

General Administration Command Reference for Cisco ASR 9000 Series Routers

First Published: 2023-11-01

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

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.

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.



CDP Commands

- cdp, on page 2
- cdp advertise v1, on page 3
- cdp holdtime, on page 5
- cdp log adjacency changes, on page 6
- cdp timer, on page 7
- clear cdp counters, on page 8
- clear cdp table, on page 9
- show cdp, on page 11
- show cdp entry, on page 13
- show cdp interface, on page 15
- show cdp neighbors, on page 17
- show cdp traffic, on page 20

cdp

To enable the Cisco Discovery Protocol (CDP) globally or on an interface, use the **cdp** command in the appropriate configuration mode. To disable CDP globally or on an interface, use the **no** form of this command.

cdp
no cdp

Syntax Description

This command has no keywords or arguments.

Command Default

CDP is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

By default, CDP is disabled globally. To enable CDP, CDP must be enabled globally and then enabled for each interface.

To enable CDP globally, use the **cdp** command in global configuration mode. To disable CDP globally, use the **no** form of this command in global configuration mode.

To enable CDP on a specific interface, use the **cdp** command in interface configuration mode. To disable CDP on a specific interface, use the **no** form of this command in interface configuration mode.

Task ID

Task ID	Operations
cdp	read, write

The following example shows how to globally enable CDP:

```
RP/0/RSP0/CPU0:router(config)# cdp
```

The following example shows how to enable CDP on an interface:

```
RP/0/RSP0/CPU0:router(config-if)# cdp
```

Related Topics

show cdp, on page 11

cdp advertise v1

To change the version of Cisco Discovery Protocol (CDP) that is used to communicate with neighboring devices to version 1 (CDPv1), use the **cdp advertise v1** command in the appropriate configuration mode. To remove the **cdp advertise v1** command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

cdp advertise v1
no cdp advertise [**v1**]

Syntax Description

This command has no keywords or arguments.

Command Default

Version 2 is enabled.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

CDPv2 packets are sent by default. CDP also sends and receives CDPv1 packets if the device with which CDP is interacting does not process CDPv2 packets.

CDPv2 adds device information over CDPv1. The additional information that is contained in the CDPv2 messages relates to Native VLAN, VLAN Trunking Protocol (VTP) Management Domain, Ethernet Duplex, and other features.

Task ID

Task ID	Operations
cdp	read, write

The following example shows how to set a networking device to send and receive only CDPv1 advertisements:

```
RP/0/RSP0/CPU0:router(config)# cdp advertise v1
```

The following example shows how to restore the default condition (sending and receiving CDPv2 advertisements):

```
RP/0/RSP0/CPU0:router(config)# no cdp advertise
```

Related Topics

cdp, on page 2
show cdp, on page 11

cdp holdtime

To specify the time for which the receiving device should hold a Cisco Discovery Protocol (CDP) packet from your networking device before discarding it, use the **cdp holdtime** command in the appropriate configuration mode. To remove the **cdp holdtime** command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

cdp holdtime *seconds*
no cdp holdtime

Syntax Description

seconds	Holdtime to be sent in the CDP update packets, in seconds. Range is 10 to 255.

Command Default

seconds : 180

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

CDP packets are sent with a time-to-live value or holdtime, that is nonzero after an interface is enabled.

The CDP holdtime must be set to a higher number of seconds than the time between CDP transmissions, which is set using the **cdp time** command.

Task ID

Task ID	Operations
cdp	read, write

The following example shows how to specify that the CDP packets sent from the networking device are held by the receiving device for 60 seconds before being discarded. You might want to set the holdtime lower than the default setting of 180 seconds if information about your networking device changes often and you want the receiving devices to purge this information more quickly.

```
RP/0/RSP0/CPU0:router(config)# cdp holdtime 60
```

Related Topics

cdp timer, on page 7
show cdp, on page 11

cdp log adjacency changes

To log changes to the Cisco Discovery Protocol (CDP) adjacency table, use the **cdp log adjacency changes** command in the appropriate configuration mode. To disable the logging, use the **no** form of this command.

cdp log adjacency changes
no cdp log adjacency changes

Syntax Description

This command has no keywords or arguments.

Command Default

CDP adjacency table logging is disabled.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

When CDP adjacency table logging is enabled, a syslog is generated each time a CDP neighbor is added or removed.

Task ID

Task ID	Operations
cdp	read, write

The following example shows how to enable CDP adjacency table logging:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# cdp log adjacency changes
```

When CDP adjacency table logging is enabled, a syslog is generated each time a CDP neighbor is added or removed. The following is an example of the log entry:

```
LC/0/5/CPU0:Jun 5 10:51:18.081 : cdp[109]: %L2-CDP-6-DELETED_NEIGHBOR :
CDP Neighbour TBA04110127 on interface GigabitEthernet0/5/0/0
  has been deleted, remote interface 3/2

LC/0/5/CPU0:Jun  5 10:51:33.120 : cdp[109]: %L2-CDP-6-NEW_NEIGHBOR :
New CDP neighbor TBA04110127 detected on interface GigabitEthernet0/5/0/0,
  remote interface 3/2
```

Related Topics

show cdp, on page 11

cdp timer

To specify how often the software sends Cisco Discovery Protocol (CDP) updates, use the **cdp timer** command in the appropriate configuration mode. To remove the **cdp timer** configuration command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

cdp timer *seconds*
no cdp timer

Syntax Description

seconds	Frequency with which the Cisco IOS XR software sends CDP updates, in seconds. Range is 5 to 254. The default is 60.

Command Default

seconds : 60

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

A lower timer setting causes CDP updates to be sent more frequently.

Task ID

Task ID	Operations
cdp	read, write

The following example shows how to set the CDP timer to 80 seconds, which is less frequent than the default setting of 60 seconds:

```
RP/0/RSP0/CPU0:router(config)# cdp timer 80
```

Related Topics

cdp holdtime, on page 5
show cdp, on page 11

clear cdp counters

To reset Cisco Discovery Protocol (CDP) traffic counters to zero (0), use the **clear cdp counters** command in EXEC mode.

clear cdp counters location *node-id*

Syntax Description

location *node-id*	Clears CDP traffic counters for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

The counters are set to zero.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
cdp	read, write

The following example shows how to clear CDP counters. The **show cdp traffic** output shows that all traffic counters have been reset to zero (0).

```
RP/0/RSP0/CPU0:router# clear cdp counters
RP/0/RSP0/CPU0:router# show cdp traffic

  CDP counters:
          Packets output: 0, Input: 0
          Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
          No memory: 0, Invalid packet: 0, Truncated: 0
          CDP version 1 advertisements output: 0, Input: 0
          CDP version 2 advertisements output: 0, Input: 0
          Unrecognize Hdr version: 0, File open failed: 0
```

Related Topics

show cdp traffic, on page 20
clear cdp table, on page 9

clear cdp table

To clear and automatically resize the table that contains Cisco Discovery Protocol (CDP) information about neighbors, use the **clear cdp table** command in EXEC mode.

clear cdp table location *node-id*

Syntax Description

location *node-id*	Clears and resizes the CDP table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **clear cdp table** command to clear and resize the CDP table that contains the neighbor entries. The new table size is calculated according to the recommended hash table size, as seen in the **show cdp** command output.

Task ID

Task ID	Operations
cdp	read, write

The following example shows how to clear and resize the CDP table. The output of the **show cdp neighbors** command before and after use of the **clear cdp table** command shows that all information has been deleted from the table:

```
RP/0/RSP0/CPU0:router# show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
TBA04341195(15la Mg0/RP1/CPU0/0    171        T S         WS-C2924  0/1

RP/0/RSP0/CPU0:router# clear cdp table
RP/0/RSP0/CPU0:router# show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
```

The **show cdp** command shows that the table has been resized:

```
RP/0/RSP0/CPU0:router# show cdp

Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is enabled
```

Related Topics

show cdp, on page 11
show cdp neighbors, on page 17

show cdp

To display global Cisco Discovery Protocol (CDP) information, including CDP version, timer, and holdtime information, use the **show cdp** command in

EXEC

mode.

show cdp

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

EXEC

Release	Modification
Release 3.7.2	This command was introduced.
Release 3.9.0	No modification.

Usage Guidelines

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

Use the **show cdp** command to display CDP version, timer, and holdtime information relative to CDP operations.

Task ID

Task ID	Operations
cdp	read

The following example shows how to use the **show cdp** command to verify the CDP global settings:

```
RP/0/RSP0/CPU0:router# show cdp

Global CDP information:
        Sending CDP packets every 20 seconds
        Sending a holdtime value of 30 seconds
        Sending CDPv2 advertisements is not enabled
```

Table 1: show cdp Field Descriptions

Field	Definition
Sending CDP packets every 20 seconds	Interval between transmissions of CDP advertisements. This field is controlled by the **cdp timer** command.

Field	Definition
Sending a holdtime value of 30 seconds	Time for which the device directs the neighbor to hold a CDP advertisement before discarding it. This field is controlled by the **cdp holdtime** command.
Sending CDPv2 advertisements is not enabled	State of being enabled or disabled for the transmission of CDP version 2-type advertisements. This field is controlled by the **cdp advertise v1** command.

Related Topics

cdp advertise v1, on page 3
cdp holdtime, on page 5
cdp timer, on page 7
show cdp entry, on page 13
show cdp neighbors, on page 17
show cdp traffic, on page 20
clear cdp table, on page 9
show cdp interface, on page 15

show cdp entry

To display information about a specific neighboring device or all neighboring devices discovered using Cisco Discovery Protocol (CDP), use the **show cdp entry** command in

EXEC

mode.

show cdp entry {*****_entry-name_} [**protocol** | **version**]

Syntax Description

*****	Displays all CDP neighbors.
entry-name	Name of a neighbor about which you want information.
protocol	(Optional) Displays protocol information associated with CDP neighbor entries.
version	(Optional) Displays version information associated with CDP neighbor entries.

Command Default

This command displays information about a particular device that has been discovered by CDP.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
cdp	read, write

The following example shows sample output from the **show cdp entry** command. Information about device ID, address, platform, interface, holdtime, and version is displayed.

```
RP/0/RSP0/CPU0:router# show cdp entry TBA04341195

-------------------------
Device ID: TBA04341195(sys-235)
SysName : sys-235
Entry address(es):
  IP address: 172.16.23.9
Platform: WS-C6006,  Capabilities: Trans-Bridge Switch
Interface: MgmtEth0/RP1/CPU0/0
Port ID (outgoing port): 4/18
Holdtime : 157 sec
```

```
Version :
WS-C6006 Software, Version McpSW: 7.2(2) NmpSW: 7.2(2)
Copyright (c) 1995-2002 by Cisco Systems

advertisement version: 2
VTP Management Domain: 'sys'
Native VLAN: 125
Duplex: full
```

Table 2: show cdp entry Field Descriptions

Field	Description
Device ID	ID code assigned during installation of the router.
Entry address(es)	Addresses of the platform, selected interface, and port ID.
Platform	Platform name.
Capabilities	Special functions that the platform can perform (in this case the platform is a trans-bridge switch).
Interface	Interface location expressed in *rack* / *slot* / *module* / *port* notation.
Port ID (outgoing port)	Location of the port in use by the interface.
Holdtime	Time (in seconds) for which the device directs the neighbor to hold a CDP advertisement before discarding it. This field is controlled by the **cdp holdtime** command.
Version	Software version.
advertisement version	Version number of the advertising protocol.
VTP Management Domain	VLAN Trunking Protocol (VTP) domain name of neighbor device.
Native VLAN	VLAN ID.
Duplex	Duplex setting: half or full.

Related Topics

show cdp, on page 11
show cdp neighbors, on page 17
show cdp traffic, on page 20
show cdp interface, on page 15

show cdp interface

To display information about the interfaces on which Cisco Discovery Protocol (CDP) is enabled, use the **show cdp interface** command in the appropriate mode.

show cdp interface [*type interface-path-id* | **location** *node-id*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location *node-id*	(Optional) Displays detailed CDP information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

This command displays information about the interfaces on which CDP has been enabled.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **show cdp interface** command to display information about any CDP interfaces. When an interface is specified in the command syntax, information is displayed about the specific interface. Not specifying the interface displays information about all interfaces.

Task ID

Task ID	Operations
cdp	read, write

The following example shows sample output from the **show cdp interface** command. Information about the status, CDP timer, and holdtime settings is displayed for all interfaces on which CDP is enabled.

```
RP/0/RSP0/CPU0:router# show cdp interface
```

```
POS0/2/0/0 is Up
    Encapsulation HDLC
    Sending CDP packets every 120 seconds
    Holdtime is 240 seconds
POS0/2/0/1 is Up
    Encapsulation HDLC
    Sending CDP packets every 120 seconds
    Holdtime is 240 seconds
POS0/2/0/2 is Up
    Encapsulation HDLC
    Sending CDP packets every 120 seconds
    Holdtime is 240 seconds
POS0/2/0/3 is Up
    Encapsulation HDLC
    Sending CDP packets every 120 seconds
    Holdtime is 240 seconds
MgmtEth0/RP1/CPU0/0 is Up
    Encapsulation ARPA
    Sending CDP packets every 120 seconds
    Holdtime is 240 seconds
```

The following example shows sample output from the **show cdp interface** command with an interface specified. Information about the status, CDP timer, and holdtime settings is displayed for Packet-over-SONET/SDH (POS) interface 0/2/0/1 only.

```
RP/0/RSP0/CPU0:router# show cdp interface pos 0/2/0/1

POS0/2/0/1 is Up
    Encapsulation HDLC
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
```

Table 3: show cdp interface Field Descriptions

Field	Description
POS0/2/0/1 is Up	Current condition of POS interface 0/0/2/1.
Encapsulation HDLC	Interface is encoding packets using the Cisco HDLC Layer 2 encapsulation.
Sending CDP packets every 60 seconds	Interval between transmissions of CDP advertisements. This field is controlled by the **cdp timer** command.
Holdtime is 180 seconds	Time for which the device directs the neighbor to hold a CDP advertisement before discarding it. This field is controlled by the **cdp holdtime** command.

Related Topics

show cdp, on page 11
show cdp entry, on page 13
show cdp neighbors, on page 17
show cdp traffic, on page 20

show cdp neighbors

To display detailed information about neighboring devices discovered using Cisco Discovery Protocol (CDP), use the **show cpd neighbors** command in

EXEC

mode.

show cdp neighbors [*type interface-path-id* | **location** *node-id*] [**detail**]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location *node-id*	(Optional) Displays detailed CDP information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
detail	(Optional) Displays detailed information about a neighbor or neighbors, including network address, enabled protocols, holdtime, and software version. The output includes information about both IPv4 and IPv6 addresses.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **show cpd neighbors** command to display information about any CDP neighbors. When a location is specified in the command syntax, information about the neighbor is displayed for the specified node. Not specifying the location displays information about the neighbor for all interfaces.

Use the command with the **detail** keyword to display additional information, including IPv6 neighbors.

Task ID

Task ID	Operations
cdp	read

The following example shows sample output from the **show cpd neighbors** command:

```
RP/0/RSP0/CPU0:router# show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce   Holdtme  Capability  Platform  Port ID

TBA04110127      Gi0/7/0/0       173      T S         WS-C6506  3/9
cisco_1          Gi0/7/0/2       171      R
ASR9K
     Gi0/4/0/2
```

Table 4: show cdp neighbors Field Descriptions

Field	Description
Capability Codes	Type of device that can be discovered.
Device ID	Name of the neighbor device.
Local Intrfce	Protocol being used by the connectivity media and the interface number.
Holdtme	Remaining time, in seconds, for which the current device holds the CDP advertisement from a sending router before discarding it.
Capability	Type of the device listed in the CDP Neighbors table. Values are as follows: R—Router T—Transparent bridge B—Source-routing bridge S—Switch H—Host I—Internet Group Management Protocol (IGMP) device r—Repeater
Platform	Product number of the device.
Port ID	Protocol and port number of the device.

The following examples illustrates sample output for IPv4 and IPv6 neighbors from the **show cpd neighbors** command with the **detail** keyword:

```
RP/0/RSP0/CPU0:router# show cdp neighbor detail
```

```
-------------------------
Device ID: uut-user
SysName : uut-user
Entry address(es):
IPv4 address: 10.0.0.1
IPv6 address: 1::1
IPv6 address: 2::2
Platform: cisco 12008/GRP, Capabilities: Router
Interface: Gi0/4/0/3
Port ID (outgoing port): Gi0/2/0/3
Holdtime : 177 sec

Version :
Cisco IOS XR Software, Version 0.0.0[Default]
Copyright (c) 2005 by cisco Systems, Inc.

advertisement version: 2
```

Table 5: show cdp neighbors detail Field Descriptions

Field	Definition
Device ID	Name of the neighbor device.
Entry address(es)	List of network addresses of neighbor devices. The address can be in IP or in Connectionless Network Service (CLNS) protocol conventions.
Platform	Product name and number of the neighbor device.
Capabilities	Device type of the neighbor. This device can be a router, a bridge, a transparent bridge, a source-routing bridge, a switch, a host, an IGMP device, or a repeater.
Interface	Interface being used by the connectivity medium.
Port ID	Port number of the port on the current device.
Holdtime	Remaining time (in seconds) for which the current device holds the CDP advertisement from a sending router before discarding it.
Version	Software version of the neighbor device.
advertisement version	Version number of the advertising protocol.

Related Topics

show cdp, on page 11
show cdp entry, on page 13
show cdp traffic, on page 20
show cdp interface, on page 15

show cdp traffic

To display information about the traffic gathered between devices using Cisco Discovery Protocol (CDP), use the **show cdp traffic** command in

EXEC

mode.

show cdp traffic [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays CDP information for the CDP packets sent and received on the designated node only. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

Displays CDP information aggregated across all nodes.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
cdp	read

The following example illustrates sample output from the **show cdp traffic** command:

```
RP/0/RSP0/CPU0:router# show cdp traffic

CDP counters :
          Packets output: 50662, Input: 40414
          Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
        No memory: 0, Invalid packet: 0, Truncated: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 50662, Input: 40414
          Unrecognize Hdr version: 0, File open failed: 0
```

Table 6: show cdp traffic Field Descriptions

Field	Definition
Packets output	Number of CDP advertisements sent by the local device. Note that this value is the sum of the CDP version 1 advertisements output field and the CDP version 2 advertisements output field.
Input	Number of CDP advertisements received by the local device. Note that this value is the sum of the CDP version 1 advertisements input field and the CDP version 2 advertisements input field.
Hdr syntax	Number of CDP advertisements having bad headers that have been received by the local device.
Chksum error	Number of times the checksum (verifying) operation failed on incoming CDP advertisements.
Encaps failed	Number of times CDP failed to send advertisements on an interface because of a failure caused by the bridge port of the local device.
No memory	Number of times that the local device did not have enough memory to store the CDP advertisements in the advertisement cache table when the device was attempting to assemble advertisement packets for transmission and parse them when receiving them.
Invalid packet	Number of invalid CDP advertisements received and sent by the local device.
Truncated	Number of times truncated CDP advertisements were sent because there was not enough space in the CDP packet to hold all CDP type-length-values (TLVs).
CDP version 1 advertisements output	Number of CDP version 1 advertisements sent by the local device.
Input	Number of CDP version 1 advertisements received by the local device.
CDP version 2 advertisements output	Number of CDP version 2 advertisements sent by the local device.
Input	Number of CDP version 2 advertisements received by the local device.
Unrecognize Hdr version	Number of packets received from a CDP version that was outside the current configuration.
File open failed	Number of times that CDP failed to connect to one of the underlying services it uses.

Related Topics

show cdp, on page 11
show cdp entry, on page 13
show cdp neighbors, on page 17
show cdp interface, on page 15



Disk Mirroring Commands

- mirror, on page 24
- mirror resume, on page 26
- mirror verify, on page 27
- mirror pause, on page 28
- show mirror, on page 29

mirror

To configure disk mirroring on a node, use the **mirror** command in global configuration mode. To disable disk mirroring, use the **no** form of this command.

mirror location [**preconfigure**] *node-id primary-device***:***secondary-device***:**
no mirror location

Syntax Description

location *node-id*	Specifies the node of the RP. It can be a node that is not yet installed if the **preconfigure** keyword is used. The *node-id* argument is entered in the *rack*/*slot*/*module* notation.
preconfigure	(Optional) Enables you to specify a node that is not yet installed.
primary-device **:**	Specifies the primary boot device used to store installation packages and configuration files. Supported devices are: • **disk0:** • **disk1:** (if installed) • **compactflash:** (if installed)
secondary-device **:**	Storage device on the same RP as the *primary-device*, to where critical data is replicated. Supported devices are the same as for *primary-device* **:**, but *secondary-device* **:** must be different than the *primary-device* **:**.

Command Default

None

Command Modes

Global configuration

Command History

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

The **mirror** command replicates all critical data contained in the primary partition of the primary boot device, onto a second storage device on the same RSP. Therefore, if the primary boot device fails, applications continue to be serviced transparently by the secondary device, without having to switch control to a standby RSP.

Before the **mirror** command can be used, the secondary storage device must be partitioned using the **format** command. If the primary boot device is not partitioned, once mirroring is enabled and all data on the primary boot device is replicated to the secondary device, the primary boot device is partitioned automatically. This guarantees that only critical data on the primary boot device is mirrored to the secondary device. Noncritical

data, such as logging data, should not be mirrored and should, therefore, be saved to the secondary partition on the storage device.

To temporarily suspend disk mirroring without changing the configuration, use the **mirror pause** command in EXEC mode.

Task ID

Task ID	Operations
root-lr	read, write

The following example shows how to configure disk mirroring from the primary boot device (disk0:) to the secondary storage device (disk1:):

```
RP/0/RSP0/CPU0:(config)# mirror location 0/rp0/cpu0 disk0: disk1:
```

mirror resume

To resume disk mirroring on a node after it has been temporarily stopped, use the **mirror resume** command in EXEC or administration EXEC mode.

mirror resume [**location** {*node-id* | **all**}]

Syntax Description

location {*node-id* | **all**}	(Optional) Specifies the node of the RSP. The *node-id* argument is entered in the *rack*/*slot*/*module* notation. The **all** keyword specifies all RSP nodes.

Command Modes

EXEC

Administration EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

The **mirror resume** command resumes the mirroring of the primary boot device after it has been temporarily paused with the **mirror pause** command.

The **mirror resume** command has no affect if the **mirror** configuration command is not enabled and the **mirror pause** command has not been used.

Task ID

Task ID	Operations
root-lr	read, write

The following example shows how to resume disk mirroring on the active RSP:

```
RP/0/RSP0/CPU0:router# mirror resume
```

mirror verify

To verify disk synchronization for disk mirroring on a node, use the **mirror verify** command in EXEC or administration EXEC mode.

mirror verify [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Specifies the node of the RSP. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If no node is specified, the verification is done on the active RSP.

Command Modes

EXEC

Administration EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

The **mirror verify** command verifies the synchronization consistency between the primary and secondary media devices being used in mirroring. The command verifies that the full contents are identical between the mirrored devices and reports any inconsistencies found.

Task ID

Task ID	Operations
root-lr	read, write

The following example shows how to verify the disk mirroring on the active RSP:

```
RP/0/RSP0/CPU0:router# mirror verify


  Mirror Verify Information for 0/RSP0/CPU0.
  ==========================================================
  Primary device and secondary device are fully synchronized.
```

mirror pause

To temporarily pause disk mirroring on a node, use the **mirror pause** command in EXEC or administration EXEC mode.

mirror pause [**location** {*node-id* | **all**}]

Syntax Description

location {*node-id* | **all**}	(Optional) Specifies the node of the RSP. The *node-id* argument is entered in the *rack*/*slot*/*module* notation. The **all** keyword specifies all RSP nodes.

Command Default

If no node is specified, disk mirroring is paused on the active RSP.

Command Modes

EXEC

Administration EXEC

Command History

Usage Guidelines

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

The **mirror pause** command temporarily pauses the mirroring of the primary boot device. This command is primarily useful during an installation operation to prevent significant performance degradation on single CPU boards. The **mirror pause** command does not change the configured state of mirroring, but rather causes the mirroring to be suspended until the **mirror resume** command is used.

The **mirror pause** command has no affect if the **mirror** configuration command is not enabled.

Task ID

Task ID	Operations
root-lr	read, write

The following example shows how to pause disk mirroring on the active RSP:

```
RP/0/RSP0/CPU0:# mirror pause
```

show mirror

To display disk mirroring information, use the **show mirror** command in EXEC or administration EXEC mode.

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

Syntax Description

location {*node-id* | **all**}	(Optional) Specifies the node of the RSP for which to display the mirroring information. The *node-id* argument is entered in the *rack*/*slot*/*module* notation. The **all** keyword specifies all RSP nodes.

Command Default

No default behavior or values

Command Modes

EXEC

Administration EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
filesystem	read

The following is sample output from the **show mirror** command:

```
RP/0/RSP0/CPU0:router# show mirror


 Mirror Information for 0/RSP0/CPU0.
 ===========================================================
  Mirroring Enabled
    Configured Primary:         disk0:
    Configured Secondary:       disk1:

  Current Mirroring State:      Syncing Files
    Current Physical Primary:   disk1:
    Current Physical Secondary: disk0:

  Mirroring Logical Device:     disk0:

  Physical Device     State       Flags
 -----------------------------------------------------------
   disk0:           Available     Enabled Formatted
   disk1:           Available     Enabled Formatted
   compactflash:    Not Present
```

```
   disk0a:          Available     Formatted
   disk1a:          Available     Formatted
   compactflasha:   Not Present

 Mirroring Rommon Variable
  BOOT_DEV_SEQ_CONF = disk0:;disk1:
  BOOT_DEV_SEQ_OPER = disk1:
  MIRROR_ENABLE = Y
```

Table 7: show mirror Field Descriptions

Field	Description
Mirroring Enabled	Indicates whether mirroring is enabled or disabled.
Configured Primary	If mirroring is enabled, the configured primary disk for mirroring.
Configured Secondary	If mirroring is enabled, the configured secondary disk for mirroring.
Current Mirroring State	Current status of mirroring. Possible values are as follows: Syncing files—Files are being synchronized between the primary and secondary disks. Not Configured—Mirroring is not configured. Mirroring Paused—In this state, no mirroring is being done to the secondary device and the disk redundancy has been removed. The values of the BOOT_DEV_SEQ_OPER and MIRROR_ENABLE variables reflect this. Redundant—The primary and secondary disks are totally in synchronization. Any read or write failure on the primary device results in disk redundancy switchover such that all operations are performed on the secondary device.
Current Physical Primary	Current primary disk.
Current Physical Secondary	Current secondary disk.
Mirroring Logical Device	Device name used by the mirroring process to intercept all application requests to that named device before passing them through to one of the mirrored physical devices.
Physical Device	Physical disk in router.
State	Status of the disk. Possible values are as follows: Available—Disk exists in router and is available. Not present—Disk does not exist in router. Partitioning of disks is available only after the disk has been formatted with the **partition** keyword.
Flags	Enabled—Disk mirroring has been enabled on this device and the device is part of the mirroring process. Repaired—During the boot, some minor inconsistencies were discovered on the disk and were repaired to make the file system consistent. Formatted—Disk was formatted before mirroring was enabled.

Field	Description
BOOT_DEV_SEQ_CONF=	ROM Monitor environmental variable for the boot disk sequence. This variable is is set when mirroring is enabled through the **mirror** configuration command. The devices in this ROMMON variable declare the primary and the secondary devices of the mirroring process. The first device is the primary device and the second device is the secondary device in the mirroring process. **Note** This variable is also shared by the disk backup feature. This variable can also be set or unset using the system boot-sequence command of the disk backup feature. But the use of system boot-sequence and system backup commands is blocked, if mirroring is enabled.
BOOT_DEV_SEQ_OPER=	ROM Monitor environmental variable that reflects the state of the disk redundancy status. When mirroring is enabled and the state is redundant, this variable is set to the primary device followed by the secondary device. When mirroring is not in the redundancy state, then this variable is updated to contain only the primary device.
MIRROR_ENABLE	ROM Monitor environmental variable whose value reflects the mirroring status. If it is set to Y, then mirroring is enabled. If it is set to P, then mirroring is paused. If empty, mirroring is not enabled.



Call Home Commands

- active, on page 34
- alert-group disable, on page 35
- call-home, on page 36
- call-home request, on page 37
- call-home send, on page 39
- call-home send alert-group inventory, on page 41
- call-home test, on page 42
- contact smart-licensing, on page 43
- contact-email-addr, on page 44
- contract-id, on page 45
- customer-id, on page 46
- destination address, on page 47
- destination message-size-limit, on page 48
- destination preferred-msg-format, on page 49
- destination transport-method, on page 50
- mail-server, on page 51
- phone-number, on page 53
- profile (call home), on page 54
- rate-limit, on page 55
- sender, on page 56
- service active, on page 57
- show call-home, on page 58
- show call-home alert-group, on page 60
- show call-home mail-server status, on page 61
- show call-home profile, on page 62
- show call-home statistics, on page 64
- show call-home trace, on page 66
- site-id, on page 68
- street-address, on page 69
- subscribe-to-alert-group environment, on page 70
- subscribe-to-alert-group inventory, on page 72
- subscribe-to-alert-group syslog, on page 74

active

To enable a Call Home profile, use the **active** command in call home profile configuration mode. To disable a profile, use the **no** form of this command.

active
no active

Syntax Description

This command has no keywords or arguments.

Command Default

A profile is disabled by default.

Command Modes

Call home configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

You must enable a profile using the **active** command so that call home messages can be triggered.

Task ID

Task ID	Operation
call-home	read, write

The following example shows how to activate a profile:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config) call-home
RP/0/RSP0/CPU0:router(config-call-home)# profile my-profile
RP/0/RSP0/CPU0:router(config-call-home-profile)# active
```

Related Topics

call-home, on page 36
profile (call home), on page 54

alert-group disable

To disable an individual Call Home alert-group, use the **alert group disable** command in call home configuration mode. To enable an individual Call Home alert-group, use the **no** form of this command.

alert-group *alert-group-name* **disable**
no alert-group *alert-group-name* **disable**

Syntax Description

alert-group-name	A keyword that identifies an alert group. Valid values are: • syslog • environment • inventory

Command Default

Alert groups are enabled by default.

Command Modes

Call home configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

By default, alert groups are enabled. Use the **alert-group disable** command to disable alert groups.

Task ID

Task ID	Operation
call-home	read, write

Example

The following example shows how to disable the inventory alert group:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config) call-home
RP/0/RSP0/CPU0:router(config-call-home)# alert-group inventory disable
```

Related Commands

Command	Description
call-home, on page 36	Enters call home configuration mode to configure the call home feature.

call-home

To enter call home configuration mode to configure Call Home, use the **call-home** command in global configuration mode. To remove all Call Home settings and set the technical assistance center (TAC) profile as the default, use the **no** form of this command.

call-home
no call-home

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
call-home	read, write

The following example shows how to enter call home configuration mode:

```
RP/0/RSP0/CPU0:router(config)# call-home
RP/0/RSP0/CPU0:router(config-call-home)#
```

Related Commands

Command	Description
show call-home, on page 58	Displays information regarding the Call Home configuration.

call-home request

To send a customer request to Cisco, use the **call-home request** command in EXEC mode.

call-home request {**bugs-list** | **command-reference** | **config-sanity** | **output-analysis** "*show-command*" | **product-advisory**} {**ccoid** *ccoid* | **profile** *profile-name*}

Syntax Description

bugs-list	Sends output of the following commands: • **show running-config sanitized** • **show version** • **show diag**
command-reference	Sends output of the following commands: • **show running-config sanitized** • **show version** • **show diag**
config-sanity	Sends output of the following commands: • **show running-config sanitized** • **show version**
output-analysis *show-command*	Sends output from the specified show command. The *show-command* argument should be enclosed in quotes ("").
product-advisory	Sends output of all commands included in the enventory message in addition to the output from the **show running-config sanitized** command.
ccoid *ccoid*	Specifies the Smart Call Home user registered ID.
profile *profile-name*	Specifies the profile to which to send the message.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

The message uses the specified profile or the CiscoTAC-1 profile if no profile name is specified to send out the request the the Cisco backend. This ensures that users who use a transport gateway can use a different profile than the CiscoTAC-1 profile to send the request to their email server first before forwarding to the Cisco backend. CiscoTAC-1 or any profile specified needs to be enabled before you can send out the request.

If the CCO ID is not specified, the contact email address of the device is used.

Each message sent includes the CLI command ouput specified for each subcommand. After the message is sent, a syslog message is displayed indicating whether the request was sent successfully or not.

Task ID

Task ID	Operation
call-home	read, write

The following example shows how to send a message with output from the **show version** command to engineer@cisco.com:

```
RP/0/RSP0/CPU0:router(config)# call-home request config-sanity ccoid
xyz
RP/0/RSP0/CPU0:router(config)# call-home request bugs-list
RP/0/RSP0/CPU0:router(config)# call-home request output-analysis "show log"
profile TG
RP/0/RSP0/CPU0:router(config)#  call-home request output-analysis "show
running-config"
```

Related Commands

Command	Description
call-home, on page 36	Enters call home configuration mode to configure the call home feature.
show call-home, on page 58	Displays information regarding the Call Home configuration.

call-home send

To send the output from a specific command as a Call Home message, use the **call-home send** command in EXEC mode.

call-home send "*cli-command*" {**email** *email-address* | **tac-service-request** *service-number*}

Syntax Description

cli-command	Any CLI command that can be run at the prompt.
email *email-address*	Specifies the email address to which to send the call home message.
tac-service-request *service-number*	Specifies the Technical Assistance Center (TAC) service request number.

Command Default

If no email address is specified, attach@cisco.com is used.

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

The specified CLI command is generally a show command with output that is required by the TAC to analyze a specific issue. The CLI command must be enclosed in quotes. The CLI command output is sent to the specified email address in long text format with the service request number in the subject of the email. If no email address is specified, the TAC service request number must be specified. By default, messages are sent to attach@cisco.com. If no TAC service request number is specified, TAC email is rejected.

Task ID

Task ID	Operation
call-home	read, write

The following example shows how to send a message with output from the **show version** command to engineer@cisco.com:

```
RP/0/RSP0/CPU0:router(config)# call-home send "show version" engineer@cisco.com
```

Related Commands

Command	Description
call-home, on page 36	Enters call home configuration mode to configure the call home feature.

Command	Description
show call-home, on page 58	Displays information regarding the Call Home configuration.

call-home send alert-group inventory

To send an inventory Call Home message to all subscribed profiles or the specified profile, use the **call-home send alert-group inventory** command in EXEC mode.

call-home send alert-group inventory [**profile** *profile-name*]

Syntax Description

profile *profile-name*	Specifies the profile to which to send the inventory Call Home message.

Command Default

If no profile is specified, the message is sent to all subscribed profiles.

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

The profile specified by the *profile-name* argument does not need to be subscribed to the inventory alert-group.

Task ID

Task ID	Operation
call-home	read, write

The following example shows how to send an inventory message to the myprofile profile:

```
RP/0/RSP0/CPU0:router(config)# call-home send alert-group inventory profile myprofile
```

Related Commands

Command	Description
call-home, on page 36	Enters call home configuration mode to configure the call home feature.
show call-home, on page 58	Displays information regarding the Call Home configuration.

call-home test

To send a test Call Home message to the specified profile, use the **call-home test** command in EXEC mode.

call-home test [*test-message-text*] **profile** *profile-name*

Syntax Description

test-message-text	Text to be sent in the test message. If the message text is not specified, a default message is sent.
profile *profile-name*	Specifies the profile to which to send the test call home message.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
call-home	read, write

The following example shows how to send a test Call Home message:

```
RP/0/RSP0/CPU0:router(config)# call-home test "this is a test message" profile myprofile
```

Related Commands

Command	Description
call-home, on page 36	Enters call home configuration mode to configure the call home feature.
show call-home, on page 58	Displays information regarding the Call Home configuration.

contact smart-licensing

To send notification emails to your Smart Licensing account, use **contact smart-licensing** command in the **call-home** configuration mode. To disable the contact, use the **no** form of this command.

contact smart-licensing
no contact smart-licensing

Syntax Description

This command has no keywords or arguments.

Command Default

contact smart-licensing is not configured.

Command Modes

call-home configuration mode.

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

The Smart Call Home back-end service uses the email address configured in your Smart Licensing account as the destination address for the notification mails. Enabling Smart Licensing also enables call-home which changes several mandatory configurations in call-home. **contact smart-licensing** is one of the configurations that is automatically added when you enable smart-licensing.

Note The **contact-email-addr** command and the **contact smart-licensing** command cannot be configured simultaneously.

Task ID

Task ID	Operation
call-home	Read, Write

Example

This example shows how to configure the contact email address:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# call-home
RP/0/RSP0/CPU0:router(config-call-home)# contact smart-licensing
```

contact-email-addr

To specify a contact email address for the system, use the **contact-email-addr** command in call home configuration mode. To disable the contact email address, use the **no** form of this command.

contact-email-addr *email-addr*
no contact-email-addr *email-addr*

Syntax Description

email-addr	The email address of the system contact.

Command Default

No contact email address is defined.

Command Modes

Call home configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

The contact email address is a mandatory user-configurable field that must be configured before Call Home messages are triggered.

Task ID

Task ID	Operation
call-home	read, write

The following example shows how to configure the contact email address:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config) call-home
RP/0/RSP0/CPU0:router(config-call-home)# contact-email-addr contact@cisco.com
```

contract-id

To specify a contract identifier for the system, use the **contract-id** command in call home configuration mode. To disable the contract identifier, use the **no** form of this command.

contract-id *contract-id-string*
no contract-id *contract-id-string*

Syntax Description

contract-id-string	A string that identifies a service contract.

Command Default

No contract ID is defined.

Command Modes

Call home configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

The contract ID is an optional user-configurable field that can be used for contract information or any other identification information for the support service.

Task ID

Task ID	Operation
call-home	read, write

The following example shows how to configure the contract ID:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config) call-home
RP/0/RSP0/CPU0:router(config-call-home)# contract-id contract
```

customer-id

To specify a customer identifier for the system, use the **customer-id** command in call home configuration mode. To disable the customer identifier, use the **no** form of this command.

customer-id *contract-id-string*
no customer-id *contract-id-string*

Syntax Description

customer-id-string	A string that identifies the customer.

Command Default

No customer ID is defined.

Command Modes

Call home configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

The customer ID is an optional user-configurable field that can be used for contract information or any other identification information of a support service.

Task ID

Task ID	Operation
call-home	read, write

The following example shows how to configure the customer ID:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config) call-home
RP/0/RSP0/CPU0:router(config-call-home)# customer-id cisco
```

destination address

To specify an email address to which Call Home messages are sent, use the **destination address** command in call home profile configuration mode. To disable the contract identifier, use the **no** form of this command.

destination address *email-address*
no destination address *email-address*

Syntax Description

email-address	Email address to which short-text and long-text Call Home messages and XML-based Call Home messages are to be sent.

Command Default

No destination email address is defined.

Command Modes

Call home profile configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

You must define a destination email address to send out Call Home messages.

Task ID

Task ID	Operation
call-home	read, write

The following example shows how to configure the destination email address:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config) call-home
RP/0/RSP0/CPU0:router(config-call-home)# profile my-profile
RP/0/RSP0/CPU0:router(config-call-home-profile)# destination address user@cisco.com
```

Related Commands

Command	Description
profile (call home), on page 54	Enters call home profile configuration mode to create or configure a Call Home profile.

destination message-size-limit

To specify the message size limit for call home messages for a specific profile, use the **destination message-size-limit** command in Call Home profile configuration mode. To disable the message size limit, use the **no** form of this command.

destination message-size-limit *maximum-size*
no destination message-size-limit *maximum-size*

Syntax Description

maximum-size	Maximum message size in bytes.

Command Default

The default maximum message size is 3 Mbytes.

Command Modes

Call home profile configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

The destination maximum message size can be optionally set to limit the size of Call Home messages.

Task ID

Task ID	Operation
call-home	read, write

The following example shows how to configure the contract ID:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config) call-home
RP/0/RSP0/CPU0:router(config-call-home)# profile my-profile
RP/0/RSP0/CPU0:router(config-call-home-profile)# destination maximum-message-size 2000
```

Related Commands

Command	Description
profile (call home), on page 54	Enters call home profile configuration mode to create or configure a Call Home profile.

destination preferred-msg-format

To specify the message format for a profile, use the **destination preferred-msg-format** command in call home profile configuration mode. To revert to the default message format, use the **no** form of this command.

destination preferred-msg-format {**long-text** | **short-text** | **xml**}
no destination preferred-msg-format {**long-text** | **short-text** | **xml**}

Syntax Description

long-text	Specifies to send clear text long Call Home messages, that contain formatting to enable easy readability.
short-text	Specifies to send clear text short Call Home messages, that are designed for use with text pagers.
xml	Specifies to send the same text as the long text messages, with the addition of XML tagging and Adaptive Messaging Language (AML) specific transport information to allow machine-readable parsing and correct routing of the message.

Command Default

The default message format is xml.

Command Modes

Call home profile configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
call-home	read, write

The following example shows how to configure the message format to short text:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config) call-home
RP/0/RSP0/CPU0:router(config-call-home)# profile my-profile
RP/0/RSP0/CPU0:router(config-call-home-profile)# destination preferred-msg-format short-text
```

Related Commands

Command	Description
profile (call home), on page 54	Enters call home profile configuration mode to create or configure a Call Home profile.

destination transport-method

To specify the transport method for Call Home messages for a specific profile, use the **destination transport-method** command in call home profile configuration mode. To disable the transport method, use the **no** form of this command.

destination transport-method email
no destination transport-method email

Syntax Description

email	Email is used to send call home messages.

Command Default

The default transport method is email.

Command Modes

Call home profile configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

The only transport method supported in this release is email.

Task ID

Task ID	Operation
call-home	read, write

The following example shows how to configure the transport method to be email:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config) call-home
RP/0/RSP0/CPU0:router(config-call-home)# profile my-profile
RP/0/RSP0/CPU0:router(config-call-home-profile)# destination transport-method email
```

Related Commands

Command	Description
profile (call home), on page 54	Enters call home profile configuration mode to create or configure a Call Home profile.

mail-server

To specify and configure the various mail servers for sending Call Home messages, use the **mail-server** command in call home configuration mode. To remove the mail server configuration, use the **no** form of this command.

mail-server {*ip-addressname*} **priority** *priority*
no mail-server {*ip-addressname*} **priority** *priority*

Syntax Description

ip-address	An IPv4 address to use as the mail server.
name	Name of server to use as the mail server.
priority *priority*	Priority to be used to determine which of multiple configured servers to use as the mail server. Values can be from 1 to 100. A server with a lower priority is tried first.

Command Default

No mail server is defined.

Command Modes

Call home configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

You must configure a mail server if the user profile is configured to send email messages only. Only IPv4 addresses are supported.

Up to five mail servers can be configured. Specify a priority for each mail server so the system knows which to try first.

Task ID

Task ID	Operation
call-home	read, write

The following example shows how to configure a mail server:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config) call-home
RP/0/RSP0/CPU0:router(config-call-home)# email-server 209.165.200.225
```

Related Commands

Command	Description
call-home, on page 36	Enters call home configuration mode to configure the call home feature.

phone-number

To specify a phone number to contact regarding the system, use the **phone-number** command in call home configuration mode. To remove the configured phone number, use the **no** form of this command.

phone-number *phone-number-string*
no phone-number *phone-number-string*

Syntax Description

phone-number-string	Phone number of the contact for the system. The number should always begin with a plus sign (+).

Command Default

No phone number is defined.

Command Modes

Call home configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

The phone number is an optional user-configurable field.

Task ID

Task ID	Operation
call-home	read, write

The following example shows how to configure the phone number of the system contact:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config) call-home
RP/0/RSP0/CPU0:router(config-call-home)# phone-number +15435432101
```

profile (call home)

To enter call home profile configuration mode to create a user-defined profile or configure an existing Call Home profile, use the **profile** command in call home configuration mode. To delete a user-defined profile, use the **no** form of this command.

profile *profile-name*
no profile *profile-name*

Syntax Description

profile-name	A string that identifies the name of profile to create or configure.

Command Default

The tac profile exists by default.

Command Modes

Call home configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Use the profile command to create a new profile or modify an existing profile. When you use the **no profile** command, the user-defined profile is deleted and the CiscoTAC-1 profile is set to default. A warning message is displayed when the CiscoTAC-1 profile is set to default.

Task ID

Task ID	Operation
call-home	read, write

The following example shows how to create a profile called new-profile:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config) call-home
RP/0/RSP0/CPU0:router(config-call-home)# profile new-profile
RP/0/RSP0/CPU0:router(config-call-home-profile)#
```

Related Commands

Command	Description
active, on page 34	Enables a Call Home profile.
destination address, on page 47	Specifies an email address to which Call Home messages are sent.

rate-limit

To specify a Call Home event trigger rate limit, use the **rate-limit** command in call home configuration mode. To disable the configured rate limit, use the **no** form of this command.

rate-limit *events-count*
no rate-limit *events-count*

Syntax Description

events-count	Number of events that can be triggered per minute. The default is five events. The maximum is five events.

Command Default

5 events per minute

Command Modes

Call home configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
call-home	read, write

Example

The following example shows how to configure the rate limit to be 3 events per minute:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config) call-home
RP/0/RSP0/CPU0:router(config-call-home)# rate-limit 3
```

sender

To specify the from and reply-to email addresses for Call Home email messages, use the **sender** command in call-home configuration mode. To remove these email addresses from the configuration, use the **no** form of this command.

sender {**from** | **reply-to**}*email-address*
no sender {**from** | **reply-to**}*email-address*

Syntax Description

from	Specifies the email address to be used as the from field in Call Home email messages.
reply-to	Specifies the email address to be used as the reply-to field in Call Home email messages.
email-address	A string that identifies a valid email address.

Command Default

No sender email is configured.

Command Modes

Call-home configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
call-home	read, write

The following example shows how to configure the from and reply-to email addresses:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config) call-home
RP/0/RSP0/CPU0:router(config-call-home)# sender from user1@cisco.com
RP/0/RSP0/CPU0:router(config-call-home)# sender reply-to user1@cisco.com
```

service active

To enable the Call Home capability, use the **service active** command in call home configuration mode. To disable the Call Home capability, use the **no** form of this command.

service active
no service active

Syntax Description

This command has no keywords or arguments.

Command Default

Call Home is disabled by default.

Command Modes

Call home configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

It is mandatory to enable the Call Home capability using the **service active** command to allow events to get triggered and send out Call Home messages.

Task ID

Task ID	Operation
call-home	read, write

The following example shows how to enable the Call Home capability:

```
RP/0/RSP0/CPU0:router(config-call-home)# service active
```

show call-home

To display information regarding the Call Home configuration, use the **show call-home** command in EXEC mode.

show call-home [**detail**]

Syntax Description

detail	Displays Call Home general settings, alert group settings, and all available profiles.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
call-home	read

The following example shows how to display detailed call home configuration information:

```
RP/0/RSP0/CPU0:router# show call-home detail

Wed Apr  6 02:00:27.789 DST

Current call home settings:
    call home feature : disable
    call home message's from address: Not yet set up
    call home message's reply-to address: Not yet set up

    contact person's email address: Not yet set up

    contact person's phone number: Not yet set up
    street address: Not yet set up
    customer ID: Not yet set up
    contract ID: Not yet set up
    site ID: Not yet set up

    Mail-server: Not yet set up
    Rate-limit: 5 event(s) per minute

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- --------------------------------
    environment              Enable  environmental info
```

```
    inventory               Enable  inventory info
    syslog                  Enable  syslog info

Profiles:

Profile Name: CiscoTAC-1
    Profile status: INACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): callhome@cisco.com

    Periodic inventory info message is scheduled every 24 day of the month at 16:35

    Alert-group               Severity
    ------------------------  ------------
    environment               minor
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major
```

Related Commands

Command	Description
call-home, on page 36	Enters call home configuration mode to configure the call home feature.

show call-home alert-group

To display available Call Home alert groups, use the **show call-home alert-group** command in EXEC mode.

show call-home alert-group

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
call-home	read, write

The following example shows how to display Call Home alert group information:

```
RP/0/RSP0/CPU0:router# show call-home alert-group

Tue Apr  5 06:51:02.860 DST

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- --------------------------------
    environment              Enable  environmental info
    inventory                Enable  inventory info
    syslog                   Enable  syslog info
```

show call-home mail-server status

To displays the status of the configured mail servers, use the **show call-home mail-server status** command in EXEC mode.

show call-home mail-server status

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
call-home	read

The following example shows sample output from the **show call-home mail-server status** command:

```
RP/0/RSP0/CPU0:router# show call-home mail-server status

Please wait. Checking for mail server status ...

Mail-server[1]: Address: 64.102.124.15 Priority: 50 [Available]
```

Related Commands

Command	Description
call-home, on page 36	Enters call home configuration mode to configure the call home feature.

show call-home profile

To display the Call Home profiles, use the **show call-home profile** command in EXEC mode.

show call-home profile {**all***profile-name*}

Syntax Description

all	Displays information for all profiles.
profile-name	Name of the profile for which to display information.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
call-home	read

The following example shows sample output from the **show call-home profile** command:

```
RP/0/RSP0/CPU0:router# show call-home profile CiscoTAC-1

Profile Name: CiscoTAC-1
    Profile status: INACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): callhome@cisco.com

   Periodic inventory info message is scheduled every 4 day of the month at 12:19

    Alert-group               Severity
    ------------------------  ------------
    environment               minor

    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major
```

Related Commands

Command	Description
call-home, on page 36	Enters call home configuration mode to configure the call home feature.

show call-home statistics

To display Call Home statistics, use the **show call-home statistics** command in EXEC mode.

show call-home statistics

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
call-home	read

The following example shows sample output from the **show call-home statistics** command:

```
RP/0/RSP0/CPU0:router# show call-home statistics

Message Types    Total                Email
-------------   -------------------- --------------------
Total Success   2                    2
    Environment 0                    0
    Inventory   2                    2
    SysLog      0                    0
    Test        0                    0
    Request     0                    0
    Send-CLI    0                    0

Total In-Queue  0                    0
    Environment 0                    0
    Inventory   0                    0
    SysLog      0                    0
    Test        0                    0
    Request     0                    0
    Send-CLI    0                    0

Total Failed    0                    0
    Environment 0                    0
    Inventory   0                    0
    SysLog      0                    0
    Test        0                    0
    Request     0                    0
    Send-CLI    0                    0
```

```
Total Ratelimit
      -dropped  0                    0
    Environment 0                    0
    Inventory   0                    0
    SysLog      0                    0
    Test        0                    0
    Request     0                    0
    Send-CLI    0                    0

Last call-home message sent time: 2010-04-21 01:06:44 GMT+00:00
```

Related Commands

Command	Description
call-home, on page 36	Enters call home configuration mode to configure the call home feature.

show call-home trace

To display Call Home trace information, use the **show call-home trace** command in EXEC mode.

show call-home trace {**all** | **error** | **event**} {**file** *filename* **original location** *node-id* | **hexdump** | **last** *n* | **location** {*node-id* | **all**} | **reverse** | **stats** | **tailf** | **unique** | **verbose** | **wrapping**}

Syntax Description

all	(Optional) Displays both error and event traces.
error	(Optional) Displays error trace entries.
event	(Optional) Displays event trace entries.
file *filename* **original location** *node-id*	(Optional) Specifies a filename and original location of the file to display.
hexdump	(Optional) Displays traces in hexadecimal format.
last *n*	(Optional) Displays the last *n* number of traces only.
location {*node-id* | **all**}	Specifies the RP node for which to display the execution path monitoring information. The *node-id* argument is expressed in the *rack/slot/module* notation. The **all** keyword specifies all RP nodes.
reverse	(Optional) Displays the most recent traces first.
stats	(Optional) Displays execution path statistics.
tailf	(Optional) Displays new traces as they are added.
unique	(Optional) Displays unique entries only, along with the count of the number of times this entry appears.
verbose	(Optional) Displays additional internal debugging information.
wrapping	(Optional) Displays wrapping entries.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
call-home	read

The following example shows how to display Call Home trace information:

```
RP/0/RSP0/CPU0:router# show call-home trace event last 15 stats

Wed Apr  6 05:11:59.984 DST
/dev/shmem/ltrace/call_home/trace wrapping: 28.672 Mbytes/sec for 512 entries
59 wrapping entries (512 possible, 0 filtered, 59 total)
Mar  3 13:26:20.281 call_home/trace 0/RSP0/CPU0 t14 Checking mail server access during
boot-up
Mar  3 13:26:20.281 call_home/trace 0/RSP0/CPU0 t9  processing mail server status checking
 event: data1 0x5005784c, str1
Mar  3 13:27:20.283 call_home/trace 0/RSP0/CPU0 t9  Checking mail server access during
boot-up
Mar  3 13:27:20.283 call_home/trace 0/RSP0/CPU0 t14 processing mail server status checking
 event: data1 0x5005784c, str1
Mar  3 13:28:20.285 call_home/trace 0/RSP0/CPU0 t14 Checking mail server access during
boot-up
Mar  3 13:28:20.285 call_home/trace 0/RSP0/CPU0 t9  processing mail server status checking
 event: data1 0x5005784c, str1
Mar  3 13:29:20.287 call_home/trace 0/RSP0/CPU0 t9  Checking mail server access during
boot-up
Mar  3 13:29:20.287 call_home/trace 0/RSP0/CPU0 t14 processing mail server status checking
 event: data1 0x5005784c, str1
Mar  3 13:30:20.289 call_home/trace 0/RSP0/CPU0 t14 Checking mail server access during
boot-up
Mar  3 13:30:20.289 call_home/trace 0/RSP0/CPU0 t9  processing mail server status checking
 event: data1 0x5005784c, str1
Mar  3 13:31:20.290 call_home/trace 0/RSP0/CPU0 t9  Checking mail server access during
boot-up
Mar  3 13:31:20.290 call_home/trace 0/RSP0/CPU0 t14 processing mail server status checking
 event: data1 0x5005784c, str1
Mar  3 13:32:21.067 call_home/trace 0/RSP0/CPU0 t14 Checking mail server access during
boot-up
Mar  3 13:32:21.067 call_home/trace 0/RSP0/CPU0 t9  processing mail server status checking
 event: data1 0x5005784c, str1
Mar  3 13:33:21.069 call_home/trace 0/RSP0/CPU0 t9  Checking mail server access during
boot-up
```

Related Commands

Command	Description
call-home, on page 36	Enters call home configuration mode to configure the call home feature.

site-id

To specify a site identifier for the system, use the **site-id** command in call-home configuration mode. To disable the site identifier, use the **no** form of this command.

site-id *site-id-string*
no site-id *site-id-string*

Syntax Description

site-id-string	A string that identifies the site.

Command Default

No site ID is defined.

Command Modes

Call-home configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

The site ID is an optional user-configurable field that can be used to specify a Cisco-supplied site ID or other data meaningful to the support service.

Task ID

Task ID	Operation
call-home	read, write

This example shows how to configure the site ID:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config) call-home
RP/0/RSP0/CPU0:router(config-call-home)# site-id Cisco-site
```

street-address

To specify the street address of the system, use the **street-address** command in call home configuration mode. To remove the street address configuration, use the **no** form of this command.

street-address *street-address*
no street-address *street-address*

Syntax Description

street address	A string that identifies the street address of the system.

Command Default

No street address is defined.

Command Modes

Call home configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

The street address is an optional user-configurable field that can be used to provide the address of the system to the support service.

Task ID

Task ID	Operation
call-home	read, write

This example shows how to configure the street address:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config) call-home
RP/0/RSP0/CPU0:router(config-call-home)# street-address 170 West Tasman Dr.
San Jose, CA 95134 USA
```

subscribe-to-alert-group environment

To configure a destination profile to receive messages for the environment alert group, use the **subscribe-to-alert-group environment** command in call home profile configuration mode. To disable the subscription, use the **no** form of this command.

subscribe-to-alert-group environment severity *severity-level*
no subscribe-to-alert-group environment severity *severity-level*

Syntax Description

severity	Specifies the the lowest level of severity events to include in an environment alert.
severity-level	• **catastrophic**—Includes network-wide catastrophic events in the alert. This is the highest severity. • **critical**—Includes events requiring immediate attention (system log level 1). • **debugging**—Includes debug events (system log level 7). This is the lowest severity. • **disaster**—Includes events with significant network impact. • **fatal**—Includes events where the system is unusable (system log level 0). • **major**—Includes events classified as major conditions (system log level 2). • **minor**—Includes events classified as minor conditions (system log level 3) • **normal**—Specifies the normal state and includes events classified as informational (system log level 6). This is the default. • **notification**—Includes events informational message events (system log level 5). • **warning**—Includes events classified as warning conditions (system log level 4).

Command Default

The environment alert group is disabled by default. The default severity for the environment alert group is debugging.

Command Modes

Call home profile configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

At least one alert group subscription is mandatory for a profile so that a valid event can be triggered.

Task ID

Task ID	Operation
call-home	read, write

The following example shows how to configure the environment alert group to include severity major:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config) call-home
RP/0/RSP0/CPU0:router(config-call-home)# profile my-profile
RP/0/RSP0/CPU0:router(config-call-home-profile)# subscribe-to-alert-group environment major
```

Related Commands

Command	Description
profile (call home), on page 54	Enters call home profile configuration mode to create or configure a Call Home profile.
subscribe-to-alert-group syslog, on page 74	Configures a destination profile to receive messages for the syslog alert group.
subscribe-to-alert-group inventory, on page 72	Configures a destination profile to receive messages for the inventory alert group.

subscribe-to-alert-group inventory

To configure a destination profile to receive messages for the inventory alert group, use the **subscribe-to-alert-group inventory** command in call home profile configuration mode. To disable the subscription, use the **no** form of this command.

subscribe-to-alert-group inventory [**periodic** {**daily** | **monthly** *day-of-month* | **weekly** *day-of-week*} *time*]
no subscribe-to-alert-group inventory [**periodic** {**daily** | **monthly** *day-of-month* | **weekly** *day-of-week*} *time*]

Syntax Description

periodic	Specifies to send an inventory message periodically.
daily	Sends daily inventory messages.
monthly *day-of-month*	Sends monthly inventory messages on the day of the month specified.
weekly *day-of-week*	Sends weekly inventory messages on the day of the week specified.
time	Time to send the inventory message, in the format `hour:minutes`.

Command Default

The inventory alert group is disabled by default. The default severity for the inventory alert group is normal.

Command Modes

Call home profile configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

At least one alert group subscription is mandatory for a profile so that a valid event can be triggered.

There are two types of subscription for an inventory alert group. One is normal subscription, meaning that the severity is set to normal, and any (online insertion and removal) OIR event triggers the event. The second is periodic subscription, using the **periodic** keyword, meaning that an event is triggered only when the specified time arrives.

Task ID

Task ID	Operation
call-home	read, write

This example shows how to configure the sending of inventory messages every Monday:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config) call-home
```

```
RP/0/RSP0/CPU0:router(config-call-home)# profile my-profile
RP/0/RSP0/CPU0:router(config-call-home-profile)# subscribe-to-alert-group inventory periodic
 weekly monday
```

Related Commands

Command	Description
profile (call home), on page 54	Enters call home profile configuration mode to create or configure a Call Home profile.
subscribe-to-alert-group environment, on page 70	Configures a destination profile to receive messages for the environment alert group.
subscribe-to-alert-group syslog, on page 74	Configures a destination profile to receive messages for the syslog alert group.

subscribe-to-alert-group syslog

To configure a destination profile to receive messages for the syslog alert group, use the **subscribe-to-alert-group syslog** command in call home profile configuration mode. To disable the subscription, use the **no** form of this command.

subscribe-to-alert-group syslog severity *severity-level* **pattern** *match*
no subscribe-to-alert-group syslog severity *severity-level* **pattern** *match*

Syntax Description

severity	Specifies the the lowest level of severity events to include in a syslog alert.
severity-level	• **catastrophic**—Includes network-wide catastrophic events in the alert. This is the highest severity. • **critical**—Includes events requiring immediate attention (system log level 1). • **debugging**—Includes debug events (system log level 7). This is the lowest severity. • **disaster**—Includes events with significant network impact. • **fatal**—Includes events where the system is unusable (system log level 0). • **major**—Includes events classified as major conditions (system log level 2). • **minor**—Includes events classified as minor conditions (system log level 3) • **normal**—Specifies the normal state and includes events classified as informational (system log level 6). This is the default. • **notification**—Includes events informational message events (system log level 5). • **warning**—Includes events classified as warning conditions (system log level 4).
pattern	Specifies a syslog string pattern to match.
match	A string that when matched in the syslog message, is included in the alert notification. If the pattern contains spaces, you must enclose it in quotes (" ").

