **sd-ber** | **sf-ber** | **slof** | **slos**]

Syntax Description

b1-tca	(Optional) Reports bit 1 (B1) bit error rate (BER) threshold crossing alert (TCA) errors.
b2-tca	(Optional) Reports bit 2 (B2) BER TCA errors.
lais	(Optional) Reports line alarm indication signal (LAIS) errors.
lrdi	(Optional) Reports line remote defect indication errors.
sd-ber	(Optional) Reports signal degradation BER errors.
sf-ber	(Optional) Reports signal failure BER errors.
slof	(Optional) Reports section loss of frame (SLOF) errors.
slos	(Optional) Reports section loss of signal (SLOS) errors.

Defaults

Alarms from the following keywords are reported by default:

- **b1-tca**
- **b2-tca**
- **sd-ber**
- **sf-ber**
- **slof**
- **slos**

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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.

report (SONET path)

To configure whether or not selected SONET alarms are logged to the console for a SONET path controller, use the **report** command in SONET/SDH path configuration mode. To disable or re-enable the logging of select SONET alarms, use the **no** form of this command.

report [**b3-tca 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/SDH path configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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.

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

The following example shows how to enable the reporting path of the PAIS alarms:

```
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.

revert

To enable automatic switchover from the protect interface to the working interface after the working interface becomes available, use the **revert** command in APS configuration mode. To disable automatic switchover, use the **no** form of this command.

revert *minutes*

no revert *minutes*

Syntax Description

minutes	Number of minutes until the circuit is switched back to the working interface after the working interface is available.

Defaults

minutes: 0

Automatic switchover is disabled.

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **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.

The revertive APS operation mode is the recommended operation mode because it offers better traffic protection during various possible software failures and upgrade or downgrade scenarios.

The *minutes* argument indicates how many minutes will elapse until automatic protection switching (APS) decides to switch traffic back from protect to working after the condition that caused an automatic (Signal Failed or Signal Degrade) switch to protect disappears. A value of 0 (default) disables APS revertive mode.

In a multirouter APS topology, the **revert** command is allowed only on the protect router.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to enable APS to revert to the protect or working channel after 5 minutes have elapsed:

