Cisco IOS Network Management Command Reference

May 2008

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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805R)

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

Cisco IOS Network Management Command Reference
© 2007-2008 Cisco Systems, Inc. All rights reserved.

Introduction

This document describes the commands used to configure network management features with Cisco IOS software.

Note Prior to Cisco IOS Release 12.4, the commands for configuring network management features were included in the *Cisco IOS Configuration Fundamentals Command Reference*.

For information about configuration, refer to the *Cisco IOS Network Management Configuration Guide*.

Network Management Commands

absolute

To specify an absolute time for a time-range, use the **absolute** command in time-range configuration mode. To remove the time limitation, use the **no** form of this command.

absolute [**start** *time date*] [**end** *time date*]

no absolute

Syntax Description

start *time date*	(Optional) Absolute time and date that the **permit** or **deny** statement of the associated access list starts going into effect. The *time* is expressed in 24-hour notation, in the form of *hours*:*minutes*. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m. The *date* is expressed in the format *day month year*. The minimum start is 00:00 1 January 1993. If no start time and date are specified, the **permit** or **deny** statement is in effect immediately.
end *time date*	(Optional) Absolute time and date that the **permit** or **deny** statement of the associated access list is no longer in effect. Same *time* and *date* format as described for the **start** keyword. The end time and date must be after the start time and date. The maximum end time is 23:59 31 December 2035. If no end time and date are specified, the associated **permit** or **deny** statement is in effect indefinitely.

Defaults

There is no absolute time when the time range is in effect.

Command Modes

Time-range configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Time ranges are used by IP and Internetwork Packet Exchange (IPX) extended access lists. For more information on using these functions, see the *Cisco IOS IP Configuration Guide* and the *Cisco IOS AppleTalk and Novell IPX Configuration Guide*. Time ranges are applied to the **permit** or **deny** statements found in these access lists.

The **absolute** command is one way to specify when a time range is in effect. Another way is to specify a periodic length of time with the **periodic** command. Use either of these commands after the **time-range** command, which enables time-range configuration mode and specifies a name for the time range. Only one **absolute** entry is allowed per **time-range** command.

If a **time-range** command has both **absolute** and **periodic** values specified, then the **periodic** items are evaluated only after the **absolute start** time is reached, and are not further evaluated after the **absolute end** time is reached.

Note All time specifications are interpreted as local time. To ensure that the time range entries take effect at the desired times, the software clock should be synchronized using the Network Time Protocol (NTP), or some other authoritative time source. For more information, refer to the "Performing Basic System Management" document on Cisco.com.

Examples

In the following example, an access list named 'northeast' references a time range named 'xyz'. The access list and time range configuration permits traffic on Ethernet interface 0, starting at noon on January 1, 2005 and going forever.

```
time-range xyz
 absolute start 12:00 1 January 2005
!
ip access-list extended northeast
 permit ip any any time-range xyz
!
interface ethernet 0
 ip access-group northeast in
```

The configuration sample permits UDP traffic until noon on December 31, 2005. After that time, UDP traffic is no longer allowed out Ethernet interface 0.

```
time-range abc
 absolute end 12:00 31 December 2005
!
ip access-list extended northeast
 permit udp any any time-range abc
!
interface ethernet 0
 ip access-group northeast out
```

The configuration sample permits outgoing UDP traffic on Ethernet interface 0 on weekends only, from 8:00 a.m. on January 1, 2005, to 6:00 p.m. on December 31, 2006:

```
time-range weekend1
 absolute start 8:00 1 January 2005 end 18:00 31 December 2006
 periodic weekends 00:00 to 23:59
!
ip access-list extended northeast1
 permit udp any any time-range weekend1
!
interface ethernet 0
 ip access-group northeast1 out
```

Related Commands

Command	Description
deny	Sets conditions under which a packet does not pass a named access list.
periodic	Specifies a recurring (weekly) start and end time for a time range.
permit	Sets conditions under which a packet passes a named access list.
time-range	Enables time-range configuration mode and names a time range definition.

action

To set the packet action clause, use the **action** command in VLAN access-map configuration submode. To remove an action element, use the **no** form of this command.

action {**drop** [**log**] | **forward** [**capture**] | **redirect** *interface interface-number* | **port-channel** *channel-id interface interface-number* | **port-channel** *channel-id* **...**}

no action {**drop** [**log**] | **forward** [**capture**] | **redirect** *interface interface-number* | **port-channel** *channel-id interface interface-number* | **port-channel** *channel-id* **...**}

Syntax Description

drop	Drops the packets.
log	(Optional) Logs the dropped packets in the software.
forward	Forwards (switched by hardware) the packets to its destination.
capture	(Optional) Sets the capture bit for the forwarded packets so that ports with the capture function enabled also receive the packets.
redirect *interface*	Redirects packets to the specified interfaces; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, and **tengigabitethernet**. See the "Usage Guidelines" section for additional valid values.
interface-number	Module and port number; see the "Usage Guidelines" section for valid values.
port-channel *channel-id*	Port channel to redirect traffic; valid values are a maximum of 64 values ranging from 1 to 256.