Command Default

The syslog alert group is disabled by default. The default severity for the syslog alert group is debugging.

Command Modes

Call home profile configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

At least one alert group subscription is mandatory for a profile so that a valid event can be triggered.

Task ID

Task ID	Operation
call-home	read, write

The following example shows how to configure the syslog alert group to include severity notification:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config) call-home
RP/0/RSP0/CPU0:router(config-call-home)# profile my-profile
RP/0/RSP0/CPU0:router(config-call-home-profile)# subscribe-to-alert-group syslog severity
notification pattern "UPDOWN"
```

Related Commands

Command	Description
profile (call home), on page 54	Enters call home profile configuration mode to create or configure a Call Home profile.
subscribe-to-alert-group environment, on page 70	Configures a destination profile to receive messages for the environment alert group.



Configuration Management Commands

- abort, on page 79
- admin, on page 80
- activate advanced, on page 81
- alias, on page 82
- apply-group, on page 85
- apply-group-remove, on page 87
- apply-template, on page 88
- clear comment, on page 89
- clear configuration commits, on page 90
- clear configuration inconsistency, on page 92
- clear configuration inconsistency replica, on page 95
- clear configuration sessions, on page 97
- commit, on page 99
- configuration commit auto-save, on page 103
- configure, on page 105
- description (interface), on page 107
- do, on page 108
- end, on page 109
- end-group, on page 111
- end-template, on page 112
- exclude-group, on page 113
- exit, on page 114
- group (configuration), on page 116
- hostname, on page 121
- ipv6-enable, on page 122
- load, on page 123
- load commit changes, on page 125
- load configuration failed, on page 126
- load configuration removed, on page 127
- load rollback changes, on page 128
- man, on page 129
- more, on page 132
- pwd (config), on page 136

- rollback configuration, on page 137
- root, on page 140
- save configuration, on page 142
- save configuration changes, on page 144
- save configuration commit changes, on page 146
- save configuration failed, on page 148
- save configuration merge, on page 150
- save configuration removed, on page 151
- save rollback changes, on page 153
- set default-afi, on page 155
- set default-safi, on page 156
- set default-vrf, on page 157
- show, on page 159
- show aliases, on page 162
- show apply-group, on page 163
- show commit changes diff, on page 164
- show configuration (config), on page 167
- show configuration changes, on page 169
- Show configuration commit changes, on page 171
- show configuration commit list, on page 174
- show configuration failed, on page 176
- show configuration failed (config), on page 177
- show configuration failed incompatible, on page 179
- show configuration failed remove, on page 180
- show configuration failed rollback, on page 182
- show configuration failed startup, on page 183
- show configuration history, on page 184
- show configuration inconsistency replica, on page 188
- show configuration persistent, on page 190
- show configuration removed, on page 192
- show configuration rollback changes, on page 194
- show configuration running, on page 196
- show configuration running-config, on page 198
- show configuration sessions, on page 200
- show default-afi-safi-vrf, on page 202
- show history, on page 203
- snmp-server script, on page 205
- show running-config, on page 206
- service cli commit-optimized enable, on page 209
- template, on page 210

abort

To terminate a configuration session and discard all uncommitted changes without system confirmations, use the **abort** command in any configuration mode.

abort

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **abort** command to terminate a configuration session and return to EXEC mode from any configuration mode. This command discards all uncommitted configuration changes. You are prompted to commit the changes.

Task ID

Task ID	Operations
Task ID for the feature or mode impacted by the command	Operation for the feature or mode impacted by the command

The following example shows how to use the **abort** command to discard all changes made during a configuration session:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/0
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 10.0.0.1 255.0.0.0
RP/0/RSP0/CPU0:router(config-if)# abort
RP/0/RSP0/CPU0:router#
```

Related Topics

end, on page 109
exit, on page 114

admin

To enter Admin EXEC mode, use the **admin** command in EXEC mode.

admin

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **admin** command to enter Admin EXEC mode mode. Administration commands are used to execute various administration plane commands.

Note Administration commands can be run only by entering administration mode and not by prefixing the **admin** command with the keyword in EXEC mode mode.

Task ID

Task ID	Operations
admin	read, write, execute

The following example shows how to enter Admin EXEC mode mode:

```
RP/0/RSP0/CPU0:router# admin
RP/0/RSP0/CPU0:router(admin)#
```

To use administration configuration mode, use the **configure** command in Admin EXEC mode mode:

```
RP/0/RSP0/CPU0:router# admin
RP/0/RSP0/CPU0:router(admin)# configure
RP/0/RSP0/CPU0:router(admin-config)#
```

Related Topics

configure, on page 105

activate advanced

To enable access to advanced system admin commands and configurations, use the **activate advanced** command in Admin EXEC mode mode. These commands and configurations allow access to the advanced functionalities of the system admin services.

activate advanced

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Admin EXEC

Command History

Release	Modification
Release 6.2.1	This command was introduced.

Usage Guidelines

This command should not be used unless specifically requested by Cisco TAC or another Cisco support representative.

This example shows sample output from the **activate advanced** command:

```
# activate advanced
Advanced commands must be used carefully. Continue? [yes,NO] yes
Tue Aug  29 20:05:16.635 UTC
```

alias

To create a command alias, use the **alias** command in Global Configuration mode. To delete an alias, use the **no** form of this command.

alias *alias-name*[*(param-list)*]*content*
no alias *alias-name*

Syntax Description

alias-name	Name of the command alias. Alias names can be a single word or multiple words joined by a hyphen (-) or an underscore (_).
param-list	(Optional) Parameters assigned to the alias. These parameters are filled in at execution time.
content	Original command syntax. Valid abbreviations of the original command syntax can be entered for the *content* argument.

Command Default

No command aliases are configured.

Command Modes

Global Configuration mode

Admin EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Cisco IOS XR software supports generic alias definitions for various entities. Any physical or logical entity can have an alias as a reference. For example, an alias can refer to a command, a partial command, a group of commands, a location, or an IP address.

An alias must first be defined. The alias can then be used in command lines in place of the defined entity.

Following is a list of properties for an alias:

- An alias can be used anywhere and in any mode.
- An alias can have zero, one, or many parameters.
- An alias can refer to those parameters with the $ sign.
- If an alias refers to more than one command, the commands must be separated by a semicolon (;).
- The size of the **alias** command is limited to 1024 characters.

The alias command can be used anywhere. If the content referenced by the alias is invalid or inappropriate in that context or mode, the system issues a warning message containing the substituted content.

An alias name should not be a subset of the keywords that it represents as alias. Substitution is done only when the entered input match fails completely. For instance, the attempt to define an alias with “config? as the alias name fails, as shown in the following example:

```
RP/0/RSP0/CPU0:router(config)# alias config set_host hostname router
```

```
RP/0/RSP0/CPU0:router(config)# show configuration

alias set_host hostname router
```

Use the **show aliases** command to display all command aliases or the command aliases in a specified mode.

Task ID

Task ID	Operations
logging	read, write

The following example shows how to create an alias named ipbr for the **show ipv4 interface brief** command, commit the configuration, enter EXEC mode and then enter the configured alias:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# alias ipbr show ipv4 interface brief
RP/0/RSP0/CPU0:router(config)# show configuration

Building configuration...
alias ipbr show ipv4 interface brief
end
RP/0/RSP0/CPU0:router(config)# commit
RP/0/RSP0/CPU0:Feb 21 04:42:57.017 : config[65689]: %MGBL-LIBTARCFG-6-COMMIT :
Configuration committed by user 'lab'.   Use 'show configuration commit changes 1000000022'
 to view the changes.
RP/0/RSP0/CPU0:router(config)# end
RP/0/RP0/CPU0:Mar 27 22:19:05 : config[65739]: %SYS-5-CONFIG_I : Configured from console
by lab
RP/0/RSP0/CPU0:router# ipbr
RP/0/RSP0/CPU0:router# show ipv4 interface brief

Interface                      IP-Address      Status                Protocol
Loopback0                      10.0.0.1         Up                    Up
Loopback999                    unassigned      Up                    Up
MgmtEth0/0/CPU0/0              12.29.56.21     Up                    Up
RP/0/RSP0/CPU0:router#
```

The following example shows how to define an alias, mycompany-10ge, for POS interface 1/0/2/3 and then how to use that alias to shut down the interface:

```
RP/0/RSP0/CPU0:router(config)# alias mycompany-10ge gigabitethernet1/0/2/3
RP/0/RSP0/CPU0:router(config)# interface mycompany-10ge
RP/0/RSP0/CPU0:router(config-if)# shutdown
RP/0/RSP0/CPU0:router(config-if)# exit
RP/0/RSP0/CPU0:router(config)#
```

The following example shows the use of a parameter name in an alias definition:

```
RP/0/RSP0/CPU0:router(config)# alias shint (intname) show interface $intname
```

The following example shows an alias defined with one parameter and two commands:

```
RP/0/RSP0/CPU0:router(config)# alias shint_both (intname) show interface $intname;show run
```

```
interface $intname
```

The following example shows the use of the alias shint_both inEXEC mode:

```
RP/0/RSP0/CPU0:router(exec)# shint_both(gigabitethernet1/2/3/4)
```

Two commands are issued, as follows:

```
RP/0/RSP0/CPU0:router(exec)# show interface gigabitethernet1/2/3/4; show run interface
gigabitethernet1/2/3/4
```

Related Topics

show aliases, on page 162

apply-group

To cause the configuration commands contained in a group or multiple groups to be inherited by the router configuration within which it is applied, use the **apply-group** command in the appropriate configuration mode. To remove a group configuration, use the **no** form of this command.

apply-group *group-name* [*group-name*]
no apply-group

Syntax Description

group-name	Name of the configuration group to apply. The group must be previously defined. Up to eight group names can be specified at one time.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

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

Configuration statements in configuration groups come into effect only when the configuration groups are applied in the system configuration, and the configuration statements have the correct context and inheritance priority in the mode in which the configuration groups are applied. The maximum number of configuration groups that can be specified in a single **apply-group** command is eight.

To change the composition of an **apply-group** command, you must specify all desired groups. For example, if you used the command `apply-group g10 g20 g30`, and now you want to add the group g15, use the command `apply-group g10 g15 g20 g30`. If you now want to delete group g20, use the command `apply-group g10 g15 g30`. If you use the **no apply-group** command, all groups are removed from the configuration.

Note From the Release 6.3.1 onwards, you are able to enter the Flexible CLI config group definition, **apply-group** and **exclude-group** command in any order as long as the entire commit has all the group definitions needed.

Note Use multi-line configuration style to configure Flexible CLI configuration groups by entering each configuration mode in a separate line, one configuration per line. This is important so that the configuration properties are fully inherited and for better readability during troubleshooting.

Task ID

Task ID	Operation
config-services	read, write

This example applies a configuration group to a specific OSPF instance:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router ospf 0
RP/0/RSP0/CPU0:router(config-ospf)# apply-group G-OSPF-B
```

Related Topics

group (configuration), on page 116

apply-group-remove

To remove one or more configuration groups from an existing apply-group, use the **apply-group-remove** command in the same configuration mode in which the group was applied.

apply-group-remove *group-nameexisting-group-name*

Syntax Description

group-name	Name of the group you want to remove from an existing group. Up to eight group names can be specified in this command at a time.
existing-group-name	Name of the applied (pre-defined) group from which a group will be removed.

Command Default

None

Command Modes

Global configuration or any configuration mode

Command History

Release	Modification
Release 5.1.1	This command was introduced.

Usage Guidelines

Consider, you have configured four groups, g10 g20 g30 g40 using the **apply-group** command. To remove g20, you can use the **apply-group-remove** command to edit the **apply-group** command configuration.

Note This command is not a configuration command and will not be seen in **show configuration** or **show run** commands.

Note This command has to be executed in the same configuration mode as the **apply-group** command used to configure the groups.

Task ID

Task ID	Operation
config-services	read, write

Example

This example shows how to remove the group, G-OSPF-B, using this command:

```
RP/0/RSP0/CPU0:router configure
RP/0/RSP0/CPU0:router (config)# router ospf 0
RP/0/RSP0/CPU0:router (config-ospf)# apply-group-remove G-OSPF-B
```

apply-template

To apply a template to the target configuration, use the **apply-template** command in Global Configuration mode.

apply-template *template-name* [**(***param-list***)**]

Syntax Description

template-name	Name of the template to be applied to the running configuration. Use the **template** command to define a template.
param-list	(Optional) Up to five template parameters.

Command Default

No templates are applied to the target configuration.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **apply-template** command to apply a template to the target configuration. Templates allow you to create a template name that represents a group of configuration commands.

Use the **template** command to define a template. Use the **end-template** command to exit template configuration mode and return to global configuration mode. Use the **show-running** command with the optional **template** *template-name* keyword and argument to display the contents of a template.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to define a template and then apply the template to the target configuration:

```
RP/0/RSP0/CPU0:router(config)# template hostname-template
RP/0/RSP0/CPU0:router(config-TPL)# hostname router1
RP/0/RSP0/CPU0:router(config-TPL)# end-template
RP/0/RSP0/CPU0:router(config)# apply-template hostname-template
```

Related Topics

end-template, on page 112
show running-config, on page 206
template, on page 210

clear comment

To discard a comment associated with a configuration, use the **clear comment** command in any configurationorGlobal Configuration mode.

clear comment

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Any configuration mode

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

The **clear comment** command clears any comments that were added for a specific configuration in the configuration file. After you enter the **clear comment** command, enter the configuration for which you want to delete the comment on a separate line.

To enter configuration comments, enter ! followed by the comment. The comment you enter is associated with the next configuration entered. For example:

```
RP/0/RSP0/CPU0:router#!router1 is located in xxx
RP/0/RSP0/CPU0:router# hostname router1
RP/0/RSP0/CPU0:router# commit
```

The comment is displayed in the output of the **show running-config** command:

```
RP/0/RSP0/CPU0:router# show running-config
...
!router1 is located in xxx
hostname router1
...
```

Task ID

Task ID	Operations
Task ID for the feature or configuration mode impacted by the command	Operation for the feature or configuration mode impacted by the command

The following example shows how to discard the comment associated with the configuration ipv4 address 10.0.0.1 255.0.0.0.

```
RP/0/RSP0/CPU0:router(config-if)# clear comment
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 10.0.0.1 255.0.0.0
```

clear configuration commits

To delete old commit IDs from the commit database to free up disk space, use the **clear configuration commits** command in Admin EXEC modeor EXEC mode.

clear configuration commits {**diskspace** *kilobytes* | **oldest** *number-of-commits*}

Syntax Description

diskspace *kilobytes*	Deletes as many commit IDs (beginning with the oldest available commit ID) from the commit database as required to free the number of kilobytes (KB) specified for the *kilobytes* argument. The range for the number of kilobytes of disk space to free is 1 to 4194304. **Note** The amount of disk space freed may vary depending on the size and number of commits present in the commit database.
oldest *number-of-commits*	Deletes the number of commit IDs specified for the *number-of-commits* argument. **Note** Use the online help (**?**) function to display the range of commit IDs available for deletion.

Command Default

None

Command Modes

EXEC mode

Admin EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **clear configuration commits** command to delete the number of commit IDs available for rollback operations. The most recent 100 commits are retained by the system. As new commit IDs are added, the oldest commit IDs are discarded and are no longer available for rollback operations.

Note The **clear configuration commits** command deletes commits from the commit database only. The running configuration, thus, is not changed.

Note When a commit ID is deleted from the commit database, it is no longer available for rollback and can no longer be used to display commit changes (with the **show configuration rollback changes** command).

Use the **rollback configuration** command to roll back the current running configuration to a previous configuration. Use the **show configuration rollback changes** command to display a list of the commit IDs available for rollback operations or to display the changes that would be made by the **rollback configuration** command.

Task ID

Task ID	Operations
config-services	execute

The following example shows how to delete the oldest 16 commit IDs to free up disk space. After entering this command, you will be prompted to confirm the deletion.

```
RP/0/RSP0/CPU0:router# clear configuration commits oldest 16

Deleting 16 rollback points '1000000021' to '1000000036'
256 KB of disk space will be freed. Continue with deletion?[confirm] y
```

Related Topics

rollback configuration, on page 137
show configuration rollback changes, on page 194

clear configuration inconsistency

To clear an inconsistency alarm for a router configuration or admin plane configuration, use the **clear configuration inconsistency** command in Admin EXEC mode or EXEC mode.

clear configuration inconsistency

Syntax Description

This command has no keywords or arguments.

Command Default

Administration EXEC mode: Clears the inconsistency alarms for the admin plane configuration.

EXEC mode: Clears the inconsistency alarms for an SDR configuration.

Command Modes

Admin EXEC mode

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

An inconsistency alarm is set when there is a failure to restore the configuration; this can occur during router startup, or when a line card or route switch processor (RSP) card is inserted or removed.

If an inconsistency alarm is set, a message similar to the following example is displayed:

```
RP/0/0/CPU0:May 26 11:58:40.662 : cfgmgr-rp[130]: %MGBL-CONFIGCLI-3
   BATCH_CONFIG_FAIL : 28 config(s) failed during startup. To view
   failed config(s) use the command - "show configuration failed startup"

RP/0/0/CPU0:May 26 11:58:41.731 : cfgmgr-rp[130]:
   %MGBL-CONFIG-3-ADMIN_INCONSISTENCY_ALARM : Admin plane configuration
   inconsistency alarm has been raised. Configuration commits will be
   blocked until an ADMIN plane 'clear configuration inconsistency' command
   has been run to synchronize persisted admin plane configuration with
   running admin configuration.
```

When the inconsistency alarm is set, all configuration commit operations fail until the alarm is cleared using the **clear configuration inconsistency** command. This command clears the alarm and removes the failed configuration.

For example, the following configuration commit fails to finish due to an existing inconsistency alarm:

```
RP/0/RSP0/CPU0:router# configure

ADMIN plane running configuration is inconsistent with persistent
  configuration.
No configuration commits will be allowed until an admin plane
'clear configuration inconsistency' command is performed.
RP/0/RSP0/CPU0:router(config)# hostname router2
RP/0/RSP0/CPU0:router(config)#commit
```

```
ADMIN plane running configuration is inconsistent with persistent
  configuration.
No configuration commits will be allowed until an admin plane
'clear configuration inconsistency' command is performed.
```

Enter the **clear configuration inconsistency** command to clear the alarm and allow commit operations to continue.



Note To reapply the failed configuration, you must reapply and recommit the configuration. Use the **load configuration failed** command with the **startup** keyword to populate the target configuration with the contents of the previous failed configuration from the startup configuration.

Use the **show configuration history** command with the **alarm** keyword to view the inconsistency alarm set and alarm clear events in the configuration history log.

Command Modes

To clear the inconsistency alarms for the admin plane configuration, enter the **clear configuration inconsistency** command in administration EXEC mode.

To clear the inconsistency alarms for the router, enter the **clear configuration inconsistency** command in EXEC mode.

Task ID

Task ID	Operations
config-services	execute

The following example shows how to clear the inconsistency alarms for the admin plane configuration by entering the **clear configuration inconsistency** command in administration EXEC mode:

```
RP/0/RSP0/CPU0:router# admin
RP/0/RSP0/CPU0:router(admin)# clear configuration inconsistency

Creating any missing directories in Configuration File system...OK
Initializing Configuration Version Manager...OK
Syncing ADMIN commit database with running configuration...OK
Re-initializing cache files...OK
Updating Commit Database.  Please wait...[OK]
```

The following example shows how to clear the inconsistency alarms for a router configuration. The command is entered in EXEC mode.

```
RP/0/RSP0/CPU0:router# clear configuration inconsistency

Creating any missing directories in Configuration File system...OK
Initializing Configuration Version Manager...OK
Syncing commit database with running configuration...OK
Re-initializing cache files...OK
Updating Commit Database.  Please wait...[OK]
```

In the following example, a history of the inconsistency alarms set and cleared for the router configuration are displayed using the **show configuration history** command with the **alarm** keyword:

```
RP/0/RSP0/CPU0:router# show configuration history alarm

  Sno.  Event      Info                          Time Stamp
  ~~~~  ~~~~~      ~~~~                          ~~~~~~~~~~
  1     alarm      inconsistency alarm raised    Thu Jun 22 15:23:15 2009
  2     alarm      inconsistency alarm cleared   Thu Jun 22 15:42:30 2009
  3     alarm      inconsistency alarm raised    Sun Jul  9 13:39:57 2009
  4     alarm      inconsistency alarm cleared   Sun Jul  9 14:15:48 2009
  5     alarm      inconsistency alarm raised    Sat Jul 15 18:18:26 2009
  6     alarm      inconsistency alarm cleared   Sat Jul 15 19:21:03 2009
```

Related Topics

load configuration failed, on page 126
show configuration history, on page 184
show configuration failed startup, on page 183

clear configuration inconsistency replica

To resolve configuration inconsistencies on a replica node, use the **clear configuration inconsistency replica** command in administration EXECorEXEC mode.

clear configuration inconsistency replica location *node-id*

Syntax Description

location *node-id*	Resolves the configuration inconsistencies on the designated node. The *node-id* argument is expressed in the *rack*/*slot*/*module* notation.

Command Default

Administration EXEC mode: Resolves any configuration inconsistencies for the admin plane configuration.

EXEC mode: Resolves any configuration inconsistencies for the router configuration.

Command Modes

Admin EXEC mode

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

In administration EXEC mode, the replica node for the **clear configuration inconsistency replica** command is the standby designated system controller (DSC). In EXEC mode, the replica nodes are the route switch processors (RSPs) that can become the designated shelf controller (DSC).

Use the **clear configuration inconsistency replica** command if there is a configuration inconsistency between the standby DSC and the current active DSC; or alternatively, if the configuration on any nodes that could become the DSC is not the same as the configuration on the current DSC. To determine if you have a configuration inconsistency, use the **show configuration inconsistency replica** command.

To clear configuration inconsistencies for the admin plane configuration, enter the **clear configuration inconsistency replica** command in administration EXEC mode.

To clear configuration inconsistencies for an SDR configuration, enter the **clear configuration inconsistency replica** command in EXEC mode for that SDR.

Task ID

Task ID	Operations
config-services	execute

The following example shows how to clear any configuration inconsistencies for the DSC configuration by using the **clear configuration inconsistency replica** command in EXEC mode:

```
RP/0/RSP0/CPU0:router# clear configuration inconsistency replica location 0/rp1/cpu0
```

```
The replica has been repaired.
```

Related Topics

show configuration inconsistency replica, on page 188

clear configuration sessions

To clear (end) an active configuration session, use the **clear configuration sessions** command in administration EXEC orEXEC mode.

clear configuration sessions *session-id*

Syntax Description

session-id	Identifier for the configuration session to be terminated.

Command Default

None

Command Modes

Administration EXEC

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **clear configuration sessions** command to clear a configuration session. This command can be used to end the configuration sessions of another user. Any uncommitted changes to a user's target configuration are discarded.

Use the **show configuration sessions** command to identify active configuration sessions.

When a configuration session is cleared, a message is displayed on the terminal of the terminated user. For example:

```
RP/0/RSP0/CPU0:router(config)# This configuration session was terminated by user 'user_a'
from line 'aux0_0_CPU0'
```

Task ID

Task ID	Operations
config-services	execute

The following example shows how to clear an active configuration session. In this example, the **show configuration sessions** command displays the active configuration session. The **clear configuration sessions** command clears the active configuration session.

```
RP/0/RSP0/CPU0:router# show configuration sessions

Current Configuration Session   Line           User      Date                      Lock
00000211-002c409b-00000000      con0_RSPs1_CPU0  UNKNOWN   Mon Feb  2 01:02:09 2009

RP/0/RSP0/CPU0:router# clear configuration sessions 00000211-002c409b-00000000
```

```
session ID '00000211-002cb09b-00000000' terminated
```

Related Topics

show configuration sessions, on page 200

commit

To commit the target configuration to the active (running) configuration, use the **commit** command in any configuration Global Configuration mode Admin Configuration mode.

commit [**best-effort**] [**comment** *line*] [**confirmed** [*seconds* | **minutes** *minutes*]] [**force**] [**label** *line*] [**replace**] [**save-running filename** *file_path*]

Syntax Description

best-effort	(Optional) Merges the target configuration with the running configuration and commits only valid changes (best effort). Some configuration changes might fail due to semantic errors.
comment *line*	(Optional) Assigns a comment to a commit. This text comment is displayed in the commit entry displayed in the output for the **show configuration commit list** command with the optional **detail** keyword.
confirmed [*seconds* | **minutes** *minutes*]	(Optional) Commits the configuration on a trial basis for the time specified in seconds or minutes. **Note** The **confirmed** option is not available in administration configuration mode.
force	(Optional) Forces a commit operation in low-memory conditions.
label *line*	(Optional) Assigns a meaningful label. This label is displayed (instead of the autogenerated commit ID) in the output for the **show configuration commit list** .
replace	(Optional) Replaces the entire running configuration with the contents of the target configuration.
save-running filename *file_path*	(Optional) Saves the running configuration to a specified file.

Command Default

The default behavior is *pseudo-atomic*, meaning that all changes must succeed for the entire commit operation to succeed. If any errors are found, none of the configuration changes take effect.

Command Modes

Any configuration mode

Global Configuration mode

Admin Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Changes made during a configuration session are inactive until the **commit** command is entered. By default, the commit operation is *pseudo-atomic*, meaning that all changes must succeed for the entire commit operation to succeed. If any errors are found, none of the configuration changes takes effect.

To replace the default numeric ID for the commit, use the optional **label** keyword. This label is displayed (instead of the autogenerated commit ID) in the output for the **show configuration commit list** command.

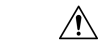
Enter an optional comment with the **comment** keyword to provide additional information about the commit action. This comment is displayed in the output for the **show configuration commit list** command with the **detail** keyword.

Use the optional **confirmed** *minutes* keyword and argument to commit a configuration on a trial basis for a minimum of 30 seconds and a maximum of 300 seconds (5 minutes). During the trial configuration period, enter the **commit** command to confirm the configuration. If the **commit** command is not entered, then the system reverts to the previous configuration when the trial time period expires. The confirmed option is not available in administration configuration mode.

You can use the **commit** command in conjunction with the **load** command. Load a new configuration with the **load** command, and use the **commit** command with the **replace** keyword to have the loaded configuration become the active (running) configuration.

Use the optional **save-running filename** *file_path* keywords and argument to save the running configuration to a specified file. To configure automatic saving of the configuration file on every commit, use the **configuration commit auto-save** command. If automatic saving of the configuration file is already enabled, specifying **save-running filename** *file_path* with the **commit** command has no additional effect.

In pseudo-atomic commit, if an error occurs on one or more of the configurations in a commit, other configurations which are already part of the running configuration in the same commit are reverted.



Caution Saving the running configuration to a file is CPU intensive.



Note If you use the **commit** command without previously loading a target configuration, a blank configuration is committed.



Note If you use the **commit** command with the **replace** keyword, it does not affect the mode of an 8-port E1/T1 SPA. If the mode is E1 before using the **commit replace** command, it remains E1. However, since the default mode is T1, the router does not recognize that the mode is E1. To change the mode to T1, you must first use the **hw-module subslot cardtype e1** command to add the E1 mode into the configuration so that it correlates with the system. Then manually reload the router and it boots in T1 mode.

For more information regarding the **hw-module subslot cardtype** command, refer to *Interface and Hardware Component Command Reference for Cisco ASR 9000 Series Routers*.

Task ID

Task ID	Operations
Task ID for the feature or configuration mode impacted by the command	Operation for the feature or configuration mode impacted by the command

Committing the Target Configuration to the Active Running Configuration

The following example shows how to commit the target configuration to the active running configuration. In this example, the **commit** command saves changes to the router hostname.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# hostname router1
RP/0/RSP0/CPU0:router(config)# commit

RP/0/RSP0/CPU0:Feb 21 04:42:57.017 : config[65689]: %MGBL-LIBTARCFG-6-COMMIT :
Configuration committed by user 'user_a'.
Use 'show configuration commit changes 1000000033' to view the changes.
```

Adding a Comment to a Configuration Commit

The following example shows how to use the **commit** command with the optional **comment** *line* keyword and argument to assign a text description to the commit operation. The comment is then displayed in the output of the **show configuration commit list** command with the **detail** keyword.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# hostname router2
RP/0/RSP0/CPU0:router(config)# commit comment new name for router

RP/0/RP0/CPU0:Feb 21 04:42:57.017 : config[65689]: %MGBL-LIBTARCFG-6-COMMIT :
Configuration committed by user 'user_a'.   Use 'show configuration commit
changes 1000000226' to view the changes.

RP/0/RSP0/CPU0:router2(config)# end
RP/0/RSP0/CPU0:router2# show configuration commit list detail

1) CommitId: 1000000226                Label: NONE
   UserId:   user_a                    Line:  con0_RP1_CPU0
   Client:   CLI                       Time:  12:59:26 UTC Wed Feb 04 2004
   Comment:  new name for router

2) CommitId: 1000000225                Label: NONE
   UserId:   user_a                    Line:  con0_RP1_CPU0
   Client:   CLI                       Time:  12:58:32 UTC Wed Feb 04 2004
   Comment:  NONE
```

Changing the Commit ID to a Text Label

The following example shows how to use the **commit** command with the optional **label** *line* keyword and argument to change the commit ID to a text label for easier identification. The label is then displayed in the output of the **show configuration commit list** command.

```
RP/0/RSP0/CPU0:router2# configure
```

```
RP/0/RSP0/CPU0:router2(config)# hostname router3
RP/0/RSP0/CPU0:router2(config)# commit label new_name

RP/0/RP0/CPU0:Feb 21 04:42:57.017 : config[65689]: %MGBL-LIBTARCFG-6-COMMIT :
Configuration committed by user 'user_a'.
Use 'show configuration commit changes 1000000227' to view the changes.

RP/0/RSP0/CPU0:router3(config)# end
RP/0/RSP0/CPU0:router3# show configuration commit list

SNo. Label/ID    User      Line        Client      Time Stamp
~~~~ ~~~~~~~~    ~~~~      ~~~~        ~~~~~~      ~~~~~~~~~~
1    new_name    user_a    con0_RSPs1_C  CLI         13:00:53 UTC Wed Feb 04 2004
2    1000000226  user_a    con0_RSPs1_C  CLI         12:59:26 UTC Wed Feb 04 2004
3    1000000225  user_a    con0_RSPs1_C  CLI         12:58:32 UTC Wed Feb 04 2004
```

Commit a Configuration for a Specified Time

The following example shows how to use the **commit** command with the optional **confirmed** keyword and number *argument*. The configuration changes are committed only for the specified number of seconds. You can then either confirm the commit operation or discard the changes.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# hostname router3
RP/0/RSP0/CPU0:router(config)# commit confirmed 30
RP/0/RSP0/CPU0:router3(config)# end
```

Related Topics

abort, on page 79
end, on page 109
exit, on page 114
configuration commit auto-save, on page 103
load, on page 123
show configuration rollback changes, on page 194

configuration commit auto-save

To enable automatic saving of the running configuration to a specified file on every commit, use the **configuration commit auto-save** command in Global Configuration mode mode. To disable automatic saving of the running configuration to a specified file on every commit, use the **no** form of the command.

Caution Saving the running configuration to a file is CPU intensive.

configuration commit auto-save [**filename** *file_path* | **password** { **clear** { **encryption-aes** | **encryption-default** } *password* | **encrypted** | { **encryption-aes** | **encryption-default** } *password* } | **maximum** *number* | **timestamp** | **wait-time** *duration*]

Syntax Description

filename *file_path*	Specifies the location to which to save the running configuration.
password *password*	Specifies the password of the remote URL.
clear	Specifies an unencrypted password.
encryption-aes	Saves the password in aes encrypted form.
encryption-default	Saves password in default encrypted form.
encrypted	Specifies an encrypted password.
maximum *number*	Specifies how many maximum auto-saves are possible.
timestamp	Includes the timestamp in the auto-save filename.
wait-time*duration*	Specifies how long to wait to auto-save after the commit done to start the next auto-save.The *duration*can be specified as: days *days* | hours *hours* | minutes *minutes* | seconds *seconds*

Command Default

None

Command Modes

Global Configuration mode

Admin Configuration mode

Command History

Release	Modification
Release 7.10.1	This command was modified to support public key authentication.
Release 7.9.1	This command was modified to include, **scp**,**sftp**, **password**, **wait-time**, **timestamp**, and **maximum** keywords.
Release 6.1.2	The command was enhanced to save the copy of your config with unique filename

Release	Modification
Release 3.7.2	This command was introduced

Usage Guidelines

The **configuration commit auto-save** command configures the system to save the running configuration to the specified file and location every time a **commit** command is run. Alternatively, you can save the configuration on a one-time basis by specifying the **save-running** keyword when you run the **commit** command. Use the following syntax when using **tftp**, **ftp**, **scp**, **sftp** or **rcp** as options.

[***tftp***|***ftp******rcp******scp******sftp***]

Caution Saving the running configuration to a file is CPU intensive.

Task ID

Task ID	Operations
config-services	write

The following example shows how to configure the system to save the running configuration to the file `//test-folder/test_123`, backup encrypted password,append time-stamp, configure maximum number of auto-save files possible, and specify wait-time before backing up the files whenever the configuration is commited:

```
Router#configure
Router(config)#configuration commit auto-save
Router(config-cfg-autosave)#filename sftp://user1@server1://test-folder/test_123
Router(config-cfg-autosave)#password clear encryption-default cisco
Router(config-cfg-autosave)#timestamp
Router(config-cfg-autosave)#maximum 10
Router(config-cfg-autosave)#wait-time days 0 hours 0 minutes 0 seconds 5
Router(config-cfg-autosave)#commit
```

While you are using public key authentication to save the running configuration, you don't need to mention password.

Related Topics

commit, on page 99

configure

To enter global configuration mode or administration configuration mode, use the **configure** command inEXEC mode or Admin EXEC mode.

configure [**exclusive** | **terminal**]

Syntax Description

exclusive	(Optional) Locks the router configuration. The system configuration can be made only from the login terminal.
terminal	(Optional) Configures the system from the login terminal. This is the default.

Command Default

If the **configure** command is entered without a keyword, the system is configured from the login terminal.

Command Modes

EXEC mode

Admin EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Configuration modes are used to enter changes to a target configuration session and commit those changes to the running configuration. A router running Cisco IOS XR software contains multiple configurations:

- The configuration for a router. This mode is used to configure router- specific features such as routing protocols.
- The administration configuration for system-wide resources and settings. Some features can be configured only in administration configuration mode.

Global Configuration mode

Use the **configure** command in EXEC mode to enter Global Configuration mode and create a new target configuration for an SDR. From global configuration mode, you can enter any configuration mode. Configuration changes entered in global configuration mode impact the SDR to which the user is currently logged in.

Admin Configuration mode

Use the **configure** command in Admin EXEC mode to enter Admin Configuration mode and create a new target configuration. From Admin EXEC mode , you can enter any configuration mode. Configuration changes entered in Admin EXEC mode can impact resources for the entire router. See the command reference documentation for a specific command to determine the impact of commands entered in Admin EXEC mode.

Router Prompt

After you enter the **configure** command, the system appends "(config)" to the router prompt, indicating that the router is in a configuration mode. For example:

- The following prompt indicates that you are in global configuration mode for an SDR:

```
RP/0/RSP0/CPU0:router(config)#
```

- The following prompt indicates that you are in administration configuration mode:

```
RP/0/RSP0/CPU0:router(admin-config)#
```

Locking a Configuration Session

To lock the configuration so that no other user can commit changes to the running configuration during your configuration session, issue the **configure** command with the **exclusive** keyword.

Committing Changes and Returning to EXEC mode or Admin EXEC mode

Changes to the target configuration remain inactive until the **commit** command is entered. To leave global configuration or administration configuration mode and return to the EXEC mode or Admin EXEC mode prompt, issue the **end** or **exit** command; you are prompted to commit any uncommitted changes.

To leave configuration mode and return directly to EXEC mode or Admin EXEC mode without being prompted to commit changes and without saving changes to the target configuration, enter the **abort** command in any configuration mode.

The following example shows how to enter global configuration mode from EXEC mode and then enter interface configuration mode to configure an IPv4 address , the **configure** command commits the configuration, and the **end** command terminates the configuration session and return the router to EXEC mode.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tengige 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 10.0.0.1 255.0.0.0
RP/0/RSP0/CPU0:router(config-if)# commit
RP/0/RSP0/CPU0:router(config-if)# end
RP/0/RSP0/CPU0:router#
```

Related Topics

abort, on page 79
end, on page 109
exit, on page 114
show configuration (config), on page 167
show running-config, on page 206

description (interface)

To add a description to an interface configuration, use the **description** command in interface configuration mode. To remove the description, use the **no** form of this command.

description *comment*
no description

Syntax Description

comment	Comment or a description applied to the interface. The maximum number of characters is 1022.

Command Default

No description is configured.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **description** command to add a description to an interface configuration. The maximum number of characters is 1022.

Task ID

Task ID	Operations
interface	read, write

The following example shows how to add a description to an interface configuration. In this example, the **description** command names a Management Ethernet interface.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface mgmteth 0/
RSP
1/CPU0/0
RP/0/RSP0/CPU0:router(config-if)# description Management Ethernet Interface
```

Related Topics

show interfaces

do

To execute an EXEC mode command from a configuration mode, use the **do** command in any configuration mode.

do *exec-command*

Syntax Description

exec-command	EXEC mode command to be executed.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

To display the various EXEC mode commands that are available to execute with the **do** command, use the online help (?) function at the configuration mode prompt.

Note The **configure** and **describe** commands are not supported with the **do** command.

Task ID

Task ID	Operations
Task ID for the EXEC command that you are using	read

The following example shows how to execute an EXEC command from interface configuration mode. In this example, the **do** command displays output from the **show protocols** command within interface configuration mode:

```
RP/0/RSP0/CPU0:router(config)# interface tengige 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# do show protocols

Routing Protocol "BGP 1"

Address Family IPv4 Unicast:
  Distance: external 20 internal 200 local 200
```

end

To terminate a configuration session and return directly to EXEC modeAdmin EXEC mode , use the **end** command in any configuration mode.

end

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **end** command to exit any configuration mode and return directly to EXEC mode Admin EXEC mode. If you enter this command without committing the changes to the target configuration, you are prompted to do so:

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)?[cancel]:
```

- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode Admin EXEC mode.

  If errors are found in the running configuration, the configuration session does not end. To view the errors, enter the **show configuration** (config) command with the **failed** keyword.

- Entering **no** exits the configuration session and returns the router to EXEC mode Admin EXEC mode without committing the configuration changes.
- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.



Note Entering **Ctrl-Z** is functionally equivalent to entering the **end** command.

Use the **abort** command to exit the configuration session and return to EXEC mode Admin EXEC mode without being prompted to commit changes and without saving changes to the target configuration.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to use the **end** command to end a configuration session. Changes stored in the target configuration are committed by answering **yes**.

```
RP/0/RSP0/CPU0:router# configure
```

```
RP/0/RSP0/CPU0:router(config)# interface tengige 0/2/0/0
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 10.0.0.1 255.0.0.0
RP/0/RSP0/CPU0:router(config-if)# end

Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: yes
RP/0/RSP0/CPU0:router#
```

Related Topics

abort, on page 79
exit, on page 114
show configuration (config), on page 167
commit, on page 99

end-group

To exit from configuration group submode and return to global configuration mode, use the end-group command in group configuration mode.

end-group

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Group configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

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

After you have included all configuration statements that you want in a particular configuration group, use the **end-group** command to exit group configuration mode.

Task ID

Task ID	Operation
config-services	read, write

This example shows how to complete the configuration of a configuration group and exit group configuration mode:

```
RP/0/RSP0/CPU0:router(config)# group g-int-gige
RP/0/RSP0/CPU0:router(config-GRP)# interface 'GigabitEthernet.*'
RP/0/RSP0/CPU0:router(config-GRP-if)# mtu 1514
RP/0/RSP0/CPU0:router(config-GRP-if)# end-group
RP/0/RSP0/CPU0:router(config)#
```

Related Topics

group (configuration), on page 116

end-template

To exit template configuration mode and return to Global Configuration mode, use the **end-template** command in template configuration mode.

end-template

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

Template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **end-template** command to exit template configuration mode after you have completed the template definition.

To define a template, use the **template** command. To apply a template to the target configuration, use the **apply-template** command. To view the contents of a template, use the **show running-config** command with the optional **template** *template-name* keyword and argument.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to enter template configuration mode, define a template named "hostname-template" and then exit from template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# template hostname-template
RP/0/RSP0/CPU0:router(config-TPL)# hostname router-cs1
RP/0/RSP0/CPU0:router(config-TPL)# end-template
RP/0/RSP0/CPU0:router(config)#
```

Related Topics

end, on page 109

exclude-group

To exclude (or override) a configuration group (or groups) to be inherited by the router configuration, use the **exclude-group** command in the appropriate configuration mode. To delete the set exclusion, use the **no** form of this command.

exclude-group *group-name*

Syntax Description

group-name	Configuration group name that needs to be excluded.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 5.1.1	This command was introduced.

Usage Guidelines

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

More than one configuration group can be excluded simultaneously. A maximum of eight groups can be specified at one time.

Note From Release 6.3.1 onwards, you can enter Flexible CLI config groups, **apply-group** and **exclude-group** command in any order as long as the entire commit has all the group definitions needed.

Task ID

Task ID	Operation
config-services	read, write

Example

This example shows how to delete the group G_interface using the **exclude-group** command:

```
RP/0/RSP0/CPU0:router (config) # exclude-group G_interface

exclude-group G_INTERFACE
ipv4 address 12.21.50.100 255.255.0.0
!
interface GigabitEthernet0/0/0/1
ipv4 address 12.21.51.100 255.255.0.0
```

exit

To close an active terminal session and log off the router, use the **exit** command in EXEC mode Admin EXEC mode.

To return the router to the next higher configuration mode, use the **exit** command in any configuration mode.

exit

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Any configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

To log off from a terminal session, enter the **exit** command in EXEC mode Admin EXEC mode.

When exiting from global or administration configuration mode to EXEC mode Admin EXEC mode, you are prompted to commit any uncommitted configuration changes.

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)?[cancel]:
```

- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode Admin EXEC mode.

  If errors are found in the running configuration, the configuration session does not end. To view the errors, enter the **show configuration** (config) command with the **failed** keyword.
- Entering **no** exits the configuration session and returns the router to EXEC mode Admin EXEC mode without committing the configuration changes.
- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.



Note Entering the **exit** command from global configuration is functionally equivalent to entering the **end** command.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to return the router to the next higher command mode. In this example, the **exit** command exits from interface configuration mode and returns to global configuration mode. The **exit** command is entered a second time to exit from global configuration mode and return to EXEC mode. Because the configuration has not been committed explicitly (with the **commit** command), the system prompts to commit the configuration changes made during the session.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tengige 0/2/0/0
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 10.0.0.1 255.0.0.0
RP/0/RSP0/CPU0:router(config-if)# exit
RP/0/RSP0/CPU0:router(config)# exit
Uncommitted changes found, commit them before exiting(yes/no/cancel)?[cancel]: yes
```

The following example shows how to use the **exit** command from EXEC mode to log off from a terminal session:

```
RP/0/RSP0/CPU0:router# exit

router con0_RP1_CPU0 is now available

Press RETURN to get started.
```

Related Topics

abort, on page 79
end, on page 109
commit, on page 99

group (configuration)

To define a configuration group containing configuration statements that can be applied in the router configuration, use the **group** command in global configuration mode. To remove a configuration group from the running configuration, use the **no** form of this command.

group *group-name config-statements*
no group *group-name*

Syntax Description

group-name	Name of the configuration group.
config-statements	Series of configuration statements, starting in global configuration mode, that comprise this configuration group.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

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

The **group** command enters group configuration mode where you can list a series of configuration statements that can then be used elsewhere in the router configuration. Most configuration commands can be used in group configuration mode. You must be in a user group associated with a task group that includes the appropriate task IDs for each of the command statements that you list within a configuration group.

The *group-name* argument is limited to 32 characters and is case-sensitive. It must not contain any of these special characters:

- ` - grave
- ' - single quote
- " - double quote
- < - less than
- > - greater than
- (- open parenthesis
-) - close parenthesis
- [- open bracket
-] - close bracket
- { - open brace

- } - close brace
- / - slash
- \ - backslash
- & - ampersand
- ^ - caret
- ! - exclamation point
- ? - question mark
- ~ - tilde
- * - asterisk
- % - percent sign
- = - equal sign
- , - comma
- + - plus sign
- | - vertical bar
- - space

A configuration group can be removed from the running configuration, only if it is not used by a configured **apply-group** command.

To exit from configuration group submode and return to global configuration mode, use the **end-group** command.

Regular expressions are used within the configuration statements to make them widely applicable. POSIX 1003.2 regular expressions are supported in the names of configuration statements. Single quotes are used to delimit a regular expression. For example, to specify the regular expression GigabitEthernet.* that matches all GigabitEthernet interfaces, enter the regular expression within single quotes as 'GigabitEthernet.*'.

To display a list of available interface types for your router configuration, enter **interface ?** at the configuration group prompt:

```
RP/0/RSP0/CPU0:router(config-GRP)# interface ?

  ATM              'RegExp': ATM Network Interface(s)
  BVI              'RegExp': Bridge-Group Virtual Interface
  Bundle-Ether     'RegExp': Aggregated Ethernet interface(s)
  Bundle-POS       'RegExp': Aggregated POS interface(s)
  GigabitEthernet  'RegExp': GigabitEthernet/IEEE 802.3 interface(s)
  IMA              'RegExp': ATM Network Interface(s)
  Loopback         'RegExp': Loopback interface(s)
  MgmtEth          'RegExp': Ethernet/IEEE 802.3 interface(s)
  Multilink        'RegExp': Multilink network interface(s)
  Null             'RegExp': Null interface
  POS              'RegExp': Packet over SONET/SDH network interface(s)
  PW-Ether         'RegExp': PWHE Ethernet Interface
  PW-IW            'RegExp': PWHE VC11 IP Interworking Interface
  Serial           'RegExp': Serial network interface(s)
  tunnel-ip        'RegExp': GRE/IPinIP Tunnel Interface(s)
```

```
tunnel-mte       'RegExp': MPLS Traffic Engineering P2MP Tunnel interface(s)
tunnel-te        'RegExp': MPLS Traffic Engineering Tunnel interface(s)
tunnel-tp        'RegExp': MPLS Transport Protocol Tunnel interface
```



Note Although you are required to enter only enough characters for the interface type to be unique, it is recommended that you enter the entire phrase. All interface types used in regular expressions are case-sensitive.

For example, you can use the command `interface 'GigabitEthernet.*'`, but not `interface 'gigabite.*'`. To specify a subinterface, prefix the expression with the characters \. (backslash period), for example: `interface 'GigabitEthernet.*\..*'`. Refer to the *Configuring Flexible Command Line Interface Configuration Groups* module in the *System Management Configuration Guide for Cisco ASR 9000 Series Routers* for more extensive examples.

Task ID

Task ID	Operation
config-services	read, write

This example shows the definition of a configuration group to configure Gigabit Ethernet interfaces with ISIS routing parameters:

```
RP/0/RSP0/CPU0:router(config)# group g-isis-gige
RP/0/RSP0/CPU0:router(config-GRP)# router isis '.*'
RP/0/RSP0/CPU0:router(config-GRP-isis)# interface 'GigabitEthernet.*'
RP/0/RSP0/CPU0:router(config-GRP-isis-if)# lsp-interval 20
RP/0/RSP0/CPU0:router(config-GRP-isis-if)# hello-interval 40
RP/0/RSP0/CPU0:router(config-GRP-isis-if)# address-family ipv4 unicast
RP/0/RSP0/CPU0:router(config-GRP-isis-if-af)# metric 10
RP/0/RSP0/CPU0:router(config-GRP-isis-if-af)# end-group
RP/0/RSP0/CPU0:router(config)#
```

To illustrate the use of this configuration group, assume that you want to configure Gigabit Ethernet interfaces with ISIS routing parameters, as shown here:

```
router isis green
 interface GigabitEthernet0/0/0/0
  lsp-interval 20
  hello-interval 40
  address-family ipv4 unicast
   metric 10
  !
 !
 interface GigabitEthernet0/0/0/1
  lsp-interval 20
  hello-interval 40
  address-family ipv4 unicast
   metric 10
  !
 !
 interface GigabitEthernet0/0/0/2
  lsp-interval 20
  hello-interval 40
  address-family ipv4 unicast
```

```
   metric 10
  !
 !
 interface GigabitEthernet0/0/0/3
  lsp-interval 20
  hello-interval 40
  address-family ipv4 unicast
   metric 10
  !
 !
!
```

There are three possible ways to use the configuration group to configure these interfaces. The first is by applying the group within the interface configuration, as shown here:

```
router isis green
 interface GigabitEthernet0/0/0/0
  apply-group g-isis-gige
  !
 !
 interface GigabitEthernet0/0/0/1
  apply-group g-isis-gige
  !
 !
 interface GigabitEthernet0/0/0/2
  apply-group g-isis-gige
  !
 !
 interface GigabitEthernet0/0/0/3
  apply-group g-isis-gige
 !
!
```

The second way to configure these interfaces using the configuration group is to apply the configuration group within the **router isis** configuration, as shown here:

```
router isis green
 apply-group g-isis-gige
 interface GigabitEthernet0/0/0/0
 !
 interface GigabitEthernet0/0/0/1
 !
 interface GigabitEthernet0/0/0/2
 !
 interface GigabitEthernet0/0/0/3
 !
!
```

In this situation, any other Gigabit Ethernet interfaces that you configure in ISIS green configuration inherit the configuration group configurations.

The third way to configure these interfaces using the configuration group is to apply the group at the global level, as shown here:

```
apply-group g-isis-gige
router isis green
 interface GigabitEthernet0/0/0/0
 !
 interface GigabitEthernet0/0/0/1
```

```
 !
 interface GigabitEthernet0/0/0/2
 !
 interface GigabitEthernet0/0/0/3
 !
!
```

In this example, the configuration of the group is applied to all Gigabit Ethernet interfaces configured for ISIS.

Related Topics

end-group, on page 111
apply-group, on page 85

hostname

To specify or modify the hostname for the router, use the **hostname** command in Global Configuration mode.

hostname *name*

Syntax Description

name	New hostname for the router.

Command Default

The factory-assigned default hostname is “ios.”

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

The hostname is used in prompts and default configuration filenames.

No blank or space characters are permitted as part of a name. Do not expect case to be preserved. Uppercase and lowercase characters look the same to many Internet software applications. It may seem appropriate to capitalize a name the same way you might do in English, but conventions dictate that computer names appear all lowercase. For more information, see RFC 1178, *Choosing a Name for Your Computer*.

Task ID

Task ID	Operations
root-lr	read, write

The following example shows how to change the router hostname:

```
RP/0/RSP0/CPU0:router(config)# hostname router1
```

ipv6-enable

To enable IPv6, use **ipv6-enable** command in the . To disable IPv6, use the **no** form of this command.

ipv6-enable

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Command History

Release	Modification
Release 7.6.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
config-services	read

Examples

This example shows how enable ipv6 using the **ipv6-enable** command:

```
Router#configure terminal
Router(config)#interface CSI-Ether
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address 2001:0DB8:0:1::/64
Router(config-if)#exit
```

load

To populate the target configuration with the contents of a previously saved configuration file, use the **load** command in global configuration or administration configuration mode.

load *device*:*directory-path*

Syntax Description

device: directory-path	Storage device and directory path of the configuration file to be loaded into the target configuration.

Command Default

If the full path of the file is not specified, the present working directory is used.

Command Modes

Global configuration

Administration configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **load** command to populate the target configuration with the contents of a previously saved configuration. When loading a file, you must specify the device, directory path, and filename of the configuration file.

Use the **commit** command in conjunction with the **load** command. Load a new configuration with the **load** command, and use the **commit** command with the **replace** keyword to have the loaded configuration become the active (running) configuration.

Use the **show configuration failed** (config) command with the optional **load** keyword to display syntax errors that occurred during the last load operation.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to load a target configuration file into the current configuration session. The current configuration session is then populated with the contents of the file.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# load disk1:myconfig.cfg
RP/0/RSP0/CPU0:router(config)# show config

Building configuration...
interface TenGigE 0/3/0/0
 description My 10 GE Interface
 ipv4 address 10.10.11.20 255.0.0.0
```

```
!
end
```

Related Topics

show configuration failed (config), on page 177
commit, on page 99

load commit changes

To populate the target configuration with changes from previous configuration commits, use the **load commit changes** command in global configuration or administration configuration mode.

load commit changes {*commit-id* | **since** *commit-id* | **last** *number-of-commits*}

Syntax Description

commit-id	Specific configuration commit.
since *commit-id*	Loads all configuration changes committed into the target buffer since (and including) a specific configuration commit, *commit-id*.
last *number-of-commits*	Loads the configuration changes into the target buffer that have been made during the last number of configuration commits specified with the *number-of-commits* argument.

Command Default

None

Command Modes

Global configuration

Administration configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **load commit changes** command to populate the target configuration with changes from previous configuration commits. The changes are not applied until you enter the **commit** command.

Use the **show configuration** (config) command to display the target configuration.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to populate the target configuration with changes from a previous configuration commit:

```
RP/0/RSP0/CPU0:router(config)# load commit changes since 1000000006

Building configuration...
Loading.
223 bytes parsed in 1 sec (222)bytes/sec
```

load configuration failed

To populate the target configuration with the contents of the previous failed configuration commit, use the **load configuration failed** command in global configuration or administration configuration mode.

load configuration failed {**commit** | **startup** [**previous** *number-of-reloads*] [**noerror**]}

Syntax Description

commit	Loads the failed configuration from the last commit.
startup	Loads the failed configuration from the startup configuration.
previous *number-of-reloads*	(Optional) Loads the failed configurations from a previous router reload. Valid *number-of-reloads* values are 1 to 4.
noerror	(Optional) Excludes the error reasons when the failed configurations are loaded.

Command Default

None

Command Modes

Global configuration

Administration configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **load configuration failed** command to populate the target configuration with the contents of the previous failed configuration commit.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to populate the target configuration with the contents of the previous failed configuration commit:

```
RP/0/RSP0/CPU0:router(config)# load configuration failed startup
Loading.
32 bytes parsed in 1 sec (31)bytes/sec
```

Related Topics

show configuration (config), on page 167

load configuration removed

To populate the target configuration with the contents of the previous removed configuration, use the **load configuration removed** command in global configuration or administration configuration mode.

load configuration removed *config-id*

Syntax Description

config-id	Identifier of the removed configuration to load.

Command Default

None

Command Modes

Global configuration

Administration configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **load configuration removed** command to populate the target configuration with the contents of the removed configuration during installation operations.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to populate the target configuration with the contents of the removed configuration during installation:

```
RP/0/RSP0/CPU0:router(config)# load configuration removed 20070316021626.cfg
```

Related Topics

show configuration persistent, on page 190

load rollback changes

To populate the target configuration with the contents of a previous configuration, use the **load rollback changes** command in global configuration or administration configuration mode.

load rollback changes {*commit-id* | **last** *number-of-commits* | **to** *commit-id*}

Syntax Description

commit-id	Rolls back the configuration changes for a specific configuration commit.
last *number-of-commits*	Rolls back to the configuration that existed before the last number of commits (specified with the *number-of-commits* argument) were made.
to *commit-id*	Rolls back to the running configuration that existed before the configuration specified with the *commit-id* argument.

Command Default

None

Command Modes

Global configuration

Administration configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **load rollback changes** command to load rollback configuration changes to the target configuration. This command is similar to the **rollback configuration** command. The difference between the commands is that the **load rollback changes** command copies the rollback changes to the target configuration and does not commit the changes until the changes are explicitly committed with the **commit** command.

Use the **show configuration rollback changes** command to display rollback changes.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to populate the target configuration with the contents of a previous configuration:

```
RP/0/RSP0/CPU0:router(config)# load rollback changes 1000000004

Building configuration...
Loading.
302 bytes parsed in 1 sec (301)bytes/sec
```

man

Cisco IOS XR software provides online help for standard command-line interface (CLI) commands using manual (man) pages. To display manual pages, use the **man** command in EXEC mode.

man {**command** *command-name* | **feature** [*feature-name*] | **keyword** *keywords*}

Syntax Description

command *command-name*	Displays the manual pages for a specific command. The *command-name* argument must include the complete command name.
feature [*feature-name*]	Displays all commands available in the feature. Use the **man** command with the **feature** keyword to list the available feature names.
keyword *keywords*	Displays a list of command names that match the keywords. Enter one or more keywords to match in a command. When entering multiple keywords, the keywords must be entered in the same sequential order as they are in the command.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

You must have the documentation PIE installed before you can use the **man** command. If you attempt to run this command without the documentation PIE installed, an error is displayed as shown in the following example:

```
RP/0/RSP0/CPU0:router# man command show install

Building index table...
Warning. Unable to get directory info for '/pkg/man' :No such file or directory.
 Discarding!
man [5521656]:Building index table failed. No entries found
```

For information about installing optional software PIEs, see the *Upgrading and Managing Cisco IOS XR Software* module in *System Management Configuration Guide for Cisco ASR 9000 Series Routers*.

Use the **man** command to display the manual pages for a specific command on the basis of the command name, a feature, or a keyword. Each man page contains the command name, syntax, command mode, usage, examples, and related commands.

The **man** command queries and displays command information about the router. A query can be based on keywords or a feature. The **feature** *feature-name* keyword and argument display all commands that match the feature. For example, entering **man feature asr9k- base-1** displays all commands that match the asr9k-base-1 feature. The **keyword** *keywords* keyword and argument display all commands that contain the specified keyword. For example, **man keyword ipv4** displays all commands that contain ipv4.