```
RP/0/RP0/CPU0:router(config)# aps group 1
RP/0/RP0/CPU0:router(config-aps)# revert 5
```

Related Commands

Command	Description
show aps	Displays the operational status for all configured SONET automatic protection switching (APS) groups.

scrambling disable (SONET path)

To disable payload scrambling on a SONET path, use the **scrambling disable** command in SONET/SDH path configuration mode. To enable payload scrambling after it has been disabled, use the **no** form of this command.

scrambling disable

no scrambling disable

Syntax Description

This command has no arguments or keywords.

Defaults

The default is enable (SONET payload scrambling is on).

Command Modes

SONET/SDH path configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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 can be rejected.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to disable scrambling 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.

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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

Displaying the SONET APS operational data is considered of lower priority than the APS operation itself. Because the information is collected from several sources scattered across the various nodes involved, there is a small probability that some states will change while the command is being run.

The command should be reissued for confirmation before decisions are made based on the results displayed.

Task ID

Task ID	Operations
sonet-sdh	read

Examples

The following sample output is 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 39 describes the significant fields shown in the display.

Table 39   show aps Field Descriptions

Field	Description
APS Group	Assigned number of the APS group. Range is from 1 through 255.
Protect ch	Number and address of the protect channel interface.
Working ch	Number and address of the working channel interface.

Related Commands

Command	Description
show aps agents	Displays the status of the automatic protection switching (APS) working-to-protect (WP) distributed communication subsystem.
show aps group	Displays information about the automatic protection switching (APS) groups.

show aps agents

To display the status of the automatic protection switching (APS) working-to-protect (WP) distributed communication subsystem, use the **show aps agents** command in EXEC mode.

show aps agents

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

The WP communication is critical for the APS functionality. The **show aps agents** command is typically used as a debugging aid for unexpected or unusual APS operation.

Displaying the APS operational data is considered of lower priority than the APS operation itself. Because the information is collected from several sources scattered across the various nodes involved, there is a small probability that some states will change while the command is being run.

The command should be reissued for confirmation before decisions are made based on the results displayed.

Task ID

Task ID	Operations
sonet-sdh	read

Examples

The following sample output is 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 40 describes the significant fields shown in the display.

Table 40 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	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 the operational status for all configured SONET automatic protection switching (APS) groups.

show aps group

To display information about the automatic protection switching (APS) groups, use the **show aps group** command in EXEC mode.

show aps group [*number*]

Syntax Description

number	(Optional) Assigned group number.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

The **show aps group** command displays information about APS groups, and is useful if multiple APS groups are configured.

Displaying the APS operational data is considered of lower priority than the APS operation itself. Because the information is collected from several sources scattered across the various nodes involved, there is a small probability that some states will change while the command is being run.

The command should be reissued for confirmation before decisions are made based on the results displayed.

Task ID

Task ID	Operations
sonet-sdh	read

Examples

The following sample output is 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 41 describes the significant fields shown in the display.

Table 41 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 the operational status for all configured SONET automatic protection switching (APS) groups.
show aps agents	Displays the status of the automatic protection switching (APS) working-to-protect (WP) distributed communication subsystem.

show controllers pos

To display information on the Packet-over-SONET/SDH (POS) controllers, use the **show controllers pos** command in EXEC mode.

show controllers pos *interface-path-id* [**all** | **framer** {**internal** | **register** | **statistics**} | **internal**] [**begin** *line* | **exclude** *line* | **file** *filename* | **include** *line*]

Syntax Description

interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
all	(Optional) Displays information for all POS interface controllers.
framer	(Optional) Displays all POS framer information.
internal	(Optional) Displays all POS internal information.
register	(Optional) Displays the POS framer registers.
statistics	(Optional) Displays the POS framer cumulative counters.
begin *line*	(Optional) Displays information beginning with the line that includes the regular expression given by the *line* argument.
exclude *line*	(Optional) Displays information excluding all lines that contain regular expressions that match the *line* argument.
file *filename*	(Optional) Saves the configuration to the designated file. For more information on which standard filenames are recognized, use the question mark (?) online help function.
include *line*	(Optional) Displays only those lines that contain the regular expression given by the *line* argument.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Releases	Modifications
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

The information displayed is generally useful for diagnostic tasks performed only by technical support personnel.

Task ID

Task ID	Operations
interface	read

Examples

The following sample output is 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 sample output is from the **show controllers pos all** command:

```
RP/0/RP0/CPU0:router# show controllers POS 0/3/0/2 all

Port Number         : 2
Interface           : POS0_3_0_2
Ifhandle            : 0x1380120
CRC                 : 32
MTU                 : 4474
Port Bandwidth Kbps : 2488320
Admin state         : Up
Driver Link state   : Up


Bundle member       : No
Bundle MTU          : 4474
Bundle Adminstate   : Up


POS Driver Internal Cooked Stats Values for port 2
===================================================
Rx Statistics                   Tx Statistics
-------------                   -------------
Total Bytes:    1200            Total Bytes:    0
Good Bytes:     1200            Good Bytes:     0
Good Packets:   25              Good Packets:   0
Aborts:         0               Aborts:         0
FCS Errors:     0               Min-len errors: 0
Runts:          0               Max-len errors: 0
FIFO Overflows: 0               FIFO Underruns: 0
Giants:         0
Drops:          0



Sky4402 asic #2 registers:


0x000 general_cntrl                0x00
0x002 sys_intf_cntrl_1             0x06
```