Defaults

This command has no default settings.

Command Modes

VLAN access-map configuration submode

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2(17d)SXB release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The valid values for *interface* include the **ge-wan**, **atm**, and **pos** keywords that are supported on Catalyst 6500 series switches that are configured with a Supervisor Engine 2.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Each redirect action allows you to specify a list of up to five destination interfaces. There is also a limit of up to 255 different interface lists that can be used by redirect actions.

The redirect action supports interface lists instead of single interfaces as shown in the following example:

[. . .] {**redirect** {{**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot*/port} | {**port-channel** *channel-id*}

The action clause specifies the action to be taken when a match occurs.

The forwarded packets are subject to any applied Cisco IOS ACLs. The **capture** keyword sets the capture bit in VACL-forwarded packets. Ports with the capture function enabled can receive VACL-forwarded packets that have the capture bit set. Only VACL-forwarded packets that have the capture bit set can be captured.

When the **log** keyword is specified, dropped packets are logged in the software. Only dropped IP packets can be logged. The **redirect** keyword allows you to specify up to five interfaces, which can be physical interfaces or EtherChannels. An EtherChannel member is not allowed to be a redirect interface.

VACLs on WAN interfaces support only the **action forward capture** command.

The action clause in a VACL can be forward, drop, capture, or redirect. Traffic can also be logged. VACLs applied to WAN interfaces do not support the redirect or log actions.

The redirect interface must be in the VLAN for which the VACL map is configured.

In a VLAN access map, if at least one ACL is configured for a packet type (IP, IPX, or MAC), the default action for the packet type is **drop** (deny).

If an ACL is not configured for a packet type, the default action for the packet type is **forward** (permit).

If an ACL for a packet type is configured and the ACL is empty or undefined, the configured action will be applied to the packet type.

Examples

This example shows how to define a drop and log action:

```
Router(config-access-map)# action drop log
Router(config-access-map)#
```

This example shows how to define a forward action:

```
Router(config-access-map)# action forward
Router(config-access-map)#
```

Related Commands

Command	Description
match	Specifies the match clause by selecting one or more ACLs for a VLAN access-map sequence.
show vlan access-map	Displays the contents of a VLAN-access map.
vlan access-map	Creates a VLAN access map or enter the VLAN access-map command mode.

action cli

To specify the action of executing a Cisco IOS command-line interface (CLI) command when an Embedded Event Manager (EEM) applet is triggered, use the **action cli** command in applet configuration mode. To remove the action of executing a CLI command, use the **no** form of this command.

action *label* **cli command** *cli-string*

no action *label* **cli command** *cli-string*

Syntax Description

label	Unique identifier that can be any string value. Actions are sorted and run in ascending alphanumeric key sequence using the label as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
command	Specifies the message to be sent to the CNS Event Bus.
cli-string	CLI command to be executed. If the string contains embedded blanks, enclose it in double quotation marks.

Command Default

No CLI commands are executed when an EEM applet is triggered.

Command Modes

Applet configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

Use the **action cli** command to specify the action of executing a Cisco IOS CLI command when an EEM applet is triggered.

Table 1 shows the built-in variable that is set when the **action cli** command is run.

Table 1 EEM Built-in Variables for action cli Command

Built-in Variable	Description
$_cli_result	The result of the execution of the CLI command.