Task ID

Task ID	Operations
basic-services	read

The following example shows how to display the manual page for the **arp timeout** command:

```
RP/0/RSP0/CPU0:router# man command arp timeout

COMMAND
arp timeout

DESCRIPTION


To specify how long dynamic entries learned on an interface remain in the
Address Resolution Protocol (ARP) cache, use the arp timeout command in
interface configuration mode. To remove the arp timeout command from the
configuration file and restore the system to its default condition with
respect to this command, use the no form of this command.

arp timeout seconds

no arp timeout<seconds>

SYNTAX DESCRIPTION

seconds
Time, in seconds, for which an entry remains in the ARP cache. The
range is from 0 to 4294967. A value of 0 means that entries are never
cleared from the cache. The default is 14400.

DEFAULTS

Entries remain in the ARP cache for 14400 seconds (4 hours).

COMMAND MODES

Interface configuration

COMMAND HISTORY

Release
Modification

Release 2.0
This command was introduced.
```

```
USAGE GUIDELINES

To use the arp timeout command, you must be a member of a user group
associated with the cef task ID.

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

This command is ignored when issued on interfaces that do not use ARP. Also,
ARP entries that correspond to the local interface or that are statically
configured by the user never time out.

The show interfaces command displays the ARP timeout value in
hours:minutes:seconds, as follows:

* * * * * * * * * * * * * * * * * START OF LISTING * * * * * * * * * * * * * * * * *

ARP type: ARPA, ARP Timeout 04:00:00
* * * * * * * * * * * * * * * * * END OF LISTING * * * * * * * * * * * * * * * * *

EXAMPLES

The following example shows how to set the ARP timeout to 3600 seconds to
allow entries to time out more quickly than the default:

* * * * * * * * * * * * * * * * * START OF LISTING * * * * * * * * * * * * * * * * *
RP/0/RSP0/CPU0:router# configure

RP/0/RSP0/CPU0:router(config)# interface MgmtEth 0/RP1/CPU0/0

RP/0/RSP0/CPU0:router(config-if)# arp timeout 3600
* * * * * * * * * * * * * * * * * END OF LISTING * * * * * * * * * * * * * * * * *

RELATED COMMANDS

Command
Description

clear arp-cache
Deletes all dynamic entries from the ARP cache.

show arp (cache)
Displays the entries in the ARP table.

show interfaces
Displays statistics for all interfaces configured on the networking
device.
```

more

To display the contents of a file, use the **more** command in EXEC or administration EXEC mode.

more [**/ascii** | **/binary** | **/ebcdic**] *filesystem***:***directory-path* **location** [*node-id* | **all**] {**| begin** *regular-expression* | **| exclude** *regular-expression* | **| include** *regular-expression*}

Syntax Description

/ascii	(Optional) Displays a binary file in ASCII format.
/binary	(Optional) Displays a file in hexadecimal or text format.
/ebcdic	(Optional) Displays a binary file in ebcdic format.
filesystem:directory-path	File system location of the file to be displayed. Include the file system alias for the *filesystem* argument, followed by a colon, and the directory path of the file to be displayed.
location [*node-id* **| all**]	(Optional) Displays the contents of a file on a designated node or all nodes.
regular-expression	(Optional) Regular expression found in the file.
|	Vertical bar (the "pipe" symbol) indicates that an output processing specification follows.
begin	(Optional) Begins unfiltered output of the **more** command with the first line that contains the regular expression.
exclude	(Optional) Displays output lines that do not contain the regular expression.
include	(Optional) Displays output lines that contain the regular expression.

Command Default

None

Command Modes

EXEC

Administration EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **more** command to display any text file, especially an ASCII file stored on the router or accessible through the network. The file can be a configuration file or any other text file.

Filtering Output

This table shows filter options for the output displayed by the **more** command.

Table 8: Filtering Options

Command	Purpose
more *filesystem:* **| begin** *regular-expression*	Begins unfiltered output of the **more** command with the first line that contains the regular expression.
more *filesystem:* **| exclude** *regular-expression*	Displays output lines that do not contain the regular expression.
more *filesystem:* **| include** *regular-expression*	Displays output lines that contain the regular expression.

Adding a Filter at the --More-- Prompt

You can also specify a filter at the --More-- prompt of a **more** command output. To filter output from the --More-- prompt, enter a forward slash (**/**) followed by a regular expression. The filter remains active until the command output finishes or is interrupted (using **Ctrl-Z** or **Ctrl-C**).

- A second filter cannot be specified at a --More-- prompt if a filter has already been specified at the original command or at a previous --More-- prompt.
- The minus sign (–) preceding a regular expression displays output lines that do not contain the regular expression.
- The plus sign (+) preceding a regular expression displays output lines that contain the regular expression.



Note After you specify a filter for a **more** command, you cannot specify another filter at the next --More-- prompt. The first specified filter remains until the **more begin** command output finishes or until you interrupt the output. The use of the keyword does not constitute a filter.

Task ID

Task ID	Operations
filesystem	execute

The following example shows partial sample output from the **more** command. The output displays a configuration file saved on the hard disk drive.

```
router# more harddisk:/user/alternate.cfg

!! Last configuration change at 15:52:55 UTC Fri Feb 13 2009 by UNKNOWN
!
line console
exec-timeout 0 0
!
interface MgmtEth0/RP1/CPU0/0
 ipv4 address 10.32.45.154 255.0.0.0
 !
interface TenGigE0/1/0/0
 ipv4 address 10.32.45.155 255.0.0.0
 keepalive disable
```

```
 !
interface TenGigE0/1/0/1
 ipv4 address 10.32.45.156 255.0.0.0
 keepalive disable
 !
interface TenGigE0/1/0/2
/ip
 ipv4 address 10.32.45.157 255.0.0.0
 keepalive disable
 !
interface TenGigE0/1/0/3
 ipv4 address 10.32.45.158 255.0.0.0
 keepalive disable
 !
interface TenGigE0/2/0/0
 ipv4 address 10.32.45.159 255.0.0.0
 keepalive disable
 !
 --More--
```

The following example shows partial sample output from the **more** command. The output begins with unfiltered output from the first line that contains the regular expression “ipv4.” In this example, a new search is specified that begins with output lines that contain the regular expression “ipv4.”

```
RP/0/RSP0/CPU0:router# more disk0:config.backup | begin ipv4

ipv4 address 2.2.2.2 255.255.255.255
!
interface TenGigE0/3/1/0
 shutdown
!
interface TenGigE0/3/1/2
 shutdown
!
interface TenGigE0/2/1/0
 ipv4 address 10.0.0.1 255.255.255.0
 keepalive disable
!
interface TenGigE0/2/1/1
  ipv4 address 10.0.0.1 255.255.255.0
  keepalive disable
!
interface TenGigE0/2/1/2
  ipv4 address 10.0.0.1 255.255.255.0
  keepalive disable
!
interface TenGigE0/2/1/3
 shutdown
!
  /ipv4

filtering...
 ipv4 address 10.0.0.1 255.255.255.0
 proxy-arp disable
 shutdown
!
interface TenGigE 0/1/0/0
 ipv4 address 10.0.0.1 255.255.255.0
 proxy-arp disable
!
route ipv4 0.0.0.0/0 12.25.26.5
route ipv4 223.255.254.254/32 12.25.0.1
```

```
end
```

The following example shows partial sample output of the **more** command on the sample file config.backup in disk0:. The command usage is `more disk0:config.backup | include log`. At the --More-- prompt, a new search is specified that begins with output lines that contain the regular expression “aaa.”

```
RP/0/RSP0/CPU0:router# more disk0:config.backup | include log

logging trap
logging trap informational
logging console debugging
logging history size 1
.
.
.
/aaa

filtering...
aaa authentication login default none
```

The following example shows partial sample output from the **more** command. The output excludes lines that contain the regular expression “alias.” In this example, at the --More-- prompt, a new search is specified, beginning with output lines that contain the regular expression “ipv4 address.”

```
RP/0/RSP0/CPU0:router# more disk0:myconfig/file | exclude alias

Building configuration...
!! Last configuration change at 18:17:00 UTC Thu May 16 2009 by lab
!
hostname router
line console
 exec-timeout 0 0
 width 132
 length 0
 session-timeout 0
/ipv4 address

filtering...
ipv4 address 10.10.1.1 255.255.255.255
!
interface Loopback200
 ipv4 address 10.20.1.1 255.255.255.255
!
interface TenGigE0/0/0/0
 ipv4 address 10.30.1.1 255.255.0.0
 keepalive 100
!
interface preconfigure TenGigE0/1/0/1
 shutdown
end
```

Related Topics

show, on page 159

pwd (config)

To display the current configuration submode from a configuration submode, use the **pwd** command in any supported configuration submode.

pwd

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Any subconfiguration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

The following example shows how to use the **pwd** command from an interface configuration submode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tengige 0/6/4/5
RP/0/RSP0/CPU0:router(config-if)# pwd

interface TenGigE0/6/4/5
RP/0/RSP0/CPU0:router(config-if)#
```

rollback configuration

To roll back the running configuration to a previous configuration, use the **rollback configuration** command inEXEC or administration EXEC mode.

rollback configuration {**last** *number-of-commits* | **to** *commit-id*} [**force**] [**label** *label*] **comment** *comment*

Syntax Description

last *number-of-commits*	Rolls back to the configuration that existed before the last number of commits (specified with the *number-of-commits* argument) were made.
to *commit-id*	Rolls back to the running configuration that existed before the configuration specified with the *commit-id* argument.
force	(Optional) Specifies to override any commit blocks.
label *label*	(Optional) Assigns a text label to this rollback. The *label* argument must begin with a letter.
comment *comment*	(Optional) Assigns a text comment to this rollback. The *comment* argument can be up to 60 characters long.

Command Default

None

Command Modes

EXEC

Administration EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Each time the **commit** command is entered, a commit ID is assigned to the new configuration. You can revert the system to the configuration of a previous commit ID with the **rollback configuration** command:

- Use the **to** keyword to revert to the configuration that existed *before* the configuration specified with the *commit-id* argument.

- Use the **last** keyword to revert to the configuration that existed *before* the last number of configuration commits (specified with the *number-of-commits* argument) were made.
- Use **show configuration commit list** to display a list of the commit IDs available for rollback operations.

Note The most recent 100 commits are retained by the system. As new commit IDs are added, the oldest commit IDs are discarded and are no longer available for rollback operations.

Use the **force** keyword to override commits that would fail otherwise. This is useful in the event of a low-memory condition on the router, to revert to a commit that would remove a configuration that caused the low-memory condition.

Note The rollback operation may fail if you try to rollback two (or more) commits where the individual commits involve the configuration and removing of the configuration of the same item, and there is a dependency of one item over another in any of the individual commit operations.

Task ID

Task ID	Operations
root-lr (EXEC)	read, write
root-system (administration EXEC)	read, write

Rolling Back to a Specific Commit ID

The following example shows how to roll back to a specific commit ID. In this example, the **show configuration commit list** command displays the available rollback points. The configuration is then rolled back to a prior commit with the **rollback configuration** command.

```
RP/0/RSP0/CPU0:router# show configuration commit list

SNo. Label/ID    User      Line        Client      Time Stamp
~~~~ ~~~~~~~~    ~~~~      ~~~~        ~~~~~~      ~~~~~~~~~~
1    1000000009  lab       con0_RSPs0_C  Rollback    02:41:08 UTC Sun Sep 26 2009
2    1000000008  lab       con0_RSPs0_C  CLI         02:40:30 UTC Sun Sep 26 2009
3    1000000007  lab       con0_RSPs0_C  CLI         02:39:54 UTC Sun Sep 26 2009
4    1000000006  lab       con0_RSPs0_C  Rollback    02:38:40 UTC Sun Sep 26 2009
5    1000000005  lab       con0_RSPs0_C  CLI         02:37:35 UTC Sun Sep 26 2009
6    1000000004  lab       con0_RSPs0_C  CLI         02:37:04 UTC Sun Sep 26 2009

RP/0/RSP0/CPU0:router# rollback configuration to 1000000008

Loading Rollback Changes.
Loaded Rollback Changes in 1 sec
Committing.
1 items committed in 1 sec (0)items/sec
Updating.RP/0/RP0/CPU0:Sep 26 02:42:09.318 : config_rollback[65707]: %LIBTARCFG-
6-COMMIT : Configuration committed by user 'lab'.   Use 'show commit changes 100
0000010' to view the changes.

Updated Commit database in 1 sec
```

```
Configuration successfully rolled back to '1000000008'.
```

Rolling Back to a Span of Configuration Commits

The following example shows how to roll back to the configuration that existed prior to the last two configuration commits:

```
RP/0/RSP0/CPU0:router# rollback configuration last 2

Loading Rollback Changes.
Loaded Rollback Changes in 1 sec
Committing.
1 items committed in 1 sec (0)items/sec
Updating.
Updated Commit database in 1 sec
Configuration successfully rolled back 2 commits.
```

Related Topics

load rollback changes, on page 128
show configuration rollback changes, on page 194

root

To return to configuration mode from a configuration submode, use the **root** command in any supported configuration submode.

root

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Any subconfiguration mode except the following:

- The **root** command is not available under the route-policy submodes, because it requires the **end-policy** command to exit out of the configuration.
- The **root** command is not available in template submode, but is available in the submodes configurable under the template submode.

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
config-services	read

The following example shows how to use the **root** command to return to configuration mode from the interface configuration submode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tengige 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# root
RP/0/RSP0/CPU0:router(config)#
```

The following example shows how to use the **root** command from a submode configurable under the template submode. In this example, the **root** command is used to return to configuration mode from the username submode:

Note The recommended range for a user-defined username is 2-253 characters.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# template test
RP/0/RSP0/CPU0:router(config-TPL)# username xyz
```

```
RP/0/RSP0/CPU0:router(config-un)# root
RP/0/RSP0/CPU0:router(config)# show conf

Building configuration...
template test
 username xyz
 !
 end-template
 end
```



Tip The **root** command is not available from the template submode, but is available in the submodes configurable under the template submode.

save configuration

To save the contents of a configuration to a file, use the **save configuration** command in global configuration or administration configuration mode.

save configuration [**running**] *device***:***directory-path*

Syntax Description

running	(Optional) Saves the contents of the running configuration.
device: directory-path	Storage device and directory path of the configuration file to be loaded into the target configuration.

Command Default

None

Command Modes

Global configuration

Administration configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

To save a configuration to a file, use the **save configuration** command.

To save a configuration that failed to a file, use the **save configuration failed** command.

Task ID

Task ID	Operations
config-services	read

The following example shows the configuration saved to disk0: from global configuration mode:

```
RP/0/RSP0/CPU0:router(config)# save configuration disk0:sample3

Destination file name (control-c to abort): [/sample3]?
Building configuration.
1 lines built in 1 second
[OK]
```

The following example shows the configuration saved to disk1 from administration EXEC mode:

```
RP/0/RSP0/CPU0:router(admin-config)# save configuration disk1:sample4

Destination file name (control-c to abort): [/sample4]?
Building configuration.
1 lines built in 1 second
```

```
[OK]
```

Related Topics

save configuration commit changes, on page 146
save configuration failed, on page 148
save configuration merge, on page 150
save rollback changes, on page 153
save configuration removed, on page 151
Show configuration commit changes, on page 171
show configuration commit list, on page 174
show configuration rollback changes, on page 194

save configuration changes

To save the changes of a configuration to a file, use the **save configuration changes** command in global configuration or administration configuration mode.

save configuration changes *device*:*directory-path*

Syntax Description

device: directory-path	Storage device and directory path of the configuration file to be loaded into the target configuration.

Command Default

None

Command Modes

Global configuration

Administration configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

To save the configuration changes to be made during a replace operation to a file, use the **save configuration changes** command.

Task ID

Task ID	Operations
config-services	read

The following example shows the configuration saved to disk0: from global configuration mode:

```
RP/0/RSP0/CPU0:router(config)# save configuration changes disk0:sample3

Destination file name (control-c to abort): [/sample3]?
Building configuration.
1 lines built in 1 second
[OK]
```

Related Topics

save configuration commit changes, on page 146
save configuration failed, on page 148
save configuration merge, on page 150
save rollback changes, on page 153
save configuration removed, on page 151
Show configuration commit changes, on page 171

show configuration commit list, on page 174
show configuration rollback changes, on page 194

save configuration commit changes

To save the changes for a commit, or a series of commits, to a file, use the **save configuration commit changes** command in global configuration or administration configuration mode.

save configuration commit changes {*commit-id* | **last** *number-of-commits* | **since** *commit-id*} *device***:***directory-path*

Syntax Description

commit-id	Specific commit ID.
last *number-of-commits*	Saves changes made in the most recent *number-of-commits*.
since *commit-id*	Saves changes made since (and including) a specific *commit-id*.
device: directory-path	Storage device and directory path of the configuration file to be loaded into the target configuration.

Command Default

None

Command Modes

Global configuration

Administration configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 3.9.0	No modification.

Usage Guidelines

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

Use the **save configuration commit changes** command to save the changes made in a commit operation to a file. You can specify a specific commit ID, all the changes since a specified commit ID, or the changes that occurred during the last *n* commits.

Task ID

Task ID	Operations
config-services	read

The following example saves the changes from the last two commit operations to disk0:

```
RP/0/RSP0/CPU0:router(admin-config)# save configuration commit changes last 2 disk0:sample1

Destination file name (control-c to abort): [/sample1]?
Building configuration.
5 lines built in 1 second
```

```
[OK]
```

Related Topics

save configuration, on page 142
save configuration changes, on page 144
save configuration failed, on page 148
save configuration merge, on page 150
save rollback changes, on page 153
show configuration history, on page 184
save configuration removed, on page 151
Show configuration commit changes, on page 171
show configuration commit list, on page 174
show configuration rollback changes, on page 194

save configuration failed

To save the contents of the failed configuration, use the **save configuration failed** command inglobal configuration or administration configuration mode.

save configuration failed [**load** | **noerrors** | **startup** [**previous** *number*] [**noerror**]] *device***:***directory-path*

Syntax Description

load	(Optional) Saves the failed configuration (syntax errors) in the last reload.
noerrors	(Optional) Excludes the error reasons from the saved configuration.
startup	(Optional) Saves the failed configuration during startup.
previous *number*	(Optional) Saves a failed startup configuration from the specified previous sessions. The *number* argument is a value between 1 and 4 that indicates how many failed startup configurations to save.
device: directory-path	Storage device and directory path of the configuration file to be saved.

Command Default

None

Command Modes

Global configuration

Administration configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

To save a configuration to a file, use the **save configuration** command.

To save a configuration that failed to a file, use the**save configuration failed** command.

To save a configuration that failed during startup to a file, use the **save configuration failed** command with the **startup** keyword.

Task ID

Task ID	Operations
config-services	read

The following example saves the failed configuration to disk0:

```
RP/0/RSP0/CPU0:router(admin-config)# save configuration failed disk1:/configs
```

Related Topics

save rollback changes, on page 153
show configuration history, on page 184
save configuration removed, on page 151
Show configuration commit changes, on page 171
show configuration commit list, on page 174
show configuration rollback changes, on page 194

save configuration merge

To save the contents of a merged configuration to a file, use the **save configuration merge** command in global configuration or administration configuration mode.

save configuration merge *device*:*directory-path*

Syntax Description

device : *directory-path*	Storage device and directory path of the configuration file to be loaded into the target configuration.

Command Default

None

Command Modes

Global configuration

Administration configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
config-services	read

The following example shows the configuration saved to disk0:

```
RP/0/RSP0/CPU0:router(admin-config)# save configuration merge disk0:sample3

Destination file name (control-c to abort): [/sample3]?
Building configuration.
1 lines built in 1 second
[OK]
```

Related Topics

save rollback changes, on page 153
show configuration history, on page 184
save configuration removed, on page 151
Show configuration commit changes, on page 171
show configuration commit list, on page 174
show configuration rollback changes, on page 194

save configuration removed

To save the contents of a removed configuration to a file, use the **save configuration removed** command in global configuration or administration configuration mode.

save configuration removed *removed-configuration-file device*:*directory-path*

Syntax Description

removed-configuration-file	Specifies the name of the removed configuration file.
device:*directory-path*	Storage device and directory path of the configuration file to be loaded into the target configuration.

Command Default

None

Command Modes

Global configuration

Administration configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

When a package is deactivated, the configuration belonging to that package is removed from the running configuration and saved to a file. To save a copy of the removed configuration file, use the **save configuration removed** command.

Task ID

Task ID	Operations
config-services	read

To view a list of the available removed configuration files, use the **save configuration removed** command followed by a question mark:

```
RP/0/RSP0/CPU0:router(config)# save configuration removed ?

    20051208042507.cfg  Removed configuration.
    20051208044553.cfg  Removed configuration.
    <cr>
```

In the following example, a removed configuration is saved to disk0: and assigned the filename "sample3:"

```
RP/0/RSP0/CPU0:router(config)# save configuration removed 20051208042507.cfg disk0:sample3

  Destination file name (control-c to abort): [/sample3]?
```

```
Building configuration.
1 lines built in 1 second
[OK]
```

Related Topics

save configuration, on page 142
save configuration commit changes, on page 146
save configuration failed, on page 148
save configuration merge, on page 150
save rollback changes, on page 153
show configuration history, on page 184
Show configuration commit changes, on page 171
show configuration commit list, on page 174
show configuration rollback changes, on page 194

save rollback changes

To save the rollback changes, use the **save rollback changes** command in global configuration or administration configuration mode.

save rollback changes {*commit-id* | **last** *number-of-commits* | **to commit-id**} *device***:***directory-path*

Syntax Description

commit-id	Specific commit ID.
last *number-of-commits*	Saves the rollback changes for the last *n* commits
to *commit-id*	Saves rollback changes up to a specific *commit-id*.
device: directory-path	Storage device and directory path of the configuration file to be loaded into the target configuration.

Command Default

None

Command Modes

Global configuration

Administration configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **save rollback changes** command to save the changes that would be made in a configuration rollback to a specific commit point or for a series of commits.

Task ID

Task ID	Operations
config-services	read

The following example shows that the rollback changes for the commit point 5 are saved to the file sample4 on disk0:

```
RP/0/RSP0/CPU0:router(admin-config)# save rollback changes last 1 disk0:sample4

Destination file name (control-c to abort): [/sample4]?
Building configuration.
6 lines built in 1 second
[OK]
```

Related Topics

save configuration, on page 142

save configuration commit changes, on page 146
show configuration history, on page 184
show configuration commit list, on page 174
show configuration rollback changes, on page 194

set default-afi

To set the default address family identifier (AFI) for the current session, use the **set default-afi** command in EXEC mode.

set default-afi {**all** | **ipv4** | **ipv6**}

Syntax Description

all	Sets the default AFI to IPv4 and IPv6 for the current session.
ipv4	Sets the default AFI to IPv4 for the current session. This is the default setting.
ipv6	Sets the default AFI to IPv6 for the current session.

Command Default

The default AFI setting is set to IPv4 for all sessions.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **set default-afi** command to set the default AFI for the current session. This command acts as a keystroke shortcut for **show** commands. If the default AFI setting is set to IPv4, then you would not have to specify the **ipv4** keyword for **show** commands that support the **ipv4** keyword. For example, if the AFI setting is set to IPv4, you could issue the **show route** command without specifying the **ipv4** keyword to display IPv4 routes in the Routing Information Base (RIB).

Use the **show default-afi-safi-vrf** command to display the default AFI setting.

Task ID

Task ID	Operations
basic-services	read, write

The following example shows how to set the default AFI to IPv6:

```
RP/0/RSP0/CPU0:router# set default-afi ipv6

%% Default Address Family Identifier is set to 'ipv6'
```

Related Topics

set default-safi, on page 156
set default-vrf, on page 157
show default-afi-safi-vrf, on page 202

set default-safi

To set the default subaddress family identifier (SAFI) for the current session, use the **set default-safi** command in EXEC mode.

set default-safi {**all** | **multicast** | **unicast**}

Syntax Description

all	Sets the default SAFI to multicast and unicast for the current session.
multicast	Sets the default SAFI to multicast for the current session.
unicast	Sets the default SAFI to unicast for the current session. This is the default setting.

Command Default

The default SAFI setting is set to unicast for all sessions.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **set default-safi** command to set the default SAFI setting for the current session. This command acts as a keystroke shortcut for **show** commands. If the default SAFI setting is set to unicast, you would not have to specify the **unicast** keyword for **show** commands that support that keyword. For example, if the default SAFI setting is set to unicast, you could issue the **show router** command without specifying the **unicast** keyword to display information about unicast address prefixes in the Routing Information Base (RIB).

Use the **show default-afi-safi-vrf** command to display the default SAFI setting.

Task ID

Task ID	Operations
basic-services	read, write

The following example shows how to set the default SAFI to multicast:

```
RP/0/RSP0/CPU0:router# set default-safi multicast

%% Default Sub-Address Family Identifier is set to 'multicast'
```

Related Topics

set default-afi, on page 155
set default-vrf, on page 157
show default-afi-safi-vrf, on page 202

set default-vrf

To set the default VPN routing and forwarding (VRF) instance for the current session, use the **set default-vrf** command in EXEC mode.

set default-vrf {*name* | **none**}

Syntax Description

name	Default VPN routing and forwarding name.
none	Sets the default VPN routing and forwarding name to empty.

Command Default

The default VRF setting is set to empty.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **set default-vrf** command to set the default VRF setting for the current session. This command acts as a keystroke shortcut for **show** commands. For example, if the default VRF is configured, you can issue the **show route** command without specifying the VRF name.

When the default VRF for the session is set to **none**, then IPv4 routes for the system default VRF are displayed.



Note To override the default VRF setting, specify the VRF name in the **show** command.

Use the **show default-afi-safi-vrf** command to display the default VRF setting.

Task ID

Task ID	Operations
basic-services	read, write

In the following example, the default VRF is set to “dft_vrf:”

```
RP/0/RSP0/CPU0:router# set default-vrf dft_vrf

  %% Default Virtual Routing/Forwarding is set to 'dft_vrf'
```

In the following command, the **show route** command is entered without specifying a VRF name. The results for the "dft_vrf" VRF are displayed because the default VRF was set to “dft_vrf.”

```
RP/0/RSP0/CPU0:router# show route ipv4

  % No matching vrf found
```

When the default VRF for the session is set to **none**, the system default VRF routes are displayed. In the following example, the default VRF is set to (empty) and the **show route** command displays the system default VRF information:

```
RP/0/RSP0/CPU0:router# set default-vrf none

%% Default Virtual Routing/Forwarding is set to ''

RP/0/RSP0/CPU0:router# show route ipv4

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
       U - per-user static route, o - ODR, L - local

Gateway of last resort is 12.29.0.1 to network 0.0.0.0

  S*   0.0.0.0/0 [1/0] via 12.29.0.1, 00:31:30
  L    10.10.10.10/32 is directly connected, 3d02h, Loopback1
  C    12.29.0.0/16 is directly connected, 00:31:30, MgmtEth0/0/CPU0/0
  L    12.29.56.21/32 is directly connected, 00:31:30, MgmtEth0/0/CPU0/0
```

Related Topics

set default-afi, on page 155
set default-safi, on page 156
show default-afi-safi-vrf, on page 202

show

To display information about the system configuration or operational state, use the **show** command in EXEC mode, administration EXEC mode, or any configuration mode.

show *command*[| **begin** *regular-expression* | | **exclude** *regular-expression* | | **file** *filesystem:* | | **include** *regular-expression*]

Syntax Description

command	Supported **show** command.
|	Vertical bar (the "pipe" symbol) indicates that an output processing specification follows.
regular-expression	(Optional) Regular expression found in **show** command output.
begin	(Optional) Begins unfiltered output of the **show** command with the first line that contains the regular expression.
exclude	(Optional) Displays output lines that do not contain the regular expression.
file *filesystem:*	(Optional) Writes the output lines that contain the regular expression to the specified file on the specified file system. Include the file system alias for the *filesystem* argument, followed by a colon, and the directory path and filename.
include	(Optional) Displays output lines that contain the regular expression.

Command Default

None

Command Modes

EXEC

Administration EXEC

Any configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

The **show** commands display information about the system and its configuration. To display a list of the available **show** commands, use the question mark (?) online help function.

Filtering Output

Search options for the **show** command are shown in this table.

Table 9: Show Command Search Options

Command	Purpose
show *command* | **begin** *regular-expression*	Begins unfiltered output of the **show** command command with the first line that contains the regular expression.
show *command* | **exclude** *regular-expression*	Displays output lines that do not contain the regular expression.
show *command* | **include** *regular-expression*	Displays output lines that contain the regular expression.
show *command* | **file** *filesystem:*	Writes the output lines that contain the regular expression to the specified file on the specified file system.

Adding a Filter at the --More-- Prompt

You can also specify a filter at the --More-- prompt of a **show** command output. To filter output from the --More-- prompt, enter a forward slash (/) followed by a regular expression. The filter remains active until the command output finishes or is interrupted (using **Ctrl-Z** or **Ctrl-C**).

- If a filter is specified at the original command or a previous --More-- prompt, a second filter cannot be applied.
- The use of the **begin** keyword does not constitute a filter.
- The minus sign (–) preceding a regular expression displays output lines that do not contain the regular expression.
- The plus sign (+) preceding a regular expression displays output lines that contain the regular expression.

Task ID

Task ID	Operations
Task ID for the feature used with the **show** command	read

For example, the **show interfaces** command requires read privileges in the interface task ID.

The following example shows output from the **show interface | include protocol** command. In this example, the **show** command command includes only lines in which the regular expression “protocol” appears:

```
RP/0/RSP0/CPU0:router# show interface | include protocol

  Null0 is up, line protocol is up
  0 drops for unrecognized upper-level protocol
  TenGigE0/2/0/0 is administratively down, line protocol is administratively down
  0 drops for unrecognized upper-level protocol
  TenGigE0/2/0/1 is administratively down, line protocol is administratively down
  0 drops for unrecognized upper-level protocol
  TenGigE0/2/0/2 is administratively down, line protocol is administratively down
  0 drops for unrecognized upper-level protocol
  TenGigE0/2/0/3 is administratively down, line protocol is administratively down
  0 drops for unrecognized upper-level protocol
```

```
  FastEthernet0/RP0/CPU0/0 is administratively down, line protocol is administratively
  down
  FastEthernet0/RP0/CPU0/0 is administratively down, line protocol is administratively
  down
  0 drops for unrecognized upper-level protocol
```

On most systems, the **Ctrl-Z** key combination can be entered at any time to interrupt the output and return to EXEC mode. For example, use the **show running-config | begin hostname** command to start the display of the running configuration file at the line containing the hostname setting, then use **Ctrl-Z** when you get to the end of the information you are interested in.

The following example shows sample output from the **show configuration running | begin line** command. The output begins with unfiltered output from the first line that contains the regular expression "line." In this example, at the --More-- prompt, a new search is specified that begins with output lines that contain the regular expression "ipv4."



Note The use of the **begin** keyword does not constitute a filter.

```
RP/0/RSP0/CPU0:router# show configuration running | begin line

  Building configuration...
  line console
   exec-timeout 120 120
  !
  logging trap
  --More--
  /ipv4

  filtering...
  route ipv4 0.0.0.0 255.255.0.0 pos0/2/0/0
  interface TenGigE0/2/0/0
   ipv4 address 172.19.73.215 255.255.0.0
  end
```

Related Topics

more, on page 132

show aliases

To display all defined aliases or the aliases defined in a specified mode, use the **show aliases** command in EXEC mode.

show aliases

Syntax Description

This command has no keywords or arguments.

Command Default

Displays all aliases currently configured on the system.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **show aliases** command to display all aliases currently configured on the system.

Task ID

Task ID	Operations
basic-services	read

The following example illustrates sample output from the **show aliases** command. The output displays a summary of all the command aliases configured.

```
RP/0/RSP0/CPU0:router# show aliases

exec mode aliases:
ipv4_brief              show ipv4 interface brief

interface mode aliases:
sample_int              tengige 0/2/0/0
```

Related Topics

alias, on page 82

show apply-group

To display the applied configuration groups, use the **show apply-group** command in EXEC mode.

show apply group

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 5.1.1	This command was introduced.

Usage Guidelines

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

The output of this show command indicates if the group is a part of the global apply-group or is a part of the sub-mode level apply-group.

Task ID

Task ID	Operation
config-services	read

Example

This example shows how to use the **show apply-group** command:

```
RP/0/RSP0/CPU0:router #  show apply-group
             Global       Non-Global
Groups Reference Count Reference Count
------ --------------- ---------------
B               1             0
C               1             0
```

Reference count can either be 0 ro 1. 0 indicates that the group is not applied globally; 1 indicates that the group is globally applied.

show commit changes diff

To display the difference between the currently running configuration and the target configuration (the configuration before the commit command), use the **show commit changes diff** command in the appropriate mode.

show commit changes diff

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Release 5.2.0	This command was introduced.
Release 5.2.1	Class-map was supported.
Release 5.3.1	Policy-map was supported.

Usage Guidelines

The **show commit changes diff** command displays the output by prepending symbols based on the configuration event:

Symbol	Event
+	Add
-	Delete
<-	Modify for old value
+>	Modify for new value

Task ID

Task ID	Operations
config-services	read

This example shows the output of **show commit changes diff** command for adding a policy-map:

```
RP/0/RSP0/CPU0:router# show commit changes diff
+  policy-map pshow
+   class c1
+    set precedence 1
+   !
+   class c2
+    police rate 100 kbps
+    !
+   !
+   class class-default
+   !
```

```
+   end-policy-map
+  !
```

This example shows the output of **show commit changes diff** command for adding a class-map:

```
RP/0/RSP0/CPU0:router# show commit changes diff
 !
+  class-map match-any c
+   match precedence 1 2 3
+   match qos-group 2
+   end-class-map
end
```

This example shows the output of **show commit changes diff** command for deleting a policy-map:

```
RP/0/RSP0/CPU0:router# show commit changes diff
-  policy-map pshow
-   class c1
-    set precedence 1
-   !
-   class c2
-    police rate 100 kbps
-    !
-   !
-   class class-default
-   !
-   end-policy-map
-  !
```

This example shows the output of **show commit changes diff** command for deleting a class-map:

```
RP/0/RSP0/CPU0:router# show commit changes diff
  !
-  class-map match-any c1
-   match precedence 1
-   end-class-map
end
```

This example shows the output of **show commit changes diff** command for modifying a policy-map:

```
RP/0/RSP0/CPU0:router# show commit changes diff
   policy-map pshow
   -  class c1
   -   set precedence 1
    !
    class c2
   <-  police rate 100 kbps
   +>  police rate 200 kbps
      !
   +    set precedence 1
    !
   +   class c3
   +    shape average 100 kbps
     !
    end-policy-map
   !
end
```

This example shows the output of **show commit changes diff** command for modifying a class -map:

```
RP/0/RSP0/CPU0:router# show commit changes diff
   policy-map pshow
  class-map match-any c
    - match precedence 1 2 3
    <- match qos-group 2
    +> match qos-group 2 4 5
    + match dscp 1 2 3
  end-class-map
```

show configuration (config)

To display information about the current configuration session (target configuration), use the **show configuration** command in any configuration mode.

show configuration [**merge**] [**running**]

Syntax Description

merge	(Optional) Displays the configuration that occurs if the contents of the uncommitted changed (target configuration) are committed to the running configuration.
running	(Optional) Displays the running (committed) configuration.

Command Default

When the **show configuration** command is entered without an argument, the uncommitted changes to the target configuration are displayed.

Command Modes

Any configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **show configuration** command to display details on uncommitted configuration changes.

Use the **show configuration** command with the **running** keyword to display the running (active) configuration.

Prior to committing the target configuration, use the **show configuration** command with the **merge** keyword from any configuration mode to display the result of merging the target configuration with the running configuration.

Task ID

Task ID	Operations
basic-services	read

In this example, the **show configuration** command displays uncommitted changes made during a configuration session:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tengige0/3/0/3
RP/0/RSP0/CPU0:router(config-if)# description faq
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 10.10.11.20 255.0.0.0
RP/0/RSP0/CPU0:router(config-if)# show configuration

Building configuration...
interface TenGigE0/3/0/3
 description faq
 ipv4 address 10.10.11.20 255.0.0.0
```

```
 end
```

The following example shows sample output from the **show configuration** command with the optional **merge** keyword. The command is entered during a configuration session. The output displays the result of merging the target and running configuration, without committing the changes.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tengige0/3/0/3
RP/0/RSP0/CPU0:router(config-if)# description faq
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 10.10.11.20 255.0.0.0
RP/0/RSP0/CPU0:router(config-if)# show configuration merge

Building configuration...
hostname router
interface TenGigE0/0/0/0
 ipv4 address 1.2.3.4 255.0.0.0
 exit
interface TenGigE0/3/0/3
 description faq
 ipv4 address 1.1.1.1 255.0.0.0
 shutdown
 end
```

Related Topics

show configuration failed (config), on page 177
show configuration history, on page 184
show configuration sessions, on page 200
show running-config, on page 206
commit, on page 99
load, on page 123
Show configuration commit changes, on page 171
show configuration commit list, on page 174
show configuration failed startup, on page 183
show configuration rollback changes, on page 194
show configuration running-config, on page 198

show configuration changes

To display the configuration changes to be made during a replace operation, use the **show configuration changes** command in global configuration or administration configuration Admin Configuration mode .

show configuration changes [**diff**]

Syntax Description

diff	(Optional) Displays the changes in UNIX-like format.

Command Default

None

Command Modes

Global Configuration mode

Admin Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
config-services	read
basic-services	read

The following example shows the changes to be made during a replace operation:

```
RP/0/RSP0/CPU0:router(config)# show configuration changes diff

  Building configuration...
  # hostname router
  # hostname bla
  - logging console
  - telnet vrf default ipv4 server disable
  - domain ipv4 host xhu-u5
  - domain ipv4 host coax-u10
  - domain ipv4 host coax-u10.cisco.com
  - domain name
  - interface Loopback1
  -  ipv4 address 10.0.0.2 255.255.255.224
  - !
  - interface Loopback2
  -  description
  - !
  - interface Loopback5
  -  description
  - !
  - interface Loopback6
```

```
-  description
- !
- interface MgmtEth0/0/CPU0/0
-  ipv4 address 10.0.0.1 255.255.255.224
- !
- interface GigabitEthernet0/2/0/0
-  shutdown
- !
- interface GigabitEthernet0/2/0/1
-  shutdown
- !
- interface GigabitEthernet0/2/0/2
-  shutdown
- !
- router static
-  address-family ipv4 unicast
-   0.0.0.0/0 255.255.255.224
-  !
- !
end
```

Show configuration commit changes

To display the changes made to the running configuration by previous configuration commits, a configuration commit, or for a range of configuration commits, use the **show configuration commit changes** command in EXEC, administration EXEC, administration configuration, or global configuration mode.

show configuration commit changes {*commit-id* | **since** *commit-id* | **last** *number-of-commits* } [**diff**]

Syntax Description

since	Displays all changes committed to the running configuration since (and including) a specific configuration commit.
commit-id	Displays configuration changes for a specific configuration commit.
last *number-of-commits*	Displays the changes made to the running configuration during the last number of configuration commits specified for the *number-of-commits* argument.
diff	(Optional) Displays added lines, changed lines, and deleted lines.

Command Default

None

Command Modes

EXEC

Administration EXEC

Administration configuration

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Each time a configuration is committed with the **commit** command, the configuration commit operation is assigned a commit ID. The **show configuration commit changes** command displays the configuration changes made since the specified commit.

To display a list of the available commit IDs, enter the **show configuration commit list** command. You can also display the commit IDs by entering the **show configuration commit changes** command with the online help function (**?**).

You can’t view commit IDs from a different release if the syntax or semantics of the configuration changed in the current release.



Note Syntax of a configuration refers to its structure and format, while the semantics of a configuration refers to its backend interpretation.

Task ID

Task ID	Operations
config-services	read

The following example shows sample output from the **show configuration commit changes** command. The output displays commit IDs.

```
RP/0/RSP0/CPU0:router# show configuration commit list

SNo. Label/ID    User      Line         Client      Time Stamp
~~~~ ~~~~~~~~    ~~~~      ~~~~         ~~~~~~      ~~~~~~~~~~
1    1000000077  lab       con0_RSPs1_C  CLI          15:42:45 UTC Fri Jan 30 2009
2    1000000076  lab       con0_RSPs1_C  Rollback     15:30:39 UTC Fri Jan 30 2009
3    1000000075  lab       con0_RSPs1_C  Rollback     15:25:26 UTC Fri Jan 30 2009
4    1000000074  lab       con0_RSPs1_C  Rollback     15:04:29 UTC Fri Jan 30 2009
5    1000000073  lab       con0_RSPs1_C  CLI          14:49:07 UTC Fri Jan 30 2009
6    1000000072  lab       con0_RSPs1_C  CLI          14:48:35 UTC Fri Jan 30 2009
```

The following example shows sample output from the **show configuration commit changes** command with the *commit-id* argument. In this example, the output displays the changes made in the configuration commit assigned commit ID 1000000077.

```
RP/0/RSP0/CPU0:router# show configuration commit changes 1000000077

Building configuration...
alias exec shrun show configuration running
alias exec shver show version
end
```

The following example shows sample output from the **show configuration commit changes** command with the **since** *commit-id* keyword and argument. In this example, the output displays the configuration changes made since the configuration commit assigned commit ID 1000000077 was committed.

```
RP/0/RSP0/CPU0:router# show configuration commit changes since 1000000077

Building configuration...
no hw-module node 0/RP0/CPU0 shutdown
hostname router
logging trap
no logging console
logging history size 1
alias exec shrun show configuration running
alias exec shver show version
interface MgmtEth0/RP1/CPU0/0
 ipv4 address 12.25.34.10 255.255.0.0
 no shutdown
 !
 interface preconfigure MgmtEth0/RP0/CPU0/0
 no shutdown
```

```
 !
no route ipv4 0.0.0.0/0 12.7.0.1
route ipv4 0.0.0.0/0 12.25.0.1
route ipv4 223.255.254.254/32 12.25.0.1
telnet ipv4 server enable
end
```

The following example shows sample output from the **show configuration commit changes** command with the **diff** keyword. In the display, the following symbols signify changes:

+ indicates an added line.

– indicates a deleted line.

# indicates a modified line.

```
RP/0/RSP0/CPU0:router# show configuration commit changes last 1 diff

Building configuration...
+ interface Loopback1000
+ ipv4 address 190.190.180.1 255.255.255.255
!
end

+ interface Loopback1000
+ ipv4 address 190.190.180.1 255.255.255.255
  !
  end
```

Related Topics

rollback configuration, on page 137
show configuration rollback changes, on page 194

show configuration commit list

To display information about the configuration commits stored in the commit database, use the **show configuration commit list** command in EXEC, administration EXEC, administration configuration, or global configuration mode.

show configuration commit list [*number-of-commits*] [**detail**]

Syntax Description

number-of-commits	(Optional) Number of commits (beginning with the most recent commit) that are available for rollback.
detail	(Optional) Displays detailed commit information, including comments.

Command Default

If this command is entered without any optional arguments or keywords, the output displays information about all the configuration commits stored in the commit database.

Command Modes

EXEC

Administration EXEC

Administration configuration

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **show configuration commit list** command to list the commit IDs (up to 100) that are available for rollback.

Note The most recent 100 commits are retained by the system. As new commit IDs are added, the oldest commit IDs are discarded and are no longer available for rollback operations.

Task ID

Task ID	Operations
config-services	read

The following example shows sample output from the **show configuration commit list** command. The output displays the commit IDs that are available for rollback.

```
RP/0/RSP0/CPU0:router# show configuration commit list
```

```
SNo. Label/ID    User      Line        Client      Time Stamp
~~~~ ~~~~~~~~    ~~~~      ~~~~        ~~~~~~      ~~~~~~~~~~
1    1000000010  UNKNOWN   con0_RSP0_C  Rollback    02:25:53 UTC Fri Feb 06 2009
2    1000000009  UNKNOWN   con0_RSP0_C  CLI         02:23:09 UTC Fri Feb 06 2009
3    1000000008  UNKNOWN   con0_RSP0_C  CLI         02:22:54 UTC Fri Feb 06 2009
4    1000000007  UNKNOWN   con0_RSP0_C  CLI         02:22:18 UTC Fri Feb 06 2009
5    1000000006  UNKNOWN   con0_RSP0_C  CLI         02:07:21 UTC Fri Feb 06 2009
```

Table 10: show configuration commit list Field Descriptions, on page 175describes the significant fields shown in the display.

Table 10: show configuration commit list Field Descriptions

Field	Description
SNo.	Serial number of the commit entry.
Label/ID	If a label was assigned to a commit, the first 10 characters of the label display; otherwise, the autogenerated commit ID displays.
User	User who executed the commit.
Line	Line in which the user session was established. In some cases, this field may display "UNKNOWN" or "SYSTEM". These fields indicate that an internal commit was made by the system.
Client	The management interface used to make the commit.
Time Stamp	Time and date when the commit was executed.

Related Topics

show configuration (config), on page 167
show configuration failed (config), on page 177
show configuration history, on page 184
show configuration running, on page 196
show configuration sessions, on page 200
show running-config, on page 206
Show configuration commit changes, on page 171
show configuration failed startup, on page 183
show configuration rollback changes, on page 194
show configuration running-config, on page 198

show configuration failed

To display information about a configuration that failed during the last commit , use the **show configuration failed** command in EXEC mode.

show configuration failed [**inheritance**]

Syntax Description

inheritance	Displays the failed configuration details at the inheritance level.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 5.1.1	This command was introduced.

Usage Guidelines

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

Without the inheritance keyword, this command displays the failed configuration information in brief.

Task ID

Task ID	Operation
config-services	read

Example

This example shows how to run the **show configuration failed** command:

Note When there are two (or more) groups that have failed, the ordering of the failed groups is displayed in the same order as the apply-group statement.

```
RP/0/RSP0/CPU0:router (config) #  show config failed
!! SEMANTIC ERRORS: This configuration was rejected by
!! the system due to semantic errors. The individual
!! errors with each failed configuration command can be
!! found below.
apply-group GROUP-1 GROUP-2 GROUP-3 GROUP-4 GROUP-5
!% Please issue "show configuration failed inheritance" for details.
Applying following groups failed: GROUP-2 GROUP-4 GROUP-5
```

show configuration failed (config)

To display information about a configuration that failed during the last commit, use the **show configuration failed** command in any configuration mode.

show configuration failed [**load** | **noerrors**]

Syntax Description

load	(Optional) Displays any syntax errors found in a configuration loaded with the **load** command.
noerrors	(Optional) Displays the configuration that failed in last commit without the error reasons.

Command Default

Displays the details of the failed configuration including error reasons.

Command Modes

Any configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
basic-services	read

The following example shows a failed commit operation:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# taskgroup bgp
RP/0/RSP0/CPU0:router(config-tg)# description this is an example of an invalid task group
RP/0/RSP0/CPU0:router(config-tg)# commit
% Failed to commit one or more configuration items.
Please use 'show configuration failed' to view the errors
```

The following example shows sample output from the **show configuration failed** command. The output displays the configuration items that failed during the last commit operation.

```
RP/0/RSP0/CPU0:router(config-tg)# show configuration failed

!! CONFIGURATION FAILED DUE TO SEMANTIC ERRORS
taskgroup bgp
!!% Usergroup/Taskgroup names cannot be taskid names
!
```

The following example shows sample output from the **show configuration failed** command with the optional **no errors** keyword. The output displays the configuration items that failed during the last commit operation without an error description.

```
RP/0/RSP0/CPU0:router(config-tg)# show configuration failed noerrors

!! CONFIGURATION FAILED DUE TO SEMANTIC ERRORS
taskgroup bgp
!
```

Related Topics

show configuration (config), on page 167
show configuration history, on page 184
show configuration running, on page 196
show configuration sessions, on page 200
show running-config, on page 206
Show configuration commit changes, on page 171
show configuration commit list, on page 174
show configuration failed startup, on page 183
show configuration rollback changes, on page 194
show configuration running-config, on page 198

show configuration failed incompatible

To display any configurations that were removed from the running configuration because they were not understood by the software being activated, use the **show configuration failed incompatible** command in EXEC or administration EXEC mode.

show configuration failed incompatible

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Administration EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Any configurations in the running configuration that are not understood by new software being installed are removed from the running configuration. To see which configurations were removed, use the **show configuration failed incompatible** command.

Task ID

Task ID	Operations
config-services	read

Related Topics

show running-config, on page 206

show configuration failed remove

To display information about a configuration that failed while being removed during installation operations, use the **show configuration failed remove** command in EXEC or administration EXEC mode.

show configuration failed remove

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Administration EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
config-services	read

The following example shows a failed commit operation:

```
RP/0/RSP0/CPU0:router# show configuration failed remove

!! SEMANTIC ERRORS: This configuration was rejected by
!! the system due to semantic errors. The individual
!! errors with each failed configuration command can be
!! found below.

multicast-routing
 no address-family ipv4
 !!% Process did not respond to sysmgr
 address-family ipv4
  no interface all enable
!!% Process did not respond to sysmgr
!
!
```

Because the configuration failed to be removed, it is still displayed in the output from the **show running-configuration** command as expected:

```
RP/0/RSP0/CPU0:router# show running-configuration
...
router pim vrf default address-family ipv4
 auto-rp candidate-rp GigabitEthernet0/2/0/3 scope 255 group-list 224/4 interval 10
```

```
!
multicast-routing
 address-family ipv4
  interface all enable
!
!
```

Related Topics

show configuration (config), on page 167
show configuration failed (config), on page 177
show configuration history, on page 184
show configuration running, on page 196
show configuration sessions, on page 200
show running-config, on page 206
Show configuration commit changes, on page 171
show configuration commit list, on page 174
show configuration rollback changes, on page 194
show configuration running-config, on page 198

show configuration failed rollback

To display information about a configuration that failed in the last rollback operation, use the **show configuration failed rollback** command in EXEC or administration EXEC mode.

show configuration failed rollback

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Administration EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
config-services	read
root-lr	read

Related Topics

show configuration (config), on page 167
show configuration failed (config), on page 177
show configuration running, on page 196
show configuration sessions, on page 200
show running-config, on page 206
Show configuration commit changes, on page 171
show configuration commit list, on page 174
show configuration failed startup, on page 183
show configuration rollback changes, on page 194
show configuration running-config, on page 198

show configuration failed startup

To display information about a configuration that failed at startup, use the **show configuration failed** command inEXEC or administration EXEC mode.

show configuration failed startup [**noerror** | **previous** *number*]

Syntax Description

noerror	(Optional) Displays the configuration that failed at startup without an error reason.
previous *number*	(Optional) Displays the previous failed startup configuration or configurations. The *number* argument is a value from 1 to 4, which displays the failed startup configurations in previous of sessions.

Command Default

If no keywords are specified, this command displays the details of the failed startup configuration including error reasons.

Command Modes

EXEC

Administration EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
config-services	read

Related Topics

show configuration (config), on page 167
show configuration failed (config), on page 177
show configuration history, on page 184
show configuration running, on page 196
show configuration sessions, on page 200
show running-config, on page 206
Show configuration commit changes, on page 171
show configuration commit list, on page 174
show configuration rollback changes, on page 194
show configuration running-config, on page 198

show configuration history

To display a history of configuration events, use the **show configuration history** command in EXEC, administration EXEC, administration configuration, or global configuration mode.

show configuration history [**alarm** | **backup** | **cfs-check** | **commit** | **rebase** | **shutdown** | **startup**] [**first** *number* | **last** *number* | **reverse**] [**detail**]

Syntax Description

alarm	(Optional) Displays alarm events.
backup	(Optional) Displays configuration backup events.
cfs-check	(Optional) Displays CFS check events.
commit	(Optional) Displays commit events.
rebase	(Optional) Displays commit database consolidation events.
shutdown	(Optional) Displays shutdown events.
startup	(Optional) Displays startup events, including alternate configurations, failed configurations, and other events.
first *number*	(Optional) Displays the first x number of events, where x is the *number* argument.
last *number*	(Optional) Displays the last *x number* events. Replace with the number of events to display.
reverse	(Optional) Displays the most recent events first.
detail	(Optional) Displays detailed information, including comments.

Command Default

When entered without any optional arguments or keywords, this command displays all configuration events. The oldest events are displayed at the top of the list for each event type.

Command Modes

EXEC

Administration EXEC

Administration configuration

Global Configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **show configuration history** command to display information about the last (up to) 1500 configuration events.

Use one of the available keywords to display the configuration event only for that event type. Use the **first** *number* and **last** *number* keywords and arguments to display a specified number of events. Use the **reverse** keyword to display the newest events at the top of the list.

Task ID

Task ID	Operations
config-services	read

In the following example, the **show configuration history** command is used to display the history of all configuration events for an SDR:

```
RP/0/RSP0/CPU0:router# show configuration history

Sno.  Event      Info                          Time Stamp
~~~~  ~~~~~      ~~~~                          ~~~~~~~~~~
1     alarm      inconsistency alarm raised    Thu Jun 22 15:23:15 2009
2     startup    configuration applied         Thu Jun 22 15:23:32 2009
3     OIR config restore                       Thu Jun 22 15:23:25 2009
4     OIR config restore                       Thu Jun 22 15:23:33 2009
5     OIR config restore                       Thu Jun 22 15:23:33 2009
6     OIR config restore                       Thu Jun 22 15:23:34 2009
7     OIR config restore                       Thu Jun 22 15:23:34 2009
8     OIR config restore                       Thu Jun 22 15:23:35 2009
9     OIR config restore                       Thu Jun 22 15:23:36 2009
10    OIR config restore                       Thu Jun 22 15:23:37 2009
11    OIR config restore                       Thu Jun 22 15:23:37 2009
12    OIR config restore                       Thu Jun 22 15:23:38 2009
13    OIR config restore                       Thu Jun 22 15:23:38 2009
14    OIR config restore                       Thu Jun 22 15:23:39 2009
15    OIR config restore                       Thu Jun 22 15:23:39 2009
16    OIR config restore                       Thu Jun 22 15:23:40 2009
17    OIR config restore                       Thu Jun 22 15:23:40 2009
18    OIR config restore                       Thu Jun 22 15:23:42 2009
19    OIR config restore                       Thu Jun 22 15:23:42 2009
20    OIR config restore                       Thu Jun 22 15:23:42 2009
21    OIR config restore                       Thu Jun 22 15:23:43 2009
 --More--
```

In the following example, the **show configuration history** command is used to display only the startup configuration events:

```
RP/0/RSP0/CPU0:router# show configuration history startup

Sno.  Event      Info                          Time Stamp
~~~~  ~~~~~      ~~~~                          ~~~~~~~~~~
1     startup    configuration applied         Thu Jun 22 15:23:32 2009
2     startup    configuration applied         Sat Jul  1 15:02:24 2009
3     startup    configuration applied         Sat Jul  8 17:36:52 2009
4     startup    configuration applied         Sun Jul  9 13:40:27 2009
5     startup    configuration applied         Sat Jul 15 18:18:54 2009
```

In the following example, the **show configuration history** command with the **commit detail** keywords is used to display additional details regarding the commit events:

```
RP/0/RSP0/CPU0:router# show configuration history commit detail

1)  Event: commit         Time: Thu Jun 22 15:44:33 2009
```

```
     Commit ID: 1000000001 Label:
     User: lab        Line: vty0
     Client: CLI           Comment:

2)   Event: commit         Time: Thu Jun 22 16:58:18 2009
     Commit ID: 1000000002 Label:
     User: lab        Line: vty2
     Client: CLI           Comment:

3)   Event: commit         Time: Thu Jun 22 16:58:39 2009
     Commit ID: 1000000003 Label:
     User: lab        Line: vty2
     Client: CLI           Comment:

4)   Event: commit         Time: Sat Jul  1 15:29:31 2009
     Commit ID: 1000000001 Label:
     User: lab        Line: vty0
     Client: CLI           Comment:

5)   Event: commit         Time: Sat Jul  1 15:32:25 2009
     Commit ID: 1000000002 Label:
     User: lab        Line: vty0
  --More--
```

Table 11: show configuration history Field Descriptions

Field	Description
SNo.	Serial number of the entry.
Event	Type of configuration event.
Info	Summary of the configuration action.
Time Stamp	Time and date when the event was run.
Label/ID	If a label was assigned to a commit, the first 10 characters display; otherwise, the autogenerated commit ID displays.
User	User who issued the command.
Line	Line in which the user session was established. In some cases, this field may display "UNKNOWN" or "SYSTEM". These fields indicate that an internal action was made by the system.
Client	The management interface used to make the event.

Related Topics

show configuration (config), on page 167
show configuration failed (config), on page 177
show configuration history, on page 184
show configuration running, on page 196
show configuration sessions, on page 200
show running-config, on page 206

Show configuration commit changes, on page 171
show configuration commit list, on page 174
show configuration rollback changes, on page 194
show configuration running-config, on page 198

show configuration inconsistency replica

To display any configuration inconsistencies on a replica node, use the **show configuration inconsistency replica** command in EXEC or administration EXEC mode.

show configuration inconsistency replica location *node-id* [**detail**]

Syntax Description

location *node-id*	Displays any configuration inconsistencies on the designated node. The *node-id* argument is expressed in the *rack/slot/module* notation.
detail	Displays a detailed list of inconsistencies.

Command Default

Administration EXEC mode: Displays configuration inconsistencies for the admin plane configuration.

EXEC mode: Displays configuration inconsistencies for an SDR configuration.

Command Modes

EXEC

Administration EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

In administration EXEC or EXEC mode, the replica node for the **show configuration inconsistency replica** command is the standby designated system controller (DSC). .

Use the **show configuration inconsistency replica** command, before performing a manual switchover or DSC migration, to verify that the node in line to take over for the DSC is in good shape. If any problems are reported, use the **clear configuration inconsistency replica** command to correct them.

Task ID

Task ID	Operations
config-services	read

The following example shows a configuration with inconsistencies:

```
RP/0/RSP0/CPU0:router# show configuration inconsistency replica location 0/rsp1/cpu0

The replica at location 0/RSP1/CPU0 is inconsistent.
Please run 'clear configuration inconsistency replica location 0/RP1/CPU0'.
```

The following example shows sample output after the inconsistencies have been resolved:

```
RP/0/RSP0/CPU0:Router# show configuration inconsistency replica location 0/rsp1/cpu0

Replica is consistent
```

Related Topics

clear configuration inconsistency replica, on page 95

show configuration persistent

To display the persistent configuration, use the **show configuration persistent** command in EXEC mode.

show configuration persistent [**diff**]

Syntax Description

diff	(Optional) Displays the difference between the running configuration and persistent configuration. This option is available only on the DSC.

Command Default

If no argument is specified, the **show configuration persistent** command displays the entire contents of the persistent configuration file.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

The persistent configuration is the configuration stored in nonvolatile memory, from which the running configuration is restored after the router is reloaded. The running configuration should be the same as the persistent configuration. Use the **show configuration persistent** command with the **diff** keyword to check if there is a difference between the running configuration and the persistent configuration.

Task ID

Task ID	Operations
config-services	read

The following example shows that there is no difference between the running configuration and the persistent configuration:

```
RP/0/RSP0/CPU0:router# show configuration persistent diff

Building configuration...
  end
```

The following example shows a difference between the running configuration and the persistent configuration:

```
RP/0/RSP0/CPU0:router# show configuration persistent diff

Building configuration...
router vrrp
interface tengige0/1/0/1.1
vrrp 1 preempt delay 300
```

```
!
interface tengiget0/1/0/1.2
vrrp 1 preempt delay 300
!
interface tengige0/1/0/1.3
vrrp 1 preempt delay 300
```

Related Topics

show running-config, on page 206

show configuration removed

To display a configuration removed during installation operations, use the **show configuration removed** command in EXEC or administration EXEC mode.

show configuration removed *config-id*

Syntax Description

config-id	Name of removed configuration. Type (?) to see a list of the names of all removed configurations.

Command Default

None

Command Modes

EXEC

Administration EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
config-services	read

The following example shows a removed configuration:

```
RP/0/RSP0/CPU0:router# show configuration removed 20060301112919.cfg

xml agent corba
http server
end
```

Related Topics

show configuration (config), on page 167
show configuration failed (config), on page 177
show configuration history, on page 184
show configuration running, on page 196
show configuration sessions, on page 200
show running-config, on page 206
commit, on page 99
load, on page 123
Show configuration commit changes, on page 171

show configuration commit list, on page 174
show configuration failed startup, on page 183
show configuration rollback changes, on page 194

show configuration rollback changes

To display changes that would be made by the **rollback configuration** command or to display the list of commit IDs, use the **show configuration rollback changes** command in EXEC, administration EXEC, administration configuration, or global configuration mode.

show configuration rollback changes {*commit-id* | **to** *commit-id* | **last** *number-of-commits*} [**diff**]

Syntax Description

commit-id	Name of configuration. When a specific *commit-id* is specified, only the changes that would occur if only the specified commit is rolled back are displayed.
to *commit-id*	Displays the changes that will occur to the running configuration if the system is rolled back to the configuration specified with the *commit-id* argument.
last *number-of-commits*	Displays the changes that will occur to the running configuration if the system is rolled back to the last number of commits specified with the *number-of-commits* argument.
diff	(Optional) Displays added lines, changed lines, and deleted lines.

Command Default

None

Command Modes

EXEC

Administration EXEC

Administration configuration

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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



Note The most recent 100 commits are retained by the system. As new commit IDs are added, the oldest commit IDs are discarded and are no longer available for rollback operations.

Use the *commit-id* argument without the **to** keyword to display the changes for a particular commit. This can be useful for troubleshooting actions of the **rollback configuration** command.

Task ID

Task ID	Operations
config-services	read

The following example shows sample output from the **show configuration rollback changes** command with the **to** *commit-id* keyword and argument. The output displays the configuration changes that would occur if the configuration were to be rolled back to the configuration commit specified for the argument.