```
0x003 sys_intf_cntrl_2             0x00
0x004 JTAG3                        0x10
0x005 JTAG2                        0x10
0x006 JTAG1                        0x10
0x007 JTAG0                        0x2f
0x010 active_led                   0x01
0x011 gpio_port_mode               0x01
0x012 gpio_port_fault              0x00
0x013 gpio_port_data               0x58
0x015 gpio_port_cntrl              0x3f
0x017 gpio_port_transition         0x00
0x019 gpio_port_intr_mask          0xff
0x01b gpio_port_intr               0x3f
0x01c master_intr_status           0x00
0x01d master_mask                  0x00
0x020 interrupt_4                  0x04
0x021 interrupt_3                  0x00
0x022 interrupt_2                  0x00
0x023 interrupt_1                  0x00
0x024 status_4                     0x04
0x025 status_3                     0x00
0x026 status_2                     0x0c
0x027 status_1                     0x80
0x028 mask_4                       0x07
0x029 mask_3                       0x03
0x02a mask_2                       0x1c
0x02b mask_1                       0x8f
0x02d link_state_cntrl             0x80
0x041 diag                         0x00
0x042 stcks                        0x03
0x043 short_frame_cntrl            0x00
0x0c0 ror_ram_c2                   0x16
0x0c1 ror_ram_g1                   0x00
0x0c2 ror_ram_f2                   0x00
0x0c3 ror_ram_h4                   0x00
0x0c4 ror_ram_z3                   0x00
0x0c5 ror_ram_z4                   0x00
0x0c6 ror_ram_z5                   0x00
0x0c7 ror_ram_db_c2                0x16
0x0c8 ror_ram_db_g1                0x00
0x142 tor_ram_c2                   0x16
0x143 tor_ram_g1                   0x00
0x144 tor_ram_f2                   0x00
0x145 tor_ram_h4                   0x00
0x146 tor_ram_z3                   0x00
0x147 tor_ram_z4                   0x00
0x148 tor_ram_z5                   0x00
0x170 tor_ram_s1                   0x00
0x171 tor_ram_e2                   0x00
0x172 tor_ram_e1                   0x00
0x173 tor_ram_f1                   0x00
0x174 tor_ram_k1                   0x00
0x175 tor_ram_k2                   0x00
0x177 tor_ram_z2                   0x00
0x180 rsp_cntrl_1                  0x00
0x181 rsp_cntrl_2                  0x02
0x184 rtop_f1_ovrhd                0x00
0x185 rtop_k1_ovrhd                0x00
0x186 rtop_k2_ovrhd                0x00
0x187 rtop_s1_ovrhd                0x00
0x188 rtop_e1_ovrhd                0x00
0x189 rtop_e2_ovrhd                0x00
0x18a rtop_deb_s1_ovrhd            0x00
0x18c rtop_b1_mismatch_cnt_u       0x00
```