Examples

The following example shows how to specify an EEM applet to run when the Cisco IOS **interface loopback** CLI command is configured three times. The applet executes the **no shutdown** command to ensure that the loopback interfaces are operational.

```
Router(config)# event manager applet cli-match
Router(config-applet)# event cli pattern {.*interface loopback*} sync yes occurs 3
Router(config-applet)# action 1.0 cli command "no shutdown"
```

Related Commands

Command	Description
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

action cns-event

To specify the action of sending a message to the CNS Event Bus when an Embedded Event Manager (EEM) applet is triggered, use the **action cns-event** command in applet configuration mode. To remove the action of sending a message to the CNS Event Bus, use the **no** form of this command.

action *label* **cns-event msg** *msg-text*

no action *label* **cns-event msg** *msg-text*

Syntax Description

label	Unique identifier that can be any string value. Actions are sorted and run in ascending alphanumeric key sequence using the label as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
msg	Specifies the message to be sent to the CNS Event Bus.
msg-text	Character text, an environment variable, or a combination of the two. If the string contains embedded blanks, enclose it in double quotation marks.

Command Default

No messages are sent to the CNS Event Bus.

Command Modes

Applet configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Examples

The following example shows how to specify a message to be sent to the CNS Event Bus when the memory-fail applet is triggered:

```
Router(config)# event manager applet memory-fail
Router(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.48.1.1.1.6.1 get-type exact entry-op
lt entry-val 5120000 poll-interval 10
Router(config-applet)# action 1.0 cns-event msg "Memory exhausted; current available
memory is $_snmp_oid_val bytes"
```

Related Commands

Command	Description
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

action counter

To specify the action of setting or modifying a named counter when an Embedded Event Manager (EEM) applet is triggered, use the **action counter** command in applet configuration mode. To restore the default value to the counter, use the **no** form of this command.

action *label* **counter name** *counter-name* **value** *counter-value* **op** {**dec** | **inc** | **nop** | **set**}

no action *label* **counter name** *counter-name* **value** *counter-value* **op** {**dec** | **inc** | **nop** | **set**}

Syntax Description

label	Unique identifier that can be any string value. Actions are sorted and run in ascending alphanumeric key sequence using the label as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
name	Specifies the name of the counter to be set or modified.
counter-name	Name of the counter to be set or modified. The counter name is referenced in a registered counter type policy.
value	Specifies the value to be used to set or modify the counter.
counter-value	Number in the range from –2147483648 to 2147483647, inclusive.
op	Indicates the operator to be used with the *counter-value* to set or modify the specified counter.
dec	Specifies that the counter is decreased in value by the amount specified in the *counter-value* argument.
inc	Specifies that the counter is increased in value by the amount specified in the *counter-value* argument.
nop	Specifies that the counter value is read from the environment variable $_counter_value_remain.
set	Specifies that the counter is set to the value specified in the *counter-value* argument.

Command Default

No counter values are set or modified.

Command Modes

Applet configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

Use the **action counter** command when an event occurs periodically and you want an action to be implemented after a specified number of occurrences of that event. When the **action counter** command completes, an environment variable is updated as shown in Table 2.

Table 2 shows the built-in variable that is set when the **action counter** command is run.

Table 2 EEM Built-in Variables for action counter Command

Built-in Variable	Description
$_counter_value_remain	The value of the counter after the execution of the **action counter** command.

Use the **event counter** command with the **action counter** command when an event occurs periodically and you want an action to be implemented after a specified number of occurrences of the event.

Examples

The following example shows an EEM applet called IPSLAping1 being registered to run when there is an exact match on the value of a specified SNMP object ID that represents a successful IP SLA ICMP echo operation (this is equivalent to a **ping** command). Four actions are triggered when the echo operation fails, and event monitoring is disabled until after the second failure. A message saying that the ICMP echo operation to a server failed is sent to syslog, an SNMP trap is generated, EEM publishes an application-specific event, and a counter called IPSLA1F is incrimented by a value of one.

```
Router(config)# event manager applet IPSLAping1
Router(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.42.1.2.9.1.6.4 get-type exact
entry-op eq entry-val 1 exit-op eq exit-val 2 poll-interval 5
Router(config-applet)# action 1.0 syslog priority critical msg "Server IP echo failed:
OID=$_snmp_oid_val"
Router(config-applet)# action 1.1 snmp-trap strdata "EEM detected server reachability
failure to 10.1.88.9"
Router(config-applet)# action 1.2 publish-event sub-system 88000101 type 1 arg1 10.1.88.9
arg2 IPSLAEcho arg3 fail
Router(config-applet)# action 1.3 counter name _IPSLA1F value 1 op inc
```