```
RP/0/RSP0/CPU0:router# show configuration rollback changes to 1000000007

Building configuration...
hostname old-name
end
```

The following example shows sample output from the **show configuration rollback changes** command **last** *number-of-commits* keyword and argument. The output displays the configuration changes that would occur if the configuration were to be rolled back to the number of configuration commits specified for the argument.

```
RP/0/RSP0/CPU0:router# show configuration rollback changes last 2

Building configuration...
hostname orig_name
interface POS0/1/0/1
 shutdown
!
end
```

The following example shows sample output from the **show configuration rollback changes** command with the **diff** keyword.

In the display, the following symbols signify changes:

- + indicates an added line.
- – indicates a deleted line.
- # indicates a modified line.

```
RP/0/RSP0/CPU0:router
show configuration rollback changes last 1 diff

Building configuration...
 interface Loopback1000
#  ipv4 address 1.1.1.1 255.255.255.255
!
end
```

Related Topics

load rollback changes, on page 128
rollback configuration, on page 137

show configuration running

To display the running configuration, use the **show configuration running** command in the appropriate mode.

show configuration running [*config-keyword*]

Syntax Description

config-keyword	(Optional) Specific configuration to display.

Command Default

None

Command Modes

Administration EXEC

Administration configuration

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **show configuration running** command to display the currently active configuration.

Task ID

Task ID	Operations
basic-services	read

This example shows the currently running (committed) configuration from administration mode.

```
RP/0/RSP0/CPU0:router(admin)# show configuration running

Building configuration...
username lab
 secret 5 $1$XNWt$j8RscNdncKSRoMSnqSpbj/
 group root-system
!
end
```

Related Topics

show configuration (config), on page 167
show configuration failed (config), on page 177
show configuration history, on page 184
show configuration sessions, on page 200
show running-config, on page 206
commit, on page 99

load, on page 123
Show configuration commit changes, on page 171
show configuration commit list, on page 174
show configuration failed startup, on page 183
show configuration rollback changes, on page 194
show configuration running-config, on page 198

show configuration running-config

To display the running configuration, use the **show configuration running-config** command in EXEC mode.

show configuration running-config [*config-keyword*]

Syntax Description

config-keyword	(Optional) Specific configuration to display.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the *config-keyword* argument to display the running configuration for a specific keyword only.

Task ID

Task ID	Operations
basic-services	read

This example shows the currently running (committed) configuration:

```
RP/0/RSP0/CPU0:router# show configuration running-config

Building configuration...

  !! Last configuration change at 15:36:31 UTC Thu Nov 17 2009 by lab
  sessions  Users with active configuration sess
!n
hostname router
line consolestartup   Sh
 exec-timeout 0 0onfiguration
!
logging console debugging
  |         Ou
snmp-server community public RW
  <cr>
RP/0/0/
ipv4 source-routeadmin)#show confi
key chain IPSLA ?
 key 10
  key-string password 1
  ipv4 address 10.0.0.0 255.255.255.0
  encapsulation ppp
  keepalive disable
!
 interface POS0/7/0/0
```

```
 shutdown
!
interface POS0/7/0/1
  shutdown
!
interface POS0/7/0/2
 shutdown
!
interface POS0/7/0/3
 shutdown
!
 route ipv4 0.0.0.0/0 12.7.0.1
ipsla
  responder
 !
!
end
```

Related Topics

show configuration (config), on page 167
show configuration failed (config), on page 177
show configuration history, on page 184
show configuration running, on page 196
show configuration sessions, on page 200
show running-config, on page 206
commit, on page 99
load, on page 123
Show configuration commit changes, on page 171
show configuration commit list, on page 174
show configuration failed startup, on page 183
show configuration rollback changes, on page 194

show configuration sessions

To display the active configuration sessions, use the **show configuration sessions** command in EXEC or administration EXEC mode.

show configuration sessions [**detail**]

Syntax Description

detail	(Optional) Displays detailed information.

Command Default

None

Command Modes

EXEC

Administration EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **show configuration sessions** command to display the active configuration sessions. Use the **clear configuration sessions** command to clear a configuration session. The **show configuration sessions** command can be used with the **clear configuration sessions** command to verify that an active configuration session was cleared.

Task ID

Task ID	Operations
config-services	read

The following example shows sample output from the **show configuration sessions** command:

```
RP/0/RSP0/CPU0:router# show configuration sessions

Current Configuration Session  Line       User     Date                     Lock
00000050-001200bb-00000000     con0_5_CPU cisco    Fri Feb 16 17:23:47 2007
```

Table 12: show configuration sessions Field Descriptions

Field	Description
Session	System-generated configuration session ID number.
Line	Line in which the user session was established. In some cases, this field may display “UNKNOWN” or “SYSTEM.” These fields indicate that an internal commit was made by the system.
User	User who initiated the configuration session.

Field	Description
Date	Time and date the configuration session was started.
Lock	Locked running-configuration. An asterisk (*) displayed in this field means the session has been locked. Only one session can lock the running configuration at a time.

Related Topics

clear configuration sessions, on page 97

show default-afi-safi-vrf

To display the default address family identifier (AFI), subaddress family identifier (SAFI), and VPN routing and forwarding (VRF) instance for the current session, use the **show default-afi-safi-vrf** command in EXEC mode.

show default-afi-safi-vrf

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **show default-afi-safi-vrf** command to display the default AFI and SAFI settings for the current session. The AFI and SAFI settings are controlled by the following commands:

- set default-afi, on page 155
- set default-safi, on page 156
- set default-vrf, on page 157

Task ID

Task ID	Operations
basic-services	read

The following example shows sample output from the **show default-afi-safi-vrf** command:

```
RP/0/RSP0/CPU0:router# show default-afi-safi-vrf

%% Default AFI/SAFI/VRF for this session is:
     Address Family Identifier:       'ipv4'
     Sub-Address Family Identifier:   'unicast'
     Virtual Routing/Forwarding:      ''
```

Related Topics

set default-afi, on page 155
set default-safi, on page 156
set default-vrf, on page 157

show history

To display a history of commands executed in EXEC, administration EXEC, administration configuration, or global configuration mode use the **show history** command in one of the supported modes.

show history [**detail**]

Syntax Description

detail	(Optional) Displays detailed history information.

Command Default

None

Command Modes

EXEC

Administration EXEC

Administration configuration

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

The **show history** command displays a history of the command entered for the current command mode. For example, enter the **show history** command to display a history of commands entered in EXEC mode. Enter the **show history** command in global configuration mode to display a history of the commands entered in global configuration mode.

Task ID

Task ID	Operations
config-services	read
basic-services	read

In the following example, the **show history** command is run in EXEC mode to display a history of the command entered inEXEC mode:

```
RP/0/RSP0/CPU0:router# show history
configure
admin
show history
```

In the following example, the **show history** command is run in global configuration mode to display a history of the command entered in global configuration mode:

```
RP/0/RSP0/CPU0:router(config)# show history
interface pos 0/1/0/0
ipv4 address 10.0.0.0
root
end
describe line default autocommand config
line default autocommand configure
end
show history
```

snmp-server script

To map the script file with custom OID, use the **snmp-server script** command in

mode.

snmp-server script script-oid *oid-number* **script-filename** *file-name*

Syntax Description

script-oid*oid-number*	The OID number to be added as custom OID. The custom OID number has to be followed by root OID 1.3.6.1.4.1.9.9.999998.
script-filename*file-name*	The name of the script file to be mapped.

Command Default

None

Command Modes

Command History

Release	Modification
Release 7.5.3	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
snmp	read,write

Examples

This example shows how to map the script file with custom OID.

```
Router(config)#snmp-server script script-oid 1.3.6.1.4.1.9.9.999998.10 script-filename
show_lldp_string.py
```

show running-config

To display the contents of the currently running configuration or a subset of that configuration, use the **show running-config** command in the appropriate mode.

show running-config [[**exclude**] *command*] [**sanitized**]

Syntax Description

exclude	(Optional) Excludes a specific configuration from the display.
command	(Optional) Command for which to display the configuration.
sanitized	(Optional) Displays a sanitized configuration for safe distribution and analysis.

Command Default

The **show running-config** command without any arguments or keywords displays the entire contents of the running configuration file.

Command Modes

EXEC

Administration EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

You can display either the entire running configuration, or a subset of the running configuration. The subset may be all the commands within a specified command mode.



Note In Cisco IOS XR software, the running configuration is automatically used at system startup, reset, or power cycle. The running configuration is the committed configuration.

Sanitized Output

Use the **show running-config** command with the **sanitized** keyword to display the contents of the active running configuration without installation-specific parameters. Some configuration details, such as IP addresses, are replaced with different addresses. The sanitized configuration can be used to share a configuration without exposing the configuration details.

Command Modes

When the **show running-config** command is entered in administration configuration mode, the configuration for the administration plane is displayed, including the configured logical routers for the system. When the **show running-config** command is entered in any global configuration mode, or in EXEC mode, the configuration for the specific secure domain router (SDR) is displayed.

The **inheritance** and **no-annotations** keywords are not supported in administration EXEC or configuration modes.

Excluding Parts of the Display

Use the **exclude** keyword followed by a *command* argument to exclude a specific configuration from the display.

Task ID

Task ID	Operations
config-services	read

This example shows how to enter the **show running-config** command with the question mark (?) online help function to display the available subsets of the running configuration that can be entered to display a subset of the running configuration:

```
RP/0/RSP0/CPU0:router# show running-config ?

aaa                Authentication, Authorization and Accounting
alias              Create an alias for entity
aps                Configure SONET Automatic Protection Switching (APS)
arp                Global ARP configuration subcommands
as-path            BGP autonomous system path filter
as-path-set        Define an AS-path set
banner             Define a login banner
cdp                Enable CDP, or configure global CDP subcommands
cef                CEF configuration commands
cinetd             Global Cisco inetd configuration commands
class-map          Configure QoS Class-map command
clock              Configure time-of-day clock
community-list     Add a community list entry
community-set      Define a community set
controller         Controller configuration subcommands
dhcp               Dynamic Host Configuration Protocol
domain             Domain service related commands
exception          Coredump configuration commands
exclude            Exclude a feature or configuration item from display
explicit-path      Explicit-path config commands
extcommunity-set   Define an extended communitiy set
fault              Fault related commands
forward-protocol   Controls forwarding of physical and directed IP broadcasts
ftp                Global FTP configuration commands
--More--
```

In this example, the **show running-config** command is used to display the running configuration for Packet-over-SONET/SDH (POS) interface 0/2/0/1:

```
RP/0/RSP0/CPU0:router# show running-config interface pos 0/2/0/1

interface POS0/2/0/1
ipv4 address 10.0.0.0 255.0.0.0
```

This example shows sample output from the **show running-config** command with the **sanitized** keyword displays a sanitized version of the running configuration. The sanitized configuration can be used to share a configuration without exposing specific configuration details.

```
RP/0/RSP0/CPU0:router# show running-config sanitized


Building configuration...

!! Last configuration change at 05:26:50 UTC Thu Jan 19 2009 by <removed>
!
snmp-server traps fabric plane
snmp-server traps fabric bundle state
hostname <removed>
line console
exec-timeout 0 0
!
exception choice 1 compress off filepath <removed>
logging console debugging
telnet vrf <removed> ipv4 server max-servers no-limit
snmp-server ifindex persist
snmp-server host 10.0.0.1 traps version <removed> priv <removed> udp-port 2555
snmp-server view <removed> <removed> included
snmp-server community <removed> RO LROwner
snmp-server community <removed> RO LROwner
snmp-server group <removed> v3 priv read <removed> write <removed>
snmp-server traps snmp
snmp-server traps syslog
interface Loopback10
!
interface Loopback1000
!
 --More--
```

Related Topics

show configuration (config), on page 167
show configuration running-config, on page 198

service cli commit-optimized enable

To prevent the re-application of the commands which are already present in the running configuration of the router, use the **service cli commit-optimized enable** command in XR Config mode.

service cli commit-optimized enable

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.4.1	This command was introduced.

Usage Guidelines

None

Example

```
Router# configure
Router(config)# service cli commit-optimized enable
Router(config)# commit
```

template

To create a template name and enter template configuration mode, use the **template** command in global configuration mode. To remove a template definition, use the **no** form of this command.

template *name*
no template *name*

Syntax Description

name	Unique name for the template to be created.

Command Default

No templates are defined.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **template** command to enter template configuration mode. From template configuration mode, you can group a subset of configuration commands in a named template. Commonly used sets of configuration commands can be grouped into a named template. Defining a template is similar to creating a C macro function. A template provides modularity and ease of use during user configuration.

Use the **end-template** command to exit template configuration mode. After defining a template, use the **apply-template** command to apply the template. Use the **show running-config** command with the optional **template** keyword and *template-name* argument to display the contents of a template.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to enter template configuration mode to create a template. In this example, a template named “pre-pos” is defined for the preconfigured Packet-over-SONET/SDH (POS) interface 0/1/0/1. The **end-template** command is used to exit from template configuration mode.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# template pre-pos
RP/0/RSP0/CPU0:router(config-TPL)# interface preconfigure pos0/1/0/0
RP/0/RSP0/CPU0:router(config-if-pre)# ipv4 address 10.3.32.154 255.0.0.0
RP/0/RSP0/CPU0:router(config-if-pre)# end-template
RP/0/RSP0/CPU0:router(config)#
```

Note After configuring a template, you may want to display the contents of the configured template. To display a template configuration, use the **show running-config** command with the **template** *name* keyword and argument.

The following example shows sample output from the **show running-config** command with the **template** *name* keyword and argument. In this example, the output displays the contents of a template named "pre-pos."

```
RP/0/RSP0/CPU0:router# show running-config template pre-pos

template pre-pos
 interface preconfigure POS0/1/0/0
  ipv4 address 10.3.32.154 255.0.0.0
!
end-template
```

Related Topics

apply-template, on page 88
end-template, on page 112
show running-config, on page 206



File System Commands

- cd, on page 214
- cfs check, on page 215
- copy, on page 217
- delete, on page 223
- dir, on page 224
- mkdir, on page 226
- pwd, on page 227
- rmdir, on page 228
- show filesystem, on page 229
- show media, on page 231

cd

To change the current working directory, use **cd** command in EXEC mode or XR EXEC mode.

cd *filesystem* **:**

Syntax Description

filesystem **:**	(Optional) Location of the new working directory. Include the file system alias for the *filesystem* argument, followed by a colon and optionally, the name of a directory.

Command Default

The default file directory is **disk0:/usr**.

Command Modes

EXEC

XR EXEC

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The current working directory is the directory used when EXEC commands that have an optional argument are entered without that argument. Use **cd** command to define the working directory. For example, when the **dir** command is entered without specifying the *filesystem* argument, the files in the current working directory are displayed.

Use **cd** command without an argument to set the working directory back to the default directory, **disk0:/usr**.

The following example shows how to change the current working directory to the root directory on the hard disk. In this example, the **pwd** command confirms that the working directory has changed to the root directory on the hard disk.

```
RP/0/RSP0/CPU0:router# cd harddisk:
RP/0/RSP0/CPU0:router# pwd

harddisk:
```

The following example shows how to change the current working directory to the default file directory by specifying the **cd** command without a location. In this example, the **pwd** command confirms that the working directory has changed to the default file directory.

```
RP/0/RSP0/CPU0:router# cd
RP/0/RSP0/CPU0:router# pwd

disk0:/usr
```

cfs check

To clear any inconsistencies between running configuration and binary startup configuration maintained on the disk use **cfs check** command in EXEC mode.

cfs check

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

Use this command to clear any inconsistencies between running configuration and binary startup configuration maintained on the disk.

On executing this command the existing binary startup configuration maintained on the disk will be discarded and the entire binary startup configuration will be recreated from system's running configuration. This will clear any inconsistency between the two.

Note While this command runs, redundancy of the designated shelf controller (DSC) is disabled.

Note Executing this command will take a lock to the configuration database, which will prevent any commit operation until this operation completes.

Task ID

Task ID	Operations
root-lr	read, write

Examples

The following example shows how to perform a CFS check:

```
Router# cfs check

Creating any missing directories in Configuration File system...OK
Initializing Configuration Version Manager...OK
Syncing commit database with running configuration...OK
Re-initializing cache files...OK
Updating Commit Database.  Please wait...[OK]
```

Related Commands

Command	Description
show configuration history	Displays **cfs check** events executed successfully.
clear configuration inconsistency	Performs the same operation as **cfs check**, can be used interchangeably.

copy

To copy a file from a source (such as a network server) to a destination (such as a flash disk), use **copy** command in EXEC or Admin EXEC mode.

copy *source* {**location** *node-id* *destination* **location** {*node-id* | **all**} | **running-config**[**atomic**]}

Syntax Description

source	Filename including the directory path or network location of the file. The possible sources are: *directory-path* —Directory path of the file from which the file is copied. **access-list** { **ipv4**	**ipv6** }—Copies an access list (EXEC mode only). **bootflash:** —Copies from the bootflash: file system. **compactflash:** —Copies from the compactflash: file system. **compactflasha:** —Copies from the compactflasha: file system partition. **disk0:** —Copies from disk0: file system. **disk0a:** —Copies from disk0a: file system partition. **disk1:** —Copies from disk1: file system. **disk1a:** —Copies from disk1a: file system partition. **flash:** —Copies from the flash: file system. The **flash:** keyword is an alias for bootflash:. **ftp:** —Copies from an FTP network server. The syntax is **ftp:**[[[//*username* [:*password*]@] *location*]/*directory*]/*filename.* **harddisk:** —Copies from the hard disk drive file system (if present). **harddiska:** —Copies from the hard disk partition a. **harddiskb:** —Copies from the hard disk partition b. **nvram:** —Copies from the NVRAM file system. **prefix-list** {**ipv4**	**ipv6**}—Copies from a prefix list (EXEC mode only). **rcp:** —Copies from a remote copy protocol (rcp) network server. The syntax is **rcp:**[[[//*username@*]*location*]/*directory*]/*filename.* **running-config** —Copies from the current system configuration. **tftp:** —Copies from a TFTP network server. The syntax is **tftp:**[[//*location*]/*directory*]/*filename* **xml-schema** —Copies the XML schema files as a tar ball file (.tar.gz) [EXEC mode only]. **sftp:** —Copies from an SFTP network server. The syntax is **sftp:**[[[//*username* [:*password*]@] *location*]/*directory*]/*filename.* **scp:** —Copies from an SCP network server. The syntax is **scp:**[[[//*username* [:*password*]@] *location*]/*directory*]/*filename.*
destination	Filename including the directory path or network location of the file.

location *node-id*	Specifies a node. The *node-id* argument is expressed in the *rack/slot/module* notation.
location all	Copies to all nodes.
running-config	Applies the source configuration file to the running configuration of the system.
atomic	(Optional) Applies the changes to the running configuration only if there are no errors

Command Default

No default behavior or values

Command Modes

EXEC mode.

Admin EXEC mode.

Command History

Release	Modification
Release 7.10.1	This command was modified to support public key authentication.
Release 7.9.1	This command was modified to support SFTP and SCP options.
Release 7.0.12	This command was introduced.

Usage Guidelines

Source and destination can each be a configuration file, a text file, or a file system. Enter source and destination URL information, usernames, and passwords and issue the **copy** command. The networking device prompts for any missing information.

The exact format of the *source* and *destination* arguments vary according to the file or directory location. Enter the device or network location for the file system type.

Filenames can include the following characters:

! # $ % & ' + 0 1 2 3 4 5 6 7 8 9 ; @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ ] ^ _ a b c d e f g h i j k l m n o p q r s t u v w x y z { } ~

The following characters can be used with the stated limitations:

- ` needs backslash before this character
- – cannot be the first character
- . cannot be the last character
- = cannot be the filename without other characters

The following characters cannot be used in filenames:

" ( ) * , / : < > ? \ |

The maximum length allowed for a filename is 254 characters including the path. If a filename longer than 254 characters is specified, the filename is truncated to 254 characters.

To copy a file from a source on the router to a destination on the router, specify a source **location** *node-id* and a destination **location** *node-id* . To copy the file to all nodes, use the **location all** keywords.

In the alias syntax for the **ftp:** , **rcp:** , **tftp:** , **sftp:** , and **scp:** keywords, the location is either an IP address or a hostname. The filename is specified relative to the directory used for file transfers.

When no alias is specified, the networking device looks for a file in the current directory. To view the current directory, enter the **pwd** command.

Note During processing of the **copy** command, you might see the "C" character. For all files being copied, "C" indicates that the copy process is taking place. The entire copying process might take several minutes and differs from protocol to protocol and from network to network.

Table 13: Network Protocols Supported by Cisco IOS XR Software

Prefix	Name	Description
tftp:	Trivial File Transfer Protocol	*TFTP* is a simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).
ftp:	File Transfer Protocol	*FTP* is an application protocol, part of the TCP/IP protocol stack, and is used for transferring files between network nodes. FTP requires a username and password.
rcp:	Remote Copy Protocol	The rcp protocol allows users to copy files to and from a file system residing on a remote host or server on the network. The rcp protocol uses TCP to ensure the reliable delivery of data. The rcp protocol downloads require a username.
sftp:	Secure File Transfer Protocol	*SFTP* is an application protocol is used for secure transferring files between the router and and an archieve server. SFTP requires a username and password.
scp:	Secure Copy Protocol	*SCP* is an application protocol is used for secure transferring files between the router and and an archieve server. SFTP requires a username and password.

Additional usage guidelines are in the following sections.

Invalid Combinations of Source and Destination

Some combinations of source and destination are invalid. Specifically, you cannot copy the following:

- From a running configuration to a running configuration
- From a network device to a network device (for example, **copy ftp: rcp:**)

Using TFTP

TFTP is a simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).

The syntax is as follows:

copy tftp://*hostname* /*ipaddress*/*directory-path pie name target-device* [**location** {*node-id* | **all**}]

Example:

```
RP/0/RSP0/CPU0:router# copy tftp://1.1.1.1/images/software.pie disk1:
```



Note Some Cisco IOS XR images may be larger than 32 MB, and the TFTP services provided by some vendors may not support a file this large. If you do not have access to a TFTP server that supports files larger than 32 MB, download the software image using FTP or rcp as described in the following sections.

Using FTP

FTP servers require a username and password for each client request. Cisco IOS XR software sends the first valid username in the following list:

1. The username and password specified in the **copy** command, if a username is specified.

   The syntax is as follows:

   copy ftp:// *username* **:** *password* **@** *hostname or ipaddress*/*directory-path*/*pie-name target-device* [**location** {*node-id* | **all**}]

   Example:

   ```
   RP/0/RSP0/CPU0:router# copy ftp://john:secret@10.1.1.1/images/software.pie disk1:
   ```

2. An "anonymous" username and password. The anonymous password is "root@ip address," where "ip address" is the IP address of the local networking device.
3. A password "username@iosname.domain" formed by the networking device. The variable "username" is the username associated with the current session, "iosname" is the configured hostname, and "domain" is the domain of the networking device.

The username and password must be associated with an account on the FTP server. If you are writing to the network server, the FTP server must be properly configured to accept the FTP write request from the user on the networking device.

If the network server has a directory structure, the configuration file or image is written to or copied from the directory associated with the username on the network server. For example, if the system image resides in the home directory of a user on the network server, specify the name of that user as the remote username.

Refer to the documentation for your FTP server for more details.

Using rcp

The rcp protocol requires a username upon each request. When you copy a configuration file or image between the networking device and an rcp server, the Cisco IOS XR software sends the first valid username in the following list:

1. The remote username specified in the **copy** command, if one is specified.
2. The username set by the **rcp client username** command, if the command is configured.
3. The networking device hostname.

For the rcp copy request to process successfully, an account must be defined on the network server for the remote username. If the network administrator of the destination server did not establish an account for the remote username, this command does not run successfully. If the network server has a directory structure, the

configuration file or image is written to or copied from the directory associated with the remote username on the network server. For example, if the system image resides in the home directory of a user on the network server, specify the name of that user as the remote username.

If you are writing to the network server, the rcp server must be properly configured to accept the rcp write request from the user on the networking device. For UNIX systems, add an entry to the .rhosts file for the remote user on the rcp server. Suppose the networking device contains the following configuration lines:

```
hostname Rtr1
ip rcp remote-username User0
```

If the IP address of the networking device translates to company.com, then the .rhosts file for User0 on the rcp server should contain the following line:

```
company.com Rtr1
```

See the documentation for your rcp server for more details.

If you are using a personal computer as a file server, the computer must support remote shell (rsh) protocol.

Using xml-schema

Use the **xml-schema** keyword to obtain the most up-to-date XML schemas (.xsd files) from the router. Using this keyword is useful to prevent the use of outdated schemas in the event that router software updates include schema updates. The tar ball file includes all active schema files. It does not include schemas that are activated by specific package installation envelopes (PIEs) if those PIEs are not installed and activated on the router.

Copying to the Running Configuration

When you use the **copy** command to copy a configuration file to the **running-config** destination, the configuration in the file is applied to the running configuration of the system. This is a configuration operation. By default, the copy is carried out in a best-effort manner. This means that if some configuration lines from the file cannot be applied, the remaining configuration is still integrated into the system. In this case, a partial configuration is committed. When the **atomic** keyword is used, partial configurations are not committed. This means that even if one error occurs in the parsing or committing phase, no changes are made to the system. To view any errors when applying the configuration, use the **show configuration failed** command.

Task ID

Task ID	Operations
filesystem	execute

The following example shows how to copy a file from a FTP server to disk1:

```
RP/0/RSP0/CPU0:router#
copy ftp://john:secret@10.1.1.1/images/comp-asr9k-full.pie disk1:
```

The following example shows how to copy a file from an rcp server to disk1:

```
RP/0/RSP0/CPU0:router#
```

```
copy rcp://john@10.1.1.1/images/comp-asr9k-full.pie disk1:
```

The following example shows how to copy a file from a TFTP server to disk1:

```
RP/0/RSP0/CPU0:router#
copy tftp://10.1.1.1/images/comp-asr9k-full.pie disk1:
```

The following example shows how to copy a file from a SCP and SFTP server using public key authentication:

```
Router#copy running-config scp://root@192.0.4.2//var/opt/run_conf_scp.txt
Router#copy running-config sftp://root@192.0.4.2//var/opt/run_conf_sftp.txt
```

delete

To delete files, use **delete** command in the appropriate mode.

delete [/**noprompt**] [/**ena**] *filesystem*: *filename* **location** {*node-id* | **all**}

Syntax Description

/noprompt	(Optional) Causes no prompt for confirmation before deleting the specified files.
/ena	(Optional) Deletes all files from and below the current working directory.
filesystem **:**	(Optional) Location of the file to be deleted. Include the file system alias for the *filesystem* argument, followed by a colon, and, optionally, the name of a directory.
filename	Filename of the file to be deleted.
harddisk	Deletes the harddisk
location {*node-id* | **all**}	Deletes a file from a designated node. The *node-id* argument is entered in the *rack*/*slot*/*module* notation. The **all** keyword specifies to delete the file from all nodes.

Command Default

A filename must be specified. If a filename is entered without a file system or directory path, the present working directory is used.

Command Modes

EXEC mode.

Admin EXEC mode.

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

When a file is deleted, it is removed from the system and cannot be restored (undeleted).

Use the **dir** command to display the list of files on a storage device.

The following example shows how to delete a file:

```
RP/0/RSP0/CPU0:router# delete rbtest

Delete disk1:/rbtest[confirm]y
```

dir

To display a list of files on a file system or in a specific directory, use the **dir** command in the appropriate mode.

dir [/**all** | /**ena** | /**recurse**] [*filesystem***:**] [*filename*] **location** {*node-id* | **all**}

Syntax Description

/all	(Optional) Lists deleted files, undeleted files, and files with errors.
/ena	(Optional) Recognizes subdirectories.
/recurse	(Optional) Recursively lists subdirectories.
filesystem **:**	(Optional) Name of the directory containing the files to be displayed. Include the file system alias for the *filesystem* argument, followed by a colon, and, optionally, the name of a directory.
filename	(Optional) Name of the files to display. The files can be of any type. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings following a wildcard are ignored.
location {*node-id* | **all**}	(Optional) Specifies the node from which to display a list of files. The *node-id* argument is entered in the *rack*/*slot*/*module* notation. The **all** keyword specifies to display files on all nodes.

Command Default

When **dir** command is entered without keywords or arguments, the contents of the present working directory are displayed.

Command Modes

EXEC mode.

Admin EXEC mode.

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

If you enter the **dir** command without specifying a directory, the contents of the present working directory are displayed. The **all** keyword displays all files, including deleted files. The size associated with the directory name is the total size for all files in that directory.

The following example shows how to display the contents of a directory:

```
RP/0/RSP0/CPU0:router# dir harddisk:/log

Directory of harddisk:/log

5527        drwx  4096        Thu Aug 28 11:21:48 2008  boot_28_Aug_2008_11_21_49
5533        drwx  4096        Thu Aug 28 11:38:54 2008  boot_28_Aug_2008_11_38_54
5538        drwx  4096        Fri Sep  5 13:28:54 2008  boot_05_Sep_2008_13_28_54
5543        drwx  4096        Mon Sep  8 08:55:52 2008  boot_08_Sep_2008_06_59_08
```

```
--More--
```

mkdir

To create a new directory on a file system, use the **mkdir** command in the appropriate mode.

mkdir *filesystem*:[**location** {*node-id* | **all**}]

Syntax Description

filesystem:	File system on which to create a new directory.
location {*node-id* | **all**}	(Optional) Specifies the node where the file system is located. The *node-id* argument is expressed in the *rack/slot/module* notation. Use the **all** keyword to indicate all nodes.

Command Default

No default behavior or values

Command Modes

EXEC

Admin EXEC.

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

After you issue the **mkdir** command, Cisco IOS XR software prompts you to specify the name of the directory to be created. When specifying the name of the new directory, include the directory path where you want the new directory to reside. If you do not specify a directory path, the new directory is created in the /usr directory of the file system specified for the *filesystem:* argument.

The following example shows how to create a directory named newdir. The **dir** command is used to verify that the directory has been added.

```
RP/0/RSP0/CPU0:router# mkdir harddisk:

Create directory filename []?newdir
Created dir harddisk:/newdir
RP/0/RP0/CPU0:router# dir harddisk:

  Directory of harddisk:

  11193       drwx  4096        Fri Feb 13 06:45:05 2009  newdir
  37146       drwx  4096        Sun Dec 14 15:30:48 2008  malloc_dump
  43030       drwx  4096        Wed Dec 24 11:20:52 2008  tracebacks
  43035       drwx  4096        Thu Jan  8 18:59:18 2009  sau
  51026       drwx  4096        Sat Dec 27 02:52:46 2008  tempA
  51027       drwx  4096        Sat Dec 27 02:04:10 2008  dir.not.del
  -430307552  -rwx  342         Fri Jan 16 10:47:38 2009  running-config
  -430305504  -rwx  39790       Mon Jan 26 23:45:56 2009  cf.dat

  39929724928 bytes total (39883231232 bytes free)
```

pwd

To display the present working directory, use the **pwd** command in EXEC mode

pwd

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

Use the **pwd** command to show what directory or file system is specified as the default by the **cd** command.

The following example shows how to display the present working directory:

```
RP/0/RSP0/CPU0:router# pwd
disk0:/usr
```

rmdir

To remove an existing directory, use the **rmdir** command in the appropriate mode.

rmdir *filesystem*: **location** {*node-id* | **all**}

Syntax Description

filesystem	Name of the file system from which to delete a directory, followed by a colon.
location {*node-id* | **all**}	Specifies the node where the file system is located. The *node-id* argument is expressed in the *rack/slot/module* notation. Use the **all** keyword to indicate all nodes.

Command Default

No default behavior or values

Command Modes

EXEC

Administration EXEC

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

Use the **rmdir** command to remove directories (for example, to free up disk space) from a file system. After you issue the **rmdir** command, the Cisco IOS XR software prompts you to specify the name of the directory to be deleted.

When a directory contains files, you must remove the files before deleting the directory. Use the **delete** command to remove files.

The following example shows how to delete a subdirectory from the hard disk. The **dir** command is used to verify that the directory has been deleted.

```
RP/0/RSP0/CPU0:router# rmdir harddisk:

Remove directory filename []?newdir
Delete harddisk:/newdir[confirm]y
RP/0/RSP0/CPU0:router# dir harddisk:

  Directory of harddisk:

  37146       drwx  4096        Sun Dec 14 15:30:48 2008  malloc_dump
  43030       drwx  4096        Wed Dec 24 11:20:52 2008  tracebacks
  43035       drwx  4096        Thu Jan  8 18:59:18 2009  sau
  51026       drwx  4096        Sat Dec 27 02:52:46 2008  tempA
  51027       drwx  4096        Sat Dec 27 02:04:10 2008  dir.not.del
  -430307552  -rwx  342         Fri Jan 16 10:47:38 2009  running-config
  -430305504  -rwx  39790       Mon Jan 26 23:45:56 2009  cf.dat

  39929724928 bytes total (39883235328 bytes free)
```

show filesystem

To display the layout and contents of file systems, use the **show filesystem** command in EXEC mode.

show filesystem *filesystem*:[**firmware** | **stats** | **verbose** *level*] [**location** {*node-id* | **all**}]

Syntax Description

filesystem:	Name of the file system for which to display information, followed by a colon. Possible values are: **disk0:**, **disk1:**, **harddisk:**.
firmware	(Optional) Displays the firmware level.
stats	(Optional) Displays device statistics.
verbose *level*	(Optional) Changes the device driver verbose level.
location {*node-id* | **all**}	(Optional) Specifies the node where the file system is located. The *node-id* argument is expressed in the *rack/slot/module* notation. Use the **all** keyword to indicate all nodes.

Command Default

The file system for the active RP is displayed.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

Use the **show filesystem** command to learn the alias names (prefixes) of the file systems supported by your networking device.

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

```
RP/0/RSP0/CPU0:router# show filesystem

File Systems:

      Size(b)     Free(b)      Type  Flags  Prefixes
            -           -   network     rw  qsm/dev/fs/tftp: tftp:
            -           -   network     rw  qsm/dev/fs/rcp: rcp:
            -           -   network     rw  qsm/dev/fs/ftp: ftp:
  39929724928 39852978176  harddisk     rw  harddisk:
   1024606208   863584256 flash-disk     rw  disk0:
      2092032     2059264      nvram     rw  nvram:
     62390272    62381260      flash     rw  bootflash:
```

The following example shows sample output from the **show filesystem** command using the optional **location** *node-id* keyword and argument:

```
RP/0/RSP0/CPU0:router# show filesystem location 0/rp0/cpu0

File Systems:
```

```
      Size(b)      Free(b)        Type  Flags  Prefixes
           -            -     network     rw  qsm/dev/fs/tftp: tftp:
           -            -     network     rw  qsm/dev/fs/rcp: rcp:
           -            -     network     rw  qsm/dev/fs/ftp: ftp:
 39929724928 39883235328    harddisk     rw  harddisk:
     2092032     2019328       nvram     rw  nvram:
  1024606208   847888384  flash-disk     rw  disk0:
    62390272    62153616       flash     rw  bootflash:
```

Table 14: show filesystem Field Descriptions

Field	Description
Size(b)	Amount of memory in the file system, in bytes.
Free(b)	Amount of free memory in the file system, in bytes.
Type	Type of file system.
Flags	Permissions for file system.
Prefixes	Alias for the file system.

show media

To display the current state of the disk storage media, use the **show media** command in EXEC or Administration EXEC mode.

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

Syntax Description

location {*node-id* | **all**}	(Optional) Specifies the node where the file system is located. The *node-id* argument is expressed in the *rack/slot/module* notation. Use the **all** keyword to indicate all nodes.

Command Default

The disk storage media for the active RP is displayed.

Command Modes

Administration EXEC

EXEC

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

Use the **show media** command to view the status of the storage media on your system.

The following example displays the output of the **show media** command:.

```
sysadmin-vm:0_RP0 #show media
Thu Nov 30 14:57:14.002 WET
Media Information for local node.
-----------------------------------------------
Partition                    Size     Used  Percent    Avail
rootfs:                      2.7G     1.5G      59%     1.1G
apphost:                     1.9G      61M       4%     1.7G
/dev/sde                     870M     401M      50%     409M
harddisk:                    2.4G     966M      43%     1.3G
log:                         459M      67M      16%     359M
config:                      159M     2.5M       2%     144M
disk0:                       1.3G     108M       9%     1.1G
-------------------------------------------------
rootfs: = root file system (read-only)
log: = system log files (read-only)
config: = configuration storage (read-only)
```

Table 15: show media Field Descriptions

Field	Description
Partition	Partition on the disk.
Size	Size of the partition.
Used	Partition size used.
Percent	Percentage used.

Field	Description
Avail	Available free partition space.



Manageability Commands

- ipv4 disable, on page 234
- ipv6 enable (XML), on page 235
- iteration, on page 236
- nvgen default-sanitize, on page 238
- session timeout, on page 239
- show xml schema, on page 241
- show xml sessions, on page 242
- shutdown (VRF), on page 244
- streaming, on page 246
- throttle, on page 247
- vrf (XML), on page 248
- xml agent, on page 249
- xml agent ssl, on page 250
- xml agent tty, on page 251

ipv4 disable

To disable IPv4 XML transport, use the **ipv4 disable** command in XML agent configuration mode. To enable IPv4 XML transport, use the **no** form of this command.

ipv4 disable
no ipv4 disable

Syntax Description

This command has no keywords or arguments.

Command Default

IPv4 XML transport is enabled by default.

Command Modes

XML agent configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
config-services	read, write

This example illustrates how to disable IPv4 XML transport:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# xml agent
RP/0/RSP0/CPU0:router(config-xml-agent) ipv4 disable
```

ipv6 enable (XML)

To enable IPv6 XML transport, use the **ipv6 enable** command in XML agent configuration mode. To disable IPv6 XML transport, use the **no** form of this command.

ipv6 enable
no ipv6 enable

Syntax Description

This command has no keywords or arguments.

Command Default

IPv6 XML transport is disabled by default.

Command Modes

XML agent configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.
Release 5.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
config-services	read, write

This example illustrates how to enable IPv6 XML transport:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# xml agent
RP/0/RSP0/CPU0:router(config-xml-agent) ipv6 enable
```

iteration

To configure the iteration size for large XML agent responses, use the iteration command in xml agent configuration mode. To revert to the default iteration settings, use the **no** form of this command.

iteration {**off** | **on** **size** *iteration-size*}
no **iteration**

Syntax Description

off	Disables iteration, meaning that the entire XML response is returned, regardless of its size. Use of this option is not recommended.
on	Enables iteration, meaning that large XML responses are broken into chunks according to the iteration chunk size.
size *iteration-size*	Specifies the size of the iteration chunk, in Kbytes. Values can range from 1 to 100,000.

Command Default

Iteration is enabled; the *iteration-size* is 48.

Command Modes

XML agent

TTY XML agent

SSL XML agent

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

When the XML agent returns a large response, it splits the response into chunks and returns one chunk at a time. External clients then need to send a GetNext request to obtain the next chunk. Use the **iteration** command to control the size of iteration chunks. A larger chunk value allows larger chunks to be received in a shorter period of time, possibly making the router system busier. A smaller chunk value allows smaller chunks to be received over a longer period of time, but does not make the router busy You can also specify to disable iteration completely using the **iteration off** command.



Note It is not recommended to disable iteration, since this could result in large transient memory usage.

To specify the TTY or SSL iteration size specifically, use the **iteration** command from the appropriate command mode.

Task ID

Task ID	Operations
config-services	read, write

Example

The following example shows how to configure the iteration chunk size to 100 Kbytes.

```
RP/0/RSP0/CPU0:router(config)# xml agent
RP/0/RSP0/CPU0:router(config-xml)# iteration on size 100
```

The following example shows how to disable iteration:

```
RP/0/RSP0/CPU0:router(config)# xml agent
RP/0/RSP0/CPU0:router(config-xml)# iteration off
```

The following example shows how to turn on iteration with the default iteration size:

```
RP/0/RSP0/CPU0:router(config)# xml agent
RP/0/RSP0/CPU0:router(config-xml)# no iteration off
```

The following example shows how to change the iteration size to the default iteration size.

```
RP/0/RSP0/CPU0:router(config)# xml agent
RP/0/RSP0/CPU0:router(config-xml)# no iteration on size 100
```

The following example shows how to change the iteration size of the TTY agent to 3 Kbytes:

```
RP/0/RSP0/CPU0:router(config)# xml agent tty
RP/0/RSP0/CPU0:router(config-xml-tty)# iteration on size 3
```

The following example shows how to turn off the iteration of the SSL agent:

```
RP/0/RSP0/CPU0:router(config)# xml agent ssl
RP/0/RSP0/CPU0:router(config-xml-ssl)# iteration off
```

nvgen default-sanitize

To enable sanitizing Strings, Usernames, Passwords, Comments, or IP Addresses in the output for **show running configurations** command, use the **nvgen default-sanitize** command.

nvgen default-sanitize { **strings** | **usernames** | **passwords** | **comments** | **ipaddrs** }

Syntax Description

strings	Removes the description strings in the running configuration and replaces it with **<removed>** phrase.
usernames	Removes the usernames in the running configuration and replaces it with **<removed>** phrase.
password	Removes the passwords in the running configuration and replaces it with **<removed>** phrase.
comments	Removes the comments in the running configuration and replaces it with **<comments removed>** phrase.
ipaddrs	Removes the IP addresses in the running configuration and replaces it with **<removed>** phrase.

Command Default

The output for **show running configurations** command includes sensitive information such as Strings, Usernames, Passwords, Comments, or IP Addresses.

Command Modes

Configuration mode

Command History

Release	Modification
Release 7.5.4	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to sanitize show running configurations:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# nvgen default-sanitize strings
RP/0/RSP0/CPU0:router(config)# nvgen default-sanitize usernames
RP/0/RSP0/CPU0:router(config)# nvgen default-sanitize passwords
RP/0/RSP0/CPU0:router(config)# nvgen default-sanitize comments
RP/0/RSP0/CPU0:router(config)# nvgen default-sanitize ipaddrs
RP/0/RSP0/CPU0:router(config)# commit
```

session timeout

To configure an idle timeout for the XML agent, use the **session timeout** command in xml agent configuration mode. To remove the session timeout, use the **no** form of this command.

session timeout *timeout*

Syntax Description

timeout	Amount of idle time in minutes that must pass before the XML agent closes the session. Values can range from 1 to 1440.

Command Default

There is no session timeout.

Command Modes

xml agent

xml agent ssl

xml agent tty

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
config-services	read, write

The following example illustrates how to configure the dedicated agent to close the session after 5 minutes of idle time:

```
RP/0/RSP0/CPU0:router(config)# xml agent
RP/0/RSP0/CPU0:router(config-xml-agent)# session timeout 5
```

The following example illustrates how to configure the XML TTY agent to close the session after 60 minutes of idle time:

```
RP/0/RSP0/CPU0:router(config)# xml agent tty
RP/0/RSP0/CPU0:router(config-xml-agent-tty)# session timeout 60
```

The following example illustrates how to configure the XML TTY agent to have no timeout (the default):

```
RP/0/RSP0/CPU0:router(config)# xml agent tty
```

```
RP/0/RSP0/CPU0:router(config-xml-agent)# no session timeout
```

show xml schema

To browse the XML schema and data, use the **show xml schema** command in

EXEC

mode.

show xml schema

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

The **show xml schema** command runs the XML schema browser so that you can browse the XML schema and data.

Task ID

Task ID	Operations
config-services	read

This example shows how to enter the XML schema browser and the available commands:

```
RP/0/RSP0/CPU0:router# show xml schema

Username: xxxx
Password:
Enter 'help' or '?' for help
xml-schema[config]:> ?

config            oper              action
adminoper         adminaction       cd
pwd               classinfo         list
ls                datalist          walk
walkdata          get               hierarchy
quit              exit              help
xml-schema[config]:>
```

show xml sessions

To display the status of an Extensible Markup Language (XML) session, use the **show xml sessions** command in

EXEC

mode.

show xml sessions [**default** | **ssl** | **tty**] [**detail**]

Syntax Description

default	Displays the status of the default XML agent.
ssl	Displays the status of the XML agents over secure socket layer (SSL).
tty	Displays the status of XML agents over telnet.
detail	Displays details regarding the XML sessions.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
config-services	read

Example

This example illustrates sample output of the **show xml sessions** command with no optional keywords specified:

```
RP/0/RSP0/CPU0:router# show xml sessions

Session  Client                 Agent    User  Date                     State
00000001 192.168.10.85 (default) tty      cisco Fri Jun 19 22:42:29 2009 idle
10000001 10.12.24.15 (VRF1)      default  lab   Fri Jun 19 22:32:12 2009 busy
```

This example illustrates sample output of the **show xml sessions** command with the **tty** keyword:

```
RP/0/RSP0/CPU0:router# show xml sessions tty
```

```
Session  Client                  Agent User  Date                      State
00000001 192.168.10.85 (default) tty   cisco Fri Jun 19 22:42:29 2009 idle
00000002 10.12.24.15 (VRF1)      tty   lab   Fri Jun 19 22:32:12 2009 busy
```

This example illustrates sample output of the **show xml sessions** command with the **detail** keyword:

```
RP/0/RSP0/CPU0:router#
show xml sessions detail


Session: 00000001
  Client:                 192.168.10.85 (default)
  Agent type:             tty
  User:                   cisco
  State:                  idle
  Config session:         -
  Alarm notification:     Registered
  Start Date:             Tue Aug 24 18:21:29 2010
  Elapsed Time:           00:00:27
  Last State Changed:     00:00:27
Session: 10000001
  Client:                 10.12.24.15 (VRF1)
  Agent type:             default
  User:                   lab
  State:                  busy
  Config session:         00000010-0005b105-00000000
  Alarm notification:     Not registered
  Start date:             Tue Aug 24 18:21:29 2010
  Elapsed Time:           00:01:10
  Last State Changed:     00:01:10
```

shutdown (VRF)

To configure the dedicated XML agent to not receive or send messages via the default VRF, use the **shutdown** command in xml agent vrf configuration mode. To enable the dedicated XML agent to receive or send messages via the default VRF, use the **no** form of this command.

shutdown
no shutdown

This command has no keywords or arguments.

Command Default

The default VRF instance is enabled by default.

Command Modes

xml agent vrf configuration

xml agent ssl vrf configuration

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
config-services	read, write

Example

The following example illustrates how to configure the XML dedicated agent to send and receive messages via VRF1 only:

```
RP/0/RSP0/CPU0:router(config)# xml agent
RP/0/RSP0/CPU0:router(config-xml-agent)# vrf VRF1
RP/0/RSP0/CPU0:router(config-xml-agent)# vrf default
RP/0/RSP0/CPU0:router(config-xml-agent-vrf)# shutdown
```

The following example illustrates how to configure the XML SSL agent to send and receive messages via VRF1 only:

```
RP/0/RSP0/CPU0:router(config)# xml agent ssl
RP/0/RSP0/CPU0:router(config-xml-agent-ssl)# vrf VRF1
RP/0/RSP0/CPU0:router(config-xml-agent-ssl)# vrf default
RP/0/RSP0/CPU0:router(config-xml-agent-ssl-vrf)# shutdown
```

The following example illustrates how to enable the default VRF after it has been disabled:

```
RP/0/RSP0/CPU0:router(config)# xml agent
RP/0/RSP0/CPU0:router(config-xml-agent)# vrf default
RP/0/RSP0/CPU0:router(config-xml-agent-vrf)# no shutdown
```

streaming

To configure XML response streaming, use the **streaming** command in one of the XML agent configuration modes. To disable XML response streaming, use the **no** form of this command.

streaming on size *size*

Syntax Description

on	Turns on XML streaming.
size *size*	Specifies the size of the stream in Kbytes.

Command Default

XML streaming is disabled.

Command Modes

XML agent

XML agent ssl

XML agent tty

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
config-services	read, write

This example illustrates how to set the XML response streaming size to 5000 Kbytes.

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# xml agent
RP/0/RSP0/CPU0:router(config-xml-agent)# streaming on size 5000
```

throttle

To configure the XML agent processing capabilities, use the **throttle** command in XML agent configuration mode.

throttle {**memory** *size* | **process-rate** *tags*}

Syntax Description

memory	Specifies the XML agent memory size.
size	Maximum memory usage of XML agent per session in MB. Values can range from 100 to 600. The default is 300.
process-rate	Specifies the XML agent processing rate.
tags	Number of tags that the XML agent can process per second. Values can range from 1000 to 30000.

Command Default

The process rate is not throttled; memory size is 300 MB.

Command Modes

XML agent configuration

Command History

Release	Modification
Release 3.8.2	This command was introduced.

Usage Guidelines

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

Use the **throttle** command to control CPU time used by the XML agent when it handles large data.

Task ID

Task ID	Operation
config-services	read, write

Example

This example illustrates how to configure the number of tags that the XML agent can process to 1000:

```
RP/0/RSP0/CPU0:router(config)# xml agent
RP/0/RSP0/CPU0:router(config-xml-agent)# throttle process-rate 1000
```

vrf (XML)

To configure a dedicated agent to receive and send messages via the specified VPN routing and forwarding (VRF) instance, use the vrf command in one of the xml agent configuration mode. To disable the receiving and sending of messages via a specific VRF instance, use the **no** form of this command.

vrf {**default***vrf-name*}

Syntax Description

default	Configures the default VRF instance.
vrf-name	Configures the specified VRF instance.

Command Default

The default VRF is enabled by default.

Command Modes

XML agent configuration

XML agent SSL configuration

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

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

The default VRF is enabled by default. To disable the default VRF, use the **shutdown** command.

Task ID

Task ID	Operation
config-services	read, write

Example

This example shows how to configure the dedicated XML agent to receive and send messages via VRF1, VRF2 and the default VRF:

```
RP/0/RSP0/CPU0:router(config)# xml agent
RP/0/RSP0/CPU0:router(config-xml-agent)# vrf VRF1
RP/0/RSP0/CPU0:router(config-xml-agent)# vrf VRF2
```

This example shows how to remove access to VRF2 from the dedicated agent:

```
RP/0/RSP0/CPU0:router(config)# xml agent
RP/0/RSP0/CPU0:router(config-xml-agent)# no vrf VRF2
```

xml agent

To enable Extensible Markup Language (XML) requests over a dedicated TCP connection and enter XML agent configuration mode, use the **xml agent** command in

global configuration

mode. To disable XML requests over the dedicated TCP connection, use the **no** form of this command.



Note This command enables a new, enhanced-performance XML agent. The **xml agent tty** command enables the legacy XML agent and is supported for backward compatibility.

xml agent
no xml agent

Command Default

XML requests are disabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

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

There are two XML agents: a legacy XML agent and an enhanced-performance XML agent. We recommend that you use the enhanced-performance agent. The legacy agent is supported for backward compatibility. Use the **xml agent** command to enable the enhanced-performance XML agent. Use the **xml agent tty** command to enable the legacy XML agent.

Use the **no** form of the **xml agent** command to disable the enhanced-performance XML agent.

Task ID

Task ID	Operations
config-services	read, write

This example shows how to enable XML requests over a dedicated TCP connection:

```
RP/0/RSP0/CPU0:router(config)# xml agent
```

xml agent ssl

To enable Extensible Markup Language (XML) requests over Secure Socket Layer (SSL) and enter SSL XML agent configuration mode, use the **xml agent ssl** command in

global configuration

mode. To disable XML requests over SSL, use the **no** form of this command.

xml agent ssl
no xml agent ssl

Command Default

SSL agent is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

The k9sec package is required to use the SSL agent. The configuration is rejected during commit when the security software package is not active on the system. When the security software package is deactivated after configuring SSL agent, the following syslog message is displayed to report that the SSL agent is no longer available.

```
xml_dedicated_ssl_agent[420]:
%MGBL-XML_TTY-7-SSLINIT : K9sec pie is not active, XML service over
SSL is not available.
```

Task ID

Task ID	Operations
config-services	read, write

This example shows how to enable XML requests over SSL:

```
RP/0/RSP0/CPU0:router(config)# xml agent ssl
```

xml agent tty

To enable Extensible Markup Language (XML) requests over Secure Shell (SSH) and Telnet and enter TTY XML agent configuration mode, use the **xml agent tty** command in

global configuration

mode. To disable XML requests over SSH and Telnet, use the **no** form of this command.



Note This command enables a legacy XML agent that has been superceded by an enhanced performance XML agent and is supported only for backward compatibility. To enable the enhanced-performance XML agent, use the **xml agent** command.

xml agent tty
no xml agent tty

Command Default

XML requests over SSH and Telnet are disabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

There are two XML agents: a legacy XML agent and an enhanced-performance XML agent. We recommend that you use the enhanced-performance agent. The legacy agent is supported for backward compatibility. The **xml agent tty** command enables the legacy XML agent. Use the **xml agent** command to enable the enhanced-performance XML agent.

Use the **no** form of the **xml agent tty** command to disable the legacy XML agent.

Task ID

Task ID	Operations
config-services	read, write

This example shows how to enable XML requests over Secure Shell (SSH) and Telnet:

```
RP/0/RSP0/CPU0:router(config)# xml agent tty
```



Terminal Services Commands

- absolute-timeout, on page 255
- access-class, on page 256
- autocommand, on page 258
- banner exec, on page 261
- banner incoming, on page 263
- banner login, on page 265
- banner motd, on page 267
- banner prompt-timeout, on page 269
- clear line, on page 271
- clear line vty, on page 272
- cli interactive syntax check, on page 273
- cli whitespace completion, on page 274
- databits, on page 275
- disconnect, on page 277
- disconnect-character, on page 278
- escape-character, on page 279
- exec-timeout, on page 281
- flowcontrol hardware, on page 283
- lcd alarm-category, on page 284
- lcd message , on page 285
- lcd name, on page 286
- length, on page 287
- line, on page 288
- parity, on page 289
- resume, on page 290
- send, on page 292
- session-limit, on page 294
- session-timeout, on page 295
- show cli submode-exit, on page 296
- show diag lcd-interface, on page 297
- show line, on page 298
- show sessions, on page 301
- show terminal, on page 303

- show users, on page 305
- stopbits, on page 307
- terminal cli submode-exit, on page 309
- terminal exec prompt, on page 310
- terminal exec utility pager, on page 312
- terminal length, on page 313
- terminal width, on page 315
- timestamp disable, on page 316
- transport input, on page 317
- transport output, on page 319
- transport preferred, on page 321
- vty-pool, on page 323
- width (display), on page 325

absolute-timeout

To set the absolute timeout for line disconnection, use the **absolute-timeout** command in line template configuration mode. To remove the **absolute-timeout** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

absolute-timeout *minutes*
no absolute-timeout *minutes*

Syntax Description

minutes	Absolute timeout interval, in minutes. Range is from 10 to 10000.

Command Default

minutes: 1440

Command Modes

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 5.0.0	This command was introduced.

Usage Guidelines

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

Use the **absolute-timeout** command to terminate the connection after the specified time has elapsed, regardless of whether the connection is being used at the time of termination. You can specify an absolute-timeout value for each port. The user is notified 20 seconds before the session is terminated.

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to set the session timeout value to 2880 minutes (2 days) for the default line template:

```
RP/0/RSP0/CPU0:router(config)# line default
RP/0/RSP0/CPU0:router(config-line)# absolute-timeout 2880
```

Related Commands

Command	Description
banner incoming	Sets the idle wait timeout interval for user input over a physical terminal connection.
session timeout	Sets the idle wait timeout interval for user input over a virtual terminal connection.

access-class

To restrict incoming and outgoing connections using an IPv4 or IPv6 access list, use the **access-class** command in line template configuration mode. To remove the restriction, use the **no** form of this command.

access-class *list-name* {**in** | **out**}
no accessclass *list-name* {**in** | **out**}

Syntax Description

list-name	IPv4 or IPv6 access list name.
in	Filters incoming connections.
out	Filters outgoing connections.

Command Default

No access class is set.

Command Modes

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **access-class** command to restrict incoming or outgoing connections to addresses defined in an access list. Use the **ipv4 access-list** or **ipv6 access-list** command to define an access list by name.

Note To restrict access of incoming or outgoing connections over IPv4 and IPv6, the IPv4 access list and IPv6 access list must share the same name.

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to specify an access class assigned to outgoing connections for the default line template:

```
RP/0/RSP0/CPU0:router(config)# line default
RP/0/RSP0/CPU0:router(config-line)# access-class vtyacl out
```

The following sample output from the **show ipv4 access-lists** command displays the IPv4 access list named vtyacl:

```
RP/0/RSP0/CPU0:router# show ipv4 access-lists vtyacl

ipv4 access-list vtyacl
 10 permit ip host 10.32.162.48 any
 20 permit ip host 10.20.49.170 any
 30 permit ip host 10.60.3.5 any
```

The following sample output from the **show ipv6 access-lists** command displays the IPv6 access list name vtyacl:

```
RP/0/RSP0/CPU0:router# show ipv6 access-lists vtyacl

ipv6 access-list vtyacl
 10 permit ipv6 host 2001:db8:2222:: any
 20 permit ipv6 host 2001:db8:0:4::2 any
```

Related Commands

Command	Description
ipv4 access-list	Defines an IPv4 access list by name.
ipv6 access-list	Defines an IPv6 access list by name.

autocommand

To automatically run one or more commands after a user logs in to a vty terminal session, use the **autocommand** command in line default or line template configuration mode. To remove the **autocommand** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

autocommand *command*
no autocommand *command*

Syntax Description

command	Command or command alias to be executed on user login to a vty session.