```
0x18d rtop_b1_mismatch_cnt_l       0x00
0x190 rtop_b2_mismatch_cnt_u       0x00
0x191 rtop_b2_mismatch_cnt_l       0x00
0x194 rtop_rei_l_cnt_u             0x00
0x195 rtop_rei_l_cnt_l             0x00
0x198 rtop_ber_thresh_u            0x00
0x199 rtop_ber_thresh_l            0x00
0x19a rtop_ber_leak_u              0x00
0x19b rtop_ber_leak_l              0x00
0x19c rtop_ber_delay_u             0x00
0x19d rtop_ber_delay_l             0x00
0x1c0 rpop_signal_lbl_c2           0x16
0x1c2 rpop_valid_ptr_u             0x02
0x1c3 rpop_valid_ptr_l             0x0a
0x1c4 rpop_b3_mismatch_cnt_u       0x00
0x1c5 rpop_b3_mismatch_cnt_l       0x00
0x1c8 rpop_rei_p_cnt_u             0x00
0x1c9 rpop_rei_p_cnt_l             0x00
0x1cc rpop_ber_thresh_u            0x00
0x1cd rpop_ber_thresh_l            0x00
0x1ce rpop_ber_leak_u              0x00
0x1cf rpop_ber_leak_l              0x00
0x1d0 rpop_ber_delay_u             0x00
0x1d1 rpop_ber_delay_l             0x00
0x200 rpp_cntrl_1                  0x11
0x201 rpp_cntrl_2                  0x03
0x202 rpp_cntrl_3                  0x3e
0x203 rpp_cntrl_4                  0x00
0x204 rpp_cntrl_5                  0x00
0x208 rpp_max_pkt_len_u            0x08
0x209 rpp_max_pkt_len_l            0xbd
0x20a rpp_min_pkt_len              0x04
0x244 tpp_inter_pkt_u              0x00
0x245 tpp_inter_pkt_l              0x00
0x246 tpp_idle_cell_hdr            0x00
0x247 tpp_idle_cell_filldata       0x00
0x248 tpp_cntrl                    0x04
0x280 tpog_cntrl                   0x20
0x2c0 ttog_cntrl                   0x00
0x2c2 ttog_ovrhd_src_1             0x00
0x2c3 ttog_ovrhd_src_2             0x00
0x2c9 ttog_ovrhd_fill              0x00
```

Table 42 describes the significant fields shown in the display.

Table 42 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.

Table 42 show controllers pos Field Descriptions (continued)

Field	Description
Port 0:	Port 0 (the first port) statistics display.
Port 1:	Port 1 (the second port) statistics display.
Port 2:	Port 2 (the third port) statistics display.
Port 3:	Port 3 (the fourth port) statistics display.
Runt Threshold	Limit in packets set for runts on the specified port.
Tx Delay	Transmit delay that has been set for the specified port.
Cisco POS ASIC Register Dump (Transmit)	Header for display of the contents of the transmit ASIC register log.
POS Driver Internal Cooked Stats Values for port 0	Statistics relating to the specified POS port (POS port 0).
Rx Statistics	Receive statistics for the indicated POS port.
Total Bytes	Total number of bytes, including data and MAC encapsulation, received by the system.
Good Bytes	Number of bytes received without errors.
Good Packets	Number of packets received without errors.
Aborts	Number of receive bytes that have been aborted
FCS Errors	Number of FCS[2] errors that have been received.
Runts	Number of received packets that are discarded because they are smaller than the minimum packet size of the medium.
FIFO Overflows	Number of received packets that exceeded the FIFO stack limit.
Giants	Number of received packets that are discarded because they exceed the maximum packet size of the medium.
Drops	Number of received packets that have been dropped from the system.
Tx Statistics	Transmit statistics for the indicated POS port.
Total Bytes	Total number of bytes, including data and MAC encapsulation, sent by the system.
Good Bytes	Number of bytes sent without errors.
Good Packets	Number of packets sent without errors.
Aborts	Number of sent bytes that have been aborted.
Min-len errors	Minimum queue length violations.
Max-len errors	Maximum queue length violations.
FIFO Underruns	First-in, first-out, a buffering scheme where the first byte of data entering the buffer is the first byte retrieved by the CPU. FIFO underruns reports the number of times that the transmitter has been running faster than the router can handle.

[1] application-specific integrated circuit

[2] frame check sequence

show controllers sonet

To display information about the operational status of SONET layers, use the **show controllers sonet** command in EXEC mode.

show controllers sonet *interface-path-id* {**all** | **framers** | **internal-state**}

Syntax Description

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

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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 sample output is 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

  Clock source: line (actual) line (configured)

Optical Power Monitoring (accuracy: +/- 1dB)
  Not Supported
```

The following sample output is from the **show controllers sonet** command with the **framers** keyword:

```
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 43 describes the significant fields shown in the display.

Table 43 show controllers sonet Field Descriptions

Field	Description
Port	Slot number of the POS interface.
Status	State of the link associated with the specified port, up or down.
Loopback	Loopback identifier, if applicable.
LOF	Section loss of frame is detected when a severely error-framing (SEF) defect on the incoming SONET signal persists for 3 milliseconds.
LOS	Section loss of signal is detected when an all-zeros pattern on the incoming SONET signal lasts 19(+-3) microseconds or longer. This defect might also be reported if the received signal level drops below the specified threshold.
BIP	Bit interleaved parity error reported. • For B1, the bit interleaved parity error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B1 byte of the following frame. Differences indicate that section-level bit errors have occurred. • For B2, the bit interleaved parity error report is calculated by comparing the BIP-8/24 code with the BIP-8 code extracted from the B2 byte of the following frame. Differences indicate that line-level bit errors have occurred. • For B3, the bit interleaved parity error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B3 byte of the following frame. Differences indicate that path-level bit errors have occurred.
AIS	Alarm indication signal. • Line alarm indication signal is sent by the STE[1] to alert the downstream LTE[2] 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 PTE[3] that it has detected a defect on its incoming line signal.

Table 43 show controllers sonet Field Descriptions (continued)

Field	Description
RDI	Remote defect indication. • Line remote defect indication is reported by the downstream LTE when it detects LOF[4], LOS[5], or AIS[6]. • 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 BIP[7] (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).
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.

Table 43 show controllers sonet Field Descriptions (continued)

Field	Description
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
8. new data flag

The following sample output is 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 44 describes the significant fields shown in the display.

Table 44 show controllers sonet Field Descriptions

Field	Description
Interface (layer)	Slot number of the POS interface.
admin_up	Whether the interface and its associated layers are in the admin-up state.
if_state	Whether the interface and its associated layers are in the up or down state.

shutdown (SONET)

To disable SONET controller processing, use the **shutdown** command in SONET/SDH configuration mode. To bring back up a SONET controller and enable SONET controller processing, use the **no** form of this command.

shutdown

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/SDH configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **shutdown** command to shut down a SONET controller and disable SONET controller processing. Use the **no shutdown** command to bring back up a SONET controller and enable SONET controller processing.

The SONET controller must be brought up for the proper operation of the Layer 2 interface. The Layer 2 interface has a separate **shutdown** command available, which does not operate on the SONET controller's administrative state.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to bring down the SONET controller and disable SONET controller processing:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/1/0/2
RP/0/RP0/CPU0:router(config-sonet)# shutdown
```