Command Default

No default behavior or values

Command Modes

Line template configuration

Line default configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **autocommand** command to automatically run a command or command alias when a user logs in to a vty session. To run multiple commands, use a command alias for the *command* argument. When the user logs in, the commands included in the alias are run sequentially.

Note The **autocommand** command is supported on vty connections only; it is not supported on console or aux line connections. Use this command to automatically run a command after user login.

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to use the **autocommand** command to automatically run the **show ip interface brief** command when a user logs in to a default vty session:

```
RP/0/RSP0/CPU0:router# configure terminal
RP/0/RSP0/CPU0:router(config)# line default
RP/0/RSP0/CPU0:router(config-line)# autocommand show ip interface brief
RP/0/RSP0/CPU0:router(config-line)# end

Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:yes
```

```
RP/0/RSP0/CPU0:router# exit

  <Your 'TELNET' connection has terminated>
```

The following example shows how the **show ip interface brief** command is automatically run when the user logs on to a vty session:

```
User Access Verification

Username: lab
Password:

Executing Autocommand 'show ip interface brief'
RP/0/RSP0/CPU0:router# show ip interface brief

Interface                      IP-Address      Status                Protocol
MgmtEth0/RP0/CPU0/0            172.16.0.0      Up                    Up
POS0/0/0/0                     unassigned      Up                    Up
POS0/0/0/1                     unassigned      Up                    Up
POS0/0/0/2                     unassigned      Up                    Up
POS0/0/0/3                     unassigned      Up                    Up
POS0/3/0/0                     unassigned      Up                    Up
POS0/3/0/1                     unassigned      Up                    Up
POS0/3/0/2                     unassigned      Up                    Up
POS0/3/0/3                     unassigned      Up                    Up
```

The following example shows how to disable the feature using the **no** form of the **autocommand** command. In this example, the autocommand for the **show ip interface brief** command is disabled. When the user logs out, and logs back in, the **autocommand** command does not run.

```
RP/0/RSP0/CPU0:router# configure terminal
RP/0/RSP0/CPU0:router(config)# line default
RP/0/RSP0/CPU0:router(config-line)# no autocommand ?

  LINE  Appropriate EXEC command

RP/0/RSP0/CPU0:router(config-line)# no autocommand show ip interface brief
RP/0/RSP0/CPU0:router(config-line)# end

Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:yes

RP/0/RSP0/CPU0:router# exit

<Your 'TELNET' connection has terminated>

User Access Verification

Username: lab
Password:
RP/0/RSP0/CPU0:router#
```

The following example shows how to use a command alias with the **autocommand** command to run more than one command when a user logs in to a default vty session. In this example, the alias “test” is created to include the **show ip interface brief** command and the **show users** command. The autocommand feature is then used to run the “test” alias when a user logs in to the vty terminal:

```
RP/0/RSP0/CPU0:router# configure terminal
RP/0/RSP0/CPU0:router(config)# alias test show ip interface brief; show users
```

```
RP/0/RSP0/CPU0:router(config)# line default
RP/0/RSP0/CPU0:router(config-line)# autocommand test
RP/0/RSP0/CPU0:router(config-line)# end

Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:yes

RP/0/RSP0/CPU0:router# exit

<Your 'TELNET' connection has terminated>

User Access Verification

Username: lab
Password:

Executing Autocommand 'test'
RP/0/RSP0/CPU0:router# test

RP/0/RSP0/CPU0:router# show ip interface brief

Interface                      IP-Address      Status                Protocol
MgmtEth0/RP0/CPU0/0            172.16.0.0      Up                    Up
POS0/0/0/0                     unassigned      Up                    Up
POS0/0/0/1                     unassigned      Up                    Up
POS0/0/0/2                     unassigned      Up                    Up
POS0/0/0/3                     unassigned      Up                    Up
POS0/3/0/0                     unassigned      Up                    Up
POS0/3/0/1                     unassigned      Up                    Up
POS0/3/0/2                     unassigned      Up                    Up
POS0/3/0/3                     unassigned      Up                    Up

RP/0/RSP0/CPU0:router# show users

   Line            User                Service  Conns   Idle        Location
*  vty0            lab                 telnet       0  00:00:00    172.16.0.0
```

banner exec

To create a message that is displayed when an EXEC process is created (an EXEC banner), use the **banner exec** command in Global Configuration mode.To delete the EXEC banner, use the **no** form of this command.

banner exec *delimiter message delimiter*
no banner exec

Syntax Description

delimiter	Delimiting character is (c).
message	Message text. Text may include tokens in the form $(*token*) in the message text. Tokens are replaced with the corresponding configuration variable. Tokens are described in Table 1.

Command Default

No EXEC banner is displayed.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **banner exec** command to specify a message that is displayed when an EXEC process is created (a line is activated or an incoming connection is made to a vty). Follow this command with one or more blank spaces and the delimiting character (c). After entering one or more lines of text, terminate the message with the delimiting character (c).

When a user connects to a router, the message-of-the-day (MOTD) banner appears first, followed by the login banner and prompts. After the user logs in to the router, the EXEC banner or incoming banner is displayed, depending on the type of connection. For a reverse Telnet login, the incoming banner is displayed. For all other connections, the router displays the EXEC banner.

Use tokens in the form $(*token*) in the message text to customize the banner. Tokens display current configuration variables, such as the router hostname and IP address.

The tokens are described in this table.

Table 16: banner exec Tokens

Token	Information Displayed in the Banner
$(hostname)	Displays the hostname for the router.
$(domain)	Displays the domain name for the router.
$(line)	Displays the vty or tty (asynchronous) line number.

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to set an EXEC banner that uses tokens:

```
RP/0/RSP0/CPU0:router(config)# banner exec c

  Enter TEXT message.  End with the character 'c'.

THIS IS AN EXEC BANNER
c
```

Related Commands

Command	Description
banner incoming	Defines and enables a customized message that is displayed when there is an incoming connection to a terminal line from a host on the network.
banner login	Defines and enables a customized banner that is displayed before the username and password login prompts.
banner motd	Defines a customized MOTD banner.
banner prompt timeout	Defines a customized banner that is displayed when there is a login timeout.

banner incoming

To create a banner that is displayed when there is an incoming connection to a terminal line from a host on the network, use the **banner incoming** command in Global Configuration mode. To delete the incoming connection banner, use the **no** form of this command.

banner incoming *delimiter message delimiter*
no banner incoming

Syntax Description

delimiter	Delimiting character is (c).
message	Message text. You can include tokens in the form $(*token*) in the message text. Tokens are replaced with the corresponding configuration variable. Tokens are described in Table 1.

Command Default

No incoming banner is displayed.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Follow the **banner incoming** command with one or more blank spaces and the delimiting character (c). After entering one or more lines of text, terminate the message with the second occurrence of the delimiting character (c).

An *incoming connection* is one initiated from the network side of the router. Incoming connections are also called reverse Telnet sessions. These sessions can display message-of-the-day (MOTD) banners and incoming banners, but they do not display EXEC banners.

When a user connects to a router, the MOTD banner (if configured) appears first, followed by the login banner and prompts. After the user logs in to the router, the EXEC banner or incoming banner is displayed, depending on the type of connection. For a reverse Telnet login, the incoming banner is displayed. For all other connections, the router displays the EXEC banner.

Incoming banners cannot be suppressed. If you do not want the incoming banner to appear, you must delete it with the **no banner incoming** command.

To customize the banner, use tokens in the form $(*token*) in the message text. Tokens display current variables, such as the router hostname and IP address.

This table describes the tokens.

Table 17: banner incoming Tokens

Token	Information Displayed in the Banner
$(hostname)	Displays the hostname for the router.

Token	Information Displayed in the Banner
$(domain)	Displays the domain name for the router.
$(line)	Displays the vty or tty (asynchronous) line number.

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to create an incoming connection banner:

```
RP/0/RSP0/CPU0:router(config)# banner incoming c

  Enter TEXT message. End with the character 'c'
THIS IS AN INCOMING BANNER.
c
```

Related Commands

Command	Description
banner exec	Defines a customized banner that is displayed whenever the EXEC process is initiated.
banner login	Defines and enables a customized banner that is displayed before the username and password login prompts.
bannet motd	Defines a customized MOTD banner.
banner prompt timeout	Defines a customized banner that is displayed when there is a login timeout.

banner login

To create a customized banner that is displayed before the username and password login prompts, use the **banner login** command in Global Configuration mode. To disable the login banner, use **no** form of this command.

banner login *delimiter message delimiter*
no banner login

Syntax Description

delimiter	Delimiting character is (c).
message	Message text. You can include tokens in the form $(*token*) in the message text. Tokens are replaced with the corresponding configuration variable. Tokens are described in Table 1.

Command Default

No login banner is displayed.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Follow the **banner login** command with one or more blank spaces and the delimiting character (c). Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character (c).

When a user connects to the router, the message-of-the-day (MOTD) banner (if configured) appears first, followed by the login banner and prompts. After the user successfully logs in to the router, the EXEC banner or incoming banner is displayed, depending on the type of connection. For a reverse Telnet login, the incoming banner is displayed. For all other connections, the router displays the EXEC banner.

To customize the banner, use tokens in the form $(*token*) in the message text. Tokens display current configuration variables, such as the router hostname and IP address.

Tokens are described in the this table.

Table 18: banner login Tokens

Token	Information Displayed in the Banner
$(hostname)	Displays the hostname for the router.
$(domain)	Displays the domain name for the router.
$(line)	Displays the vty or tty (asynchronous) line number.

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to set a login banner:

```
RP/0/RSP0/CPU0:router(config)# banner login c

Enter TEXT message. End with the character 'c'.
THIS IS A LOGIN BANNER
c
```

Related Commands

Command	Description
banner exec	Defines a customized banner that is displayed whenever the EXEC process is initiated.
banner incoming	Defines and enables a customized message that is displayed when there is an incoming connection to a terminal line from a host on the network.
bannet motd	Defines a customized MOTD banner.
banner prompt timeout	Defines a customized banner that is displayed when there is a login timeout.

banner motd

To create a message-of-the-day (MOTD) banner, use the **banner motd** command in Global Configuration mode. To delete the MOTD banner, use the **no** form of this command.

banner motd *delimiter message delimiter*
no banner motd

Syntax Description

delimiter	Delimiting character is (c).
message	Message text. You can include tokens in the form $(*token*) in the message text. Tokens are replaced with the corresponding configuration variable.

Command Default

No MOTD banner is displayed.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Follow this command with one or more blank spaces and the delimiting character (c). Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character (c).

This MOTD banner is displayed to all terminals connected and is useful for sending messages that affect all users (such as impending system shutdowns). Use the **no banner motd** command to disable the MOTD banner on a line.

When a user connects to the router, the MOTD banner (if configured) appears first, followed by the login banner and prompts. After the user successfully logs in to the router, the EXEC banner or incoming banner is displayed, depending on the type of connection. For a reverse Telnet login, the incoming banner is displayed. For all other connections, the router displays the EXEC banner.

To customize the banner, use tokens in the form $(token) in the message text. Tokens display current configuration variables, such as the router hostname and IP address.

Tokens are described in this table.

Table 19: banner motd Tokens

Token	Information Displayed in the Banner
$(hostname)	Displays the hostname for the router.
$(domain)	Displays the domain name for the router.
$(line)	Displays the vty or tty (asynchronous) line number.

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to configure an MOTD banner with a token:

```
RP/0/RSP0/CPU0:router(config)# banner motd c

  Enter TEXT message.  End with the character 'c'.
Notice: all routers in $(domain) will be upgraded beginning April 20
c
```

Related Commands

Command	Description
banner exec	Defines and enables a customized banner that is displayed whenever the EXEC process is initiated.
banner incoming	Defines and enables a customized message that is displayed when there is an incoming connection to a terminal line from a host on the network.
banner login	Defines and enables a customized banner that is displayed before the username and password login prompts.
banner prompt timeout	Defines a customized banner that is displayed when there is a login timeout.

banner prompt-timeout

To create a banner that is displayed when there is a login authentication timeout, use the **banner prompt-timeout** command in Global Configuration mode. To delete the prompt timeout banner, use the **no** form of this command.

banner prompt-timeout *delimiter message delimiter*
no banner prompt-timeout

Syntax Description

delimiter	Delimiting character is (c).
message	Message text. You can include tokens in the form $(*token*) in the message text. Tokens are replaced with the corresponding configuration variable.

Command Default

No banner is displayed when there is a login authentication timeout.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Follow this command with one or more blank spaces and the delimiting character (c). Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character (c).

This prompt-timeout banner is displayed when there is a login authentication timeout at the username and password prompt.

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to configure a prompt-timeout banner:

```
RP/0/RSP0/CPU0:router(config)# banner prompt-timeout c

Enter TEXT message.  End with the character 'c'.
THIS IS A PROMPT TIMEOUT BANNER
c
```

Related Commands

Command	Description
banner exec	Defines and enables a customized banner that is displayed whenever the EXEC process is initiated.
banner incoming	Defines and enables a customized message that is displayed when there is an incoming connection to a terminal line from a host on the network.
banner login	Defines and enables a customized banner that is displayed before the username and password login prompts.
banner motd	Defines a customized MOTD banner.

clear line

To clear an auxiliary or console line to an idle state, use the **clear line** command in EXEC mode.

clear line {**aux** | **console**} **location** *node-id*

Syntax Description

aux	Clears the auxiliary line.
console	Clears the console line.
location *node-id*	Specifies the location of a route processor (RP) where the auxiliary or console line to be cleared resides. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
tty-access	execute

The following example shows how to clear the console line, putting it in an idle state:

```
RP/0/RSP0/CPU0:router# clear line console location 0/RP1/CPU0
```

Related Commands

Command	Description
show users	Displays information about the active lines on the networking device.

clear line vty

To clear a virtual terminal line (vty) to an idle state, use the **clear line vty** command in EXEC mode.

clear line vty *line-number*

Syntax Description

line-number	Line number in the range from 0 to 99.

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **show users** command to determine the origin of the connection and which lines to clear. When a line is cleared to an idle state, the user on the other end of the connection receives notice that the connection was closed by a foreign host.

Task ID

Task ID	Operations
tty-access	execute

The following example shows how to reset vty 3 to the idle state:

```
RP/0/RSP0/CPU0:router# clear line vty 3
```

Related Commands

Command	Description
show users, on page 305	Displays information about the active lines on the networking device.

cli interactive syntax check

To enable interactive syntax checking, use the **cli interactive syntax check** command in the appropriate line configuration mode. To disable interactive syntax checking, use the **no** form of this command.

cli interactive syntax check
no cli interactive syntax check

Syntax Description

This command has no keywords or arguments.

Command Default

Interactive syntax checking is disabled.

Command Modes

Line console configuration

Line default configuration

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **cli interactive syntax check** command to check command syntax as you type. You are not allowed to enter incorrect syntax.

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to enable interactive syntax checking:

```
RP/0/RSP0/CPU0:router(config)# line console
RP/0/RSP0/CPU0:router(config-line)# cli interactive syntax check
```

Related Commands

Command	Description
cli whitespace completion	Enables completion of a command when you type the space key.

cli whitespace completion

To enable completion of a command when you type the space key, use the **cli whitespace completion** command in the appropriate line configuration mode. To disable whitespace completion, use the **no** form of this command.

cli whitespace completion
no cli whitespace completion

Syntax Description

This command has no keywords or arguments.

Command Default

Whitespace completion is disabled.

Command Modes

Line console configuration

Line default configuration

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **cli whitespace completion** command to complete the next word of the command syntax if you type the space key before completing the word. If more than one option is valid, all options are displayed for you to choose one.

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to enable whitespace completion:

```
RP/0/RSP0/CPU0:router(config)# line console
RP/0/RSP0/CPU0:router(config-line)# cli whitespace completion
```

Related Commands

Command	Description
cli interactive syntax check, on page 273	Enables interactive syntax checking.

databits

To set the data bits per character for physical terminal connections, use the **databits** command in line console configuration mode. To restore the default value, use the **no** form of this command.

databits {**5** | **6** | **7** | **8**}
no databits

Syntax Description

5	Sets the data bits per character to 5.
6	Sets the data bits per character to 6.
7	Sets the data bits per character to 7.
8	Sets the data bits per character to 8.

Command Default

Eight databits per character.

Command Modes

Line console configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **databits** command to set the data bits attributes for physical terminal connections. Physical terminal connections use either the console or auxiliary line template.

The **databits** command masks the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity generation is in effect, specify 8 data bits per character. The keywords **5** and **6** are supplied for compatibility with older devices and generally are not used.

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to set the data bits per character for the console terminal template to 7:

```
RP/0/RSP0/CPU0:router(config)# line console
RP/0/RSP0/CPU0:router(config-line)# databits 7
```

Related Commands

Command	Description
show users	Displays information about the active lines on the networking device.
stopbits	Sets the number of stop bits.

disconnect

To disconnect a network connection, use the **disconnect** command in EXEC mode.

disconnect [*connection-numbernetwork-name*]

Syntax Description

connection-number	(Optional) Number of the line of the active network connection to be disconnected. Range is from 1 to 20.
network-name	(Optional) Name of the active network connection to be disconnected.

Command Modes

EXEC mode

Command Default

Disconnects the existing network connection if no arguments are provided.

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Do not disconnect a line to end a session. Instead, log off the host before ending the session to clear the connection. If you cannot log out of an active session, disconnect the line.

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to disconnect from a device (in this example “User1”) to return to the router:

```
User1% disconnect
 Connection closed by remote host

RP/0/RSP0/CPU0:router#
```

disconnect-character

To define a character to disconnect a session, use the **disconnect-character** command in line template configuration mode. To remove the **disconnect-character** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

disconnect-character [*numbercharacter*]
no disconnect-character

Syntax Description

number	(Optional) ASCII decimal equivalent of the disconnect character. Range is from 0 through 255.
character	(Optional) Disconnect character.

Command Default

No disconnect character is defined.

Command Modes

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

The break character is represented by 0; null cannot be represented.

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to set the disconnect character for the default line template to the Esc character, which is the ASCII decimal equivalent 27:

```
RP/0/RSP0/CPU0:router(config)# line default
RP/0/RSP0/CPU0:router(config-line)# disconnect-character 27
```

Related Commands

Command	Description
escape-character, on page 279	Defines an escape character.

escape-character

To define a character to escape a session, use the **escape-character** command in line template configuration mode. To remove the **escape-character** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

escape-character {**break***numbercharacter* | **default** | **none**}
no escape-character

Syntax Description

break	Sets the escape character to the Break key.
number	ASCII decimal equivalent of the escape character. Range is from 0 through 255.
character	Escape character.
default	Specifies the default escape character (^^X).
none	Disables the escape function.

Command Default

The default escape character is ^^X.

Command Modes

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **escape-character** command to define an escape character sequence that is different from the default. Use the escape character to exit from an existing connection and return to the EXEC prompt.

The default escape key sequence is Ctrl-Shift-6, X (^^X).The **escape-character** command with the **default** keyword sets the escape character to the Break key (the default setting for the Break key is Ctrl-C).

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to set the escape character for the default line template to Ctrl-P, which is the ASCII decimal character 16:

```
RP/0/RSP0/CPU0:router(config)# line default
RP/0/RSP0/CPU0:router(config-line)# escape-character 16
```

Related Commands

Command	Description
disconnect-character, on page 278	Defines a disconnect character.

exec-timeout

To set the interval that the EXEC command interpreter waits until user input is detected, use the **exec-timeout** command in the appropriate line configuration mode. To remove the **exec-timeout** command from the running configuration and restore the system to its default condition, use the **no** form of this command.

exec-timeout *minutes seconds*
no exec-timeout *minutes seconds*

Syntax Description

minutes	Minutes for the wait interval. Range is from 0 to 35791.
seconds	Seconds for the wait interval. Range is from 0 to 2147483.

Command Default

minutes: 10

seconds: 0

Command Modes

Line console configuration

Line default configuration

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

If no input is detected during the interval, the EXEC facility resumes the current connection. If no connections exist, the EXEC facility returns the terminal to the idle state and disconnects the incoming session. To disable the EXEC timeout function so that the EXEC session never timeouts, enter the following command:

```
exec-timeout 00
```

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to set the timeout interval for the console line template to 60 minutes, 0 seconds:

```
RP/0/RSP0/CPU0:router(config)# line console
RP/0/RSP0/CPU0:router(config-line)# exec-timeout 60 0
```

Related Commands

Command	Description
absolute-timeout, on page 255	Sets the absolute timeout for line disconnection.
session-timeout, on page 295	Sets the idle wait timeout interval for user input over a virtual terminal connection.

flowcontrol hardware

To configure the hardware flow control setting for physical terminal connections, use the **flowcontrol hardware** command in line console configuration mode. To remove the attribute from the configuration file and restore the system to its default condition, use the **no** form of this command.

flowcontrol hardware {**in** | **out** | **none**}
no flowcontrol hardware {**in** | **out** | **none**}

Syntax Description

in	Specifies inbound flow control.
out	Specifies outbound flow control.
none	Specifies no flow control.

Command Default

None

Command Modes

Line console configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **flowcontrol hardware** command to set the flow control attribute for physical line connections. Physical line connections use either the console or auxiliary line template.

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to restrict the hardware flow control to inbound for the console line template:

```
RP/0/RSP0/CPU0:router(config)# line console
RP/0/RSP0/CPU0:router(config-line)# flowcontrol hardware in
```

Related Commands

Command	Description
show users	Displays information about the active lines on the networking device.

lcd alarm-category

To set the alarm-category (will get displayed on the LCD panel), use the **lcd alarm-category** command in the appropriate mode. To delete the set category, use the **no** form of the command.

lcd alarm-category *number*
no lcd alarm-category *number*

Syntax Description

number Number to identify the alarm category. This lists indicates the numbers for classification:

- 1 for critical
- 2 for critical and major
- 3 for critical, major and minor
- 0 for other

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

None

Example

This example show how to use the **lcd alarm-category** command:

```
RP/0/RSP0/CPU0:router (config) # lcd alarm-category 2
```

lcd message

To set administrative messages (will get displayed on the LCD panel), use the **lcd message** command in the appropriate mode. To delete the set message, use the **no** form of the command.

lcd message *message*

Syntax Description

message	Administrative message for the operator. Limit is 512 alphanumeric characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

None

Example

This example show how to use the **lcd message** command:

```
RP/0/RSP0/CPU0:router (config) # lcd message abcd
```

lcd name

To set the rack-name (will get displayed on the LCD panel), use the **lcd name** command in the appropriate mode. To delete the set name, use the **no** form of the command.

lcd name *rack-name location*

Syntax Description

rack-name	The rack-name. Limit is 15 alphanumeric characters.
location	The location of the rack (rack-id).

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

None

Example

This example show how to use the **lcd name** command:

```
RP/0/RSP0/CPU0:router (config) # lcd name lc1
```

length

To set the number of lines that display at one time on the screen, use the **length** command in line template configuration mode. To remove the **length** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

length *lines*
no length *lines*

Syntax Description

lines	Number of lines that displays on a screen. Range is from 0 through 512. 0 specifies no pausing. The default is 24.

Command Default

lines : 24

Command Modes

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **length** command to modify the default length setting for the specified line template. The length setting determines when the screen pauses during the display of multiple-screen output. Specifying a value of 0 for the lines argument prevents the router from pausing between screens of output.

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to set the length of the default line template to 33 lines:

```
RP/0/RSP0/CPU0:router(config)# line default
RP/0/RSP0/CPU0:router(config-line)# length 33
```

Related Commands

Command	Description
terminal length	Sets the length of the display terminal for the current terminal session.

line

To specify the console, the default, or a user-defined line template and enter line template configuration mode, use the **line** command in

global configuration

mode.

line {**console** | **default** | **template** *template-name*}

Syntax Description

console	Specifies the line template for the console line.
default	Specifies the default line template.
template *template-name*	Specifies a user-defined line template to be applied to a vty pool.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **line** command to specify a line template type and enter into line template configuration mode. Line templates are a collection of attributes used to configure and manage physical terminal line connections (the console and auxiliary ports) and vty connections. The following templates are available in Cisco IOS XR software:

- Default line template—The default line template that applies to a physical and virtual terminal lines.
- Console line template—The line template that applies to the console line.
- User-defined line templates—User-defined line templates that can be applied to a range of virtual terminal lines.

The following example shows how to enter line template configuration mode to allow configuration changes to be made to the default line template:

```
RP/0/RSP0/CPU0:router(config)# line default
RP/0/RSP0/CPU0:router(config-line)#
```

parity

To set the parity bit for physical terminal connections, use the **parity** command in line console configuration mode. To specify no parity, use the **no** form of this command.

parity {**even** | **none** | **odd**}
no parity {**even** | **none** | **odd**}

Syntax Description

even	Specifies even parity.
none	Specifies no parity.
odd	Specifies odd parity.

Command Default

No parity is set.

Command Modes

Line console configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Communication protocols provided by devices such as terminals and modems often require a specific parity bit setting.

Use the **parity**command for setting the parity attribute for physical terminal connections. Physical terminal connections use either the console or auxiliary line template.

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to set the line parity configuration to even for the console line template:

```
RP/0/RSP0/CPU0:router(config)# line console
RP/0/RSP0/CPU0:router(config-line)# parity even
```

Related Commands

Command	Description
show users	Displays information about the active lines on the networking device.

resume

To switch to another active Secure Shell (SSH) or Telnet session, use the **resume** command in

EXEC

mode.

resume [*connection*]

Syntax Description

connection	(Optional) Name or number of the active network connection; the default is the most recent connection. Number range is from 1 to 20.

Command Default

The most recent connection.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

SSH and Telnet sessions can be established to another router or server.

When the network session is being established and without disconnecting the network session, you can resume the router console session by typing a special sequence of characters as shown. After switching back to the router console, the network connection can be resumed by specifying the number of the connection or the name of the connection.

You can have several concurrent sessions open and switch back and forth between them. The number of sessions that can be open is defined using the **session-limit** command.

You can switch between sessions by escaping one session and resuming a previously opened session, as follows:

1. Escape from the current session by pressing the escape sequence (Ctrl Shift-6, x [^^X]) to return to the EXEC prompt.
2. Enter the **show sessions** command to list the open sessions. All open sessions associated with the current terminal line are displayed.
3. Enter the **resume** command and the session number to make the connection.

   You can also resume the previous session by pressing the **Return** key.

   The **^^X** and commands are available for all supported connection protocols.

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to escape from one connection and resume another. You can omit the connection name and simply enter the connection number to resume that connection.

```
host1% ^^x
RP/0/RSP0/CPU0:router# resume 1

blg_router#
```

Related Commands

Command	Description
session-limit, on page 294	Sets the maximum number of outgoing terminal sessions from the current terminal.
show sessions, on page 301	Displays information about SSH and Telnet connections.
telnet	Logs in to a host that supports Telnet.

send

To send messages to one or all terminal lines, use the **send** command in

EXEC

mode.

send {***line-number** | **aux 0** | **console 0** | **vty** *number*}

Syntax Description

*****	Sends a message to all tty lines.
line-number	Line number to which the message is sent. A number from 0 to 101.
aux 0	Sends a message to the auxiliary line.
console 0	Sends a message to the console line.
vty *number*	Sends a message to a virtual terminal line (vty). Range is 0 to 99.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

The system prompts for the message, which can be up to 500 characters long. Enter **Ctrl-Z** to end the message. Enter **Ctrl-C** to abort this command.

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to send a message to all lines:

```
RP/0/RSP0/CPU0:router# send *

Enter message, end with CTRL/Z; abort with CTRL/C:
The system will be shut down in 10 minutes for repairs.^Z
Send message? [confirm]
RP/0/RSP0/CPU0:router#

***
***
```

```
*** Message from tty to all terminals:
***
The system will be shut down in 10 minutes for repairs.
```

session-limit

To set the maximum number of outgoing terminal sessions from the current terminal, use the **session-limit** command in the appropriate line configuration mode. To remove any specified session limit, use the **no** form of this command.

session-limit *connections*
no session-limit

Syntax Description

connections	Maximum number of outgoing connections. Range is from 0 through 20.

Command Default

connections : 6

Command Modes

Line console configuration

Line default configuration

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to limit the number of active outgoing connections for the default line template to eight:

```
RP/0/RSP0/CPU0:router(config)# line default
RP/0/RSP0/CPU0:router(config-line)# session-limit 8
```

session-timeout

To set the timeout interval for all outgoing connections from the current terminal, use the **session-timeout** command in the appropriate line configuration mode. To remove the **session-timeout** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

session-timeout *minutes* [**output**]
no session-timeout *minutes*

Syntax Description

minutes	Timeout interval, in minutes. Range is 0 to 35791. The default is 10.
output	(Optional) Specifies that when traffic is sent to an asynchronous line from the router (within the specified interval), the connection is retained.

Command Default

minutes : 10

Command Modes

Line console configuration

Line default configuration

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **session-timeout** command to set the interval that Cisco IOS XR software waits for traffic before closing the connection to a remote device and returning the terminal to an idle state. If the **output** keyword is not specified, the session timeout interval is based solely on detected input from the user. If the keyword is specified, the interval is based on input and output traffic.

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to set the session timeout value for the default line template to 120 minutes (2 hours):

```
RP/0/RSP0/CPU0:router(config)# line default
RP/0/RSP0/CPU0:router(config-line)# session-timeout 120
```

show cli submode-exit

To display the status of terminal submode-exit configuration, use **show cli submode-exit status** command in EXEC mode.

show cli submode-exit status

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

EXEC mode.

Command History

Release	Modification
Release 6.5.1	This command was introduced.

Usage Guidelines

You cannot enable or disable service cli submode-exit on a different users's VTY session..

```
RP/0/RSP0/CPU0:router #show cli submode-exit status
Global  submode exit feature is enabled.
Session submode exit feature is enabled
```

show diag lcd-interface

To display details about the LCD interface (of the craft panel) , use the **show diag lcd-interface** command in the appropriate mode.

show diag lcd-interface

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 5.2.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
lcd	read

Example

This example shows how to use the **show diag lcd-interface**

```
RP/0/RSP0/CPU0:router # show diag location 0/CI0

Diag Information For : 0/CI0

 0/CI0-IDPROM Info
    Controller Family        : 0084
    Controller Type          : 0932
    PID                      : NCS4K-CRAFT
    Version Identifier       : V00
    UDI Description          : NCS 4000 Craft Panel
    CLEI Code                : NOCLEICODE
    ECI Number               : 11223344
    Top Assy. Part Number    : 800-41609-01
    Top Assy. Revision       : 12
    PCB Serial Number        : SAL1818RL2G
    PCA Number               : 73-14799-03
```

show line

To display the parameters of terminal lines, use the **show line** command in

EXEC

mode.

show line [**aux location** *node-id* | **console location** *node-id* | **vty** *number*]

Syntax Description

aux	(Optional) Displays the terminal line parameters for the auxiliary line.
location *node-id*	(Optional) Specifies the location for the route processor (RP) on which the auxiliary or console port resides. The *node-id* argument is entered in the *rack/slot/module* notation.
console	(Optional) Displays the terminal line parameters for the console line.
vty *number*	(Optional) Specifies a virtual terminal line (vty) number. Range is from 0 through 99.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
tty-access	read

The following example shows sample output from the **show line** command. The asterisk (*) indicates the current terminal session.

```
RP/0/RSP0/CPU0:router# show line

    Tty             Speed     Modem  Uses   Noise Overruns           Acc I/O
    aux0_0_0         9600       -     -       -      0/0              -/-
 *  con0_0_0         9600       -     -       -      0/0              -/-
    vty0             0/0        -     -       -      0/0              -/-
    vty1             0/0        -     -       -      0/0              -/-
    vty2             0/0        -     -       -      0/0              -/-
```

```
vty3            0/0         -     -       -      0/0              -/-
vty4            0/0         -     -       -      0/0              -/-
vty100          0/0         -     -       -      0/0              -/-
vty101          0/0         -     -       -      0/0              -/-
vty102          0/0         -     -       -      0/0              -/-
vty103          0/0         -     -       -      0/0              -/-
vty104          0/0         -     -       -      0/0              -/-
vty105          0/0         -     -       -      0/0              -/-
```

Table 20: show line Field Descriptions

Field	Description
Tty	Available ttys and vtys.
Speed	Baud rate that the inbound serial connection is using, in bps.
Modem	Not implemented.
Uses	Not implemented.
Noise	Not implemented.
Overruns	Hardware Universal Asynchronous Receiver/Transmitter (UART) overruns or software buffer overflows, both defined as the number of overruns or overflows that have occurred on the specified line since the system was restarted. Hardware overruns are buffer overruns; the UART chip has received bits from the software faster than it can process them. A software overflow occurs when the software has received bits from the hardware faster than it can process them.
Acc I/O	Not implemented.

The following example shows sample output from the **show line** command with the console line specified:

```
RP/0/RSP0/CPU0:router# show line console location 0/rp0/cpu0

    Tty             Speed     Overruns             Acc I/O
    con0/RP0/CPU0    9600          0/0                 -/-

  Line con0_RP0_CPU0, Location "0/RP0/CPU0", Type "Console"
  Length: 24 lines, Width: 80 columns
  Baud rate (TX/RX) is 9600, 1 parity, 2 stopbits, 8 databits
  Template: console
  Capabilities: Timestamp Disabled
  Allowed transports are none.
```

Table 21: show line location Field Descriptions

Field	Description
Tty	Unique identifier of the tty; it contains the type of tty and, for physical ttys, it indicates the physical location of the tty.
Speed	Baud rate that the inbound serial connection is using in bps.

Field	Description
Overruns	Hardware UART overruns or software buffer overflows, both defined as the number of overruns or overflows that have occurred on the specified line since the system was restarted. Hardware overruns are buffer overruns; the UART chip has received bits from the software faster than it can process them. A software overflow occurs when the software has received bits from the hardware faster than it can process them.
Acc I/O	Not implemented.
Line	Unique identifier of the TTY. This field displays the type of TTY and the physical location of physical TTYs.
Location	Location of the line.
Type	Line type.
Length	Length of the terminal or screen display, in rows.
Width	Width of the terminal or screen display, in columns.
Baud rate (TX/RX)	Transmit rate/receive rate of the line, in bps.
parity	Parity bits value used for physical terminal connections.
stopbits	Stop bits value used for physical terminal connections.
databits	Data bits value used for physical terminal connections.
Template	Line template being sourced by the particular connection.
Config	Configuration applied to the tty. This field indicates the allowed incoming transports that can be used to access the router from this tty.
Allowed transports are	Incoming transport protocols that can be used by this tty to access the router.

show sessions

To display information about suspended Secure Shell (SSH) and Telnet connections launched from the terminal session, use the **show sessions** command in

EXEC

mode.

show sessions

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **show sessions** command to display the hostname, remote connection service used by the router to access the host, idle time, and connection name.

Task ID

Task ID	Operations
tty-access	read

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

```
RP/0/RSP0/CPU0:router# show sessions

  Conn Host               Address            Service Idle Conn Name
  *  1 10.26.25.40        10.26.25.40        telnet    15 10.26.25.40
```

The asterisk (*) indicates the current terminal session.

Table 22: show sessions Field Descriptions

Field	Description
Conn	Identifier for the connection used for resuming and disconnecting suspended sessions. An asterisk (*) indicates the current terminal session.

Field	Description
Host	Remote host to which the router is connected. This field displays either the IP address or hostname of the remote host. If the IP address of the remote host is mapped to the hostname (that is, if Domain Name System [DNS] services are enabled) and the session is initiated with the hostname, the output for this field displays the hostname of the host rather than the IP address of the host.
Address	IP address of the remote host.
Service	Remote connection service used.
Idle	Interval (in seconds) since data was last sent on the line.
Conn Name	Equivalent to the “Host” field in Cisco IOS XR software.

Related Commands

Command	Description
disconnect, on page 277	Disconnects a network connection.
resume, on page 290	Switches to another active Telnet session.

show terminal

To obtain information about the terminal configuration attribute settings for the current terminal line, use the **show terminal** command in

EXEC

mode.

show terminal

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

None.

This example shows sample output from the **show terminal** command:

```
RP/0/RSP0/CPU0:router# show terminal

Line vty0, Location "10.56.249.67", Type "VTY"
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 0, 0 parity, 0 stopbits, 0 databits
Template: default
Capabilities: Timestamp Disabled
Allowed transports are telnet ssh.
```

Table 23: show terminal Field Descriptions

Field	Description
Line	Line that is currently being used.
Location	Location of the terminal accessing the router.
Type	Type of line.
Length	Length of the terminal or screen display, in rows.
Width	Width of the terminal or screen display, in columns.
Baud rate (TX/RX)	Transmit or receive rate of the line, in bps.
parity	Parity bits value used for physical terminal connections.

Field	Description
stopbits	Stop bits value used for physical terminal connections.
databits	Data bits value used for physical terminal connections.
Template	Line template being sourced by the particular connection.
Config	Configuration applied to the tty. This field indicates the allowed incoming transports that can be used to access the router from this tty.
Allowed transports are	Incoming transport protocols that can be used by this tty to access the router.

show users

To display information about the active lines on the router, use the **show users** command in EXEC mode.

show users

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **show users** command to display the line number, connection name, idle time, hosts, and terminal location. An asterisk (*) indicates the current terminal session.

Note To display all user groups and task IDs associated with the currently logged-in user, use the **show user** command in EXEC mode. See the *Authentication, Authorization, and Accounting Commands on Cisco IOS XR Software* module in *System Security Command Reference for Cisco ASR 9000 Series Routers*.

Task ID

Task ID	Operations
tty-access	read

The following example shows sample output identifying an active vty terminal session:

```
RP/0/RSP0/CPU0:router# show users

    Line            User                Service  Conns   Idle        Location
    con0_RP0_CPU0   cisco               hardware     0  18:33:48
    vty0            cisco               telnet       0  00:30:36    10.33.54.132
  * vty1            cisco               telnet       0  00:00:00    10.33.54.132
```

Table 24: show users Command Output Field Descriptions

Field	Description
Line	All current connections. An asterisk (*) indicates the active connection.
User	Username of the user logged into the line.

Field	Description
Service	Physical or remote login service used.
Conns	Number of outgoing connections.
Idle	Interval (in hours:minutes:seconds) since last keystroke.
Location	IP address of remote login host. For local (physical) terminal connections, this field is blank.

Related Commands

Command	Description
show line	Displays the parameters of a terminal line.
show user	Displays all user groups and task IDs associated with the currently logged-in user.

stopbits

To set the stop bits used for physical terminal connections, use the **stopbits** command in line console configuration mode. To restore the default, use the **no** form of this command.

stopbits {**1** | **2**}
no stopbits

Syntax Description

1	Specifies one stop bit.
2	Specifies two stop bits. This is the default.

Command Default

Two stop bits.

Command Modes

Line console configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **stopbits** command to set the data bits attributes for physical terminal connections. Physical terminal connections use either the console or auxiliary terminal templates.

Communication protocols provided by devices such as terminals and modems often require a specific stop-bit setting.



Note The number of stop bits configured on the router and a terminal server should be same. The default number of stop bits on the router is two stop-bits.

Task ID

Task ID	Operations
tty-access	read, write

This example shows how to change the default from two stop bits to one for the console line template:

```
RP/0/RSP0/CPU0:router(config)# line console
RP/0/RSP0/CPU0:router(config-line)# stopbits 1
```

Related Commands

Command	Description
databits	Sets the number of data bits.

terminal cli submode-exit

To enable or disable submode-exit on all interactive configuration sessions per VTY, use **terminal cli submode-exit** command in EXEC mode.

terminal cli submode-exit

Syntax Description

enable	Enables submode-exit on all interactive configuration sessions per VTY.
disable	Disables submode-exit on all interactive configuration sessions per VTY.

Command Default

No default behavior or values.

Command Modes

EXEC mode.

Command History

Release	Modification
Release 6.5.1	This command was introduced.

Usage Guidelines

You cannot enable or disable service cli submode-exit on a different users's VTY session..

```
RP/0/RSP0/CPU0:router #terminal cli submode-exit ?
  disable  Disable submode-exit behavior for this config session
  enable   Enable submode-exit behavior for this config session
```

```
RP/0/RSP0/CPU0:router #terminal cli submode-exit enable
WARNING: submode-exit enable is already configured at GLOBAL level.This takes precedence
over per-session settings.
```

```
RP/0/RSP0/CPU0:router #terminal cli submode-exit disable
```

terminal exec prompt

To specify prompt attributes for the current terminal session, use the **terminal exec prompt** command in the appropriate mode.

terminal exec prompt {**no-timestamp** | **timestamp**}

Syntax Description

no-timestamp	Disables the time-stamp printing before each command.
timestamp	Enables the time-stamp printing before each command.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the**terminal exec prompt** command with the **timestamp** keyword to show the time-stamp display after each command is entered. Use the **terminal exec** command with the **no-timestamp** keyword to disable the time-stamp display.

Note The **terminal** commands are active for the current terminal session only. To apply a setting to all sessions, use the **line** commands.

This example shows how to enable the time-stamp prompt. When enabled, the date and time are displayed after each command. In this example, the **show version** command is entered, and the date and time is displayed.

```
RP/0/RSP0/CPU0:router# terminal exec prompt timestamp
RP/0/RSP0/CPU0:router# show version

Thu Jan 14 06:39:50.926 PST

Cisco IOS XR Software, Version 3.9.1.15I[DT_IMAGE]
Copyright (c) 2010 by Cisco Systems, Inc.

ROM: System Bootstrap, Version 1.2(20090903:202931) [ASR9K ROMMON],

router uptime is 6 days, 14 hours, 47 minutes
System image file is "bootflash:disk0/asr9k-os-mbi-3.9.1.15I/mbiasr9k-rp.vm"

cisco ASR9K Series (MPC8641D) processor with 4194304K bytes of memory.
MPC8641D processor at 1333MHz, Revision 2.2

2 Management Ethernet
40 GigabitEthernet
12 TenGigE
219k bytes of non-volatile configuration memory.
```

```
975M bytes of compact flash card.
33994M bytes of hard disk.
1605616k bytes of disk0: (Sector size 512 bytes).
1605616k bytes of disk1: (Sector size 512 bytes).

Configuration register on node 0/RSP0/CPU0 is 0x102
Boot device on node 0/RSP0/CPU0 is disk0:
  --More--
```

The following example shows how to disable the time-stamp prompt:

```
RP/0/RSP0/CPU0:router# terminal exec prompt no-timestamp
```

terminal exec utility pager

To configure the terminal page display options, use the **terminal exec utility pager** command in the appropriate mode.

terminal exec utility pager {**less** | **more** | **none**}

Syntax Description

less	Specifies to use unix-like "less" bidirectional paging for the terminal display.
more	Specifies to use unix-like "more" unidirectional paging for the terminal display.
none	Specifies that the display is not paginated.

Command Default

No pagination is configured by default.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **terminal exec utility pager** command with the **more** keyword to scroll forward through command display one screen at a time. "--More--" is displayed at the end of each screen. Press the Space key to advance one screen. Press the Enter key to advance one line. Press the Esc key to exit the command display.

Task ID

Task ID	Operation
tty-access	Read

This example shows how to limit command display to one screen at a time such that you can move forward through the display:

```
RP/0/RSP0/CPU0:router#terminal exec utility pager more
```

terminal length

To set the number of lines that display at one time on the screen for the current terminal session, use the **terminal length** command in

EXEC

mode.

terminal length *lines*

Syntax Description

lines	Number of lines that display on a screen. Range is from 0 through 512.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **terminal length** command to set the terminal length value for only the current terminal session and not save it to the running configuration. Exiting from the terminal session returns the terminal length value to the value configured with the **length** command.

Specifying a value of 0 for the *lines* argument prevents the router from pausing between screens of output.



Note The **terminal** commands are active for the current terminal session only. To apply a setting to all sessions, use the **line** commands.

Task ID

Task ID	Operations
tty-access	read, write

This example shows how to set the length for the current terminal session to 120 lines:

```
RP/0/RSP0/CPU0:router# terminal length 120
```

Related Commands

Command	Description
length	Sets the length of the display terminal.

terminal width

To set the width of the display terminal for the current terminal session, use the **terminal width** command in

EXEC

mode.

terminal width *characters*

Syntax Description

characters	Number of characters to display on a screen. Range is from 0 to 512.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **terminal width** command to set the terminal width value for only the current terminal session and not save it to the running configuration. Exiting from the terminal session returns the terminal width value to the value configured with the **width** (display) command.

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to set the terminal width for the current terminal session to 120 characters:

```
RP/0/RSP0/CPU0:router# terminal width 120
```

Related Commands

Command	Description
width display	Sets the width of the display terminal.

timestamp disable

To disable time-stamp recording at the top of each command output, use the **timestamp disable** command in the appropriate line configuration mode. To reenable time-stamp recording if disabled, use the **no** form of this command.

timestamp disable
no timestamp disable

Syntax Description

This command has no keywords or arguments.

Command Default

Time-stamp recording at the top of each command output is enabled.

Command Modes

Line console configuration

Line default configuration

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

By default, the time stamp is displayed at the top of any command output. The time stamp records the time at which the command was issued. You can use the **snmp-server view** command to disable this setting so that the time stamp does not appear at the top of the command output. This setting applies to all command outputs on any terminal line to which the current line template applies.

Task ID

Task ID	Operations
tty-access	read, write

This example shows how to disable time-stamp recording for the console line template:

```
RP/0/RSP0/CPU0:router(config)# line console
RP/0/RSP0/CPU0:router(config-line)#  timestamp disable
```

transport input

To define the transport protocols that can be used to access the router, use the **transport input** command in the appropriate line configuration mode. To change or remove the protocol, use the **no** form of this command.

transport input {**all** | **none** | **ssh** | **telnet**}
no transport input {**all** | **none** | **ssh** | **telnet**}

Syntax Description

all	Specifies the Secure Shell (SSH) and Telnet protocols.
none	Specifies that the router rejects incoming SSH and Telnet transport protocol connections.
ssh	Specifies the SSH transport protocol.
telnet	Specifies the Telnet transport protocol.

Command Default

All protocols are allowed on the line.

Command Modes

Line console configuration

Line default configuration

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

To be accepted, incoming network connections to an asynchronous port (terminal line) must use a transport protocol specified with the **transport input** command. This command can be useful in limiting the acceptable transport protocols to include or exclude those used by different types of users, or to restrict a line to secure connections (SSH connections).

Task ID

Task ID	Operations
tty-access	read, write

This example shows how to set the transport input setting for the default line template to SSH connections:

```
RP/0/RSP0/CPU0:router(config)# line default
RP/0/RSP0/CPU0:router(config-line)# transport input ssh
```

Related Commands

Command	Description
transport output	Determines the protocols that can be used for outgoing connections from a line.
transport preferred	Specifies the transport protocol that Cisco IOS XR software uses if the user does not specify one when initiating a connection.

transport output

To specify the transport protocols that can be used for outgoing connections from a line, use the **transport output** command in the appropriate line configuration mode. To change or remove the protocol, use the **no** form of this command.

transport output {**all** | **none** | **ssh** | **telnet**}
no transport output {**all** | **none** | **ssh** | **telnet**}

Syntax Description

all	Specifies the Secure Shell (SSH) and Telnet transport protocols.
none	Specifies that the router rejects outgoing SSH and Telnet transport protocol connections.
ssh	Specifies the SSH transport protocol.
telnet	Specifies the Telnet transport protocol.

Command Default

All protocols are allowed on the line.

Command Modes

Line console configuration

Line default configuration

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

Any settings made with the **transport output** command override settings made with the **transport preferred** command.

Task ID

Task ID	Operations
tty-access	read, write

This example shows how to set the default line template to prevent any outgoing transport protocol connections:

```
RP/0/RSP0/CPU0:router(config)# line default
```

```
RP/0/RSP0/CPU0:router(config-line)# transport output none
```

Related Commands

Command	Description
transport input	Defines which protocols to use to connect to a specific line of the router.
transport preferred	Specifies the transport protocol that Cisco IOS XR software uses if the user does not specify one when initiating a connection.

transport preferred

To specify the default outgoing transport protocol to be used for initiating network connections, use the **transport preferred** command in the appropriate line configuration mode. To change or remove the protocol, use the **no** form of this command.

transport preferred {**none** | **ssh** | **telnet**}
no transport preferred {**none** | **ssh** | **telnet**}

Syntax Description

none	Disables the feature.
ssh	Specifies the Secure Shell (SSH) transport protocol.
telnet	Specifies the Telnet transport protocol.

Command Default

No transport protocol is set as the default outgoing protocol.

Command Modes

Line console configuration

Line default configuration

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **transport preferred** command to provide a default transport protocol to use when initiating outgoing connections. The preferred outgoing transport protocol specified with the **transport preferred** command enables you to initiate an outgoing connection without explicitly specifying the transport protocol.

Cisco IOS XR software assumes that any unrecognized command is a hostname and the software attempts a connection. When the protocol is set to **none**, the system ignores unrecognized commands entered at the EXEC prompt, and does not attempt a connection.

The default setting, the same as using the **transport preferred** command with the **none** keyword, prevents errant connection attempts.

Task ID

Task ID	Operations
tty-access	read, write

The following example shows how to set the preferred transport setting for the default line template to SSH:

```
RP/0/RSP0/CPU0:router(config)# line default
RP/0/RSP0/CPU0:router(config-line)# transport preferred ssh
```

Related Commands

Command	Description
transport input	Defines which protocols to use to connect to a specific line of the router.
transport output	Determines the protocols that can be used for outgoing connections from a line.

vty-pool

To create or modify a virtual terminal line (vty) pool, use the **vty-pool** command in

global configuration

mode. To delete a vty pool, use the **no** form of this command.

vty-pool {**default** | **eem***pool-name*} *first-vty last-vty* [**line-template** {**default***template-name*}]
no vty-pool {**default** | **eem***pool-name*} *first-vty last-vty* [**line-template** {**default***template-name*}]

Syntax Description

default	Specifies the default vty pool.
eem	Specifies the embedded event manager vty pool.
pool-name	User-defined vty pool.
first-vty	First vty line in the pool. • For the default vty pool, you must specify 0 for the first vty line. • For a user-defined vty pool, the range is 5 to 99. • For the embedded event manager vty pool, you must specify 100 for the first vty line.
last-vty	Last vty line in the pool. • The default vty pool must contain at least five vtys. Range is 4 to 99. • For a user-defined vty pool, the range is 5 to 99. • The embedded event manager vty pool must contain at least six vtys. Range is 105 to 199.
line-template	(Optional) Specifies the terminal template to be used in the configuration of virtual terminals in the vty pool.
default	Specifies that the vty pool should reference the default template.
template-name	User-defined template to be applied to the vtys in the vty pool.

Command Default

default *vty-pool* : 5 vtys (vty 0 through 4) referencing the default line template.

eem *vty pool* : 6 vtys (vty 100 through 105) referencing the default line template.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

When creating or modifying vty pools, follow these usage guidelines:

- Before creating or modifying the vty pools, enable the Telnet server using the **telnet server** command in global configuration mode. See *IP Addresses and Services Configuration Guide for Cisco ASR 9000 Series Routers* and *IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers* for more information.
- The vty range for the default vty pool must start at vty 0 and must contain a minimum of five vtys.
- The vty range from 0 through 99 can reference the default vty pool.
- The vty range from 5 through 99 can reference a user-defined vty pool.
- The vty range from 100 is reserved for the embedded event manager vty pool.
- The vty range for embedded event manager vty pools must start at vty 100 and must contain a minimum of six vtys.
- A vty can be a member of only one vty pool. A vty pool configuration fails if the vty pool includes a vty that is already in another pool.

If you attempt to remove an active vty from the active vty pool when configuring a vty pool, the configuration for that vty pool fails.

This example shows how to configure a user-defined vty pool (test1) that contains vtys 10 through14 and references the user-defined line template test2:

```
RP/0/RSP0/CPU0:router(config)# vty-pool test1 10 14 line-template test2
```

width (display)

To set the width of the display terminal, use the **width** command in the appropriate line configuration mode. To remove the **width** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

width *characters*
no width *characters*

Syntax Description

characters	Number of characters to display on a screen. Range is from 0 to 512.

Command Default

characters : 80

Command Modes

Line console configuration

Line default configuration

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **width** command to modify the default width setting for the specified line template.

Task ID

Task ID	Operations
tty-access	read, write

This example shows how to set the terminal width for the default line template to 99 characters:

```
RP/0/RSP0/CPU0:router(config)# line default
RP/0/RSP0/CPU0:router(config-line)# width 99
```

Related Commands

Command	Description
terminal width	Sets the width of the display terminal for the current terminal session.



Simple Network Management Protocol (SNMP) Server Commands

This chapter describes the Cisco IOS XR software commands used to configure and monitor the Simple Network Management Protocol (SNMP) for network monitoring and management.

For detailed information about SNMP concepts, configuration tasks, and examples, see the *Implementing SNMP on Cisco IOS XR Software* configuration module in *System Management Configuration Guide for Cisco ASR 9000 Series Routers*.

Note The **snmp-server** commands enable SNMP on Management Ethernet interfaces by default. For information about how to enable SNMP server support on other inband interfaces, see the *Implementing Management Plane Protection on Cisco IOS XR Software* module in *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

- add (bulkstat object), on page 331
- buffer-size, on page 332
- clear snmp counters, on page 333
- enable (bulkstat), on page 334
- format (bulkstat), on page 336
- index persistence, on page 338
- instance (bulkstat schema), on page 339
- instance range, on page 341
- instance repetition, on page 342
- notification linkupdown, on page 344
- object-list, on page 346
- poll-interval, on page 347
- retain, on page 348
- retry, on page 350
- schema, on page 352
- show snmp, on page 353
- show snmp context, on page 356
- show snmp context-mapping, on page 357
- show snmp engineid, on page 359

- show snmp entity, on page 360
- show snmp group, on page 363
- show snmp host, on page 365
- show snmp interface, on page 367
- show snmp interface notification, on page 369
- show snmp interface regular-expression, on page 371
- show snmp mib, on page 372
- show snmp mib bulkstat transfer, on page 375
- show snmp request duplicates, on page 377
- show snmp request incoming-queue detail, on page 378
- show snmp request type summary, on page 380
- show snmp request type detail, on page 382
- show snmp request drop summary, on page 383
- show snmp request overload stats, on page 385
- show snmp statistics oid group, on page 386
- show snmp statistics pdu, on page 388
- show snmp statistics slow oid, on page 390
- show snmp statistics poll oid all, on page 392
- Show snmp statistics poll oid nms, on page 394
- show snmp statistics slow oid [after/before] hh:mm:ss day mday year, on page 395
- show snmp mib ifmib general, on page 397
- show snmp mib ifmib cache, on page 399
- show snmp mib ifmib statsd, on page 401
- show snmp traps details, on page 403
- show snmp informs details, on page 405
- show snmp users, on page 407
- show snmp view, on page 409
- snmp-server chassis-id, on page 410
- snmp-server community, on page 411
- snmp-server community-map, on page 413
- snmp-server contact, on page 415
- snmp-server context, on page 416
- snmp-server context mapping, on page 417
- snmp-server drop report acl, on page 419
- snmp-server drop unknown-user, on page 420
- snmp-server engineid local, on page 421
- snmp-server engineid remote, on page 422
- snmp-server entityindex persist, on page 423
- snmp-server group, on page 424
- snmp-server host, on page 427
- snmp-server ifindex persist, on page 431
- snmp-server ifmib ifalias long, on page 432
- snmp-server ifmib internal cache max-duration, on page 433
- snmp-server ifmib ipsubscriber, on page 434
- snmp-server ifmib stats cache, on page 435
- snmp-server inform, on page 436

- snmp-server interface, on page 437
- snmp-server interface subset, on page 439
- snmp-server ipv4 dscp, on page 441
- snmp-server ipv4 precedence , on page 442
- snmp-server location, on page 444
- snmp-server mib bulkstat max-procmem-size, on page 445
- snmp-server mib bulkstat object-list, on page 446
- snmp-server mib bulkstat schema, on page 447
- snmp-server mib bulkstat transfer-id, on page 449
- snmp-server mibs cbqosmib cache, on page 451
- snmp-server mibs cbqosmib persist, on page 453
- snmp-server mibs eventmib congestion-control, on page 454
- snmp-server mibs eventmib packet-loss, on page 456
- snmp-server mibs sensormib cache, on page 458
- snmp-server mibs subscriber threshold, on page 459
- snmp-server mibs subscriber threshold access-if, on page 461
- snmp-server notification-log-mib, on page 463
- snmp-server packetsize, on page 465
- snmp-server queue-length, on page 466
- snmp-server target list, on page 467
- snmp-server throttle-time, on page 468
- snmp-server timeouts subagent, on page 469
- snmp-server timeouts duplicate, on page 470
- snmp-server trap authentication vrf disable, on page 471
- snmp-server trap link ietf, on page 472
- snmp-server trap throttle-time, on page 473
- snmp-server traps, on page 474
- snmp-server traps bgp updown, on page 481
- snmp-server traps cbgp2 updown, on page 482
- snmp-server traps mpls l3vpn, on page 483
- snmp-server traps ospf errors, on page 485
- snmp-server traps ospf lsa, on page 487
- snmp-server traps ospf retransmit, on page 489
- snmp-server traps ospf state-change, on page 491
- snmp-server traps ospfv3 errors, on page 493
- snmp-server traps ospfv3 state-change, on page 495
- snmp-server traps pim interface-state-change, on page 497
- snmp-server traps pim invalid-message-received, on page 499
- snmp-server traps pim neighbor-change, on page 501
- snmp-server traps pim rp-mapping-change, on page 503
- snmp-server traps rsvp, on page 505
- snmp-server traps selective-vrf-download role-change, on page 506
- snmp-server traps snmp, on page 507
- snmp-server traps syslog, on page 509
- snmp-server trap-source, on page 510
- snmp-server traps subscriber session-aggregation, on page 512

- snmp-server traps updown, on page 513
- snmp-server trap-timeout, on page 515
- snmp-server user, on page 516
- snmp-server view, on page 519
- snmp-server vrf, on page 521
- snmp test trap all, on page 523
- snmp test trap entity, on page 525
- snmp test trap infra, on page 527
- snmp test trap interface, on page 529
- snmp test trap snmp, on page 530
- transfer-interval, on page 531
- url, on page 533

add (bulkstat object)

To add a MIB object to a Simple Network Management Protocol (SNMP) bulk statistics object list, use the **add** command in bulk statistics object list configuration mode. To remove a MIB object from an SNMP bulk statistics object list, use the **no** form of this command.

add {*object-nameOID*}
no add {*object-nameOID*}

Syntax Description

object-name	Name of the MIB object to add to the list. Object names are limited to those with mappings shown in the **show snmp mib object-name** command.
OID	Object identifier (OID) of the MIB object to add to the list.

Command Default

No MIB objects are configured for an object list.

Command Modes

Bulk statistics object list configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

All object names and OIDs in a single object list should belong to the same MIB index, but the objects need not belong to the same MIB table. For example, it is possible to group ifInoctets and a CISCO-IF-EXTENSION-MIB object in the same schema because the containing tables are indexed by the ifIndex (in the IF-MIB).

The **add** command should be repeated as necessary until all MIB objects have been added to the object list.