Related Commands

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

signalling

To configure the K1K2 overhead byte signaling protocol used for automatic protection switching (APS), use the **signalling** command in APS group configuration mode. To reset APS signaling to the default, use the **no** form of this command.

signalling {**sonet** | **sdh**}

no signalling {**sonet** | **sdh**}

Syntax Description

sonet	Sets signaling to SONET.
sdh	Sets signaling to Synchronous Digital Hierarchy (SDH).

Defaults

SONET signaling is set by default.

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

By default, APS uses the signaling mode matching the framing mode. The **signalling** command may be required, depending upon the transport equipment capabilities, only on "transition" links interconnecting SONET and SDH networks.

In a multirouter APS topology, the **signalling** command is allowed only on the protect router.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to reset the signaling protocol from the default SONET value to SDH:

```
RP/0/RP0/CPU0:router(config)# aps group 1
RP/0/RP0/CPU0:router(config-aps)# signalling sdh
```

Related Commands

Command	Description
show aps group	Displays information about the automatic protection switching (APS) groups.

timers (APS)

To change the time between hello packets and the time before the protect interface process declares a working interface router to be down, use the **timers** command in APS group configuration mode. To return to the default timers, use the **no** form of this command.

timers *hello-seconds hold-seconds*

no timers

Syntax Description

hello-seconds	Number of seconds to wait before sending a hello packet (hello timer). Range is from 1 through 255 seconds. Default is 1 second.
hold-seconds	Number of seconds to wait to receive a response from a hello packet before the interface is declared down (hold timer). Range is from 1 through 255 seconds. Default is 3 seconds.

Defaults

hello-seconds: 1

hold-seconds: 3

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

The hello time, in seconds, represents the interval between the periodic message exchange between the Protect Group Protocol (PGP) peers. The hold time, in seconds, represents the interval starting with the first failed periodic message after which, if no successful exchange takes place, the PGP link is declared dead.

If many multirouter APS groups are configured and the CPU load or the User Datagram Protocol (UDP) traffic associated with the PGP communication is considered too high, then the hello interval should be increased.

Increasing the hold time is suggested if the PGP link is flapping. The possible causes include high route processor (RP) CPU load, high traffic, or high error rates on the links between the working and the protect routers.

We recommend that you have a hold time at least three times longer than the hello time (allowing three or more consecutive failed periodic message exchange failures).

The **timers** command is typically used only on the protect router. After the PGP connection is established, the working router learns about the timer settings from the protect router and automatically adjusts accordingly, regardless of its own timer configuration.