Task ID

Task ID	Operation
snmp	read, write

The following example shows how to add various MIB objects to an object list.

```
RP/0/RSP0/CPU0:router(config-bulk-objects)# add 1.3.6.1.2.1.2.2.1.11
RP/0/RSP0/CPU0:router(config-bulk-objects)# add ifAdminStatus
RP/0/RSP0/CPU0:router(config-bulk-objects)# add ifDescr
```

Related Topics

show snmp mib, on page 372

buffer-size

To configure a maximum buffer size for the transfer of bulk statistics files, use the **buffer-size** command in bulk statistics transfer configuration mode. To remove a previously configured buffer size from the configuration, use the **no** form of this command.

buffer-size *bytes*
no buffer-size [*bytes*]

Syntax Description

bytes	Size of the bulk statistics transfer buffer, in bytes. The valid range is from 1024 to 2147483647. The default is 2048.

Command Default

The default bulk statistics transfer buffer is 2048 bytes.

Command Modes

Bulk statistics transfer configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

A configured buffer size limit is available primarily as a safety feature. Normal bulk statistics files should not generally meet or exceed the default value while being transferred.

Task ID

Task ID	Operation
snmp	read, write

This example shows how to set the buffer size to 1024 bytes:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat transfer bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# buffer-size 1024
```

clear snmp counters

To clear the Simple Network Management Protocol (SNMP) packet statistics shown by the **show snmp** command, use the **clear snmp counters** command in EXEC mode.

clear snmp counters

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

The **clear snmp counters** command provides the ability to clear all SNMP counters used in the **show snmp** command without restarting any processes.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to clear the SNMP counters:

```
RP/0/RSP0/CPU0:router# clear snmp counters
```

Related Topics

show snmp, on page 353

enable (bulkstat)

To begin the bulk statistics data collection and transfer process for a specific bulk statistics configuration, use the **enable** command in bulk statistics transfer configuration mode. To disable the bulk statistics data collection and transfer process for a specific bulk statistics configuration, use the **no** form of this command.

enable
no enable

Syntax Description

This command has no keywords or arguments.

Command Default

Bulk statistics transfer is disabled.

Command Modes

Bulk statistics transfer configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Specific bulk statistics configurations are identified with a name, as specified in the **snmp-server mib bulkstat transfer-id** command. The **enable** command begins the periodic MIB data collection and transfer process.

Collection (and subsequent file transfer) starts only if this command is used. Conversely, the **no enable** command stops the collection process. Subsequently, issuing the **enable** command starts the operations again.

Each time the collection process is started using the **enable** command, data is collected into a new bulk statistics file. When the **no enable** command is used, the transfer process for any collected data immediately begins (in other words, the existing bulk statistics file are transferred to the specified management station).

To successfully enable a bulk statistics configuration, at least one schema with a non-zero number of objects must be configured.

Task ID

Task ID	Operation
snmp	read, write

The following example shows the bulk statistics transfer configuration named bulkstat1 as enabled:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat transfer bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# schema ATM2/0-IFMIB
RP/0/RSP0/CPU0:router(config-bulk-tr)# url primary ftp://user:pswrd@host/folder/bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# enable
RP/0/RSP0/CPU0:router(config-bulk-tr)# exit
```

Related Topics

show snmp mib bulkstat transfer, on page 375
snmp-server mib bulkstat transfer-id, on page 449

format (bulkstat)

To specify the format to be used for the bulk statistics data file, use the **format** command in bulk statistics transfer configuration mode. To disable a previously configured format specification and return to the default, use the **no** form of this command.

format {**bulkBinary** | **bulkASCII** | **schemaASCII**}
no format [**bulkBinary** | **bulkASCII** | **schemaASCII**]

Syntax Description

bulkBinary	Binary format.
bulkASCII	ASCII format.
schemaASCII	A human-readable ASCII format that contains additional bulk statistics schema tags. This is the default.

Command Default

The default bulk statistics transfer format is schemaASCII

Command Modes

Bulk statistics transfer configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

The bulk statistics data file (VFile) contains two types of fields: tags and data. Tags are used to set off data to distinguish fields of the file. All other information is in data fields.

Transfers can only be performed using schemaASCII format.

For each transfer/schema pair there is a header with tags for each object collected, followed by the collected data. For example, if the transfer name is T1 and the schemas in it are S1 (which collects ifInOctets and ifOutOctets) and S2 (which collects ifInUcastPkts and ifInDiscards). Then the output file looks like this:

```
Schema-def cempt1.cempWild "%u, %s, %s, %d" Epochtime instanceoid
1.3.6.1.4.1.9.9.221.1.1.1.1.3 1.3.6.1.4.1.9.9.221.1.1.1.1.2
cempt1.cempWild: 1339491515, 8695772.1, processor, 2
cempt1.cempWild: 1339491515, 8695772.2, reserved, 11
cempt1.cempWild: 1339491515, 8695772.3, image, 12
cempt1.cempWild: 1339491575, 8695772.1, processor, 2
cempt1.cempWild: 1339491575, 8695772.2, reserved, 11
cempt1.cempWild: 1339491575, 8695772.3, image, 12
Schema-def cempt1.cempRepeat "%u, %s, %s, %d" Epochtime instanceoid
1.3.6.1.4.1.9.9.221.1.1.1.1.3 1.3.6.1.4.1.9.9.221.1.1.1.1.2
cempt1.cempRepeat: 1339491515, 8695772.1, processor, 2
cempt1.cempRepeat: 1339491515, 8695772.2, reserved, 11
cempt1.cempRepeat: 1339491515, 8695772.3, image, 12
cempt1.cempRepeat: 1339491515, 26932192.1, processor, 2
cempt1.cempRepeat: 1339491515, 26932192.2, reserved, 11
cempt1.cempRepeat: 1339491515, 26932192.3, image, 12
```

```
cempt1.cempRepeat: 1339491515, 35271015.1, processor, 2
cempt1.cempRepeat: 1339491515, 35271015.2, reserved, 11
cempt1.cempRepeat: 1339491515, 35271015.3, image, 12
cempt1.cempRepeat: 1339491515, 36631989.1, processor, 2
cempt1.cempRepeat: 1339491515, 36631989.2, reserved, 11
cempt1.cempRepeat: 1339491515, 36631989.3, image, 12
cempt1.cempRepeat: 1339491515, 52690955.1, processor, 2
cempt1.cempRepeat: 1339491515, 52690955.2, reserved, 11
cempt1.cempRepeat: 1339491515, 52690955.3, image, 12
```

Task ID

Task ID	Operation
snmp	read, write

This example shows how to specify the data format:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat transfer bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# format schemaASCII
```

Related Topics

show snmp mib bulkstat transfer, on page 375
snmp-server mib bulkstat transfer-id, on page 449

index persistence

To enable index persistence on an Simple Network Management Protocol (SNMP) interface, use the **index persistence** command in SNMP interface configuration mode. To restore the default conditions with respect to this command, use the **no** form of this command.

index persistence
no index persistence

Syntax Description

This command has no keywords or arguments.

Command Default

Index persistence is disabled.

Command Modes

SNMP interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **index persistence** command to enable ifIndex persistence for individual entries (corresponding to individual interfaces) in the ifIndex table of the IF-MIB. IfIndex persistence retains the mapping between the ifName object values and the ifIndex object values (generated from the IF-MIB) across reboots, allowing for consistent identification of specific interfaces using SNMP.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to assign ifIndex persistence on interface 0/0/1/0:

```
RP/0/RSP0/CPU0:router(config)# snmp-server interface tengige 0/0/1/0
RP/0/RSP0/CPU0:router(config-snmp-if)# index persistence
```

Related Topics

show snmp interface, on page 367
snmp-server engineid local, on page 421
snmp-server ifindex persist, on page 431
snmp-server interface, on page 437

instance (bulkstat schema)

To configure the MIB object instances to be used in a Simple Network Management Protocol (SNMP) bulk statistics schema, use the **instance** command in bulk statistics configuration mode. To remove the instance definition, use the **no** form of this command.

instance {**exact** | **wild** } {**interface** *interface-id* [**sub-if**] | **oid** *oid*}
no instance

Syntax Description

exact	Specifies that the specified interface or object identifier (OID), when appended to the object list, is the complete OID to be used in this schema.
wild	Specifies that all instances that fall within the the specified OID or interface are included in this schema.
interface *interface-id*	Specifies an interface to be used to define the schema instance.
[**sub-if**]	(Optional) Specifies that the object instances are polled for all subinterfaces of the specified interface in addition to the object instances for the main interface.
oid *oid*	Specifies an OID to be used to define the schema instance.

Command Default

No instances are configured.

Command Modes

Bulk statistics schema configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

The **instance** command specifies the instance information for objects in the schema being configured. The specific instances of MIB objects for which data is collected are determined by appending the value of the instance command to the objects specified in the associated object list. In other words, the schema object-list when combined with the schema instance specifies a complete MIB object identifier.

The **instance exact** command indicates that the specified instance, when appended to the object list, is the complete OID.

The **instance wild** command indicates that all subindices of the specified OID belong to this schema. For example, the command `instance wild oid 1` includes all subindices of the instance, such as 1.1, 1.2 and so on. It does not include other instances that start with the number 1, such as 10 and 11.

Instead of specifying an OID, you can specify a specific interface. The **interface** *interface-id* keyword and argument allow you to specify an interface name and number (for example, gigabitethernet 0/6/5/0) instead of specifying the ifIndex OID for the interface.

The optional **sub-if** keyword, when added after specifying an interface, includes the ifIndexes for all subinterfaces of the interface you specified.

Only one **instance** command can be configured per schema. If multiple **instance** commands are used, the later commands overwrite the earlier ones.

Task ID

Task ID	Operation
snmp	read, write

The following examples show two different ways to configure an instance.

```
RP/0/RSP0/CPU0:router(config-bulk-sc)# instance wild oid 1
```

```
RP/0/RSP0/CPU0:router(config-bulk-sc)# instance exact interface FastEthernet 0/1.25
```

Related Topics

instance range, on page 341
instance repetition, on page 342
snmp-server mib bulkstat schema, on page 447

instance range

To specify a range of instances for objects in a schema, use the **instance** command in bulk statistics schema configuration mode. To remove the configured instance information, use the **no** form of this command.

instance range start *start-oid* **end** *end-oid*
no instance

Syntax Description

start *start-oid*	Specifies the first OID value of a range of values.
end *end-oid*	Specifies the last OID value of a range of values.

Command Default

No instances are configured.

Command Modes

Bulk statistics schema configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Only one **instance** command can be configured per schema. If multiple **instance** commands are used, the later commands overwrite the earlier ones.

Task ID

Task ID	Operation
snmp	read, write

The following example shows how to configure a range of instances.

```
RP/0/RSP0/CPU0:router(config-bulk-sc)# instance range start 1 end 2
```

Related Topics

instance (bulkstat schema), on page 339
snmp-server mib bulkstat schema, on page 447

instance repetition

To configure bulk statistics data collection to begin at a particular instance of a MIB object and to repeat for a given number of instances , use the **instance repetition** command in bulk statistics schema configuration mode. To delete a previously configured repetition of instances, use the **no** form of this command.

instance repetition *oid-instance* **max** *repeat-number*
no instance

Syntax Description

oid-instance	Object ID of the instance to be monitored.
max *repeat-number*	Specifies the number of times the instance should repeat.

Command Default

No instance repetition is configured.

Command Modes

Bulk statistics schema configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

The **instance repetition** command is used to configure data collection to repeat for a certain number of instances of a MIB object.

Only one **instance** command can be configured per schema. If multiple **instance** commands are used, the later commands overwrite the earlier ones.

Task ID

Task ID	Operation
snmp	read, write

The following example configures 4 repetitions of the OID of value 1.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat object-list ifmib
RP/0/RSP0/CPU0:router(config-bulk-objects)# add ifOutOctets
RP/0/RSP0/CPU0:router(config-bulk-objects)# add ifInOctets

RP/0/RSP0/CPU0:router(config-bulk-objects)# exit
RP/0/RSP0/CPU0:router(config)# snmp mib-server bulkstat schema IFMIB

RP/0/RSP0/CPU0:router(config-bulk-sc)# object-list ifmib
RP/0/RSP0/CPU0:router(config-bulk-sc)# poll-interval 1
```

```
RP/0/RSP0/CPU0:router(config-bulk-sc)# instance repetition 1 max 4
```

Related Topics

instance (bulkstat schema), on page 339
instance range, on page 341
snmp-server mib bulkstat schema, on page 447

notification linkupdown

To enable or disable linkUp and linkDown trap notifications on a Simple Network Management Protocol (SNMP) interface, use the **notification linkupdown** command in SNMP interface configuration mode. To revert to the default setting, use the **no** form of this command.

notification linkupdown disable
no notification linkupdown disable

Syntax Description

disable	Disables linkUp and linkDown trap notifications on an SNMP interface.

Syntax Description

This command has no keywords or arguments.

Command Default

By default, for all main interfaces the linkUp and linkDown trap notifications are enabled; for all subinterfaces they are disabled.

Command Modes

SNMP interface configuration

SNMP interface subset configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 3.9.0	This command was supported in the SNMP interface subset configuration mode.

Usage Guidelines

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

Enabling of linkUp and linkDown notifications is performed globally using the **snmp-server traps snmp** command. Issue the **notification linkupdown** command to disable linkUp and linkDown notifications on an interface.

Use the **no** form of this command to enable linkUp and linkDown notifications on an interface, if linkUp and linkDown notifications have been disabled.

You can also use the **snmp-server interface subset** command to enable or disable groups of interfaces.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to disable linkUp and linkDown trap notifications on interface 0/0/1/0:

```
RP/0/RSP0/CPU0:router(config)# snmp-server interface tengige 0/0/1/0
RP/0/RSP0/CPU0:router(config-snmp-if)# notification linkupdown disable
```

Related Topics

show snmp interface, on page 367
snmp-server engineid local, on page 421
snmp-server ifindex persist, on page 431
snmp-server interface, on page 437
snmp-server interface subset, on page 439
snmp-server traps snmp, on page 507

object-list

To specify the bulk statistics object list to be used in the bulk statistics schema, use the **object-list** command in bulk statistics schema configuration mode. To remove an object list from the schema, use the **no** form of this command.

object-list *list-name*
no object-list [*list-name*]

Syntax Description

list-name	Name of a previously configured bulk statistics object list.

Command Default

No bulk statistics object list is specified.

Command Modes

Bulk statistics schema configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

This command associates a bulk statistics object list with the schema being configured. The object list should contain a list of MIB objects to be monitored. Only one object list can be specified for each schema. Use the **snmp-server mib bulkstat object-list** command to create an object list.

Task ID

Task ID	Operation
snmp	read, write

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat schema schema1
RP/0/RSP0/CPU0:router(config-bulk-sc)# object-list obj1
```

Related Topics

show snmp mib bulkstat transfer, on page 375
snmp-server mib bulkstat schema, on page 447
snmp-server mib bulkstat object-list, on page 446

poll-interval

To configure the polling interval for a bulk statistics schema, use the **poll-interval** command in bulk statistics schema configuration mode. To remove a previously configured polling interval, use the **no** form of this command.

poll-interval *minutes*
no poll-interval

Syntax Description

minutes	Integer in the range from 1 to 20000 that specifies, in minutes, the polling interval of data for this schema. The default is 5.

Command Default

Object instances are polled once every five minutes.

Command Modes

Bulk statistics schema configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

The **poll-interval** command sets how often the MIB instances specified by the schema and associated object list are to be polled. Collected data is stored in the local bulk statistics file for later transfer.

Task ID

Task ID	Operation
snmp	read, write

In this example, the polling interval for bulk statistics collection is set to once every 3 minutes in the schema called GigE2/1-CAR:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulk schema GigE2/1-CAR
RP/0/RSP0/CPU0:router(config-bulk-sc)# poll-interval 3
```

Related Topics

snmp-server mib bulkstat schema, on page 447

retain

To configure the retention interval for bulk statistics files, use the **retain** command in bulk statistics transfer configuration mode. To remove a previously configured retention interval from the configuration, use the **no** form of this command.

retain *minutes*
no retain [*minutes*]

Syntax Description

minutes	Length of time, in minutes, that the local bulk statistics file should be kept in system memory (the retention interval). The valid range is 0 to 20000. The default is 0.

Command Default

The bulk statistics file retention interval is 0 minutes.

Command Modes

Bulk statistics transfer configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

The **retain** command specifies how long the bulk statistics file should be kept in system memory, in minutes, after the completion of the collection interval and a transmission attempt is made. The default value of zero (0) indicates that the file is deleted immediately from local memory after a successful transfer.

If the **retry** command is used, you should configure a retention interval greater than 0. The interval between retries is the retention interval divided by the retry number. For example, if **retain 10** and **retry 2** are configured, retries are attempted once every 5 minutes. Therefore, if the **retain** command is not configured (retain default is 0), no retries are attempted.



Note Once a successful transmission has occurred the bulk file is not retained regardless of the retain time.

Task ID

Task ID	Operation
snmp	read, write

In the following example, the bulk statistics transfer retention interval is set to 10 minutes:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat transfer bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# schema ATM2/0-IFMIB
```

```
RP/0/RSP0/CPU0:router(config-bulk-tr)# url primary ftp://user:pswrd@host/folder/bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# retry 2
RP/0/RSP0/CPU0:router(config-bulk-tr)# retain 10
RP/0/RSP0/CPU0:router(config-bulk-tr)# exit
```

Related Topics

retry, on page 350
show snmp mib bulkstat transfer, on page 375
snmp-server mib bulkstat transfer-id, on page 449

retry

To configure the number of retries that should be attempted for a bulk statistics file transfer, use the **retry** command in bulk statistics transfer configuration mode. To return the number of bulk statistics retries to the default, use the **no** form of this command.

retry *number*
no retry [*number*]

Syntax Description

number	Number of transmission retries. The valid range is from 0 to 100.

Command Default

No retry attempts are made.

Command Modes

Bulk statistics transfer configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

If an attempt to send the bulk statistics file fails, the system can be configured to attempt to send the file again using the **retry** command. One retry includes an attempt first to the primary destination and then, if the transmission fails, to the secondary location; for example, if the retry value is 1, an attempt will be made first to the primary URL, then to the secondary URL, then to the primary URL again, and then to the secondary URL again.

If the **retry** command is used, you should also use the **retain** command to configure a retention interval greater than 0. The interval between retries is the retention interval divided by the retry number. For example, if **retain 10** and **retry 2** are configured, retries are attempted once every 5 minutes. Therefore, if the **retain** command is not configured (or the **retain 0** command is used) no retries are attempted.

Task ID

Task ID	Operation
snmp	read, write

In the following example, the number of retries for the bulk statistics transfer is set to 2:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat transfer bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# schema ATM2/0-IFMIB
RP/0/RSP0/CPU0:router(config-bulk-tr)# url primary ftp://user:pswrd@host/folder/bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# retry 2
RP/0/RSP0/CPU0:router(config-bulk-tr)# retain 10
```

```
RP/0/RSP0/CPU0:router(config-bulk-tr)# exit
```

Related Topics

retain, on page 348
show snmp mib bulkstat transfer, on page 375
snmp-server mib bulkstat transfer-id, on page 449

schema

To specify the bulk statistics schema to be used in a specific bulk statistics transfer configuration, use the **schema** command in bulk statistics transfer configuration mode. To remove a previously configured schema from a specific bulk statistics transfer configuration, use the **no** form of this command.

schema *schema-name*
no schema [*schema-name*]

Syntax Description

schema-name	Name of a previously configured bulk statistics schema.

Command Default

No bulk statistics schema is specified.

Command Modes

Bulk statistics transfer configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

The schema must be previously defined using the **snmp-server mib bulkstat schema** command.

Repeat the **schema** command as desired for a specific bulk statistics transfer configuration. Multiple schemas can be associated with a single transfer configuration; all collected data will be in a single bulk statistics data file (VFile).

Task ID

Task ID	Operation
snmp	read, write

This example adds three different schemas to a bulk statistics transfer configuration:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat transfer-id bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# schema ATM2/0-IFMIB
RP/0/RSP0/CPU0:router(config-bulk-tr)# schema ATM2/0-CAR
RP/0/RSP0/CPU0:router(config-bulk-tr)# schema Ethernet2/1-IFMIB
```

Related Topics

show snmp mib bulkstat transfer, on page 375
snmp-server mib bulkstat schema, on page 447

show snmp

To display the status of Simple Network Management Protocol (SNMP) communications, use the **show snmp** command in

EXEC

mode.

show snmp

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the `show snmp` command to show counter information for SNMP operations. It also displays the chassis ID string defined with the **snmp-server chassis-id** command.

Task ID

Task ID	Operations
snmp	read

This example shows sample output from the `show snmp` command:

```
RP/0/RSP0/CPU0:router# show snmp

  Chassis: 01506199
  37 SNMP packets input
  0 Bad SNMP version errors
  4 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  24 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  28 Get-next PDUs
  0 Set-request PDUs
  78 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
```

```
24 Response PDUs
13 Trap PDUs
SNMP logging: enabled
Logging to 172.25.58.33.162, 0/10, 13 sent, 0 dropped.
```

Table 25: show snmp Field Descriptions, on page 354 describes the significant fields shown in the display.

Table 25: show snmp Field Descriptions

Field	Description
Chassis	Chassis ID string.
SNMP packets input	Total number of SNMP packets input.
Bad SNMP version errors	Number of packets with an invalid SNMP version.
Unknown community name	Number of SNMP packets with an unknown community name.
Illegal operation for community name supplied	Number of packets requesting an operation not allowed for that community.
Encoding errors	Number of SNMP packets that were improperly encoded.
Number of requested variables	Number of variables requested by SNMP managers.
Number of altered variables	Number of variables altered by SNMP managers.
Get-request PDUs	Number of get requests received
Get-next PDUs	Number of get-next requests received.
Set-request PDUs	Number of set requests received.
SNMP packets output	Total number of SNMP packets sent by the device.
Too big errors	Number of SNMP packets that were larger than the maximum packet size.
Maximum packet size	Maximum size of SNMP packets.
No such name errors	Number of SNMP requests that specified a MIB object that does not exist.
Bad values errors	Number of SNMP set requests that specified an invalid value for a MIB object.
General errors	Number of SNMP set requests that failed due to some other error. (It is not a noSuchName error, badValue error, or any of the other specific errors.)
Response PDUs	Number of responses sent in reply to requests.
Trap PDUs	Number of SNMP traps sent.

Field	Description
SNMP logging	Enabled or disabled logging.
sent	Number of traps sent.
dropped	Number of traps dropped. Traps are dropped when the trap queue for a destination exceeds the maximum length of the queue, as set by the **snmp-server queue-length** command.

Related Topics

show snmp mib, on page 372
snmp-server chassis-id, on page 410
snmp-server queue-length, on page 466

show snmp context

To display the enhanced SNMP context mappings, use the **show snmp context** command in EXEC mode.

show snmp context

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Use the **show snmp context** command to display the protocol instance, topology and VRF mappings associated with an SNMP context.

Task ID

Task ID	Operation
snmp	read

This example illustrates sample output from the **show snmp context** command:

```
RP/0/RSP0/CPU0:router# show snmp context

Tue Dec 21 03:41:08.065 PST
Context-name       Vrf-name      Topology-Name   Instance-Name             Feature
con5                  vf5           tp5             in5                     OSPF
con6                  vf6           tp6             in6                     OSPF
con7                  vf7           tp7             in7                     OSPF
con8                  vf8           tp8             in8                     OSPF
```

Related Topics

snmp-server context mapping, on page 417

show snmp context-mapping

To display the SNMP context mapping table, use the **show snmp context-mapping** command in

EXEC

mode.

show snmp context-mapping

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

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

The SNMP agent handles queries based on SNMP contexts created by client features. Use the **show snmp context-mapping** command to display the SNMP context mapping table. Each entry in the table includes the name of an SNMP context created by a client instance and the name of the client that created the context.

Task ID

Task ID	Operations
snmp	read

The following example shows sample output from the **show snmp context-mapping** command:

```
RP/0/RSP0/CPU0:router# show snmp context-mapping

Wed Aug 6 01:42:35.227 UTC
Context-name                  Feature-name                  Feature
ControlEthernet0_RP0_CPU0_S0  ControlEthernet0_RP0_CPU0_S0  BRIDGEINST
ControlEthernet0_RP1_CPU0_S0     ControlEthernet0_RP1_CPU0_S0     BRIDGEINST
```

Table 26: show snmp context-mapping Field Descriptions

Field	Definition
Context-name	Name of an SNMP context.
Feature-name	Name of the instance that created the context.

Field	Definition
Feature	Name of the client whose instance created the context.

show snmp engineid

To display the identification of the local Simple Network Management Protocol (SNMP) engine that has been configured on the router, use the **show snmp engineid** command in EXEC mode.

show snmp engineid

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

An *SNMP engine* is a copy of SNMP that can reside on a local device.

Task ID

Task ID	Operations
snmp	read

The following example shows sample output from the **show snmp engineid** command:

```
RP/0/RSP0/CPU0:router# show snmp engineid

  Local SNMP engineID: 000000090200000000C025808
```

Related Topics

snmp-server engineid local, on page 421

show snmp entity

To display the entPhysicalName and entPhysicalIndex mappings, use the **show snmp entity** command in

EXEC

mode.

show snmp entity

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

Use the **show snmp entity** command to view the entity index to use in the **snmp test trap entity** command. To use the **show snmp entity** command, SNMP must be configured on the router.

Task ID

Task ID	Operation
snmp	read

This example illustrates sample output from the **show snmp entity** command:

```
RP/0/RSP0/CPU0:router# show snmp entity

Thu Aug 13 02:10:06.741 UTC
entPhysicalIndex:      22001 entPhysicalName: portslot 0/0/CPU0/7
entPhysicalIndex:      23006 entPhysicalName: portslot 0/0/CPU0/129
entPhysicalIndex:      23557 entPhysicalName: portslot 0/0/CPU0/3
entPhysicalIndex:      47719 entPhysicalName: 0/0/* - ingresspse - 1.2V
entPhysicalIndex:     320862 entPhysicalName: 0/0/* - host - 5V_C
entPhysicalIndex:     322450 entPhysicalName: 0/0/* - host - 1.5V
entPhysicalIndex:     428209 entPhysicalName: 0/PL2/*
entPhysicalIndex:    1038801 entPhysicalName: 0/0/* - ingressq - 2.5V
entPhysicalIndex:    1040485 entPhysicalName: 0/0/* - ingressq - 1.25V_0123
entPhysicalIndex:    1152042 entPhysicalName: 0/2/CPU0/7
entPhysicalIndex:    2031334 entPhysicalName: 0/SM0/* - host - Inlet1
entPhysicalIndex:    2032954 entPhysicalName: 0/SM0/* - host - 1.8V_L
entPhysicalIndex:    2034510 entPhysicalName: 0/SM0/* - host - brd-ok-led
entPhysicalIndex:    2110001 entPhysicalName: 0/PL2/* - plimasic - Exhaust0
entPhysicalIndex:    2111557 entPhysicalName: 0/PL2/* - plimasic - 1.8V
entPhysicalIndex:    2358084 entPhysicalName: 0/0/* - egressq
entPhysicalIndex:    2359704 entPhysicalName: 0/0/* - cpu
```

```
entPhysicalIndex:    2469162 entPhysicalName: 0/2/* - egressq - Hotspot0
entPhysicalIndex:    2559937 entPhysicalName: 0/0/* - egressq - 1.2V
entPhysicalIndex:    2577533 entPhysicalName: 0/2/CPU0/0
entPhysicalIndex:    2853020 entPhysicalName: 0/0/* - egressqse - 5V
entPhysicalIndex:    3497583 entPhysicalName: 0/SM1/* - host - brd-ok-led
entPhysicalIndex:    3500791 entPhysicalName: 0/SM1/* - host - Inlet1
 --More—
```

```
RP/0/RSP0/CPU0:router# show snmp entity

Mon Nov 15 11:19:23.609 UTC
entPhysicalIndex:     172193 entPhysicalName: portslot 0/0/CPU0/1
entPhysicalIndex:     322450 entPhysicalName: voltages 0/0/CPU0
entPhysicalIndex:     345071 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:     346659 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:     349835 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:     546880 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:     845998 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:     847586 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:    1192623 entPhysicalName: 0/25/CPU0
entPhysicalIndex:    1227530 entPhysicalName: voltages 0/21/CPU0
entPhysicalIndex:    1460256 entPhysicalName: temperatures 0/18/CPU0
entPhysicalIndex:    1795138 entPhysicalName: temperatures 0/20/CPU0
entPhysicalIndex:    3079213 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:    3080801 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:    3082421 entPhysicalName: slot 7/0
entPhysicalIndex:    5037675 entPhysicalName: 0/21/CPU0
entPhysicalIndex:    5509481 entPhysicalName: voltages 0/9/CPU0
entPhysicalIndex:    6182130 entPhysicalName: voltages 0/9/CPU0
entPhysicalIndex:    6369487 entPhysicalName: portslot 0/9/CPU0/2
entPhysicalIndex:    8392407 entPhysicalName: temperatures 0/17/CPU0
entPhysicalIndex:    8548798 entPhysicalName: 0/21/CPU0 - host
entPhysicalIndex:   10735504 entPhysicalName: voltages 0/1/CPU0
entPhysicalIndex:   10737188 entPhysicalName: voltages 0/1/CPU0
entPhysicalIndex:   10738808 entPhysicalName: slot 1/1
entPhysicalIndex:   11312388 entPhysicalName: slot 7
entPhysicalIndex:   11314008 entPhysicalName: slot 3
entPhysicalIndex:   12644344 entPhysicalName: voltages 0/19/CPU0
entPhysicalIndex:   12761695 entPhysicalName: slot 24
entPhysicalIndex:   12763283 entPhysicalName: slot 20
entPhysicalIndex:   12907576 entPhysicalName: voltages 0/0/CPU0
entPhysicalIndex:   13262622 entPhysicalName: slot 16
entPhysicalIndex:   13290941 entPhysicalName: temperatures 0/16/CPU0
entPhysicalIndex:   13404457 entPhysicalName: voltages 0/2/CPU0
entPhysicalIndex:   13406077 entPhysicalName: voltages 0/2/CPU0
entPhysicalIndex:   13701859 entPhysicalName: voltages 0/2/CPU0
entPhysicalIndex:   13900492 entPhysicalName: voltages 0/2/CPU0
entPhysicalIndex:   13903700 entPhysicalName: voltages 0/2/CPU0
entPhysicalIndex:   13905384 entPhysicalName: voltages 0/2/CPU0
entPhysicalIndex:   14106204 entPhysicalName: portslot 0/8/CPU0/2
entPhysicalIndex:   14256525 entPhysicalName: voltages 0/8/CPU0
entPhysicalIndex:   14979942 entPhysicalName: slot 2/2
entPhysicalIndex:   14981562 entPhysicalName: voltages 0/2/CPU0
entPhysicalIndex:   15141782 entPhysicalName: 0/19/CPU0
entPhysicalIndex:   15873651 entPhysicalName: temperatures 0/22/CPU0
entPhysicalIndex:   15986678 entPhysicalName: voltages 0/1/CPU0
entPhysicalIndex:   15988234 entPhysicalName: voltages 0/1/CPU0
entPhysicalIndex:   15991442 entPhysicalName: voltages 0/1/CPU0
entPhysicalIndex:   16136999 entPhysicalName: voltages 0/1/CPU0
entPhysicalIndex:   16138619 entPhysicalName: voltages 0/1/CPU0
entPhysicalIndex:   16285636 entPhysicalName: temperatures 0/1/CPU0
entPhysicalIndex:   16287256 entPhysicalName: voltages 0/1/CPU0
entPhysicalIndex:   16606045 entPhysicalName: voltages 0/8/CPU0
```

```
entPhysicalIndex:   16607633 entPhysicalName: voltages 0/8/CPU0
entPhysicalIndex:   16733769 entPhysicalName: 0/2/CPU0 - host
entPhysicalIndex:   16949774 entPhysicalName: portslot 0/0/CPU0/0
entPhysicalIndex:   17098539 entPhysicalName: temperatures 0/0/CPU0
entPhysicalIndex:   17122684 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:   17124272 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:   17127448 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:   17205790 entPhysicalName: 0/2/CPU0
entPhysicalIndex:   17322905 entPhysicalName: temperatures 0/7/CPU0
entPhysicalIndex:   17324589 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:   17595466 entPhysicalName: 0/25/CPU0 - host
entPhysicalIndex:   17620307 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:   17621991 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:   17623611 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:   18003523 entPhysicalName: temperatures 0/21/CPU0
entPhysicalIndex:   18237837 entPhysicalName: voltages 0/18/CPU0
entPhysicalIndex:   18571163 entPhysicalName: voltages 0/20/CPU0
---More---
```

show snmp group

To display the names of groups on the router, security model, status of the different views, and storage type of each group, use the **show snmp group** command in

EXEC

mode.

show snmp group

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
snmp	read

This example shows sample output from the **show snmp group** command:

```
RP/0/RSP0/CPU0:router# show snmp group

  groupname: public security model:snmpv1
  readview : v1default writeview: -
  notifyview: v1default
  row status: nonVolatile

  groupname: public security model:snmpv2c
  readview : v1default writeview: -
  notifyview: v1default
  row status: nonVolatile
```

Table 27: show snmp group Field Descriptions

Field	Definition
groupname	Name of the Simple Network Management Protocol (SNMP) group or collection of users that have a common access policy.

Field	Definition
readview	String identifying the read view of the group.
security model	Security model used by the group, either v1, v2c, or v3.
writeview	String identifying the write view of the group.
notifyview	String identifying the notify view of the group.
row status	Settings that are set in volatile or temporary memory on the device, or in nonvolatile or persistent memory where settings remain after the device is turned off and on again.

Related Topics

snmp-server group, on page 424

show snmp host

To display the configured Simple Network Management Protocol (SNMP) notification recipient host, User Datagram Protocol (UDP) port number, user, and security model, use the **show snmp host** command in

EXEC

mode.

show snmp host

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
snmp	read

The following example shows sample output from the **show snmp host** command:

```
RP/0/RSP0/CPU0:router# show snmp host

  Notification host: 10.50.32.170 udp-port: 2345 type: trap
  user: userV3auth security model: v3 auth

  Notification host: 10.50.32.170 udp-port: 2345 type: trap
  user: userV3noauth security model: v3 noauth

  Notification host: 10.50.32.170 udp-port: 2345 type: trap
  user: userV3priv security model: v3 priv

  Notification host: 10.50.32.170 udp-port: 2345 type: trap
  user: userv2c security model: v2c
```

Table 28: show snmp host Field Descriptions

Field	Definition
Notification host	Name or IP address of target host.
udp-port	UDP port number to which notifications are sent.
type	Type of notification configured.
user	Security level of the user.
security model	Version of SNMP used to send the trap, either v1, v2c, or v3.

show snmp interface

To display the interface index identification numbers (ifIndex values) for all the interfaces or a specified interface, use the **show snmp interface** command in the appropriate mode.

show snmp interface [*type interface-path-id* **ifindex**]

Syntax Description

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.
ifindex	(Optional) Displays the ifIndex value for the specified interface.

Command Default

Enter the **show snmp interface** command without keywords or arguments to display the ifIndex value for all interfaces.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
snmp	read

This example displays the ifIndex value for a specific interface:

```
RP/0/RSP0/CPU0:router# show snmp interface pos 0/1/0/1 ifindex

ifName : POS0/1/0/1            ifIndex : 12
```

The following example displays the ifIndex value for all interfaces:

```
RP/0/RSP0/CPU0:router# show snmp interface
```

```
ifName : Loopback0             ifIndex : 1
ifName : POS0/1/0/1            ifIndex : 12
ifName : POS0/1/4/2            ifIndex : 14
ifName : POS0/1/4/3            ifIndex : 15
ifName : POS0/6/0/1            ifIndex : 2
ifName : POS0/6/4/4            ifIndex : 18
ifName : POS0/6/4/5            ifIndex : 19
ifName : POS0/6/4/6            ifIndex : 20
ifName : Bundle-POS24          ifIndex : 4
ifName : Bundle-Ether28        ifIndex : 5
ifName : Bundle-Ether28.1      ifIndex : 7
ifName : Bundle-Ether28.2      ifIndex : 8
ifName : Bundle-Ether28.3      ifIndex : 9
ifName : MgmtEth0/RP0/CPU0/0   ifIndex : 6
ifName : MgmtEth0/RP1/CPU0/0   ifIndex : 10
ifName : GigabitEthernet0/1/5/0  ifIndex : 11
ifName : GigabitEthernet0/1/5/1  ifIndex : 13
ifName : GigabitEthernet0/1/5/2  ifIndex : 3
ifName : GigabitEthernet0/6/5/1  ifIndex : 16
ifName : GigabitEthernet0/6/5/2  ifIndex : 17
ifName : GigabitEthernet0/6/5/7  ifIndex : 21
```

Table 29: show snmp interface Field Descriptions

Field	Definition
ifName	Interface name.
ifIndex	ifIndex value.

Related Topics

snmp-server ifindex persist, on page 431
snmp-server interface, on page 437

show snmp interface notification

To display the linkUp and linkDown notification status for a subset of interfaces, use the **show snmp interface notification** command in EXEC mode.

show snmp interface notification {**subset** *subset-number* | **regular-expression** *expression* | [*type interface-path-id*]}

Syntax Description

subset *subset-number*	Specifies the identifier of the interface subset. The subset-number argument is configured using the **snmp-server interface subset** command.
regular-expression *expression*	Specifies a subset of interfaces matching a regular expression, for which to display information.
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.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

Regular expressions have two constraints:

- Regular expressions must always be entered within double quotes to ensure that the CLI interprets each character correctly.
- All characters that are part of a regular expression are considered regular characters with no special meaning. In order to enter special characters, such as "\" or "?," they must be preceded by the backslash character "\." For example, to enter the regular expression ([A-Z][A-Z0-9]*)\b[^>]*>(.*?)<\/\1, you would enter ([A-Z][A-Z0-9]*)\\b[^>]*>(.*\?)<\/\\1.

Refer to the *Understanding Regular Expressions, Special Characters, and Patterns* module in *Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide* for more information regarding regular expressions.

When using the **subset** or **regular-expression** keywords, the actual display might not match the configuration if there are higher priority *subset-number* values that actually apply to the interface. This can happen for a set of interfaces that are included in two or more configured regular expressions or where an individual interface configuration is enabled.

Task ID

Task ID	Operation
snmp	read

The following example illustrates how to display linkUp and linkDown notification status for a subset of interfaces identified by a specific *subset-number* :

```
RP/0/RSP0/CPU0:router# show snmp interface notification subset 3
```

This example illustrates how to display linkUp and linkDown notification status for a subset of interfaces identified by a regular expression:

```
RP/0/RSP0/CPU0:router# show snmp interface notification regular-expression
"^Gig[a-zA-Z]+[0-9/]+\."
```

show snmp interface regular-expression

To display interface names and indices assigned to interfaces that match a regular expression, use the **show snmp interface regular-expression** command in EXEC mode.

show snmp interface regular-expression *expression*

Syntax Description

expression	Specifies a subset of interfaces matching a regular expression, for which to display information.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

All characters that are part of a regular expression are considered regular characters with no special meaning. In order to enter special characters, such as "\" or "?," they must be preceded by the backslash character "\." For example, to enter the regular expression ([A-Z][A-Z0-9]*)\b[^>]*>(.*?)</\1, you would enter ([A-Z][A-Z0-9]*)\\b[^>]*>(.*\?)</\\1.

Refer to the *Understanding Regular Expressions, Special Characters, and Patterns* module in *Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide* for more information regarding regular expressions.

Task ID

Task ID	Operation
snmp	read

This example illustrates how to display information for interfaces that match the given regular expression:

```
RP/0/RSP0/CPU0:router# show snmp interface regular-expression "^Gig[a-zA-Z]+[0-9/]+\."
```

Related Topics

snmp-server interface subset, on page 439

show snmp mib

To display a list of MIB module object identifiers (OIDs) registered on the system, use the **show snmp mib** command in

EXEC

mode.

show snmp mib [*object-name* | **dll**]

Syntax Description

object-name	(Optional) Specific MIB object identifier or object name.
dll	(Optional) Displays a list of all MIB DLL filenames and the OID supported by each DLL filename on the system.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 3.9.0	The **detailed** keyword was not supported.

Usage Guidelines

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

Use the **show snmp mib** command to display a list of the MIB module instance identifiers registered on the system.

Although the **show snmp mib** command can be used to display a list of MIB OIDs registered on the system, the use of a Network Management System (NMS) application is the recommended alternative for gathering this information.

The **show snmp mib** command is intended only for network managers who are familiar with Abstract Syntax Notation One (ASN.1) syntax and the Structure of Management Information (SMI) of Open Systems Interconnection (OSI) Reference Model.

SNMP management information is viewed as a collection of managed objects residing in a virtual information store termed the *MIB*. Collections of related objects are defined in MIB modules. These modules are written using a subset of ASN.1 termed the *SMI.*

The definitions for the OIDs displayed by this command can be found in the relevant RFCs and MIB modules. For example, RFC 1907 defines the system.x, sysOREntry.x, snmp.x, and snmpTrap.x OIDs, and this information is supplemented by the extensions defined in the CISCO-SYSTEM-MIB.

Use the **detailed** keyword to display a list of the MIB module instance identifiers registered on the system. The output displays additional details, such as DLL and configuration information.

Use the **dll** keyword to display a list of the MIB modules loaded into the agent. This command can be used to find the supported MIBs.



Note This command produces a high volume of output if SNMP is enabled on the system. To exit from a --More-- prompt, press **Crtl-Z**.

Task ID

Task ID	Operations
snmp	read

The following example shows sample output from the **show snmp mib** command:

```
RP/0/RSP0/CPU0:router# show snmp mib

1.3.6.1.2.1.47.1.1.1.1.2
1.3.6.1.2.1.47.1.1.1.1.3
1.3.6.1.2.1.47.1.1.1.1.4
1.3.6.1.2.1.47.1.1.1.1.5
1.3.6.1.2.1.47.1.1.1.1.6
1.3.6.1.2.1.47.1.1.1.1.7
1.3.6.1.2.1.47.1.1.1.1.8
1.3.6.1.2.1.47.1.1.1.1.9
1.3.6.1.2.1.47.1.1.1.1.10
1.3.6.1.2.1.47.1.1.1.1.11
1.3.6.1.2.1.47.1.1.1.1.12
1.3.6.1.2.1.47.1.1.1.1.13
1.3.6.1.2.1.47.1.1.1.1.14
1.3.6.1.2.1.47.1.1.1.1.15
1.3.6.1.2.1.47.1.1.1.1.16
1.3.6.1.2.1.47.1.2.1.1.2
1.3.6.1.2.1.47.1.2.1.1.3
1.3.6.1.2.1.47.1.2.1.1.4
1.3.6.1.2.1.47.1.2.1.1.5
1.3.6.1.2.1.47.1.2.1.1.6
1.3.6.1.2.1.47.1.2.1.1.7
1.3.6.1.2.1.47.1.2.1.1.8
1.3.6.1.2.1.47.1.3.1.1.1
--More-
```

This example shows sample output from the **show snmp mib** command with the **detailed** keyword:

```
RP/0/RSP0/CPU0:router# show snmp mib detailed

Entitymib:dll=/pkg/lib/mib/libEntitymib.dll, config=Entity.mib, loaded
1.3.6.1.2.1.47.1.1.1.1.2
1.3.6.1.2.1.47.1.1.1.1.3
1.3.6.1.2.1.47.1.1.1.1.4
1.3.6.1.2.1.47.1.1.1.1.5
1.3.6.1.2.1.47.1.1.1.1.6
1.3.6.1.2.1.47.1.1.1.1.7
1.3.6.1.2.1.47.1.1.1.1.8
1.3.6.1.2.1.47.1.1.1.1.9
1.3.6.1.2.1.47.1.1.1.1.10
1.3.6.1.2.1.47.1.1.1.1.11
```

```
1.3.6.1.2.1.47.1.1.1.1.12
1.3.6.1.2.1.47.1.1.1.1.13
1.3.6.1.2.1.47.1.1.1.1.14
1.3.6.1.2.1.47.1.1.1.1.15
1.3.6.1.2.1.47.1.1.1.1.16
1.3.6.1.2.1.47.1.2.1.1.2
1.3.6.1.2.1.47.1.2.1.1.3
1.3.6.1.2.1.47.1.2.1.1.4
1.3.6.1.2.1.47.1.2.1.1.5
1.3.6.1.2.1.47.1.2.1.1.6
1.3.6.1.2.1.47.1.2.1.1.7
1.3.6.1.2.1.47.1.2.1.1.8
--More--
```

This example shows sample output from the **show snmp mib** command with the **dll** keyword:

```
RP/0/RSP0/CPU0:router# show snmp mib dll

Entitymib:dll=/pkg/lib/mib/libEntitymib.dll, config=Entity.mib, loaded
bgp4mib:dll=/pkg/lib/mib/libbgp4mib.dll, config=bgp4.mib, loaded
cdpmib:dll=/pkg/lib/mib/libcdpmib.dll, config=cdp.mib, loaded
ciscoprocessmib:dll=/pkg/lib/mib/libciscoprocessmib.dll,
 config=ciscoprocess.mib, loaded
ciscosyslogmib:dll=/pkg/lib/mib/libciscosyslogmib.dll,
 config=ciscosyslog.mib, loaded
ciscosystemmib:dll=/pkg/lib/mib/libciscosystemmib.dll,
 config=ciscosystem.mib, loaded
confcopymib:dll=/pkg/lib/mib/libconfcopymib.dll, config=confcopy.mib,
 loaded
configmanmib:dll=/pkg/lib/mib/libconfigmanmib.dll, config=configman.mib,
 loaded
dot3admib:dll=/pkg/lib/mib/libdot3admib.dll, config=dot3ad.mib,
 loaded
fabhfrmib:dll=/pkg/lib/mib/libfabhfrmib.dll, config=fabhfr.mib,
 loaded
fabmcastapplmib:dll=/pkg/lib/mib/libfabmcastapplmib.dll,
 config=fabmcastappl.mib, loaded
fabmcastmib:dll=/pkg/lib/mib/libfabmcastmib.dll, config=fabmcast.mib,
 loaded
flashmib:dll=/pkg/lib/mib/libflashmib.dll, config=flash.mib,
 loaded
hsrpmib:dll=/pkg/lib/mib/libhsrpmib.dll, config=hsrp.mib, loaded
icmpmib:dll=/pkg/lib/mib/libicmpmib.dll, config=icmp.mib, loaded
ifmib:dll=/pkg/lib/mib/libifmib.dll, config=if.mib, loaded
ipmib:dll=/pkg/lib/mib/libipmib.dll, config=ip.mib, loaded
mempoolmib:dll=/pkg/lib/mib/libmempoolmib.dll, config=mempool.mib,
 loaded
mplsldpmib:dll=/pkg/lib/mib/libmplsldpmib.dll, config=mplsldp.mib,
 loaded
.
.
.
```

Related Topics

show snmp, on page 353

show snmp mib bulkstat transfer

To display completed local bulk statistics files, use the **show snmp mib bulkstat transfer** command in EXEC mode.

show snmp mib bulkstat transfer [*transfer-name*]

Syntax Description

transfer-name	Specifies a named transfer file to display.

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

The **show snmp mib bulkstat transfer** command lists all bulk statistics virtual files (VFiles) on the system that have finished collecting data. (Data files that are not complete are not displayed.)

The output lists all of the completed local bulk statistics files, the remaining time left before the bulk statistics file is deleted (remaining retention period), and the state of the bulk statistics file. The state of the bulk statistics file should be Retry. Retry indicates that one or more transfer attempts have failed and that the file transfer will be attempted again. The number of retry attempts remaining is displayed in parenthesis. After the successful retry or retry attempts, the local files created by the MIB process in the router are deleted and data collection begins again.

To display only the status of a named transfer (as opposed to all configured transfers), specify the name of the transfer in the *transfer-name* argument. The *transfer-name* argument names a file which is supposed to be created even before the retries.

Task ID

Task ID	Operation
snmp	read

```
RP/0/RSP0/CPU0:router# show snmp mib bulkstat transfer

Transfer Name : ifmib
 Retained files

 File Name        : Time Left (in seconds)   :STATE
 ----------------------------------------------------------
```

```
ifmib_Router_020421_100554683 : 173 : Retry (2 Retry attempt(s) Left)
```

show snmp request duplicates

To display the number of duplicate protocol data unit (PDU) requests dropped by the SNMP agent, use the **show snmp request duplicates** command in

EXEC

mode.

show snmp request duplicates

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
snmp	read

This example illustrates sample output from the **show snmp request duplicates** command:

```
RP/0/RSP0/CPU0:router# show snmp request duplicates

No of Duplicate request received/Dropped : 0
```

show snmp request incoming-queue detail

To show the details of the queue of incoming SNMP requests, use the **show snmp request incoming-queue detail** command in EXEC mode.

show snmp request incoming-queue detail

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

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

This command shows an output for maximum of 15 queues and an additional general queue. The entry will be deleted when any queue is not polled for 30 minutes.

This command shows these details:

Field	Description
NMS Address	Source address (IPv4 or IPv6) of network management system (NMS) queue. Specifies the NMS packet requests in this queue.
Q Depth	Number of packets to be processed in the queue.
Deque Count	Number of packets that are processed.
Priority	Priority of queue with packets to be processed. The priority ranges from 1 to 5, 1 indicates low priority and 5 indicates high priority.
Enque time	Time stamp of last request in the queue.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp request incoming-queue detail
 Wed Mar 12 05:16:59.505 PDT

NMS ADDRESS          Q Depth      Deque count          Priority             Enque time
```

```
4.5.6.7               0                1223             1                    Wed Mar 12
05:16:25

1.2.3.4               0                1193             1                    Wed Mar 12
05:15:06

General Q             0                 0               0                    Wed Mar 12
05:14:49

NMS ADDRESS       : 4:5:6::7

  Q Depth     Deque count           Priority               Enque time

  0                1220               1                    Wed Mar 12 05:16:02

NMS ADDRESS       : 1:2:3::4

  Q Depth     Deque count          Priority               Enque time

  0               1221               1                     Wed Mar 12 05:15:37
```

show snmp request type summary

To show the types of requests sent from each network management system (NMS), use the **show snmp request type summary** command in EXEC mode.

show snmp request type summary

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

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

The **show snmp request type summary** command shows these details:

Field	Description
NMS address	IP address of the NMS that sent the request.
Get	Number of requests of Get type.
Getnext	Number of requests of Getnext type.
Getbulk	Number of requests of Getbulk type.
Set	Number of requests of Set type.
Test	Number of requests of Test type that is part of Set request.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp request type summary
 Wed Mar 12 05:17:14.643 PDT
NMS Address          Get      GetNext      GetBulk      Set      Test
 1.2.3.4             0          1254         0          0         0
 4.5.6.7             0          5101         0          0         0

NMS Address : 1:2:3::4
 Get      GetNext      GetBulk      Set      Test
  0          2536        0          0         0
```

```
NMS Address : 4:5:6::7
 Get       GetNext       GetBulk       Set       Test
  0           3817          0           0          0
```

show snmp request type detail

To shows the group that is polled frequently and from which network management system (NMS), use the **show snmp reqest type detail** command in EXEC mode.

show snmp request type detail

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

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

The **show snmp request type detail** command shows these details:

Field	Description
NMS Address	Address of Network Management Station from which the request is received.
Request	Number of requests from NMS.
SNMPD	Number of requests to snmpd.
Interface	Number of requests to mibd_interface.
Entity	Number of requests to mibd_entity.
Route	Number of requests to mibd_route.
Infra	Number of requests to mibd_infra.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp request type detail
Wed Mar 12 05:17:34.838 PDT
NMS Address      Request    AGENT    INTERFACE    ENTITY    ROUTE    INFRA
1.2.3.4          1193       52          742        70       267        123
4.5.6.7          1223       52          742        100      267        123
1:2:3::4         1221       52          742        100      265        123
4:5:6::7         1220       52          742        100      265        122
```

show snmp request drop summary

To show the summary of overall packet drop, use the **show snmp request drop summary** command in EXEC mode.

show snmp request drop summary

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

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

The **show snmp request drop summary** command shows these details:

Field	Description
NMS Address	Address of network management station from which request is received.
IN Q	Number of packets dropped in incoming queue as the dropped packets are not processed more than 10 seconds.
Encode	Number of packets dropped because of encode errors.
Duplicate	Number of requests dropped with duplicate request feature.
Stack	Numbers of requests are dropped in stack.
AIPC	Number of packets dropped at AIPC module.
Overload	Number of packets dropped because of overload control notification.
Timeout	Number of packets are dropped because of slow response from MIB.
Internal	Number of packets dropped because of internal failures.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp request drop summary
 Fri Mar 14 05:32:31.732 PDT
NMS Address          INQ   Encode    Duplicate   Stack    AIPC   Overload   Timeout
Internal
 1.2.3.4              0     0         0           0      0         218        0         0

NMS Address : 1:2:3::4
INQ      Encode     Duplicate    Stack    AIPC    Overload     Timeout     Internal
0         0           0            0       0       109          0           0
```

show snmp request overload stats

To show the number of packets dropped due to overload feature, use the **snmp request overload stats** command in EXEC mode.

show snmp request overload stats

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

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

This command displays the latest 100 entries.

The show snmp request overload stats command shows these details:

Field	Description
StartTime	Time when overload control notification is received.
InQInDrop	Number of packet drops before inserting in incoming queue.
InQOutDrop	Number of packets dropped from incoming queue.
EndTime	Time when overload control notification ends.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp request overload stats
Thu Mar 13 07:00:45.575 UTC
StartTime                          InQInDrop        InQOutDrop                EndTime

Thu Mar 13 07:00:28                   1               0                        Thu Mar
13 07:00:38
```

show snmp statistics oid group

To show the statistics of object ID (OID), use the **show snmp statistics oid group** command in EXEC mode.

show snmp statistics oid group {**interface** | **infra** | **route** | **entity**}

Syntax Description

interface	mibd_interface sub-agent process
infra	mibd_infra sub-agent process
route	mibd_route sub-agent process
entity	mibd_entity sub-agent process

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

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

The latest 500 entries for each group is displayed and a maximum of 2000 entries is displayed for four groups.

The **show snmp statistics oid group** command shows these details:

Field	Description
SerNum	Unique serial number for each request processing in sub-agents.
Type	Request type.
NumObj	Number of OIDs processing in this request.
MIBMGR-IN	Time stamp of request received from AIPC.
PDU-IN	Time stamp of request sent to MIB for processing. This will be offset in milli seconds from MIBMGR_IN time stamp.
FROM-MIB	Time stamp of response sent from MIB after processing. This will be offset in milli seconds from MIBMGR_IN time stamp.
PDU-OUT	Time stamp of response sent to SNMP through AIPC . This will be offset in milli seconds from MIBMGR_IN.
OID	OID info processing this request.

Field	Description
MIB-IN	Time stamp of the request sent to MIB for each OID.
MIB-OUT	Time stamp of response sent from MIB after processing. This will be offset in milli seconds from MIB-IN.
ExpNext	Request Exp-Next.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp statistics oid group interface
Thu Mar 13 07:10:30.310 UTC
SerNum: 2489   Type: GETNEXT     NumObj: 1
  MIBMGR-IN    PDU-IN[ms]          PDU-OUT[ms]          MIBMGR-OUT[ms]
  Mar 13 07:00:49.933                1030                 1030
    OID: 1.3.6.1.2.1.10.32.4.2.0       Exp-Next: Yes
      MIB-IN : Mar 13 07:00:49.933   MIB-OUT[ms] : 1030
SerNum: 10203    Type: GETNEXT     NumObj: 1
  MIBMGR-IN      PDU-IN[ms]          PDU-OUT[ms]            MIBMGR-OUT[ms]
  Mar 13 06:36:16.976    0             1031                   1031
    OID: 1.3.6.1.2.1.10.32.4.2.0  Exp-Next: Yes
      MIB-IN : Mar 13 06:36:16.976   MIB-OUT[ms] : 1031
```

show snmp statistics pdu

To show if processing time of any protocol data unit (PDU) is more than threshold limit, use the **show snmp statistics pdu nms** command in EXEC mode.

show snmp statistics pdu nms[address]

Syntax Description

nms [address]	Address of Network Management Station from which request has arrived. The PDU statistics is filtered for each NMS.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

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

The PDU processing time can exceed the threshold limit in these scenarios:

- SNMPD not able to dispatch the request to MIB because of any failures in snmpd.
- MIB response after threshold limit.
- MIB does not respond to SNMPD.

Default threshold limit is 2 seconds. To change the default threshold value, use the command:

```
Snmp-server timeouts pdu stats <1-10>
```

The maximum number of entries per network management system (NMS) is 500 and the maximum number of NMS is 30.

This command shows these details:

Field	Description
NMS	Address of Network Management Station from which request has arrived.
Port	Port number of application that requested the SNMP query.
REQID	Request ID for each PDU.
Type	Type of PDU.
SerNum	The unique number generated for every request and sent to all MIBDs.

Field	Description
Timeout	If the request was timeout out set to TRUE, else set to FALSE.
InputQ-In	Time stamp of the PDU when queued into input Q.
InputQ-Out	Time stamp of the PDU when queued into input Q, This will be in milliseconds, Offset from INPUT-IN time stamp.
ProcQ-In	Time stamp of the PDU when queued into Processing Q. This will be in milliseconds, Offset from INPUT-IN time stamp.
Response	Time stamp in milli seconds of the PDU when response is received from sub agents. Offset from INPUT-IN time stamp.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp statistics pdu nms
 Thu Mar 13 08:03:17.322 UTC
NMS: 64.103.222.6   PORT: 35028
  REQID:962974264  TYPE: 161  SerNum: 9428 TIMEOUT: No
  INPUTQ-IN                    INPUTQ-OUT[ms]       PROCQ-IN[ms]        RESPONSE[ms]
 Mar 13 08:03:15.269            0                    0                   1056
```

show snmp statistics slow oid

To show the object ID (OID) that has exceeded beyond the threshold time for processing and the number of times that the threshold limit is exceeded with the latest timestamp, use the **show snmp statistics slow oid** command in EXEC mode.

show snmp statistics slow oid

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

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

Default threshold limit for this data as 500 milli seconds. To change the default value, use the command:

```
Snmp-server logging threshold oid-processing < <0-20000>
```

The latest 500 entries for each sub agent is displayed and a total of upto 2000 entries is maintained.

The **show snmp statistics slow oid** command shows these details:

Field	Description
Type	Request type for slow OID.
Exact OID	Requested OID from NMS.
Resp OID	Response OID for the Request type and EXACT OID.
Slow Count	Number of times OID is slow.
Slow Time	Time taken for processing the OID in milli seconds.
Time Stamp	Time stamp of the slow OID when MIB responded to MIBD.