The **timers** command is meaningful only in multirouter automatic protection switching (APS) topologies and is ignored otherwise.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to configure APS group 3 with the hello timer at *2* seconds and the hold timer at 6 seconds:

```
RP/0/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.

threshold (SONET)

To set the bit error rate (BER) threshold values of the specified alarms for a SONET controller, use the **threshold** command in SONET/SDH configuration mode. To remove the setting of the threshold from the configuration file and restore the default condition, use the **no** form of this command.

threshold {**b1-tca** | **b2-tca** | **sd-ber** | **sf-ber**} *bit-error-rate*

no threshold {**b1-tca** | **b2-tca** | **sd-ber** | **sf-ber**} *bit-error-rate*

Syntax Description

b1-tca	Sets the B1 BER threshold crossing alarm (TCA). Range is from 3 through 9. Default is 10e-6.
b2-tca	Sets the B2 BER threshold crossing alarm (TCA). Range is from 3 through 9. Default is 10e-6.
sd-ber	Sets the signal degrade BER threshold. Range is from 3 through 9. Default is 10e-6.
sf-ber	Sets the signal failure BER threshold. Range is from 3 through 9. Default is 10e-3.
bit-error-rate	BER from 3 to 9 (10 to the minus *x*).

Defaults

bit-error-rate: 10e-6 (**b1-tca**, **b2-tca**, **sd-ber**); 10e-3 (**sf-ber**)

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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.

threshold (SONET path)

To set the bit error rate (BER) threshold values of the specified alarms for a SONET path, use the **threshold** command in SONET/SDH path configuration mode. To remove the setting of the SONET path threshold from the configuration file and restore the default condition, use the **no** form of this command.

threshold b3-tca *bit-error-rate*

no threshold b3-tca *bit-error-rate*

Syntax Description

b3-tca	Sets the B3 BER threshold crossing alarm (TCA). Default is 6.
bit-error-rate	BER from 3 to 9 (10 to the minus *x*).

Defaults

bit-error-rate: 6

Command Modes

SONET/SDH path configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

For B3, the bit interleaved parity (BIP) error report is calculated by comparing the BIP-8 code with the BIP-8 code that is extracted from the B3 byte of the following frame. Differences indicate that path-level bit errors have occurred.

In addition to BIP errors detected at the local end in the receive direction, B3 error counts detected in the G1 byte (P-REI or P-FEBE) by the far-end SONET equipment are returned.

The **b3-tca** keyword prints only a log message to the console (if reports for them are enabled).

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to set the BER 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 about the operational status of SONET layers.
report (SONET)	Permits selected SONET alarms to be logged to the console for a SONET controller.

uneq-shut (SONET path)

To enable automatic insertion of P-UNEQ code (0x00) in the sent SONET path overhead C2 byte, use the **uneq-shut** command in SONET/SDH path configuration mode. To disable this feature, use the **no** form of this command.

uneq-shut

no uneq-shut

Syntax Description

This command has no arguments or keywords.

Defaults

Automatic insertion is enabled.

Command Modes

SONET/SDH path configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 **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

The following example shows that the automatic insertion of P-UNEQ code is disabled in the sent SONET path overhead C2 byte:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RP0/CPU0:router(config-sonet)# path
RP/0/RP0/CPU0:router(config-sonet-path)# uneq-shut
```

unidirectional

To configure a protect interface for unidirectional mode, use the **unidirectional** command in APS group configuration mode. To restore the default setting, bidirectional mode, use the **no** form of this command.

unidirectional

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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

The unidirectional or bidirectional automatic protection switching (APS) operation mode of the routers should be matched with the APS operation mode of the connected SONET equipment.

Note We recommend using bidirectional APS mode when it is supported by the interconnecting SONET equipment. When the protect interface is configured as unidirectional, the working and protect interfaces must cooperate to switch the transmit and receive SONET channel in a bidirectional fashion. Cooperation occurs automatically when the SONET network equipment is in bidirectional mode.

In a multirouter APS topology, the **unidirectional** command is allowed only on the protect router.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to configure an APS group for unidirectional mode:

```
RP/0/RP0/CPU0:router(config)# aps group 1
RP/0/RP0/CPU0:router(config-aps)# unidirectional
```

Related Commands

Command	Description
show aps	Displays the operational status for all configured SONET automatic protection switching (APS) groups.

802.1Q VLAN Subinterface Commands on Cisco IOS XR Software

This module contains commands for configuring and monitoring 802.1Q VLAN commands on Cisco IOS XR software.

dot1q native vlan

To assign the native VLAN ID of a physical interface trunking 802.1Q VLAN traffic, use the **dot1q native vlan** command in interface configuration mode. To remove the VLAN ID assignment, use the **no** form of this command.

dot1q native vlan *vlan-id*

no dot1q native vlan *vlan-id*

Syntax Description

vlan-id	Trunk interface ID. Range is from 1 to 4094 inclusive (0 and 4095 are reserved).

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

The **dot1q native vlan** command defines the default, or native VLAN, associated with a 802.1Q trunk interface. The native VLAN of a trunk interface is the VLAN to which all untagged VLAN packets are logically assigned.

Note The native VLAN cannot be configured on a subinterface of the trunk interface. The native VLAN must be configured with the same value at both ends of the link, or traffic can be lost or sent to the wrong VLAN.

Task ID

Task ID	Operations
vlan	read, write

Examples

The following example shows how to configure the native VLAN of a TenGigE0/2/0/4 trunk interface as 1. Packets received on this interface that are untagged, or that have an 802.1Q tag with VLAN ID 1, are received on the main interface. Packets sent from the main interface are transmitted without an 802.1Q tag.

```
RP/0/RP0/CPU0:router(config)# interface TenGigE 0/2/0/4
RP/0/RP0/CPU0:router(config-if)# dot1q native vlan 1
```

Related Commands

Command	Description
dot1q vlan	Assigns a VLAN ID to a subinterface, or changes the VLAN ID assigned to a subinterface.

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 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config-if)# interface GigabitEthernet 0/1/5/0
RP/0/RP0/CPU0:router(config-if)# dot1q tunneling ethertype 0x9100
```

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.

dot1q vlan

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

dot1q vlan *vlan-id*

no dot1q vlan *vlan-id*

Syntax Description

vlan-id	ID of the subinterface. Range is from 1 to 4094 (0 and 4095 are reserved).

Defaults

No default behavior or values

Command Modes

Subinterface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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
```

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.

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** | **Bundle-Ether**}*interface-path-id.subinterface*

no interface {**GigabitEthernet** | **TenGigE** | **Bundle-Ether**}*interface-path-id.subinterface*

Syntax Description

{**GigabitEthernet** | **TenGigE** | **Bundle-Ether**}	Type of Ethernet interface on which you want to create a VLAN. Enter **GigabitEthernet**, **TenGigE**, or **Bundle-Ether**. **Note** Ethernet bundles are available.
interface-path-id.subinterface	Physical interface or virtual interface followed by the subinterface path ID. Naming notation is *interface-path-id.subinterface*. The period in front of the subinterface value is required as part of the notation. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

For the Ethernet bundle interface, the range is from 1 through 65535.

The *subinterface* argument is replaced with the subinterface value. Range is from 0 through 4095.

To configure a large number of subinterfaces, we recommend entering all configuration data before you commit the **interface** command.

To change an interface from Layer 2 to Layer 3 mode and back, you must delete the interface first and then re-configure it in the appropriate mode.

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

Task ID

Task ID	Operations
vlan	read, write

Examples

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
```

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.

show vlan interface

To display summarized information about VLAN subinterfaces, use the **show vlan interface** command in EXEC mode.

show vlan interface [{**GigabitEthernet** | **TenGigE** | **Bundle-Ether**} *interface-path-id.subinterface*
| **location** *interface-path-id*]

Syntax Description

{**GigabitEthernet** | **TenGigE** | **Bundle-Ether**}	(Optional) Type of Ethernet interface whose VLAN information you want to display. Enter **GigabitEthernet**, **TenGigE**, or **Bundle-Ether**. **Note** Ethernet bundles are available.
interface-path-id.subinterface	Physical interface or virtual interface followed by the subinterface path ID. Naming notation is *interface-path-id.subinterface*. The period in front of the subinterface value is required as part of the notation. For more information about the syntax for the router, use the question mark (?) online help function.
location	(Optional) Displays VLAN subinterfaces on a particular port.
interface-path-id	VLAN subinterface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced on the Cisco ASR 14000 Series Router.

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 vlan interface** command without including any of the optional parameters to display summarized information about all VLANs configured on the router.

For the Ethernet bundle interface, the range is from 1 through 65535.

The *subinterface* argument is replaced with the subinterface value. The range is from 0 through 4095.

Task ID

Task ID	Operations
vlan	read

Examples

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

```
RP/0/RP0/CPU0:router#show vlan interface

Interface           Encapsulation  Outer  2nd   Service  MTU    LineP
                                   VLAN   VLAN                  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 45 describes the significant fields shown in the display.