Task ID

Task ID	Operations
snmp	read, write

This example shows a slow OIDs that exceeds the specified threshold time.

```
RP/0/RSP0/CPU0:router# show snmp statistics slow oid
```

```
 Group:agent

  TYPE                : GETNEXT
  REQ_OID           : 1.3.6.1.2.1.1.1.0
  RESP_OID         : 1.3.6.1.2.1.1.1.2
  COUNT               : 2
  TIME[ms]            : 0
  TIME_STAMP     : Mar 13 05:36:52.279

Group:infra

Group:route

  TYPE               : GETNEXT
  REQ_OID         :
1.3.6.1.2.1.4.34.1.3.4.20.254.128.0.0.0.0.0.0.254.8.255.254.203.38.197.0.0.0.2
  RESP_OID       :
1.3.6.1.2.1.4.34.1.3.4.20.254.128.0.0.0.0.0.0.254.8.255.254.203.38.197.0.0.0.2
  COUNT            : 4
  TIME[ms]         : 14
  TIME_STAMP   : Mar 13 05:36:52.279
  TYPE               : GET
  REQ_OID         :
1.3.6.1.2.1.4.34.1.3.4.20.254.128.0.0.0.0.0.0.254.8.255.254.203.38.197.0.0.0.2
  RESP_OID       :
1.3.6.1.2.1.4.34.1.3.4.20.254.128.0.0.0.0.0.0.254.8.255.254.203.38.197.0.0.0.2
  COUNT            : 4
  TIME[ms]         : 14
  TIME_STAMP   : Mar 13 05:36:52.279

Group:entity

Group:interface

  TYPE                : GETNEXT
  REQ_OID          : 1.3.6.1.2.1.2.1
  RESP_OID        : 1.3.6.1.2.1.2.1.0
  COUNT             : 1
  TIME[ms]          : 0
  TIME_STAMP    : Mar 13 05:36:52.279
```

show snmp statistics poll oid all

To show all object IDs (OIDs) polled from all network management system (NMS) and how many times it has polled, use the **show snmp statistics poll oid all** command in EXEC mode.

For this command to work, the following configuration has to be committed:

(config)#snmp-server oid-poll-stats

show snmp statistics poll oid all

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

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

The maximum number of entries equals the number of OIDs that were polled. The maximum number of NMS details for each OID is 15.

The **show snmp statistics poll oid all** command shows these details:

Field	Description
Object ID	OID requested from NMS.
NMS	List of NMS IP address requested for each OID.
Count	Number of times OID is polled for each NMS.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp statistics poll oid all
 Object ID   :   1.3.6.1.2.1.1.3
 NMS                  COUNT
 10.2.1.3               10
 10.3.1.2               30
 10.4.1.3               20
 10.12.1.3              5

Object ID    :    1.3.6.1.2.1.1.4
NMS                   COUNT
10.2.1.3                10
```

```
10.3.1.2                5
10.4.1.3                20
10.12.1.3               30

Object ID   :  1.3.6.1.2.1.1.5
NMS                    COUNT
10.2.1.3                10
10.3.1.2                3
10.4.1.3                2
```

Show snmp statistics poll oid nms

To show which object ID (OID) is polled from which network management system (NMS) and how many times it has polled, use the **show snmp statistics poll oid nms** command in EXEC mode.

show snmp statistics poll oid nms<V4 / V6 address>

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

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

The **show snmp statistics poll oid nms** command shows these details:

Field	Description
Object ID	OID requested from NMS.
NMS	List of NMS IP address requested for each OID.
Count	Number of times OID is polled for each NMS.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp statistics poll nms 1.2.3.4
 NMS Address   : 1.2.3.4
Object ID                 Count
1.3.6.1.2.1.2.2.1.2       14
```

show snmp statistics slow oid [after/before] hh:mm:ss day mday year

To show the object ID (OID) that has exceeded beyond the threshold time for processing and the number of times that the threshold limit is exceeded with the latest timestamp, use the **show snmp statistics slow oid [after/before] hh:mm:ss day mday year** command in EXEC mode.

show snmp statistics slow oid[after/before] hh:mm:ss day mday year

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

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

Default threshold limit for this data as 500 milli seconds. To change the default value, use the command:

```
Snmp-server logging threshold oid-processing < <0-20000>
```

The latest 500 entries for each sub agent is displayed and a total of upto 2000 entries is maintained.

The **show snmp statistics slow oid [after/before] hh:mm:ss day mday year** command shows these details:

Field	Description
Type	Request type for slow OID.
Exact OID	Requested OID from NMS.
Resp OID	Response OID for the Request type and EXACT OID.
Slow Count	Number of times OID is slow.
Slow Time	Time taken for processing the OID in milli seconds.
Time Stamp	Time stamp of the slow OID when MIB responded to MIBD.

Task ID

Task ID	Operations
snmp	read, write

This example shows a slow OIDs that exceeds the specified threshold time.

```
RP/0/RSP0/CPU0:router# show snmp statistics slow oid
Group:agent

  TYPE                : GETNEXT
  REQ_OID          : 1.3.6.1.2.1.1.1.0
  RESP_OID        : 1.3.6.1.2.1.1.1.2
  COUNT             : 2
  TIME[ms]          : 0
  TIME_STAMP    : Mar 13 05:36:52.279

Group:infra
Group:route
  TYPE              : GETNEXT
  REQ_OID        :
1.3.6.1.2.1.4.34.1.3.4.20.254.128.0.0.0.0.0.0.254.8.255.254.203.38.197.0.0.0.2
  RESP_OID      :
1.3.6.1.2.1.4.34.1.3.4.20.254.128.0.0.0.0.0.0.254.8.255.254.203.38.197.0.0.0.2
  COUNT           : 4
  TIME[ms]        : 14
  TIME_STAMP  : Mar 13 05:36:52.279

  TYPE              : GET
  REQ_OID        :
1.3.6.1.2.1.4.34.1.3.4.20.254.128.0.0.0.0.0.0.254.8.255.254.203.38.197.0.0.0.2
  RESP_OID      :
1.3.6.1.2.1.4.34.1.3.4.20.254.128.0.0.0.0.0.0.254.8.255.254.203.38.197.0.0.0.2
  COUNT           : 4
  TIME[ms]        : 14
  TIME_STAMP  : Mar 13 05:36:52.279

Group:entity
Group:interface
  TYPE               : GETNEXT
  REQ_OID         : 1.3.6.1.2.1.2.1
  RESP_OID       : 1.3.6.1.2.1.2.1.0
  COUNT            : 1
  TIME[ms]         : 0
  TIME_STAMP   : Mar 13 05:36:52.279
```

show snmp mib ifmib general

To show how many requests get data from internal cache and how many requests are sent to statsd to get data, use the **show snmp mib ifmib general** command in EXEC mode.

show snmp mib ifmib general

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

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

Default IFMIB internal cache is 15 seconds. To change the duration, use the command:

```
snmp-server ifmib internal cache max-duration <0-60>
```

The default duration is 15 seconds, 0 seconds to disable the IFMIB internal cache.

To service the requests from Stats cache instead of Drivers, use the command:

```
snmp-server ifmib stats cache
```

The **show snmp mib ifmib general** command shows these details:

Field	Description
Cache Hit	Number of times the request retrieves data from IFMIB internal cache.
Cache Miss	Number of times the request processed from statsd, and not from IFMIB internal cache
Last Access Time	Latest time stamp of corresponding hit or miss.
Count	Number of times the data is retrieved.

The Cache Hit and Cache Miss are 32 bit counters. The maximum value is 2^31 and reset to 0 if the maximum value is exceeded.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# Show snmp mib ifmib general
```

```
 Fri Mar 14 05:05:50.408 PDT

Type                    Count           Last Access Time

Cache Hit               328             Mar 14 05:05:47.480

Cache Miss               2              Mar 14 05:05:47.386
```

show snmp mib ifmib cache

To show the Ifindex that has exceeded the threshold time for processing, the request type and the time stamp, use the **show snmp mib ifmib cache** command in EXEC mode. The threshold time for the data to create an entry is 500 milli seconds.

show snmp mib ifmib cache

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

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

This command displays the latest 500 entries. An entry will be added when the difference between Cache in and Cache out time is more than 500 milli seconds. The timeout value cannot be changed.

The **show snmp mib ifmib cache** command shows these details:

Field	Description
Index	Interface index.
MIB IN	Time stamp of the request when IFMIB starts processing.
Cache In	Time stamp in milli seconds when data retrieval from the cache starts for the request. It is offset from MIB IN time stamp.
Cache Out	Time stamp in milli seconds when data is retrieved from cache. It is offset from MIB IN time stamp.
MIB Out	Time stamp in milli seconds of the response from IF MIB. It is offset from MIB IN time stamp.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp mib ifmib cache
IFIndex    Type          MIB IN                    CACHE IN[ms]          CACHE OUT[ms]
```

```
        MIB OUT[ms]

2          NEXT          Mar 18 07:14:41.815           4                    701
           701

2          NEXT          Mar 18 07:15:36.815           0                    679
           679

2          NEXT          Mar 18 07:16:00.735           0                    684
           684
```

show snmp mib ifmib statsd

To show the Ifindex that has exceeded the threshold time for processing, the request type and the time stamp, use the **show snmp mib ifmib statsd** command in EXEC mode. The threshold time for the data to create an entry is 500 milli seconds.

show snmp mib ifmib statsd

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

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

This command displays the latest 500 entries. An entry will be added when the difference between Stats in and Stats out time is more than 500 milli seconds. The timeout value cannot be changed.

The **show snmp mib ifmib statsd** command shows these details:

Field	Description
Index	Interface index.
MIB IN	Time stamp of the request when IFMIB starts processing.
Stats In	Time stamp in milli seconds when data retrieval from the Statsd starts for the request. It is offset from MIB IN time stamp.
Stats Out	Time stamp in milli seconds when data is retrieved from Statsd. It is offset from MIB IN time stamp.
MIB Out	Time stamp in milli seconds of the response from IF MIB. It is offset from MIB IN time stamp.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp mib ifmib statsd
IFIndex    Type          MIB IN                    STATS IN[ms]      STATS OUT[ms]     MIB
```

```
 OUT[ms]

2           NEXT          Mar 18 07:14:41.815         4                   701
701

2           NEXT          Mar 18 07:15:36.815         0                   679
679

2           NEXT          Mar 18 07:16:00.735         0                   684
684
```

show snmp traps details

To show the details about the traps generated for each host, the sent and drop count and the timestamp, use the **show snmp traps details** command in EXEC mode.

show snmp traps details

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

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

The **show snmp traps details** command shows these details:

Field	Description
TrapOID	Generated trap.
Sent	Number of times the trap sent from the host and port configured.
Drop	Number of times the trap dropped from the host and port configured.
Last-sent	Time stamp when the last trap was sent from the host and port.
Last-drop	Time stamp when the last trap dropped from the host and port.
Host	Configured address of the host to receive traps
udp-port	Configured port to receive traps

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp traps details
Mon Apr  7 17:14:07.241 UTC
HOST:9.22.24.150, udp-port:3333
------------------------------
```

```
TrapOID                             Sent    Drop     Last-sent                     Last-drop
ciscoConfigManMIB.2.0.1               2          0      Mon Apr 07 14 17:12:29          ~
ciscoFlashDeviceInsertedNotif         1          0      Mon Apr 07 14 17:12:28          ~
ciscoFlashDeviceRemovedNotif          1          0      Mon Apr 07 14 17:12:28          ~
```

show snmp informs details

To show the details about the informs generated for each host, the drop and retry count and the timestamp, use the **show snmp informs details** command in EXEC mode.

show snmp informs details

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

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

The **show snmp informs details** command shows these details:

Field	Description
InformOID	Generated inform.
Sent	Number of times the Inform is sent from the inform host and port configiured.
Drop	Number of times the Inform is sent from the inform host and port configiured.
Retry	Number of times the Inform retries from the inform host and port configiured
Last-sent	Time stamp when the last inform was sent from the host and port.
Last-drop	Time stamp when the last inform dropped from the host and port.
Host	Configured address of the host to receive traps.
udp-port	Configured port to receive traps.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp informs details
Mon Apr  7 17:14:17.212 UTC
HOST:9.22.24.150, udp-port:5555
------------------------------
InformOID                          Sent    Drop    Retry   Last-sent
Last-drop
ciscoConfigManMIB.2.0.1            8       2       6       Mon Apr 07 14 17:12:54      Mon
 Apr 07 14 17:12:42
ciscoFlashDeviceInsertedNotif      4       1       3       Mon Apr 07 14 17:12:55      Mon
 Apr 07 14 17:12:42
ciscoFlashDeviceRemovedNotif       4       1       3       Mon Apr 07 14 17:12:54      Mon
 Apr 07 14 17:12:42
ciscoMgmt.117.2.0.1                8       2       6       Mon Apr 07 14 17:12:53      Mon
 Apr 07 14 17:12:42
ciscoMgmt.117.2.0.2                4       1       3       Mon Apr 07 14 17:12:52      Mon
 Apr 07 14 17:12:42|
```

show snmp users

To display information about the configured characteristics of Simple Network Management Protocol (SNMP) users, use the **show snmp users** command in

EXEC

mode.

show snmp users

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

An SNMP user must be part of an SNMP group, as configured using the **snmp-server user** command.

Use the **show snmp users** command to display information about all configured users.

When configuring SNMP, you may see the logging message "Configuring snmpv3 USM user." USM stands for the User-Based Security Model (USM) for SNMP Version 3 (SNMPv3). For further information about USM, see RFC 3414, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.

Task ID

Task ID	Operations
snmp	read

This example shows sample output from the **show snmp users** command:

```
RP/0/RSP0/CPU0:router# show snmp users

  User name:user1
  Engine ID:localSnmpID
  storage-type:nonvolatile active
```

Table 30: show snmp users Field Descriptions

Field	Definition
User name	String identifying the name of the SNMP user.
Engine ID	String identifying the name of the copy of SNMP on the device.
storage-type	Settings that are set in volatile or temporary memory on the device, or in nonvolatile or persistent memory where settings remain after the device is turned off and on again.

Related Topics

snmp-server group, on page 424
snmp-server user, on page 516

show snmp view

To display the configured views and the associated MIB view family name, storage type, and status, use the **show snmp view** command in

EXEC

mode.

show snmp view

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
snmp	read

This example shows sample output from the **show snmp view** command:

```
RP/0/RSP0/CPU0:router# show snmp view

  view1 1.3 - included nonVolatile active
  v1default 1.3.6.1 - included nonVolatile active
```

Related Topics

snmp-server group, on page 424
snmp-server user, on page 516

snmp-server chassis-id

To provide a message line identifying the Simple Network Management Protocol (SNMP) server serial number, use the **snmp-server chassis-id** command in

global configuration

mode. To restore the default value, if any, use the **no** form of this command.

snmp-server chassis-id *serial-number*
no snmp-server chassis-id

Syntax Description

serial-number	Unique identification string to identify the chassis serial number.

Command Default

On hardware platforms, where the serial number can be read by the device, the default is the serial number. For example, some Cisco devices have default chassis ID values of their serial numbers.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **snmp-server chassis-id** command to provide a message line identifying the SNMP server serial number.

The chassis ID message can be displayed with the **show snmp** command.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to specify the chassis serial number 1234456:

```
RP/0/RSP0/CPU0:router# snmp-server chassis-id 1234456
```

Related Topics

show snmp, on page 353

snmp-server community

To configure the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** command in

global configuration

mode. To remove the specified community string, use the **no** form of this command.

snmp-server community [**clear** | **encrypted**] *community-string* [**view** *view-name*] [**RO** | **RW**] [**SDROwner** | **SystemOwner**] [*access-list-name*]
no snmp-server community *community-string*

Syntax Description

clear	(Optional) Specifies that the entered *community-string* is clear text and should be encrypted when displayed by the **show running** command.
encrypted	(Optional) Specifies that the entered *community-string* is encrypted text and should be displayed as such by the **show running** command.
community-string	Community string that acts like a password and permits access to the SNMP protocol. The maximum length of the *community-string* argument is 32 alphabetic characters. If the **clear** keyword was used, *community-string* is assumed to be clear text. If the **encrypted** keyword was used, *community-string* is assumed to be encrypted. If neither was used, *community-string* is assumed to be clear text.
view *view-name*	(Optional) Specifies the name of a previously defined view. The view defines the objects available to the community.
RO	(Optional) Specifies read-only access. Authorized management stations are able only to retrieve MIB objects.
RW	(Optional) Specifies read-write access. Authorized management stations are able both to retrieve and to modify MIB objects.
SDROwner	(Optional) Limits access to the owner service domain router (SDR).
SystemOwner	(Optional) Provides system-wide access.
access-list-name	(Optional) Name of an access list of IP addresses allowed to use the community string to gain access to the SNMP agent.

Command Default

By default, an SNMP community string permits read-only access to all MIB objects.

By default, a community string is assigned to the SDR owner.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **snmp-server community** command to configure the community access string to permit access to SNMP.

To remove the specified community string, use the **no** form of this command.

Use the **clear** keyword to specify that the clear text community string you enter is displayed encrypted in the **show running** command output. To enter an encrypted string, use the **encrypted** keyword. To enter a clear text community string that is not encrypted by the system, use neither of these keywords.

When the **snmp-server community** command is entered with the **SDROwner** keyword, SNMP access is granted only to the MIB object instances in the owner SDR.

When the **snmp-server community** command is entered with the **SystemOwner** keyword, SNMP access is granted to the entire system.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to assign the string comaccess to SNMP, allowing read-only access, and to specify that IP access list 4 can use the community string:

```
RP/0/RSP0/CPU0:router(config)# snmp-server community comaccess ro 4
```

The following example shows how to assign the string mgr to SNMP, allowing read-write access to the objects in the restricted view:

```
RP/0/RSP0/CPU0:router(config)# snmp-server community mgr view restricted rw
```

This example shows how to remove the community comaccess:

```
RP/0/RSP0/CPU0:router(config)#no snmp-server community comaccess
```

Related Topics

snmp-server view, on page 519

snmp-server community-map

To associate a Simple Network Management Protocol (SNMP) community with an SNMP context, security name, or a target-list use the **snmp-server community-map** command in

global configuration

mode. To change an SNMP community mapping to its default mapping, use the **no** form of this command.

snmp-server community-map [**clear** | **encrypted**] *community-string* [**context** *context-name*] [**security-name** *security-name*] [**target-list** *target*]
no snmp-server community-map [**clear** | **encrypted**] *community-string*

Syntax Description

clear	(Optional) Specifies that the *community-string* argument is clear text.
encrypted	(Optional) Specifies that the community-string argument is encrypted text.
community-string	Name of the community.
context *context-name*	(Optional) Name of the SNMP context to which this community name is to be mapped.
security-name *security-name*	(Optional) Security name for this community. By default, the *string* is the security name.
target-list *target*	(Optional) Name of the target list for this community.

Command Default

The value of the *community-string* argument is also the security name.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **snmp-server community-map** command to map an SNMPv1 or SNMPv2c community name to one or more of the following:

- **context name**—Maps a community name to a specific SNMP context name. This allows MIB instances in an SNMP context to be accessed through SNMPv1 or SNMPv2c using this community name.
- **security name**—By default, the community name is used to authenticate SNMPv1 and SNMPv2c. Configure a security name for a community name to override the default and authenticate SNMP with the security name.
- **target**—Target list identifies a list of valid hosts from which SNMP access can be made using a specific security name. When such mapping is done for a particular community name, SNMP access is allowed only from hosts included in the target list.

Use the **clear** keyword to specify that the clear text community string you enter is displayed encrypted in the **show running** command output. To enter an encrypted string, use the **encrypted** keyword. To enter a clear text community string that is not encrypted by the system, use neither of these keywords.

Task ID

Task ID	Operations
snmp	read, write

This example maps the community name “sample 2” to the SNMP context name “sample1”:

```
RP/0/RSP0/CPU0:router(config)# snmp-server community-map sample2 context sample1
```

Related Topics

snmp-server context, on page 416
snmp-server target list, on page 467

snmp-server contact

To set the Simple Network Management Protocol (SNMP) system contact, use the **snmp-server contact** command in

global configuration

mode. To remove the system contact information, use the **no** form of this command.

snmp-server contact *system-contact-string*
no snmp-server contact

Syntax Description

system-contact-string	String that describes the system contact information. The maximum string length is 255 alphanumeric characters.

Command Default

No system contact is set.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **snmp-server contact** command to set the system contact string. Use the **no** form of this command to remove the system contact information.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to specify a system contact string:

```
RP/0/RSP0/CPU0:router(config)# snmp-server contact Dial System Operator at beeper # 27345
```

Related Topics

snmp-server location, on page 444

snmp-server context

To create a Simple Network Management Protocol (SNMP) context, use the **snmp-server context** command in

global configuration

mode. To remove an SNMP context, use the **no** form of this command.

snmp-server context *context-name*
no snmp-server context *context-name*

Syntax Description

context-name	Name of the SNMP context.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

This command creates an SNMP context. By default, all the SNMP MIB instances are in a default context. Create an SNMP context and map it to a particular feature to enable similar instances of the same object to co-exist in different SNMP contexts.

Task ID

Task ID	Operations
snmp	read, write

This example creates a new SNMP context named “sample1:”

```
RP/0/RSP0/CPU0:router(config)# snmp-server context sample1
```

Related Topics

snmp-server community-map, on page 413
snmp-server vrf, on page 521

snmp-server context mapping

To map an SNMP context with a protocol instance, topology or VRF entity, use the **snmp-server context mapping** command in global configuration mode.

snmp-server context mapping *context-name* [**feature** *feature-name*] [**instance** *instance-name*] [**topology** *topology-name*] [**vrf** *vrf-name*]

Syntax Description

context-name	Name of the SNMP context.
feature *feature-name*	Specifies the protocol for which to map the context. Available options are: • **bridge**—Layer 2 VPN bridge • **vrf**—Virtual Routing and Forwarding
instance *instance-name*	Maps the context to the specified protocol instance.
topology *topology-name*	Maps the context to the specified protocol topology.
vrf *vrf-name*	Maps the context to the specified VRF logical entity.

Command Default

No context mappings exist by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

A device can support multiple instances of a logical network entity, such as protocol instances or VRFs. Most existing MIBs cannot distinguish between these multiple logical network entities. For example, the original OSPF-MIB assumes a single protocol instance on a device, but you can now configure multiple OSPF instances on a device.

The **snmp-server context mapping** command maps a context to a protocol instance, topology or VRF logical entity.



Note The snmp-server context mapping command does not work for OSPF and OSPFv3. Refer to the **snmp context** commands.

Task ID

Task ID	Operation
snmp	read, write

This example illustrates how to map an snmp context to an OSPF instance:

```
RP/0/RSP0/CPU0:router(config)# snmp-server context mapping con5 feature ospf instance in1
```

Related Topics

show snmp context, on page 356
snmp context (OSPF)

snmp-server drop report acl

To apply an ACL policy for restricting an SNMPv3 unknown engine-id report to be sent out to NMS, use the **snmp-server drop report acl** command in the configuration mode.

snmp-server drop report acl IPv4 *IPv4-acl-name* **IPv6** *IPv6-acl-name*

Syntax Description

acl	Specifies IP Access Control Lists (ACL) policy
IPv4 *IPv4-acl-name*	Defines an IPv4 ACL name.
IPv6 *IPv6-acl-name*	Defines an IPv6 ACL name.

Command Default

Unknown engine-id reports will be sent to all polling stations (even if other ACLs are configured).

Command Modes

Configuration mode

Command History

Release	Modification
Release 6.2.3	This command was introduced.

Usage Guidelines

To drop an unknown engine-id report, you can either configure IPv4/IPv6 ACL name or both. When router is polled with wrong engine-id or no engine-id during a snmpv3 packet exchange, the unknown engine-id report will be sent based on the ACL policy that is configured.

Unknown engine-id reports will be sent only to polling station addresses that are permitted by ACL.

Task ID

Task ID	Operation
snmp	read, write

Example

This example shows how to configure the SNMP server to drop the unknown engin-id report:

```
RP/0/RSP0/CPU0:router (config) #  snmp-server drop report acl IPv4 nms-block IPv6
nms-block-ipv6
```

snmp-server drop unknown-user

To avoid error PDUs being sent out of router when polled with incorrect SNMPv3 user name, use the **snmp-server drop unknown-user** command in the appropriate mode. If the configuration is not set, by default it will respond with error PDUs.

snmp-server drop unknown-user

Syntax Description

drop unknown-user	Drop the error PDUs to be sent when router is polled with incorrect SNMPv3 user name.

Command Default

Unknown error PDUs will be sent when router is polled with incorrect SNMPv3 user name.

Command Modes

XR config

Command History

Release	Modification
Release 6.2.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
snmp	read, write

Example

This example shows how to configure the SNMP server to drop the error PDUs:

```
RP/0/RSP0/CPU0:router (config) #  snmp-sever drop unknown-user
```

snmp-server engineid local

To specify Simple Network Management Protocol (SNMP) engine ID on the local device, use the **snmp-server engineid local** command in

global configuration

mode. To return the engine ID to the default, use the **no** form of this command.

snmp-server engineid local *engine-id*
no snmp-server engineid local *engine-id*

Syntax Description

engine-id	Character string that identifies the engine ID. Consists of up to 24 characters in hexadecimal format. Each hexadecimal number is separated by a colon (:).

Command Default

An SNMP engine ID is generated automatically.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
snmp	read, write

This example shows how to configure the SNMP engine ID on the local device:

```
RP/0/RSP0/CPU0:router(config)# snmp-server engineID local 00:00:00:09:00:00:00:a1:61:6c:20:61
```

Related Topics

show snmp engineid, on page 359

snmp-server engineid remote

To specify a Simple Network Management Protocol (SNMP) engine ID on a remote device, use the **snmp-server engineid remote** command in

global configuration

mode. To return the engine ID to the default, use the **no** form of this command.

snmp-server engineid remote *ip-address engine-id* **udp-port** *port*
no snmp-server engineid remote *ip-address engine-id* **udp-port** *port*

Syntax Description

ip-address	IP address of remote SNMP notification host
engine-id	Character string that identifies the engine ID. Consists of up to 24 characters in hexadecimal format. Each hexadecimal number is separated by a colon (:).
udp-port *port*	(Optional) Specifies the User Datagram Protocol (UDP) port of the host to use. Range is from 1 to 65535. The default UDP port is 161.

Command Default

An SNMP engine ID is generated automatically.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
snmp	read, write

This example shows how to configure the SNMP engine ID on the local device:

```
RP/0/RP0/CPU0:Router(config)# snmp-server engineID remote 172.16.4.1
00:00:00:09:00:00:00:a1:61:6c:20:61
```

Related Topics

show snmp engineid, on page 359
snmp-server engineid local, on page 421

snmp-server entityindex persist

To enable the persistent storage of ENTITY-MIB data across process restarts, switchovers, and device reloads, use the **snmp-server entityindex persist** command in

global configuration

mode. To disable the persistent storage of ENTITY-MIB data, use the **no** form of this command.

snmp-server entityindex persist
no snmp-server entityindex persist

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
snmp	read, write

Example

This example illustrates how to enable persistent storage of ENTITY-MIB indices:

```
RP/0/RSP0/CPU0:router(config)# snmp-server entityindex persist
```

Related Topics

snmp-server mibs cbqosmib persist, on page 453

snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, or a table that maps SNMP users to SNMP views, use the **snmp-server group** command in

global configuration

mode. To remove a specified SNMP group, use the **no** form of this command.

snmp-server group *name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *view*] [**write** *view*] [**notify** *view*] [**context** *context-name*] [*access-list-name*]
no snmp-server group *name*

Syntax Description

name	Name of the group.
v1	Specifies a group that uses the SNMPv1 security model. The SNMP v1 security model is the least secure of the possible security models.
v2c	Specifies a group that uses the SNMPv2c security model. The SNMPv2c security model is the second least secure of the possible security models.
v3	Specifies a group that uses the SNMPv3 security model. The SNMP v3 security is the most secure of the possible security models.
auth	Specifies authentication of a packet without encrypting it.
noauth	Specifies no authentication of a packet.
priv	Specifies authentication of a packet with encryption.
read *view*	(Optional) Specifies a read view string (not to exceed 64 characters) that is the name of the view that allows only the contents of the agent to be viewed.
write *view*	(Optional) Specifies a write view string (not to exceed 64 characters) that is the name of the view used to enter data and configure the contents of the agent.
notify *view*	(Optional) Specifies a notify view string (not to exceed 64 characters) that is the name of the view used to specify a notify or trap.
context *context-name*	(Optional) Specifies the SNMP context to associate with this SNMP group and associated views.
access-list-name	(Optional) Access list string (not to exceed 64 characters) that is the name of the access list.

Command Default

See Table 31: snmp-server group Default Descriptions, on page 425.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

This table describes the default values for the different views:

Table 31: snmp-server group Default Descriptions

Default	Definition
read *view*	Assumed to be every object belonging to the Internet (1.3.6.1) object identifier (OID) space, unless the user uses the **read** option to override this state.
write *view*	Nothing is defined for the write view (that is, the null OID). You must configure write access.
notify *view*	Nothing is defined for the notify view (that is, the null OID). If a view is specified, any notifications in that view that are generated are sent to all users associated with the group (provided an SNMP server host configuration exists for the user).

Configuring Notify Views

Do not specify a notify view when configuring an SNMP group for the following reasons:

- The **snmp-server host** command autogenerates a notify view for the user, and then adds it to the group associated with that user.
- Modifying the notify view of the group affects all users associated with that group.

The notify view option is available for two reasons:

- If a group has a notify view that is set using SNMP, you may need to change the notify view.
- The **snmp-server host** command may have been configured before the **snmp-server group** command. In this case, reconfigure the **snmp-server host** command or specify the appropriate notify view.

Instead of specifying the notify view for a group as part of the **snmp-server group** command, use the following commands in global configuration mode:

- **snmp-server user**—Configures an SNMP user.
- **snmp-server group**—Configures an SNMP group, without adding a notify view.
- **snmp-server host**—Autogenerates the notify view by specifying the recipient of a trap operation.

Working with Passwords and Digests

No default values exist for authentication or privacy algorithms when this command is configured. In addition, no default passwords exist. The minimum length for a password is one character, although we recommend using eight characters for security. A plain-text password or localized Message Digest 5 (MD5) password can be specified. Forgotten passwords cannot be recovered, and the user must be reconfigured.

SNMP Contexts

SNMP contexts provide Virtual Private Network (VPN) users with a secure way of accessing MIB data. When a VPN is associated with a context, that VPN's specific MIB data exists in that context. Associating a VPN with a context enables service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about users of other VPNs on the same networking device.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to configure an SNMP version 3 group named group1 that requires the authentication of packets with encryption:

```
RP/0/RSP0/CPU0:router(config)# snmp-server group group1 v3 priv
```

Related Topics

show snmp, on page 353
show snmp group, on page 363
snmp-server host, on page 427
snmp-server view, on page 519

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in

global configuration

mode. To remove the specified host, use the **no** form of this command.

snmp-server host *address* [**clear** | **encrypted**] [**informs**] [**traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}] *community-string* [**udp-port** *port*] [*notification-type*]
nosnmp-server host *address* [**clear** | **encrypted**] [**informs**] [**traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}] *community-string* [**udp-port** *port*] [*notification-type*]

Syntax Description

address	Name or IP address of the host (the targeted recipient).
clear	(Optional) Specifies that the *community-string* argument is clear text.
encrypted	(Optional) Specifies that the *community-string* argument is encrypted text.
informs	(Optional) Specifies to send inform messages to this host.
traps	(Optional) Specifies that notifications should be sent as traps. This is the default.
version	(Optional) Specifies the version of the SNMP used to send the traps.
1	Specifies SNMPv1, the default.
2c	Specifies SNMPv2C.
3	Specifies SNMPv3. Version 3 is the most secure model because it allows packet encryption. If you specify the SNMPv3 keyword, you must specify the security level.
auth	Enables Message Digest 5 (MD5) algorithm and Secure Hash Algorithm (SHA) packet authentication.
noauth	Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3.
priv	Enables Data Encryption Standard (DES) packet encryption (also called "privacy").
community-string	Password-like community string sent with the notification operation. We recommend defining this string using the **snmp-server community** command prior to using the **snmp-server host** command.
udp-port *port*	(Optional) Specifies the User Datagram Protocol (UDP) port of the host to use. Range is from 1 to 65535. The default UDP port is 161.

notification-type	(Optional) Type of notification to be sent to the host. If no type is specified, all available notifications are sent. The notification type can be one or more of these keywords: • **bgp** —Enables SNMP Border Gateway Protocol Version 4 (BGPv4) traps. • **config** —Controls configuration notifications, as defined in the CISCO-CONFIG-MAN-MIB (enterprise 1.3.6.1.4.1.9.9.43.2). The notification type is (1) ciscoConfigManEvent. • **copy-complete** —Enables CISCO-CONFIG-COPY-MIB ccCopyCompletion traps. • **entity** —Controls Entity MIB modification notifications. This notification type is defined in the ENTITY-MIB (enterprise 1.3.6.1.2.1.47.2) as: (1) entConfigChange. • **fabric** —Enables SNMP fabric traps. • **fru-ctrl** —Enables SNMP entity field-replaceable unit (FRU) control traps. • **mpls** —Enables SNMP Multiprotocol Label Switching (MPLS) traps. • **sensor** —Enables SNMP entity sensor traps. • **snmp** —Enables SNMP traps. • **syslog** —Controls error message notifications (Cisco-syslog-MIB). Specify the level of messages to be sent with the **logging history** command.

Command Default

This command is disabled by default. No notifications are sent.

The default UDP port is 161.

When this command is entered without keywords, the default is to send all trap types to the host.

If no version keyword is entered, the default is version 1.

If version 3 is specified, but the security level is not specified, the default security level is noauth.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

SNMP notifications can be sent as traps. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. Traps are discarded as soon as they are sent. Traps are also sent only once.

When the **snmp-server host** command is not entered, no notifications are sent. To configure the device to send SNMP notifications, configure at least one **snmp-server host** command. When the command is entered without keywords, all trap types are enabled for the host.

To enable multiple hosts, issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap), each succeeding **snmp-server host** command overwrites the previous command. Only the last **snmp-server host** command is in effect. For example, if an **snmp-server host** command with the **traps** keyword is entered for a host and then another command with the **traps** keyword is entered for the same host, the second command replaces the first.

Either a host name or IP address can be used to specify the host.

The **snmp-server host** command is used with the **snmp-server engineid** command. Use the **snmp-server traps** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server traps** command and the **snmp-server host** command for that host must be enabled.

However, some notification types cannot be controlled with the **snmp-server traps** command. For example, some notification types are always enabled. Other notification types are enabled by a different command.

The availability of a notification-type depends on the device type and Cisco software features supported on the device.

To display which notification types are available on the system, use the question mark (**?**) online help function at the end of the **snmp-server host** command.

The **no snmp-server host** command used with no keywords disables traps.

Use the **clear** keyword to specify that the clear text community string you enter is displayed encrypted in the **show running** command output. To enter an encrypted string, use the **encrypted** keyword. To enter a clear text community string that is not encrypted by the system, use neither of these keywords.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to send RFC 1157 SNMP traps to the host specified by the name myhost.cisco.com. Other traps are enabled, but only SNMP traps are sent because only the **snmp** keyword is specified in the **snmp-server host** command. The community string is defined as comaccess.

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com comaccess snmp
```

This example shows how to send the SNMP traps to address 172.30.2.160:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps snmp
RP/0/RSP0/CPU0:router(config)# snmp-server host 172.30.2.160 public snmp
```

This example shows how to enable the router to send all traps to the host, myhost.cisco.com, using the community string public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps
```

```
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com public
```

This example shows how to prevent traps from being sent to any host. The BGP traps are enabled for all hosts, but only the configuration traps are enabled to be sent to a host.

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps bgp
RP/0/RSP0/CPU0:router(config)# snmp-server host hostabc public config
```

Related Topics

snmp-server engineid local, on page 421
snmp-server inform, on page 436
snmp-server traps bgp

snmp-server ifindex persist

To enable ifIndex persistence globally on all Simple Network Management Protocol (SNMP) interfaces, use the **snmp-server ifindex persist** command in global configuration mode. To disable global interface persistence, use the **no** form of this command.

snmp-server ifindex persist
no snmp-server ifindex persist

Syntax Description

This command has no keywords or arguments.

Command Default

Global interface persistence is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **snmp-server ifindex persist** command to enable ifIndex persistence on all interfaces that have entries in the ifIndex table of the IF-MIB. When enabled, this command retains the mapping between the ifName object values and the ifIndex object values (generated from the IF-MIB) persistent during reloads, allowing for consistent identification of specific interfaces using SNMP. Applications such as device inventory, billing, and fault detection depend on this feature.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to enable ifIndex persistence globally:

```
RP/0/RSP0/CPU0:router(config)# snmp-server ifindex persist
```

Related Topics

index persistence, on page 338
notification linkupdown, on page 344
show snmp interface, on page 367

snmp-server ifmib ifalias long

To enable the ifAlias IF-MIB object to accept an interface alias name that exceeds the 64-byte default, use the **snmp-server ifmib ifalias long** command. Use the **no** form of this command to revert to the default length.

snmp-server ifmib ifalias long
no snmp-server ifmib ifalias long

Syntax Description

This command has no keywords or arguments.

Command Default

Global interface persistence is disabled.

The alias name is 64 bytes in length.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **snmp-server ifmib ifalias long** command to enable the IF-MIB object ifAlias to accept an interface alias name that is greater than 64 bytes in length. The default length for the alias name is 64 bytes.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to enable the IF-MIB object ifAlias:

```
RP/0/RSP0/CPU0:router(config)# snmp-server ifmib ifalias long
RP/0/RSP0/CPU0:router(config)# exit

Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:yes
RP/0/RSP0/CPU0:router#
```

snmp-server ifmib internal cache max-duration

To configure the refresh interval for the IF-MIB statistics cache, use the **snmp-server ifmib internal cache max-duration** command in global configuration mode. To revert to the default cache interval, use the **no** form of this command.

snmp-server ifmib internal cache max-duration *timeout*

Syntax Description

timeout	Length of time before the cache is refreshed. Values can range from 0 to 60 seconds. The default is 15.

Command Default

timeout: 15 seconds

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.3	This command was introduced.

Usage Guidelines

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

The **snmp-server ifmib internal cache max-duration** command controls the refresh interval of the cache. If the *timeout* value in the **snmp-server ifmib internal cache max-duration** command is set to zero, the cache is disabled. By default, the counters are cached for 15 secs in the ifmib internal cache, after which it will be discarded.

Task ID

Task ID	Operation
snmp	read, write

This example shows how to change the refresh interval for the IF-MIB statistics cache.

```
RP/0/RSP0/CPU0:routerrouter(config)# snmp-server ifmib internal cache max-duration 60
```

Related Topics

snmp-server ifmib stats cache, on page 435

snmp-server ifmib ipsubscriber

To enable IP subscriber interfaces in the interfaces MIB (IF-MIB), use the **snmp-server ifmib ipsubscriber** command in global configuration mode. To disable IP subscriber interfaces, use the **no** form of this command.

snmp-server ifmib ipsubscriber
no snmp-server ifmib ipsubscriber

Syntax Description

This command has no keywords or arguments.

Command Default

Ip subscriber interfaces are not enabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
snmp	read, write

This example shows how to enable IP subscriber interfaces in the IF-MIB:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server ifmib ipsubscriber
```

snmp-server ifmib stats cache

To enable retrieval of cached statistics instead of real-time statistics, use the **snmp-server ifmib stats cache** command. To revert to the default, use the **no** form of this command.

snmp-server ifmib stats cache
no snmp-server ifmib stats cache

Syntax Description

This command has no keywords or arguments.

Command Default

Cached statistics are not enabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Cisco IOS XR statistics infrastructure maintains a cache of statistics for all interfaces. This cache is updated every 30 seconds. Use the **snmp-server ifmib stats cache** command to enable the IF-MIB to retrieve these cached statistics rather than real-time statistics. Accessing cached statistics is less CPU-intensive than accessing real-time statistics.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to enable the IF-MIB caches statistics:

```
RP/0/RSP0/CPU0:router(config)# snmp-server ifmib stats cache
RP/0/RSP0/CPU0:router(config)# exit

Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:yes
RP/0/RSP0/CPU0:router#
```

Related Topics

snmp-server ifmib internal cache max-duration, on page 433

snmp-server inform

To configure Simple Network Management Protocol (SNMP) inform message options, use the **snmp-server inform** command in global configuration mode. To revert to the default informs options, use the **no** form of this command.

snmp-server inform {**pending** *max-no* | **retries** *no-retries* | **timeout** *seconds*}
no snmp-server inform {**pending** *max-no* | **retries** *no-retries* | **timeout** *seconds*}

Syntax Description

pending *max-no*	Specifies the maximum number of inform messages to hold in the queue. The default is 25.
retries *no-retries*	Specifies the retry count for inform messages. Values can be from 1 to 100. The default is three.
timeout *seconds*	Specifies the inform message timeout value in seconds. The default is 15.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

To enable the sending of SNMP inform messages, use the **snmp-server host** command with the **informs** keyword. When SNMP server informs are enabled, the SNMP version can be only SNMPv2C or SNMPv3.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to configure SNMP inform messages:

```
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com informs comaccess
RP/0/RSP0/CPU0:router(config)# snmp-server inform pending 40
RP/0/RSP0/CPU0:router(config)# snmp-server inform retries 10
```

Related Topics

snmp-server host, on page 427

snmp-server interface

To enable an interface to send Simple Network Management Protocol (SNMP) trap notifications and enter SNMP interface configuration mode, use the **snmp-server interface** command in global configuration mode. To disable the sending of SNMP trap notifications on an interface, use the **no** form of this command.

snmp-server interface *type interface-path-id*
no snmp-server interface *type interface-path-id*

Syntax Description

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

Command Default

Ethernet interfaces are enabled to send SNMP trap notifications. SNMP trap notifications are disabled on all other physical and logical interfaces.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

The **snmp-server interface** command enters SNMP interface configuration mode for you to configure the available SNMP options.

Note In references to a Management Ethernet interface located on a route switch processor card, the physical slot number is numeric (0 through n-1 where n is the number of line card slots in the chassis) and the module is CPU0. Example: interface MgmtEth0/1/CPU0/0.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to assign ifIndex persistence on Packet-over-SONET/SDH (POS) interface 0/0/1/0:

```
RP/0/RSP0/CPU0:router(config)# snmp-server interface pos 0/0/1/0
RP/0/RSP0/CPU0:router(config-snmp-if)#
```

Related Topics

show snmp interface, on page 367
snmp-server engineid local, on page 421
snmp-server ifindex persist, on page 431

snmp-server interface subset

To enter snmp-server interface subset configuration mode for a set of interfaces, use the **snmp-server interface subset** command in global configuration mode. To revert to the default interface settings, use the **no** form of this command.

snmp-server interface subset *subset-number* **regular-expression** *expression*
no snmp-server interface subset *subset-number*

Syntax Description

subset-number	Identifying number of the interface subset, which also indicates its relative priority.
regular-expression *expression*	Specifies for which subset of interfaces to enter snmp-server interface subset configuration mode. The *expression* argument must be entered surrounded by double quotes.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

The *subset-number* argument is used to set the priority for an interface that matches more than one configured regular expressions. Lower values of the *subset-number* have a higher priority. If a single interface becomes part of a multiple-interface configured regular expression, the configuration with the lower *subset-number* value is applied.

Regular expressions have two constraints:

- Regular expressions must always be entered within double quotes to ensure that the CLI interprets each character correctly.
- All characters that are part of a regular expression are considered regular characters with no special meaning. In order to enter special characters, such as "\" or "?," they must be preceded by the backslash character "\." For example, to enter the regular expression ([A-Z][A-Z0-9]*)\b[^>]*>(.*?)</\1, you would enter ([A-Z][A-Z0-9]*)\\b[^>]*>(.*\?)</\\1.

Refer to the *Understanding Regular Expressions, Special Characters, and Patterns* module in *Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide* for more information regarding regular expressions.

From the snmp-server interface mode of a subset of interfaces, SNMP linkUp and linkDown notifications can be enabled or disabled using the **notification linkupdown disable** command.

Task ID

Task ID	Operation
snmp	read, write

This example illustrates how to configure all Gigabit Ethernet interfaces:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# snmp-server int subset 2
    regular-expression "^Gig[a-zA-Z]+[0-9/]+\."
RP/0/RSP0/CPU0:router(config-snmp-if-subset)#
```

Related Topics

notification linkupdown, on page 344
show snmp interface notification, on page 369
show snmp interface regular-expression, on page 371

snmp-server ipv4 dscp

To mark packets with a specific differentiated services code point (DSCP) value, use the **snmp-server ipv4 dscp** command in global configuration mode. To remove matching criteria, use the **no** form of this command.

snmp-server ipv4 dscp *value*
no snmp-server ipv4 dscp [*value*]

Syntax Description

value	Value of the DSCP. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: **default**, **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**.

Command Default

The IP DSCP default value for SNMP traffic is 0.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **snmp-server ipv4 dscp** command to specify an IP DSCP value to give SNMP traffic higher or lower priority in your network.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to configure the DSCP value to af32:

```
RP/0/RSP0/CPU0:router(config)# snmp-server ipv4 dscp af32
```

snmp-server ipv4 precedence

To mark packets with a specific precedence level to use for packet matching, use the **snmp-server ipv4 precedence** command in global configuration mode. To restore the system to its default interval values, use the **no** form of this command.

snmp-server ipv4 precedence *value*
no snmp-server ipv4 precedence [*value*]

Syntax Description

value Value of the precedence. The precedence value can be a number from 0 to 7, or it can be one of the following keywords:

critical

Set packets with critical precedence (5)

flash

Set packets with flash precedence (3)

flash-override

Set packets with flash override precedence (4)

immediate

Set packets with immediate precedence (2)

internet

Set packets with internetwork control precedence (6)

network

Set packets with network control precedence (7)

priority

Set packets with priority precedence (1)

routine

Set packets with routine precedence (0)

Command Default

The IP Precedence default value for SNMP traffic is 0.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **snmp-server ipv4 precedence** command to specify an IP Precedence value to give SNMP traffic higher or lower priority in your network.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to set the precedence to 2:

```
RP/0/RSP0/CPU0:router(config)# snmp-server ipv4 precedence 2
```

snmp-server location

To specify the system location for Simple Network Management Protocol (SNMP), use the **snmp-server location** command in

global configuration

mode. To remove the location string, use the **no** form of this command.

snmp-server location *system-location*
no snmp-server location

Syntax Description

system-location	String indicating the physical location of this device. The maximum string length is 255 alphanumeric characters.

Command Default

No system location string is set.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
snmp	read, write

This example shows how to specify a system location string:

```
RP/0/RSP0/CPU0:router(config)# snmp-server location Building 3/Room 214
```

Related Topics

snmp-server contact, on page 415

snmp-server mib bulkstat max-procmem-size

To configure the overall per-process memory size limit used by all bulk statistics files in the process, use the **snmp-server mib bulkstat max-procmem-size** command in

global configuration

mode. To remove the overall per-process memory size, use the **no** form of this command.

snmp mib bulkstat max-procmem-size *size*
no snmp mib bulkstat max-procmem-size [*size*]

Syntax Description

size	Overall per-process memory size limit in kilobytes. The valid range is from 100 to 200000. The default is 200000.

Command Default

The maximum process memory size is 200000 KB.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Currently 300 MB is the maximum process memory available for MIB and SNMP processes.

Task ID

Task ID	Operation
snmp	read, write

This example sets the maximum process memory size to 100000 KB.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat max-procmem-size 100000
```

snmp-server mib bulkstat object-list

To configure a Simple Network Management Protocol (SNMP) bulk statistics object list and enter bulk statistics objects configuration mode, use the **snmp-server mib bulkstat object-list** in

global configuration

mode. To remove an SNMP object list configuration, use the **no** form of this command.

snmp-server mib bulkstat object-list *object-list-name*
no snmp-server mib bulkstat object-list *object-list-name*

Syntax Description

object-list-name	Name or object identifier (OID) of the bulk statistics object list to configure.

Command Default

No SNMP bulk statistics object list is configured.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

The **snmp-server mib bulkstat object-list** command allows you to name an object list. Bulk statistics object lists are used for the Periodic MIB Data Collection and Transfer Mechanism.Use the **add** command to add objects to the object list configured with the **snmp-server mib bulkstat object-list** command. Bulk statistics object lists can be reused in multiple schemas.

Task ID

Task ID	Operation
snmp	read, write

In this example, a bulk statistics object list called ifmib is configured to include two objects:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat object-list ifmib
RP/0/RSP0/CPU0:router(config-bulk-objects)# add ifOutOctets
RP/0/RSP0/CPU0:router(config-bulk-objects)# add ifInOctets
```

Related Topics

add (bulkstat object), on page 331
show snmp mib bulkstat transfer, on page 375

snmp-server mib bulkstat schema

To configure a Simple Network Management Protocol (SNMP) bulk statistics schema and enter bulk statistics schema configuration mode, use the **snmp-server mib bulkstat schema** command in

global configuration

mode. To remove the SNMP bulk statistics schema, use the **no** form of this command.

snmp-server mib bulkstat schema *schema-name*
no snmp-server mib bulkstat schema *schema-name*

Syntax Description

schema-name	Specifies the name of the schema to configure.

Command Default

No schemas are configured.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

The **snmp-server mib bulkstat schema** command names the schema and enters bulk statistics schema configuration mode. Bulk statistics schema configuration mode is used to configure the object list, instance, and polling interval to be used in the schema.

The specific instances of MIB objects for which data should be collected are determined by appending the value of the **instance** command to the objects specified in the object list.

Multiple schemas can be associated with a single bulk statistics file when configuring the bulk statistics transfer options.

Task ID

Task ID	Operation
snmp	read, write

The following example shows how to configure a bulk statistics schema called GigE0/6/5/0:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat schema tengige 0/6/5/0
RP/0/RSP0/CPU0:router(config-bulk-sc)# object-list ifmib
RP/0/RSP0/CPU0:router(config-bulk-sc)# poll-interval 3
RP/0/RSP0/CPU0:router(config-bulk-sc)# instance exact interface tengige 0/6/5/0 subif
```

```
RP/0/RSP0/CPU0:router(config-bulk-sc)# exit
```

Related Topics

instance (bulkstat schema), on page 339
poll-interval, on page 347

snmp-server mib bulkstat transfer-id

To identify the bulk statistics transfer configuration and enter bulk statistics transfer configuration mode, use the **snmp-server mib bulkstat transfer-id** command in

global configuration

mode. To remove a previously configured transfer, use the **no** form of this command

snmp-server mib bulkstat transfer-id *transfer-id*
no snmp-server mib bulkstat transfer-id *transfer-id*

Syntax Description

transfer-id	Name of the transfer configuration.

Command Default

Bulk statistics transfer is not configured.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

The name, *transfer-id*, you specify for the bulk statistics transfer configuration is used in the filename of the bulk statistics file when it is generated and is used to identify the transfer configuration in the output of the **show snmp mib bulkstat transfer** command.

Task ID

Task ID	Operation
snmp	read, write

In this example, The bulk statistics transfer is given the name bulkstat1 and contains two schemas:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat transfer-id bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# schema IFMIB
RP/0/RSP0/CPU0:router(config-bulk-tr)# schema CAR
RP/0/RSP0/CPU0:router(config-bulk-tr)# url primary
ftp://user1:pswrd@cbin2-host/users/user1/bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# url secondary
tftp://user1@10.1.0.1/tftpboot/user1/bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# format schemaASCII
RP/0/RSP0/CPU0:router(config-bulk-tr)# transfer-interval 30
RP/0/RSP0/CPU0:router(config-bulk-tr)# retry 5
RP/0/RSP0/CPU0:router(config-bulk-tr)# buffer-size 1024
```

```
RP/0/RSP0/CPU0:router(config-bulk-tr)# retain 30
RP/0/RSP0/CPU0:router(config-bulk-tr)# end
```

Related Topics

buffer-size, on page 332
format (bulkstat), on page 336
retain, on page 348
retry, on page 350
schema, on page 352
show snmp mib bulkstat transfer, on page 375
transfer-interval, on page 531
url, on page 533

snmp-server mibs cbqosmib cache

To enable and configure caching of the QoS MIB statistics, use the **snmp-server mibs cbqosmib cache** command in global configuration mode. To disable caching, use the **no** form of this command.

snmp-server mibs cbqosmib cache {**refresh time** *time* | **service-policy count** *count*}
no snmp-server mibs cbqosmib cache [**refresh time** *time* | **service-policy count** *count*]

Syntax Description

refresh	Enables QoS MIB caching with a specified cache refresh time.
time *time*	Specifies the cache refresh time, in seconds. The *time* argument can be between 5 and 60. The default is 30.
service-policy	Enables QoS MIB caching with a limited number of service policies to cache.
count *count*	Specifies the maximum number of service policies to cache. The count argument can be between 1 and 5000.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
snmp	read, write

Example

This example illustrates how to enable QoS MIB caching with a refresh time:

```
RP/0/RSP0/CPU0:router(config)# snmp-server mibs cbqosmib cache refresh time 45
```

This example illustrates how to enable QoS MIB caching with a service policy count limitation:

```
RP/0/RSP0/CPU0:router(config)# snmp-server mibs cbqosmib cache service-policy count 10
```

Related Topics

snmp-server entityindex persist, on page 423
snmp-server mibs cbqosmib persist, on page 453

snmp-server mibs cbqosmib persist

To enable persistent storage of the CISCO-CLASS-BASED-QOS-MIB data across process restarts, switchovers, and device reloads, use the **snmp-server mibs cbqosmib persist** command in global configuration mode. To disable persistent storage of the MIB data, use the **no** form of this command.

snmp-server mibs cbqosmib persist
no snmp-server mibs cbqosmib persist

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
snmp	read, write

Example

This example illustrates how to enable persistent storage of CISCO-CLASS-BASED-QOS-MIB data:

```
RP/0/RSP0/CPU0:router(config)# snmp-server mibs cbqosmib persist
```

Related Topics

snmp-server entityindex persist, on page 423

snmp-server mibs eventmib congestion-control

To configure the generation of SNMP traps when congestion exceeds configured thresholds, use the **snmp-server mibs eventmib congestion-control** command in global configuration mode. To restore the default values, use the **no** form of this command.

snmp-server mibs eventmib congestion-control *type interface-path-id* **falling** *lower-threshold* **interval** *sampling-interval* **rising** *upper-threshold*
no snmp-server mibs eventmib congestion-control *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.
falling *lower-threshold*	Specifies the lower threshold for which to determine whether an mteTriggerFalling SNMP Trap is generated.
interval *sampling-interval*	Specifies how often the congestion statistics are polled. The *interval* argument, in minutes, can be between 5 and 1440; it must be a multiple of 5.
rising *upper-threshold*	Specifies the upper threshold for which to determine whether an mteTriggerRising SNMP Trap is generated.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Note A maximum of 100 interfaces can be monitored for congestion.

Congestion configurations using the **snmp-server mibs eventmib congestion-control** command cannot be modified using SNMP SET and vice versa.

When the congestion between two intervals increases above the *upper-threshold* argument, an mteTriggerRising SNMP trap is generated. This trap is not generated until the congestion drops below the lower threshold and then rises above the upper threshold.

When the congestion between two intervals falls below the *lower-threshold* argument, and an SNMP mteTriggerRising trap was generated previously, an SNMP mteTriggerFalling trap is generated. The mteTriggreRising trap is not generated until the congestion goes above the upper threshold and then falls back below the lower threshold.

The *lower-threshold* value (falling) should be set to a value less than or equal to the *upper-threshold* value (rising).

The **snmp-server mibs eventmib congestion-control** command is configured on a specific interface and is supported on the following cards:

- 8-port 10 Gigabit Ethernet PLIM
- 16-port OC-48c/STM-16 POS/DPT PLIM
- 1-port OC-768c/STM-256 POS PLIM
- 4-port OC-192c/STM-64 POS/DPT PLIM
- All Ethernet SPAs
- 2-port and 4-port OC-3c/STM-1 POS SPAs
- 2-port, 4-port, and 8-port OC-12c/STM-4 POS SPAs
- 2-port and 4-port OC-48c/STM-16 POS/RPR SPAs
- 1-port OC-192c/STM-64 POS/RPR SPA

Task ID

Task ID	Operations
snmp	read, write

This example shows how to configure the generation of SNMP traps in response to congestion:

```
RP/0/RSP0/CPU0:router(config)# snmp-server mibs eventmib congestion-control pos 0/1/0/0
    falling 1 interval 5 rising 2
```

snmp-server mibs eventmib packet-loss

To configure the generation of SNMP traps when packet loss exceeds configured thresholds, use the **snmp-server mibs eventmib packet-loss** command in global configuration mode. To restore the default values, use the **no** form of this command.

snmp-server mibs eventmib packet-loss *type interface-path-id* **falling** *lower-threshold* **interval** *sampling-interval* **rising** *upper-threshold*
no snmp-server mibs eventmib packet-loss *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.
falling *lower-threshold*	Specifies the lower threshold for which to determine whether an mteTriggerFalling SNMP Trap is generated.
interval *sampling-interval*	Specifies how often the packet loss statistics are polled. The *interval* argument, in minutes, can be between 5 and 1440; it must be a multiple of 5.
rising *upper-threshold*	Specifies the upper threshold for which to determine whether an mteTriggerRising SNMP Trap is generated.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

Note A maximum of 100 interfaces can be monitored for packet loss.

Packet loss configurations using the **snmp-server mibs eventmib packet-loss** command cannot be modified using SNMP SET and vice versa.

When the packet loss between two intervals increases above the *upper-threshold* argument, an mteTriggerRising SNMP trap is generated. This trap is not generated until the packet loss drops below the lower threshold and then rises above the upper threshold.

When the packet loss between two intervals falls below the *lower-threshold* argument, and an SNMP mteTriggerRising trap was generated previously, an SNMP mteTriggerFalling trap is generated. The mteTriggreRising trap is not generated until the packet loss goes above the upper threshold and then falls back below the lower threshold.

The *lower-threshold* value (falling) should be set to a value less than or equal to the *upper-threshold* value (rising).

The **snmp-server mibs eventmib packet-loss** command is configured on a specific interface and is supported on the following cards:

- 8-port 10 Gigabit Ethernet PLIM
- 16-port OC-48c/STM-16 POS/DPT PLIM
- 1-port OC-768c/STM-256 POS PLIM
- 4-port OC-192c/STM-64 POS/DPT PLIM
- All Ethernet SPAs
- 2-port and 4-port OC-3c/STM-1 POS SPAs
- 2-port, 4-port, and 8-port OC-12c/STM-4 POS SPAs
- 2-port and 4-port OC-48c/STM-16 POS/RPR SPAs
- 1-port OC-192c/STM-64 POS/RPR SPA

Task ID

Task ID

Task ID	Operations
snmp	read, write

This example shows how to configure the generation of SNMP traps in response to packet loss:

```
RP/0/RSP0/CPU0:router(config)# snmp-server mibs eventmib packet-loss pos 0/1/0/0
    falling 1 interval 5 rising 2
```

snmp-server mibs sensormib cache

To enable and configure caching for sensor mib values, use **snmp-server mibs sensormib cache** command in global configuration mode. To restore the default values, use the **no** form of this command.

snmp-server mibs sensormib cache

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration mode.

Command History

Release	Modification
Release 5.3.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Example

```
RP/0/RSP0/CPU0:router(config)# snmp-server mibs sensormib cache
```

snmp-server mibs subscriber threshold

To set the snmp-server mibs server threshold parameters, use the **snmp-server mibs subscriber threshold** command in the global configuration mode. To delete any of the set parameters, use the **no** form of the command.

snmp-server mibs subscriber threshold [**rising** | **falling** | **delta-loss percent** | **delta-loss evaluation**] [**access-if location** *interface-path-id* **interval** *seconds*] [**session-count**]

nosnmp-server mibs subscriber threshold

Syntax Description

rising	Rising threshold value. The set value triggers the traps. Traps are generated when the number of sessions exceed the rising threshold value.
falling	Falling threshold value. The set value triggers the traps. Traps are generated when the number of sessions are lesser than the falling threshold value.
delta-loss percent	Delta-loss percentage.
delta-loss evaluation	The actual subscriber sessions (after delta-loss) . This is based on the set delta-loss percentage. If the number of sessions exceed the loss percentage, traps are generated.
access-if	Access-interface.
location *name*	Location name.
interval *seconds*	Interval between the rising and the falling thresholds (in seconds).
session-count	Subscriber-session count.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 5.1	This command was introduced.

Usage Guidelines

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

The minimum delta loss interval is 30 seconds and can be incremented by 10 seconds till the time period reaches 5 minutes.

Task ID

Task ID	Operation
snmp	read, write

Example

```
RP/0/RSP0/CPU0:router (config) # snmp-server mibs subscriber threshold delta-loss evaluation
 access-if tengige 0/4/0/0 interval 100
```

snmp-server mibs subscriber threshold access-if

To disable the per-session access notifications by the session monitoring process, use the **snmp-server mibs subscriber threshold access-if** in the global configuration mode. To enable notifications, use the **no** form of the command.

snmp-server mibs subscriber threshold access-if subset*number* **regular expression** *word* **notification rising-falling disable**
nosnmp-server mibs subscriber threshold access-if

Syntax Description

subset *number*	Subset number of the subscriber threshold. Lower the subset value, higher is the priority. Range is 1 to 255.
regular expression *word*	Regular expression to match the interface name. Traps on the corresponding access interface(s) are disabled.
notification	Name of the notification.
rising-falling	The rising and falling thresholds.
disable	Disables the access interface notifications.

Command Default

Session monitoring is enabled by default

Command Modes

Global configuration

Command History

Release	Modification
Release 5.1	This command was introduced.

Usage Guidelines

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

The **regular expression** keyword disables notifications of the access-interface.

Task ID

Task ID	Operation
snmp	read, write

Example

```
RP/0/RSP0/CPU0:router (config) # snmp-server mibs subscriber threshold access-if subset 100
 regular expression notification rising-falling disable
```

snmp-server notification-log-mib

To configure the NOTIFICATION-LOG-MIB, use the **snmp-server notification-log-mib** command in global configuration mode. To remove the specified configuration, use the **no** form of this command.

snmp-server notification-log-mib {**globalAgeOut** *time* | **globalSize** *size* | **default** | **disable** | **size** *size*}
no snmp-server notification-log-mib {**globalAgeOut** | **globalSize** | **default** | **disable** | **size**}

Syntax Description

globalAgeOut *time*	Specifies how much time, in minutes, a notification remains in the log. Values for the *time* argument can range from 0 to 4294967295; the default is 15.
globalSize *size*	Specifies the maximum number of notifications that can be logged in all logs. The default is 500.
default	Specifies to create a default log.
disable	Specifies to disable logging to the default log.
size *size*	Specifies the maximum number of notifications that the default log can hold. The default is 500.

Command Default

NOTIFICATION-LOG-MIB notifications are not logged.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Logging of NOTIFICATION-LOG-MIB notifications begins when the default log is created. Named logs are not supported, therefore only the default log can be created.

Task ID

Task ID	Operations
snmp	read, write

The following example creates a default log for notifications:

```
RP/0/RSP0/CPU0:router(config)# snmp-server notification-log-mib default
```

This example removes the default log:

```
RP/0/RSP0/CPU0:router(config)# no snmp-server notification-log-mib default
```

This example configures the size of all logs to be 1500:

```
RP/0/RSP0/CPU0:router(config)# snmp-server notification-log-mib globalSize 1500
```

Related Topics

snmp-server community-map, on page 413

snmp-server packetsize

To establish control over the largest Simple Network Management Protocol (SNMP) packet size permitted when the SNMP server is receiving a request or generating a reply, use the **snmp-server packetsize** command in

global configuration

mode. To restore the default value, use the **no** form of this command.

snmp-server packetsize *size*
no snmp-server packetsize

Syntax Description

size	Packet size, in bytes. Range is from 484 to 65500. The default is 1500.

Command Default

size: 1500

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **snmp-server packetsize** command to establish control over the largest SNMP packet size permitted when the SNMP server is receiving a request or generating a reply.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to set the maximum size of SNMP packets to 1024 bytes:

```
RP/0/RSP0/CPU0:router(config)# snmp-server packetsize 1024
```

snmp-server queue-length

To establish the message queue length for each trap host for Simple Network Management Protocol (SNMP), use the **snmp-server queue-length** command in

global configuration

mode. To restore the default value, use the **no** form of this command.

snmp-server queue-length *length*
no snmp-server queue-length

Syntax Description

length	Integer that specifies the number of trap events that can be held before the queue must be emptied. Range is from 1 to 5000.

Command Default

length : 100

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **snmp-server queue-length** command to define the length of the message queue for each trap host. After a trap message is successfully sent, Cisco IOS XR software continues to empty the queue at a throttled rate to prevent trap flooding.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to set the SNMP notification queue to 20 events:

```
RP/0/RSP0/CPU0:router(config)# snmp-server queue-length 20
```

snmp-server target list

To create a Simple Network Management Protocol (SNMP) target list, use the **snmp-server target list** command in

global configuration

mode. To remove an SNMP target list, use the **no** form of this command.

snmp-server target list *target-list* {**vrf** *vrf-name* | **host** *hostname*}
no snmp-server target list *target-list*

Syntax Description

target-list	Name of the target list.
vrf *vrf-name*	Specifies the name of the VRF hosts included in the target list.
host *hostname*	Assigns a hostname to the target list. The *hostname* variable is a name or IP address.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use this command to create an SNMP target list and assign hosts to the list. When a target list is mapped to a community name using the **snmp-server community-map** command, SNMP access is restricted to the hosts in the target list (for that community name).

Task ID

Task ID	Operations
snmp	read, write

In this example, a new target list “sample3” is created and assigned to the vrf server “server2:”

```
RP/0/RSP0/CPU0:router(config)# snmp-server target list sample3 vrf server2
```

Related Topics

snmp-server community-map, on page 413

snmp-server throttle-time

To specify the throttle time for handling incoming Simple Network Management Protocol (SNMP) messages, use the **snmp-server throttle-time** command in

global configuration

mode. To restore the throttle time to its default value, use the **no** form of this command.

snmp-server throttle-time *time*
no snmp-server throttle-time

Syntax Description

time	Throttle time for the incoming queue, in milliseconds. Values can be from 50 to 1000.

Command Default

time : 0

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
snmp	read, write

In the following example, the throttle time is set to 500 milliseconds:

```
RP/0/RSP0/CPU0:router(config)# snmp-server throttle-time 500
```

Related Topics

snmp-server community-map, on page 413

snmp-server timeouts subagent

To change the timeout used by the SNMP agent while it waits for a response from a subagent, use the **snmp-server timeouts subagent** command in

global configuration

mode. SNMP subagents are feature-specific entities that register with the SNMP agent and implement sets of MIB objects.

snmp-server timeouts subagent *timeout*
no snmp-server timeouts subagent *timeout*

Syntax Description

timeout	The timeout used by the SNMP agent when waiting for a response from a MIB module, in seconds. The default is 10.

Command Default

timeout : 10

Command Modes

Global configuration

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
snmp	read, write

In the following example, the timeout is set to 8 seconds:

```
RP/0/RSP0/CPU0:router(config)# snmp-server timeouts subagent 8
```

snmp-server timeouts duplicate

To set the timeout value for the snmp-sever duplicate request feature, use the **snmp-server timeouts duplicate** command in the appropriate mode. To delete the set value, use the **no** form of the command.

snmp-server timeouts duplicate *timeout-value*
no snmp-server timeouts duplicate *timeout-value*

Syntax Description

timeout-value Timeout value in seconds. Range is 0 to 20 seconds.

- 0- To Remove this feature support. i.e SNMP will process all the packets irrespective of duplicate (retry) Packets.
- 1- This is the default value, i.e if no configuration is present , then, the timeout value is set to 1. If any packet takes more than 1 second for getting processed, then the Duplicate drop feature is enabled.
- 2 to 20 - if the packet processing is done between 2 and 20 seconds, then the Duplicate drop feature is enabled.

Command Default

1 second

Command Modes

Global configuration

Command History

Release	Modification
Release 5.1.1	This feature was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
snmp	read, write

Example

This example shows how to use the **snmp-server timeouts duplicate** command:

```
RP/0/RSP0/CPU0:router (config) #  snmp-server timeouts duplicate 10
```

snmp-server trap authentication vrf disable

To disable authentication traps on VPNs, use the **snmp-server trap authentication vrf disable** command in

global configuration

mode.

snmp-server trap authentication vrf disable

Syntax Description

This command has no keywords or arguments.

Command Default

Authentication traps are enabled on VPNs by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
snmp	read, write

This example illustrates how to disable authentication traps on VPNs:

```
RP/0/RSP0/CPU0:router(config)# snmp-server trap authentication vrf disable
```

Related Topics

snmp-server vrf, on page 521

snmp-server trap link ietf

To enable the varbind used for linkUp and linkDown SNMP traps to utilize the RFC 2863 standard varbind, use the **snmp-server trap link ietf** command in

global configuration

mode. To restore the default value, use the **no** form of this command..

snmp-server trap link ietf
nosnmp-server trap link ietf

Syntax Description

This command has no keywords or arguments.

Command Default

The default varbind used is cisco.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

For more information about linkUP and linkDown notifications, see RFC 2863, *The Interface Group MIB*, and RFC 3418, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to enable the RFC 2863 standard varbind:

```
RP/0/RSP0/CPU0:router# snmp-server trap link ietf
```

Related Topics

snmp-server engineid local, on page 421
snmp-server host, on page 427
snmp-server traps bgp
snmp-server traps snmp, on page 507
snmp-server traps syslog, on page 509

snmp-server trap throttle-time

To specify the throttle time for handling more Simple Network Management Protocol (SNMP) traps, use the **snmp-server trap throttle-time** command in

global configuration

mode. To restore the throttle time to its default value, use the **no** form of this command.

snmp-server trap throttle-time *time*
no snmp-server trap throttle-time

Syntax Description

time	Throttle time in milliseconds. Values can be from 10 to 500.

Command Default

250

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
snmp	read, write

In the following example, the trap throttle time is set to 500 milliseconds:

```
RP/0/RSP0/CPU0:router(config)# snmp-server trap throttle-time 500
```

Related Topics

snmp-server throttle-time, on page 468

snmp-server traps

To enable Simple Network Management Protocol (SNMP) trap notifications, use the **snmp-server traps** command in global configuration mode. To disable SNMP notifications, use the **no** form of this command.

snmp-server traps *notification-type*
no snmp-server traps [*notification-type*]

Syntax Description *notification-type*

(Optional) Type of notification (trap) to enable or disable. If no type is specified, all notifications available on the device are enabled or disabled.

The notification type can be one or more of the following keywords:

bfd

Enables Bidirectional Forwarding Detection (BFD) traps.

bgp

Enables BGP4-MIB and CISCO-BGP4-MIB traps.

bridgemib

Enables SNMP traps for the Bridge MIB.

config

Controls configuration notifications, as defined in the CISCO-CONFIG-MAN-MIB (enterprise 1.3.6.1.4.1.9.9.43.2). The notification type is: (1) ciscoConfigManEvent.

copy-complete

Enables CISCO-CONFIG-COPY-MIB ccCopyCompletion traps.

ds1

Enables SNMP Cisco DS1 traps.

ds2

Enables SNMP Cisco DS2 traps.

entity

Controls Entity MIB modification notifications. This notification type is defined in the ENTITY-MIB (enterprise 1.3.6.1.2.1.47.2) as: (1) entConfigChange.

ethernet

Enables Ethernet link OAM and 802.1ag connectivity fault management traps.

flash insertion

Enables ciscoFlashDeviceInsertedNotif.

flash removal

Enables ciscoFlashDeviceRemovedNotif.

fru-ctrl

Enables SNMP entity field-replaceable unit (FRU) control traps.

hsrp

Enables SNMP HSRP traps.

ipsec tunnel start

Enables SNMP IPsec tunnel start traps.

ipsec tunnel stop

Enables SNMP IPsec tunnel stop traps.

isakmp

Enables ISAKMP traps.

l2vpn all

Enables all Layer 2 VPN traps.

l2vpn vc-down

Enables Layer 2 VPN VC down traps.

l2vpn vc-up

Enables Layer 2 VPN VC up traps.

mpls frr all

Enables all MPLS fast reroute MIB traps.

mpls frr protected

Enables MPLS fast reroute tunnel protected traps.

mpls ldp

Enables SNMP Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) traps.

mpls traffic-eng

Enables SNMP MPLS traffic engineering traps.

msdp peer-state-change

Enables SNMP MSDP Peer state change traps.

ntp

Enables SNMP Cisco NTP traps.

otn

Enables SNMP Cisco optical transport network (OTN) traps.

pim

Enables SNMP PIM traps.

rf

Enables RF-MIB traps.

sensor

Enables SNMP entity sensor traps.

snmp

Enables SNMP traps.

sonet

Enables SONET traps.

syslog

Controls error message notifications (Cisco-syslog-MIB). Specify the level of messages to be sent with the **logging history** command.

system

Enables SNMP SYSTEMMIB-MIB traps.

vpls

Enables virtual private LAN service (VPLS) traps.

vrrp events

Enables Virtual Router Redundancy Protocol (VRRP) traps.

Note
To display the trap notifications supported on a platform, use the online help (**?**) function.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 3.9.0	The **bridgemib** , **ds1** , **ds3** , **otn** , , **system** , and **vrrp events** keywords were introduced.

Usage Guidelines

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

Use the **snmp-server traps** command to enable trap requests for the specified notification types. To configure the router to send SNMP notifications, specify at least one **snmp-server traps** command. When the command is entered with no keyword, all notification types are enabled. When a notification type keyword is specified, only the notification type related to that keyword is enabled. To enable multiple types of notifications, issue a separate **snmp-server traps** command for each notification type.

More information about individual MIBs can be found in the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

The **snmp-server traps** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.



Note The use of **flash insertion** and **flash removal** keywords is limited to IOS XR 32-bit OS on ASR 9000.

Task ID

Task ID	Operations
snmp	read, write

Some SNMP trap notifications require additional Task IDs as indicated in the following table:

Notification Type	Task ID	Operations
bfd	bgp	read, write
	ospf	read, write
	isis	read, write
	mpls-te	read, write
	snmp	read, write
bgp	bgp	read, write
copy-complete	config-services	read, write
ipsec	crypto	read, write
isakmp	crypto	read, write
l2vpn	l2vpn	read, write
mpls frr	mpls-ldp	read, write
	mpls-te	read, write
mpls l3vpn	ipv4	read, write
	mpls-ldp	read, write
	mpls-te	read, write
mpls ldp	mpls-ldp	read, write
	mpls-te	read, write
mpls traffic-eng	mpls-ldp	read, write
	mpls-te	read, write
ospf	ospf	read, write
syslog	sysmgr	read, write
vpls	l2vpn	read, write

This example shows how to enable the router to send all traps to the host specified by the name myhost.cisco.com, using the community string defined as public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com public
```

Related Topics

snmp-server host, on page 427
snmp-server traps bgp
snmp-server traps snmp, on page 507
snmp-server traps syslog, on page 509

snmp-server traps bgp updown

To enable Border Gateway Protocol (BGP) to receive Simple Network Management Protocol (SNMP) notifications when a BGP peer changes state in IPv4 neighbor sessions, use the **snmp-server traps bgp updown** command in global configuration mode.

snmp-server traps bgp [updown]

Syntax Description

bgp	Specifies IPv4 neighbor sessions.
updown	(Optional) Specifies trap notifications.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

SNMP notifications are sent as traps.

BGP generates traps when:

- A neighbor's session state has changed.
- A neighbor prefix limit has exceeded.
- A neighbor prefix count is under the limit.

Multiple traps can be generated when the neighbor is not in steady state.

Configure **snmp-server traps bgp updown** command to prevent the generation multiple traps.

When you configure the **snmp-server traps bgp updown** command, traps are sent out only when the BGP neighbor goes to established state or moves out from the established state. The prefix limit traps remain unaffected.

When you configure the **bgp** keyword, traps are sent for IPv4 neighbor sessions only.

Example

The following example shows how to enable the router to send BGP state-change notifications to the host at the address myhost.cisco.com using the community string defined as public in IPv4 neighbor sessions only:

```
Router(config)# snmp-server traps bgp updown
Router(config)# snmp-server host myhost.cisco.com version 2c public
```

snmp-server traps cbgp2 updown

To enable Border Gateway Protocol (BGP) to receive Simple Network Management Protocol (SNMP) notifications when a BGP peer changes state in both IPv4 and IPv6 neighbor sessions, use the **snmp-server traps cbgp2 updown** command in global configuration mode.

snmp-server traps cbgp2 [updown]

Syntax Description

cbgp2	Specifies IPv4 and IPv6 neighbor sessions.
updown	(Optional) Specifies trap notifications.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

SNMP notifications are sent as traps.

BGP generates traps when:

- A neighbor's session state has changed.
- A neighbor prefix limit has exceeded.
- A neighbor prefix count is under the limit.

Multiple traps can be generated when the neighbor is not in steady state.

Configure **snmp-server traps cbgp2 updown** command to prevent the generation multiple traps.

When you configure the **snmp-server traps cbgp2 updown** command, traps are sent out only when the BGP neighbor goes to established state or moves out from the established state. The prefix limit traps remain unaffected.

When you configure the **cbgp2** keyword, traps are sent for both IPv4 and IPv6 neighbor sessions.

Example

The following example shows how to enable the router to send BGP state-change notifications to the host at the address myhost.cisco.com using the community string defined as public in both IPv4 and IPv6 neighbor sessions:

```
Router(config)# snmp-server traps cbgp2 updown
Router(config)# snmp-server host myhost.cisco.com version 2c public
```

snmp-server traps mpls l3vpn

To enable the sending of MPLS Layer 3 VPN Simple Network Management Protocol (SNMP) notifications, use the **snmp-server traps mpls l3vpn** command in global configuration mode. To disable MPLS Layer 3 VPN SNMP notifications, use the **no** form of this command.

snmp-server traps mpls l3vpn {**all** | **max-threshold-cleared** | **max-threshold-exceeded** | **max-threshold-reissue-notif-time** *seconds* | **mid-threshold-exceeded** | **vrf-down** | **vrf-up**}
no snmp-server traps mpls l3vpn

Syntax Description

all	Enables all MPLS Layer 3 VPN traps.
max-threshold-cleared	Enables maximum threshold cleared traps.
max-threshold-exceeded	Enables maximum threshold exceeded traps.
max-threshold-reissue-notif-time *seconds*	Specifies the time interval for reissuing a maximum threshold notification, in seconds.
mid-threshold-exceeded	Enables mid-threshold exceeded traps.
vrf-down	Enables VRF down traps.
vrf-up	Enables VRF up traps.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to enable the device to send MPLS Layer 3 VPN traps:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps mpls l3vpn all
```

Related Topics

snmp-server traps, on page 474

snmp-server traps ospf errors

To enable Open Shortest Path First (OSPF) error Simple Network Management Protocol (SNMP) notifications, use the **snmp-server traps ospf errors** command in global configuration mode. To disable OSPF error SNMP notifications, use the **no** form of this command.

snmp-server traps ospf errors {**authentication-failure** | **bad-packet** | **config-error** | **virt-authentication-failure** | **virt-bad-packet** | **virt-config-error**}
no snmp-server traps ospf errors {**authentication-failure** | **bad-packet** | **config-error** | **virt-authentication-failure** | **virt-bad-packet** | **virt-config-error**}

Syntax Description

authentication-failure	Enables SNMP traps for authentication failure errors on physical interfaces.
bad-packet	Enables SNMP traps for bad packet errors on physical interfaces.
config-error	Enables SNMP traps for configuration errors on physical interfaces.
virt-authentication-failure	Enables SNMP traps for authentication failure errors on virtual interfaces.
virt-bad-packet	Enables SNMP traps for bad packet errors on virtual interfaces.
virt-config-error	Enables SNMP traps for configuration errors on virtual interfaces.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

SNMP notifications can be sent as traps.

For a complete description of OSPF error notifications and additional MIB functions, see the OSPF-TRAP-MIB in the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

The **snmp-server traps ospf errors** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to enable the router to send OSPF error notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps ospf errors
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 421
snmp-server host, on page 427
snmp-server traps snmp, on page 507
snmp-server traps syslog, on page 509

snmp-server traps ospf lsa

To enable Open Shortest Path First (OSPF) link-state advertisement Simple Network Management Protocol (SNMP) notifications, use the **snmp-server traps ospf lsa** command in global configuration mode. To disable OSPF link state SNMP notifications, use the **no** form of this command.

snmp-server traps ospf lsa {**lsa-maxage** | **lsa-originate**}
no snmp-server traps ospf lsa {**lsa-maxage** | **lsa-originate**}

Syntax Description

lsa-maxage	Enables SNMP traps for link-state advertisement maxage.
lsa-originate	Enables SNMP traps for new link-state advertisement origination.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

SNMP notifications can be sent as traps.

For a complete description of OSPF link-state advertisement notifications and additional MIB functions, see the OSPF-TRAP-MIB in the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

The **snmp-server traps ospf lsa** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to enable the router to send OSPF link-state advertisement notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps ospf lsa lsa-maxage
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 421

snmp-server host, on page 427
snmp-server traps snmp, on page 507
snmp-server traps syslog, on page 509

snmp-server traps ospf retransmit

To enable Open Shortest Path First (OSPF) retransmission Simple Network Management Protocol (SNMP) notifications, use the **snmp-server traps ospf retransmit** command in global configuration mode. To disable OSPF retransmission SNMP notifications, use the **no** form of this command.

snmp-server traps ospf retransmit {**packets** | **virt-packets**}
no snmp-server traps ospf retransmit {**packets** | **virt-packets**}

Syntax Description

packets	Enables SNMP traps for packet retransmissions on physical interfaces.
virt-packets	Enables SNMP traps for packet retransmissions on virtual interfaces.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

SNMP notifications can be sent as traps.

For a complete description of OSPF retransmission notifications and additional MIB functions, see the OSPF-TRAP-MIB in the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

The **snmp-server traps ospf retransmit** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to enable the router to send OSPF retransmission notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps ospf retransmit packets
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 421

snmp-server host, on page 427
snmp-server traps snmp, on page 507
snmp-server traps syslog, on page 509

snmp-server traps ospf state-change

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) neighbor state change, use the **snmp-server traps ospf state-change** command in global configuration mode. To disable OSPF state-change SNMP notifications, use the **no** form of this command.

snmp-server traps ospf state-change {**if-state-change** | **neighbor-state-change** | **virtif-state-change** | **virtneighbor-state-change**}
no snmp-server traps ospf state-change {**if-state-change** | **neighbor-state-change** | **virtif-state-change** | **virtneighbor-state-change**}

Syntax Description

if-state-change	Enables SNMP traps for OSPF non-virtual interface state chages.
neighbor-state-change	Enables SNMP traps for OSPF neighbor state changes
virtif-state-change	Enables SNMP traps for OSPF virtual interface state changes.
virtneighbor-state-change	Enables SNMP traps for OSPF virtual neighbor state changes.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

SNMP notifications can be sent as traps.

Use the **snmp-server traps ospf state-change** command to enable or disable OSPF server state-change notifications, as defined in the MIB. One notification type is ospfNbrStateChange.

For example, the OSPF ospfNbrStateChange notification is defined in the OSPF MIB as follows:

```
!     ospfNbrStateChange NOTIFICATION-TYPE
!         OBJECTS {
!                     ospfRouterId, -- The originator of the trap
!                     ospfNbrIpAddr,
!                     ospfNbrAddressLessIndex,
!                     ospfNbrRtrId,
!                     ospfNbrState  -- The new state
!                   }
!         STATUS             current
```

For a complete description of these notifications and additional MIB functions, see the OSPF-TRAP-MIB in the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

The **snmp-server traps ospf state-change** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to enable the router to send OSPF state-change notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps ospf state-change neighbor-state-change
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 421
snmp-server host, on page 427
snmp-server traps snmp, on page 507
snmp-server traps syslog, on page 509

snmp-server traps ospfv3 errors

To enable Open Shortest Path First (OSPF) Version 3 error Simple Network Management Protocol (SNMP) notifications, use the **snmp-server traps ospfv3 errors** command in global configuration mode. To disable OSPFv3 error SNMP notifications, use the **no** form of this command.

snmp-server traps ospfv3 errors [**bad-packet** | **config-error** | **virt-bad-packet** | **virt-config-error**]
no snmp-server traps ospfv3 errors [**bad-packet** | **config-error** | **virt-bad-packet** | **virt-config-error**]

Syntax Description

bad-packet	Enables SNMP traps for bad packet errors on physical interfaces.
config-error	Enables SNMP traps for configuration errors on physical interfaces.
virt-bad-packet	Enables SNMP traps for bad packet errors on virtual interfaces.
virt-config-error	Enables SNMP traps for configuration errors on virtual interfaces.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

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

SNMP notifications can be sent as traps.

For a complete description of OSPFv3 error notifications and additional MIB functions, see the OSPFV3-MIB in the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

The **snmp-server traps ospfv3 errors** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to enable the router to send OSPF error notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps ospfv3 errors
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 421
snmp-server host, on page 427
snmp-server traps snmp, on page 507
snmp-server traps syslog, on page 509

snmp-server traps ospfv3 state-change

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) Version 3 state changes, use the **snmp-server traps ospfv3 state-change** command in global configuration mode. To disable OSPFv3 state-change SNMP notifications, use the **no** form of this command.

snmp-server traps ospfv3 state-change [**if-state-change** | **neighbor-state-change** | **nssa-state-change** | **restart-helper-status-change** | **restart-status-change** | **restart-virtual-helper-status-change** | **virtif-state-change** | **virtneighbor-state-change**]
no snmp-server traps ospfv3 state-change [**if-state-change** | **neighbor-state-change** | **nssa-state-change** | **restart-helper-status-change** | **restart-status-change** | **restart-virtual-helper-status-change** | **virtif-state-change** | **virtneighbor-state-change**]

Syntax Description

if-state-change	Enables SNMP traps for OSPFv3 non-virtual interface state chages.
neighbor-state-change	Enables SNMP traps for OSPFv3 neighbor state changes
nssa-state-change	Enables SNMP traps for OSPFv3 not so stubby area (NSSA) status changes.
restart-helper-status-change	Enables SNMP traps for OSPFv3 restart helper status changes.
restart-status-change	Enables SNMP traps for OSPFv3 restart status changes.
restart-virtual-helper-status-change	Enables SNMP traps for OSPFv3 virtual helper restart status changes.
virtif-state-change	Enables SNMP traps for OSPFv3 virtual interface state changes.
virtneighbor-state-change	Enables SNMP traps for OSPFv3 virtual neighbor state changes.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

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

SNMP notifications can be sent as traps.

Use the **snmp-server traps ospfv3 state-change** command to enable or disable the various OSPFv3 server state-change notifications, as defined in the MIB.

The **snmp-server traps ospfv3 state-change** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to enable the router to send OSPFv3 NSSA state-change notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps ospfv3 state-change nssa-state-change
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 421
snmp-server host, on page 427
snmp-server traps snmp, on page 507
snmp-server traps syslog, on page 509

snmp-server traps pim interface-state-change

To enable Protocol Independent Multicast (PIM) interface status notification, use the **snmp-server traps pim interface-state-change** command in global configuration mode. To disable this command so no notification is sent, use the **no** form of this command.

snmp-server traps pim interface-state-change
no snmp-server traps pim interface-state-change

Syntax Description

This command has no keywords or arguments.

Command Default

Simple Network Management Protocol (SNMP) notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Use the **snmp-server traps pim interface-state-change** command to send notifications when a PIM interface changes status from up to down. When the status is up, the notification signifies the restoration of a PIM interface. When the status is down, the notification signifies the loss of a PIM interface.

PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files that can be accessed from the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to use the **snmp-server traps pim interface-state-change** command:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps pim interface-state-change
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 421
snmp-server host, on page 427
snmp-server traps pim invalid-message-received, on page 499

snmp-server traps pim neighbor-change, on page 501
snmp-server traps pim rp-mapping-change, on page 503
snmp-server traps snmp, on page 507
snmp-server traps syslog, on page 509

snmp-server traps pim invalid-message-received

To enable notifications for monitoring invalid Protocol Independent Multicast (PIM) protocol operations, such as invalid register received and invalid join or prune received, use the **snmp-server traps pim invalid-message-received** command in global configuration mode. To disable this command so that no notification is sent, use the **no** form of this command.

snmp-server traps pim invalid-message-received
no snmp-server traps pim invalid-message-received

Syntax Description

This command has no keywords or arguments.

Command Default

Simple Network Management Protocol (SNMP) notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

A router can receive a join or prune message in which the RP specified in the packet is not the RP for the multicast group. Or a router can receive a register message from a multicast group in which it is not the RP.

PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files that can be accessed from the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to use the **snmp-server traps pim invalid-message-received** command:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps pim invalid-message-received
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 421
snmp-server host, on page 427
snmp-server traps pim interface-state-change, on page 497

snmp-server traps pim neighbor-change, on page 501
snmp-server traps pim rp-mapping-change, on page 503
snmp-server traps snmp, on page 507
snmp-server traps syslog, on page 509

snmp-server traps pim neighbor-change

To enable Protocol Independent Multicast (PIM) neighbor status down notifications, use the **snmp-server traps pim neighbor-change** command in global configuration mode. To disable PIM neighbor down notifications, use the **no** form of this command.

snmp-server traps pim neighbor-change
no snmp-server traps pim neighbor-change

Syntax Description

This command has no keywords or arguments.

Command Default

PIM Simple Network Management Protocol (SNMP) notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **snmp-server traps pim neighbor-change** command to send notifications when a PIM neighbor changes status from up to down on an interface. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files that can be accessed from the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to enable the router to send PIM neighbor status down notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps pim neighbor-change
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 421
snmp-server host, on page 427
snmp-server traps pim interface-state-change, on page 497
snmp-server traps pim invalid-message-received, on page 499

snmp-server traps pim rp-mapping-change, on page 503
snmp-server traps snmp, on page 507
snmp-server traps syslog, on page 509

snmp-server traps pim rp-mapping-change

To enable notifications indicating a change in the rendezvous point (RP) mapping information due to either Auto-RP or bootstrap router (BSR) messages, use the **snmp-server traps pim rp-mapping-change** command in global configuration mode. To disable this command so no notification is sent, use the **no** form of this command.

snmp-server traps pim rp-mapping-change
no snmp-server traps pim rp-mapping-change

Syntax Description

This command has no keywords or arguments.

Command Default

PIM SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files that can be accessed from the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to use the **snmp-server traps pim rp-mapping-change** command:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps pim rp-mapping-change
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 421
snmp-server host, on page 427
snmp-server traps pim interface-state-change, on page 497
snmp-server traps pim neighbor-change, on page 501
snmp-server traps pim invalid-message-received, on page 499
snmp-server traps snmp, on page 507

snmp-server traps syslog, on page 509

snmp-server traps rsvp

To enable the sending of Resource Reservation Protocol (RSVP) notifications, use the **snmp-server traps rsvp** command in global configuration mode. To disable RSVP notifications, use the **no** form of this command.

snmp-server traps rsvp {**all** | **lost-flow** | **new-flow**}

Syntax Description

all	Enables the sending of both new flow lost flow traps.
lost-flow	Enables the sending of traps when a flow is deleted.
new-flow	Enables the sending of traps when a flow is created.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
mpls-te	read, write
ouni	read, write
snmp	read, write

This example illustrates how to enable all SNMP RSVP MIB traps.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server traps rsvp all
```

snmp-server traps selective-vrf-download role-change

To attempt to download only those prefixes and labels to a physical entity required to forward traffic through the physical entity, use the **snmp-server trap selective-vrf-download role-change** command in global configuration mode.

snmp-server trap selective-vrf-download role-change

This command has no keywords or arguments.

Command Default

Selective VRF downloads are disabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

The selective VRF download feature makes a best effort to download only those prefixes and labels to a physical entity required to forward traffic through the physical entity. This is accomplished by characterizing roles for physical entities based on their configuration.

From a network management point of view the CISCO-SELECTIVE-VRF-DOWNLOAD-MIB:

- Lists the state relating to the selective VRF download feature for each physical entity capable of forwarding packets.
- Lists the role change history per address family (ipv4 and ipv6) for each physical entity capable of forwarding packets.
- Lists the VRF tables selectively downloaded to each physical entity capable of forwarding packets.

Task ID

Task ID	Operation
snmp	read, write
basic-services	read, write

This example shows how to enable the selective VRF downloads:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps selective-vrf-download role-change
```

snmp-server traps snmp

To enable the sending of RFC 1157 Simple Network Management Protocol (SNMP) notifications, use the **snmp-server traps snmp** command in the appropriate configuration mode. To disable RFC 1157 SNMP notifications, use the **no** form of this command.

snmp-server traps snmp [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]
no snmp-server traps snmp [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]

Syntax Description

authentication	(Optional) Controls the sending of SNMP authentication failure notifications.
linkup	(Optional) Controls the sending of SNMP linkUp notifications
linkdown	(Optional) Controls the sending of SNMP linkDown notifications
coldstart	(Optional) Controls the sending of SNMP coldStart notifications.
warmstart	(Optional) Controls the sending of SNMP warmStart notifications.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 3.9.0	The **authentication**, **linkup**, **linkdown**, **coldstart**, and **warmstart** keywords were added.

Usage Guidelines

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

The **snmp-server traps snmp** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

The optional **authentication** keyword controls the sending of SNMP authentication failure notifications. In order to send notifications, you must configure at least one **snmp-server host** command. An authentication Failure (4) trap signifies that the sending device is the addressee of a protocol message that is not properly authenticated. The authentication method depends on the version of SNMP being used. For SNMPv1 or SNMPv2, authentication failure occurs for packets with an incorrect community string. For SNMPv3, authentication failure occurs for packets with an incorrect Secure Hash Algorithm (SHA) or Message Digest 5 (MD5) authentication key or for a packet that is outside the authoritative SNMP engine's window, for

example, the packets that are configured outside access lists or time ranges. In such an instance, only a report Protocol Data Unit (PDU) is generated, and authentication failure traps are not generated.

The optional **linkup** keyword controls the sending of SNMP linkUp notifications. The linkUp(3) trap signifies that the sending device recognizes one of the communication links represented in the agent's configuration coming up.

The optional **linkdown** keyword controls the sending of SNMP linkDown notifications. The linkDown(2) trap signifies that the sending device recognizes a failure in one of the communication links represented in the agent's configuration.

The **snmp-server traps snmp** command with the **linkup** or **linkdown** keywords globally enables or disables SNMP linkUp and linkDown traps. After enabling either of these traps globally, you can enable or disable these traps on specific interfaces using the **no notification linkupdown disable** command in interface configuration mode. According to RFC 2863, linkUp and linkDown traps are enabled for interfaces that do not operate on top of any other interface (as defined in the ifStackTable), and are disabled otherwise. This means that you do not have to enable linkUp and linkdown notifications on such interfaces. However, linkUp and linkDown notifications will not be sent unless you enable them globally using the **snmp-server traps snmp** command.

The optional **coldstart** keyword controls the sending of SNMP coldStart notifications. The coldStart(0) trap signifies that the sending device is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.

The optional **warmstart** keyword controls the sending of SNMP coldStart notifications. The warmStart(1) trap signifies that the sending device is reinitializing itself such that neither the agent configuration nor the protocol entity implementation is altered.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to enable the device to send all traps to the host myhost.cisco.com using the community string defined as public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps snmp
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com public snmp
```

The following example shows how to enable only linkUp and linkDown traps:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps snmp linkup
RP/0/RSP0/CPU0:router(config)# snmp-server traps snmp linkdown
```

Related Topics

snmp-server engineid local, on page 421
snmp-server host, on page 427
snmp-server traps bgp
snmp-server traps syslog, on page 509

snmp-server traps syslog

To enable Simple Network Management Protocol (SNMP) notifications of Cisco-syslog-MIB error messages, use the **snmp-server traps syslog** command in the appropriate configuration mode. To disable these types of notifications, use the **no** form of this command.

snmp-server traps syslog
no snmp-server traps syslog

Syntax Description

This command has no keywords or arguments.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

The **snmp-server traps syslog** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to enable Cisco-syslog-MIB error message notifications to the host at the address myhost.cisco.com, using the community string defined as public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps syslog
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 421
snmp-server host, on page 427
snmp-server traps bgp
snmp-server traps snmp, on page 507

snmp-server trap-source

To specify the interface (and hence the corresponding IP address) from which a Simple Network Management Protocol (SNMP) trap should originate, use the **snmp-server trap-source** command in

global configuration

mode. To remove the source designation, use the **no** form of this command.

snmp-server trap-source *type interface-path-id*
no snmp-server trap-source

Syntax Description

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

Command Default

No interface is specified.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

When an SNMP trap is sent from a Cisco SNMP device, it has a notification address of the interface it happened to exit at that time. Use the **snmp-server trap-source** command to monitor notifications from a particular interface.



Note In references to a Management Ethernet interface located on a route switch processor card, the physical slot number is numeric (0 through n-1 where n is the number of line card slots in the chassis) and the module is CPU0. Example: interface MgmtEth0/1/CPU0/0.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to specify that the IP address for interface 0/0/1/0 is the source for all SNMP notifications:

```
RP/0/RSP0/CPU0:router(config)# snmp-server trap-source tengige 0/0/1/0
```

Related Topics

snmp-server engineid local, on page 421
snmp-server host, on page 427
snmp-server traps bgp
snmp-server traps snmp, on page 507
snmp-server traps syslog, on page 509

snmp-server traps subscriber session-aggregation

To set the session aggregation parameters, use the **snmp-server traps subscriber session** command in global configuration mode. To delete the set parameters, use the no form of the command.

snmp-server traps subscriber session-agregation [**access-interface** | **node**]

no snmp-server traps subscriber session-agregation [**access-interface** | **node**]

Syntax Description

access-interface	Subscriber notification at access interface level.
node	Subscriber notification at node level.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 5.1	This command was introduced.

Usage Guidelines

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

Use the **snmp-server traps subscriber session-agregation** command to enable CISCO-SUBSCRIBER-SESSION-MIB notifications (traps). Notifications will include MIB's asynchronous events.

Task ID

Task ID	Operation
snmp	read, write

Example

```
RP/0/RSP0/CPU0:router (config)# snmp-server traps subscriber session-aggregation node
```

snmp-server traps updown

To enable Border Gateway Protocol (BGP) to receive Simple Network Management Protocol (SNMP) notifications when a BGP peer changes state in IPv4 or both IPv4 and IPv6 neighbor sessions, use the **snmp-server traps updown** command in global configuration mode.

snmp-server traps {bgp | cbgp2} [updown]

Syntax Description

bgp	Specifies IPv4 neighbor sessions.
cbgp2	Specifies IPv4 and IPv6 neighbor sessions.
updown	(Optional) Specifies trap notifications.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

SNMP notifications are sent as traps.

BGP generates traps when:

- A neighbor's session state has changed.
- A neighbor prefix limit has exceeded.
- A neighbor prefix count is under the limit.

Multiple traps can be generated when the neighbor is not in steady state.

Configure **snmp-server traps updown** command to prevent the generation multiple traps.

When you configure the **snmp-server traps updown** command, traps are sent out only when the BGP neighbor goes to established state or moves out from the established state. The prefix limit traps remain unaffected.

When you configure the **bgp** keyword, traps are sent for IPv4 neighbor sessions only. When you configure the **cbgp2** keyword, traps are sent for both IPv4 and IPv6 neighbor sessions.

Example

The following example shows how to enable the router to send BGP state-change notifications to the host at the address myhost.cisco.com using the community string defined as public in IPv4 neighbor sessions only:

```
Router(config)# snmp-server traps bgp updown
Router(config)# snmp-server host myhost.cisco.com version 2c public
```

The following example shows how to enable the router to send BGP state-change notifications to the host at the address myhost.cisco.com using the community string defined as public in both IPv4 and IPv6 neighbor sessions:

```
Router(config)# snmp-server traps cbgp2 updown
Router(config)# snmp-server host myhost.cisco.com version 2c public
```

snmp-server trap-timeout

To define how often to try resending trap messages on the retransmission queue, use the **snmp-server trap-timeout** command in

global configuration

mode. To restore the default value, use the **no** form of this command.

snmp-server trap-timeout *seconds*
no snmp-server trap-timeout *seconds*

Syntax Description

seconds	Integer that sets the interval for resending the messages, in seconds). Value can be from 1 to 1000.

Command Default

seconds : 30

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Before Cisco IOS XR software tries to send a trap, it looks for a route to the destination address. If there is no known route, the trap is saved in a retransmission queue. Use the **snmp-server trap-timeout** command to determine the number of seconds between retransmission attempts.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to set an interval of 20 seconds to try resending trap messages on the retransmission queue:

```
RP/0/RSP0/CPU0:router(config)# snmp-server trap-timeout 20
```

Related Topics

snmp-server engineid local, on page 421
snmp-server host, on page 427
snmp-server traps bgp
snmp-server traps snmp, on page 507
snmp-server traps syslog, on page 509

snmp-server user

To configure a new user to a Simple Network Management Protocol (SNMP) group, use the **snmp-server user** command in

global configuration

mode. To remove a user from an SNMP group, use the **no** form of this command.

snmp-server user *username groupname* {**v1** | **v2c** | **v3** [**auth** {**md5** | **sha**} {**clear** | **encrypted**} *auth-password* [**priv** {**3des** | **aes** *aes-bit-encryption* | **des56**} {**clear** | **encrypted**} *priv-password*]]} [**SDROwner** | **SystemOwner**] [*access-list-name*]
no snmp-server user *username groupname*

Syntax Description

username	Name of the user on the host that connects to the agent. **Note** The recommended range for a user-defined username is 2-253 characters.
groupname	Name of the group to which the user belongs.
v1	Specifies that the SNMPv1 security model should be used.
v2c	Specifies that the SNMPv2c security model should be used.
v3	Specifies that the SNMPv3 security model should be used.
auth	(Optional) Specifies which authentication level should be used. If this keyword is used, you must specify an authentication level and an authorization password.
md5	Specifies the HMAC-MD5-96 authentication level.
sha	Specifies the HMAC-SHA-96 authentication level.
clear	Specifies that an unencrypted password follows.
encrypted	Specifies that an encrypted password follows.
auth-password	Authentication password, which is a string (not to exceed 64 characters) that enables the agent to receive packets from the host.
priv	(Optional) Specifies that encryption parameters follow.
3des	Specifies the 168-bit Triple Data Encryption Standard (3DES) level of encryption for the user.
aes *aes-bit-encryption*	Specifies the Advanced Encryption Standard (AES) level of encryption for the user. Supported options are 128, 192 and 256 bit encryption.

des56	Specifies the 56-bit Data Encryption Standard (DES) level of encryption for the user.
priv-password	Privacy password, which can be clear or encrypted text, according to what is specified.
SDROwner	(Optional) Limits access to the agents for the owner secure domain router (SDR) only.
SystemOwner	(Optional) Provides system-wide access to the agents for all SDRs.
access-list-name	(Optional) Access list to be associated with this SNMP user. The *access-list-name* argument represents a value from 1 to 99, that is, the identifier of the standard IP access list.

Command Default

By default, access is limited to agents on the owner SDR only.

See also Table 32: snmp-server user Default Descriptions, on page 517.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 3.9.0	AES and 3DES encryption formats were supported.

Usage Guidelines

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

To use 3DES and AES encryption standards, you must have installed the security package (k9sec). For information on installing software packages, see *Upgrading and Managing Cisco IOS XR Software* in *System Management Configuration Guide for Cisco ASR 9000 Series Routers*.



Note Only one remote host can be assigned to the same username for SNMP version 3. If you configure the same username with different remote hosts, only the last username and remote host combination will be accepted and will be seen in the **show running** configuration. In the case of multiple SNMP managers, multiple unique usernames are required.

Table 32: snmp-server user Default Descriptions

Characteristic	Default
passwords	Text strings are assumed.
access lists	Access from all IP access lists is permitted.

SDR and System-wide Access

When the **snmp-server user** command is entered with the **SDROwner** keyword, SNMP access is granted only to the MIB object instances in the owner SDR.

When the **snmp-server user** command is entered with the **SystemOwner** keyword, SNMP access is granted to the entire system.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to enter a plain-text password for the string *abcd* for user2 in group2:

```
RP/0/RSP0/CPU0:router(config)# snmp-server user user2 group2 v3 auth md5 clear abcd
```

To learn if this user has been added to the configuration, use the **show snmp user** command.

If the localized Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) digest is known, specify that string instead of the plain-text password. The digest should be formatted as AA:BB:CC:DD where AA, BB, CC, and DD are hexadecimal values. The digest should also be exactly 16 octets long.

This example shows how to specify the command with a digest name of 00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF:

```
RP/0/RSP0/CPU0:router(config)# snmp-server user user2 group2 v3 auth md5 encrypted
     00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

Related Topics

snmp-server group, on page 424

snmp-server view

To create or update a Simple Network Management Protocol (SNMP) view entry, use the **snmp-server view** command in

global configuration

mode. To remove the specified server view entry, use the **no** form of this command.

snmp-server view *view-name oid-tree* {**excluded** | **included**}
no snmp-server view *view-name oid-tree* {**excluded** | **included**}

Syntax Description

view-name	Label for the view record being updated or created. The name is used to reference the record.
oid-tree	Object identifier (OID) of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as *system*. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
excluded	Excludes the MIB family from the view.
included	Includes the MIB family in the view.

Command Default

No view entry exists.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Other SNMP commands require a view as a keyword. Use the **snmp-server view** command to create a view to be used as keywords for other commands that create records including a view.

Instead of defining a view explicitly, you can rely on the following predefined views, which are supported by the SNMP agent:

all

Predefined view indicating that a user can see all objects.

CfgProt

Predefined view indicating that a user can see all objects except the SNMPv3 configuration tables.

vacmViewTreeFamilyEntry

Predefined view indicating that a user can see the default configuration of vacmViewTreeFamilyEntry.

The predefined views supported on Cisco IOS XR software, however, do not match the predefined views specified in RFC 3415.

Task ID

Task ID	Operations
snmp	read, write

This example creates a view that includes all objects in the MIB-II subtree:

```
RP/0/RSP0/CPU0:router(config)# snmp-server view mib2 1.3.6.1.2.1 included
```

This example shows how to create a view that includes all objects in the MIB-II system group and all objects in the Cisco enterprise MIB:

```
RP/0/RSP0/CPU0:router(config)# snmp-server view view1 1.3.6.1.2.1.1 included
RP/0/RSP0/CPU0:router(config)# snmp-server view view1 1.3.6.1.4.1.9 included
```

This example shows how to create a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group:

```
RP/0/RSP0/CPU0:router(config)# snmp-server view view1 1.3.6.1.2.1.1 included
RP/0/RSP0/CPU0:router(config)# snmp-server view view1 1.3.6.1.2.1.1.7 excluded
RP/0/RSP0/CPU0:router(config)# snmp-server view view1 1.3.6.1.2.1.2.2.1.*.1 included
```

Related Topics

show snmp view, on page 409
snmp-server group, on page 424

snmp-server vrf

To configure the VPN routing and forwarding (VRF) properties of Simple Network Management Protocol (SNMP), use the **snmp-server vrf** command in

global configuration

mode. To remove the configuration, use the **no** form of this command.

snmp-server vrf *vrf-name*[**host** *address* [**clear** | **encrypted**][**traps**][**version** {**1** | **2c** | **3** *security-level*}] *community-string*[**udp-port** *port*]][**context** *context-name*]
no snmp-server vrf *vrf-name*

Syntax Description

vrf-name	Name of the VRF.
host *address*	(Optional) Specifies the name or IP address of the host (the targeted recipient).
clear	(Optional) Specifies that the *community-string* argument is clear text.
encrypted	(Optional) Specifies that the *community-string* argument is encrypted text.
traps	(Optional) Specifies that notifications should be sent as traps. This is the default.
version {**1** | **2c** | **3**}	(Optional) Specifies the version of the SNMP used to send the traps. The default is SNMPv1. When the **version** keyword is used, one of these keywords must be specified: • **1**—SNMPv1 • **2c**—SNMPv2C • **3**—SNMPv3
security-level	(Optional) Security level for SNMPv3. Options are: • **auth**—authNoPriv • **noauth**—noAuthNoPriv • **priv**—authPriv
community-string	Specifies the community string for SNMPv1 and SNMPv2, or the SNMPv3 user.
udp-port *port*	(Optional) Specifies the UDP port to which notifications should be sent.
context *context-name*	(Optional) Name of the context that must be mapped to VRF identified by value of the *vrf-name* argument.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use this command to enter SNMP VRF configuration mode and configure an SNMP notification recipient on a VRF. You can also map a VRF to an SNMP context.

SNMP notification recipient that is reachable by way of a VRF can be configured. Notification is forwarded to the recipient represented by its address using the routing table instance identified by the VRF name.

The *address* argument can be either a host name or an IP address.

Use the **clear** keyword to specify that the clear text community string you enter is displayed encrypted in the **show running** command output. To enter an encrypted string, use the **encrypted** keyword. To enter a clear text community string that is not encrypted by the system, use neither of these keywords.

An SNMP context identified by the value of the *context-name* argument can be mapped to a VRF in this mode. This context must be created using **snmp-server context** command.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to configure a host IP address for a VRF name:

```
RP/0/RSP0/CPU0:router(config)# snmp-server vrf vrfa
RP/0/RSP0/CPU0:router(config-snmp-vrf)# host 12.21.0.1 traps version
2c public udp-port 2525
```

Related Topics

snmp-server context, on page 416
snmp-server host, on page 427

snmp test trap all

To send a Simple Network Management Protocol (SNMP) trap message to the trap receivers for all supported traps, use the **snmp test trap all** command in

EXEC

mode.

snmp test trap all

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

To use the **snmp test trap** command, SNMP must be configured on the router. This command is not intended for testing scalability, performance, or high availability scenarios.

Use the **snmp test trap all** command to generate test traps for all supported traps. The following traps are supported:

- coldStart—SNMP agent Initializing and its configuration may have changed.
- warmStart—SNMP agent Initializing and its configuration is unaltered.
- linkUp—Interface ifOperStatus is Up.
- linkDown—Interface ifOperStatus is Down.
- clogMessage Generated—Syslog message generated.
- ciscoFlashDeviceInsertedNotif—Flash device inserted.
- ciscoFlashDeviceRemovedNotif—Flash device removed.
- ciscoRFProgressionNotif—RF state change.
- ciscoRFSwactNotif—Switchover.
- ciscoConfigManEvent—Command-line interface (CLI) configuration management event.
- newRoot—SNMP agent is a new root of the spanning tree.
- topologyChange—Bridge port has transitioned to the Forwarding state.
- cefcFanTrayOperStatus—Fan tray cefcFanTrayOperStatus is Up.

- cefcModuleStatusChange—Module cefcModuleOperStatus is OK (module up) or module cefcModuleOperStatus is Failed (module down).
- entSensorThresholdNotification—entSensorValue crossed the entSensorthresholdValue.
- cefcPowerStatusChange—Redundant PowerSupply fails.

Task ID

Task ID	Operation
snmp	read

This example illustrates how to use the **snmp test trap all** command:

```
RP/0/RSP0/CPU0:router# snmp test trap all
```

Related Topics

show snmp entity, on page 360

snmp test trap entity

To send a test SNMP Entity trap message to the trap receivers, use the **snmp test trap entity** command in

EXEC

mode.

snmp test trap entity {**fru** {**power status-change failed** | **module status-change** {**up** | **down**} | **fan-tray oper-status up**} | **sensor threshold-notification**}[**entity-index** *index*]

Syntax Description

fru	Sends a field replacement unit trap.
power status-change failed	Sends a cefcPowerStatusChange trap for the CISCO-ENTITY-FRU-CONTROL-MIB.
module status-change{**up** | **down**}	Sends a cefcModuleStatusChange trap for the CISCO-ENTITY-FRU-CONTROL-MIB.
fan-tray oper-status up	Sends a cefcFanTrayOperStatus trap for the CISCO-ENTITY-FRU-CONTROL-MIB.
sensor	Sends a sensor trap.
threshold-notification	Sends a entSensorThresholdNotification trap for the CISCO-ENTITY-SENSOR-MIB.
entity-index *index*	Specifies the physical index for which to generate the trap.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

The **snmp test trap entity** command tests the sending of Entity MIB traps. It is not intended for testing scalability, performance, or high availability scenarios. To use the **snmp test trap** command, SNMP must be configured on the router.

Task ID

Task ID	Operation
snmp	read

This example illustrates how to use the **snmp test trap entity** command:

```
RP/0/RSP0/CPU0:router# snmp test trap entity sensor threshold index
```

Related Topics

show snmp entity, on page 360

snmp test trap infra

To send a test Simple Network Management Protocol (SNMP) Infra trap message to the trap receivers, use the **snmp test trap infra** command in

EXEC

mode.

snmp test trap infra {**bridge** {**new-root** | **topology-change**} | **config event** | **flash** {**device-inserted** | **device-removed**} | **redundancy** {**progression** | **switch**} | **syslog message-generated**}

Syntax Description

bridge	Sends a bridge trap.
new-root	Sends a newRoot trap for the BRIDGE-MIB.
topology-change	Sends a topologyChange trap for the BRIDGE-PORT.
config event	Sends a ciscoConfigManEvent trap for the CISCO-CONFIG-MAN-MIB.
flash	Sends a flash trap.
device-inserted	Sends a ciscoFlashDeviceInsertedNotif trap for the CISCO-FLASH-MIB.
device-removed	Sends a ciscoFlashDeviceRemovedNotif trap for the CISCO-FLASH-MIB.
redundancy	Sends an RF trap.
progression	Sends a ciscoRFProgressionNotif trap for the CISCO-RF-MIB.
switch	Sends a ciscoRFSwactNotif trap for the CISCO-RF-MIB.
syslog message-generated	Sends a clogMessageGenerated for the CISCO-SYSLOG-MIB.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

The **snmp test trap infra** command tests the sending of Infra MIB traps. It is not intended for testing scalability, performance, or high availability scenarios. To use this command, SNMP must be configured on the router.

Task ID

Task ID	Operation
snmp	read

This example illustrates how to use the **snmp test trap infra** command:

```
RP/0/RSP0/CPU0:router# snmp test trap infra syslog message-generated
```

snmp test trap interface

To send a test Simple Network Management Protocol (SNMP) interface trap message to the trap receivers, use the **snmp test trap interface** command in

EXEC

mode.

snmp test trap interface {**link-down** | **link-up**}**ifindex** *index*

Syntax Description

link-down	Sends a linkDown trap for the IF-MIB.
link-up	Sends a linkUp trap for the IF-MIB.
ifindex *index*	Specifies the interface index for which to send the IF-MIB trap.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

The **snmp test trap interface** command tests the sending of IF-MIB traps. It is not intended for testing scalability, performance, or high availability scenarios. To use this command, SNMP must be configured on the router.

Task ID

Task ID	Operation
snmp	read

This example illustrates how to use the **snmp test trap interface** command:

```
RP/0/RSP0/CPU0:router# snmp test trap interface link-down
```

snmp test trap snmp

To send a test Simple Network Management Protocol (SNMP) trap message to the trap receivers, use the **snmp test trap snmp** command in

EXEC

mode.

snmp test trap snmp {**cold-start** | **warm-start**}

Syntax Description

cold-start	Sends a coldStart trap for the SNMPv2-MIB.
warm-start	Sends a warmStart trap for the SNMPv2-MIB.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

The **snmp test trap snmp** command tests the sending of MIB traps. It is not intended for testing scalability, performance, or high availability scenarios. To use this command, SNMP must be configured on the router.

Task ID

Task ID	Operation
snmp	read

The following example illustrates how to use the **snmp test trap snmp** command:

```
RP/0/RSP0/CPU0:router# snmp test trap snmp cold-start
```

transfer-interval

To configure how long bulk statistics should be collected before a bulk statistics transfer is initiated, use the **transfer-interval** command in bulk statistics transfer configuration mode. To remove a previously configured interval from a bulk statistics configuration, use the **no** form of this command.

transfer-interval *minutes*
no transfer-interval *minutes*

Syntax Description

minutes	Length of time, in minutes, that the system should collect MIB data before attempting the transfer operation. The valid range is from 1 to 2147483647. The default is 30.

Command Default

Bulk statistics file transfer operations start 30 minutes after the **enable (bulkstat)** command is used.

Command Modes

Bulk statistics transfer configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Bulk statistics data is collected into a new file when a transfer attempt begins, which means that this command also configures the collection interval.

If the maximum buffer size for a bulk statistics file is reached before the transfer interval time expires, the transfer operation is still initiated, and bulk statistics MIB data are collected into a new file in the system buffer.

Task ID

Task ID	Operation
snmp	read, write

The following example shows how to configure a transfer interval of 20 minutes for the bulk statistics configuration bulkstat1:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat transfer-id bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# transfer-interval 20
```

Related Topics

enable (bulkstat), on page 334
show snmp mib bulkstat transfer, on page 375

snmp-server mib bulkstat transfer-id, on page 449

url

To specify the host to which bulk statistics files should be transferred, use the **url** command in bulk statistics transfer configuration mode. To remove a previously configured destination host, use the **no** form of this command.

url [**primary** | **secondary**] *url*
no url [**primary** | **secondary**] *url*

Syntax Description

primary	Specifies the URL to be used first for bulk statistics transfer attempts.
secondary	Specifies the URL to be used for bulk statistics transfer attempts if the transfer to the primary URL is not successful.
url	Destination URL address for the bulk statistics file transfer. Use FTP or TFTP. The syntax for these URLs is as follows: • **ftp:**[[[//*username* [:*password*]**@**]*location*]/*directory*]/*filename* • **tftp:**[[/*location*]/*directory*]/*filename* The location argument is typically an IP address.

Command Default

No host is specified.

Command Modes

Bulk statistics transfer configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

For bulk statistics transfer retry attempts, a single retry consists of an attempt to send first to the primary URL, and then to the secondary URL.

Task ID

Task ID	Operation
snmp	read, write

In the following example, an FTP server is used as the primary destination for the bulk statistics file. If a transfer to that address fails, an attempt is made to send the file to the TFTP server at 192.168.10.5. No retry command is specified, which means that only one attempt to each destination will be made.

```
RP/0/RSP0/CPU0:router# configure
```

```
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat transfer ifMibTesting
RP/0/RSP0/CPU0:router(config-bulk-tr)# schema carMibTesting1
RP/0/RSP0/CPU0:router(config-bulk-tr)# schema carMibTesting2
RP/0/RSP0/CPU0:router(config-bulk-tr)# url primary
ftp://user2:pswd@192.168.10.5/functionality/
RP/0/RSP0/CPU0:router(config-bulk-tr)# url secondary tftp://user2@192.168.10.8/tftpboot/
RP/0/RSP0/CPU0:router(config-bulk-tr)# enable
RP/0/RSP0/CPU0:router(config-bulk-tr)# exit
```

Related Topics

show snmp mib bulkstat transfer, on page 375