Table 45 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. The services are Layer 2 and Layer 3.
MTU	Maximum transmission unit (MTU) value configured for the specified VLAN, in bytes.
LineP state	Line protocol state of the VLAN interface. The states are up, down, or 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 or for a specific node.
show vlan trunks	Displays summary information about VLAN trunk interfaces.

show vlan tags

To display VLAN tagging allocation information, use the **show vlan tags** command in EXEC mode.

show vlan tags [**Bundle-Ether** *interface-path-id* | **GigabitEthernet** *interface-path-id* | **TenGigE** *interface-path-id* | **location** *node-id*]

Syntax Description

Bundle-Ether *interface-path-id*	(Optional) Displays VLAN tagging information for a specific Ethernet bundle. Use the **show interfaces bundle-ether** command to see a list of all Ethernet bundles currently configured on the router
GigabitEthernet *interface-path-id*	(Optional) 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 *interface-path-id*	(Optional) Displays VLAN tagging information for a specific 10-Gigabit Ethernet interface. **Note** Use the **show interfaces TenGigE** command to see a list of all10-Gigabit Ethernet interfaces currently configured on the router.
location *node-id*	(Optional) Displays VLAN tagging information for a specific node.

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 3.7.1	This command was first introduced on the Cisco ASR 14000 Series Router.

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
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  2nd    Service  MTU    LineP
                    VLAN   VLAN                   State
Gi0/1/5/0.1           10          L3        1518  up
```

```
Gi0/1/5/0.2           20         L3         1518  up
Gi0/1/5/0.3           30         L3         1518  up
```

Table 46 describes the significant fields shown in the display.

Table 46 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, this field is empty.
Service	Service currently assigned to the subinterface. The services are Layer 2 or Layer 3.
MTU	Maximum transmission unit (MTU) value configured for the specified VLAN, in bytes.
LineP state	State of the VLAN interface. The states are up, down, or 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.

show vlan trunks

To display information about VLAN trunks, use the **show vlan trunks** command in EXEC mode.

show vlan trunks [**brief**] [**location** *node-id*] [*type interface-path-id*] [**summary**]

Syntax Description

type	(Optional) Type of Ethernet interface whose VLAN trunk information you want to display. Possible Ethernet types are **GigabitEthernet**, **TenGigE**, or **Bundle-Ether**. Ethernet bundles are available.
interface-path-id	(Optional) Physical interface or an Ethernet bundle interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
brief	(Optional) Displays a short summary output.
summary	(Optional) Displays a summarize output. **Note** The **summary** option is specified only if the trunk interface is not specified.
location *node-id*	(Optional) Displays VLAN trunk information for a specific node.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was first introduced on the Cisco ASR 14000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

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.

For the Ethernet bundle interface, the range is from 1 through 65535.

Task ID

Task ID	Operations
vlan	read

Examples

The following sample output is 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 47 describes the significant fields shown in the display.

Table 47 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. The following Layer 3 encapsulations are listed: • Nat—Native VLAN is configured. • Q—One or more subinterfaces are configured with either 0 or 1 802.1Q VLAN tags. • 2Q—One or more subinterfaces 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. The 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	Native VLAN ID is not configured on this interface.
L2 Encapsulations:	VLAN encapsulations currently used for terminated Layer 2 traffic. The following Layer 2 encapsulations are listed: • Q—One or more single 802.1Q tag ACs are configured. • 2Q—One or more double 802.1Q tag ACs are configured. • Qany—One or more double 802.1Q tag ACs are configured that have a wildcard “any” innertag.

Table 47 show vlan trunks summary Field Descriptions (continued)

Field	Description
VLAN ACs	Number of ACs currently configured under the specified interface.
Single tag ACs	Number of sub-interfaces subinterfaces 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.

INDEX

HR	Cisco ASR 14000 Series Router Interface and Hardware Component Command Reference
MCR	Cisco ASR 14000 Series Router Multicast Command Reference
MPR	Cisco ASR 14000 Series Router MPLS Command Reference
QR	Cisco ASR 14000 Series Router Modular Quality of Service Command Reference
RR	Cisco ASR 14000 Series Router Routing Command Reference
SMR	Cisco ASR 14000 Series Router System Management Command Reference