The following example shows a policy—EventCounter_A—that is configured to run once a minute and to increment a well-known counter called critical_errors. A second policy—EventCounter_B—is registered to be triggered when the well-known counter called critical_errors exceeds a threshold of 3. When policy EventCounter_B runs, it resets the counter back to 0.

```
Router(config)# event manager applet EventCounter_A
Router(config-applet)# event timer watchdog time 60.0
Router(config-applet)# action 1.0 syslog msg “EventCounter_A”
Router(config-applet)# action 2.0 counter name critical_errors value 1 op inc
Router(config-applet)# exit
```

action force-switchover

To specify the action of switching to a secondary processor in a fully redundant environment when an Embedded Event Manager (EEM) applet is triggered, use the **action force-switchover** command in applet configuration mode. To remove the action of switching to a secondary processor, use the **no** form of this command.

action *label* **force-switchover**

no action *label* **force-switchover**

Syntax Description

label	Unique identifier that can be any string value. Actions are sorted and run in ascending alphanumeric key sequence using the label as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.

Command Default

A switch to a secondary processor is not made.

Command Modes

Applet configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

Before using the **action force-switchover** command, you must install a backup processor in the device. If the hardware is not fully redundant, the switchover action will not be performed.

Examples

The following example shows how to specify a switch to the secondary Route Processor (RP) when the memory-fail applet is triggered:

```
Router(config)# event manager applet memory-fail
Router(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.48.1.1.1.6.1 get-type exact entry-op
lt entry-val 5120000 poll-interval 10
Router(config-applet)# action 2.0 force-switchover
```

Related Commands

Command	Description
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

action info

To specify the action of obtaining system information when an Embedded Event Manager (EEM) applet is triggered, use the **action info** command in applet configuration mode. To remove the **action info** command from the configuration, use the **no** form of this command.

action *label* **info type** {**cli frequency** | **cli history** | **syslog frequency** | **syslog history** | **routername** | **snmp oid** *oid-value* **get-type** {**exact** | **next**}}

no action *label* **info type** {**cli frequency** | **cli history** | **syslog frequency** | **syslog history** | **routername** | **snmp oid** *oid-value* **get-type** {**exact** | **next**}}

Syntax Description

label	Unique identifier that can be any string value. Actions are sorted and run in ascending alphanumeric key sequence using the label as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
type	Specifies the type of information requested.
cli frequency	Requests information about the frequency of recent command-line interface (CLI) commands.
cli history	Requests information about the history of recent CLI commands.
syslog frequency	Requests information about the frequency of syslog messages.
syslog history	Requests information about the history of recent syslog messages.
routername	Requests the name of the specified router.
snmp oid	Requests the value of the SNMP object as specified by the SNMP object identifier (object ID).
oid-value	Object ID (OID) value of the data element, in Simple Network Management Protocol (SNMP) dotted notation. An OID is defined as a type in the associated MIB, CISCO-EMBEDDED-EVENT-MGR-MIB, and each type has an object value. Monitoring of some OID types is supported. The following types are valid: • INTEGER_TYPE • COUNTER_TYPE • GAUGE_TYPE • TIME_TICKS_TYPE • COUNTER_64_TYPE • OCTET_PRIM_TYPE • OPAQUE_PRIM_TYPE
get-type	Specifies that a type of SNMP get operation is to be applied to the object ID specified by the *oid-value* argument. • **exact**—Retrieves the object ID specified by the *oid-value* argument. • **next**—Retrieves the object ID that is the alphanumeric successor to the object ID specified by the *oid-value* argument.

Command Default

No system information is requested.

Command Modes

Applet configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

Use the **action info** command when an event occurs and you want to request some system information. When the **snmp oid** keyword is used, an error message is returned when the OID is not one of the defined types.

Table 3 shows the built-in variables that are set for the various **action info** keywords. The notation [1-N] represents that the built-in variable ends in a sequential number starting at 1 up to the maximum number of entries returned.

Table 3 EEM Built-in Variables for action info Command

Built-in Variable	Description
action info cli frequency	
$_info_cli_freq_num_entries	The number of CLI event entries.
$_info_cli_freq_pattern_[1-N]	A regular expression used to perform CLI command pattern matching.
$_info_cli_freq_time_sec_[1-N]	The seconds in Posix timer units since January 1, 1970, which represents the time the last CLI event was raised.
$_info_cli_freq_time_msec_[1-N]	The milliseconds in Posix timer units since January 1, 1970, which represents the time the last CLI event was raised.
$_info_cli_freq_match_count_[1-N]	The number of times that a CLI command matches the pattern specified by this CLI event specification.
$_info_cli_freq_raise_count_[1-N]	The number of times that this CLI event was raised.
$_info_cli_freq_sync_[1-N]	A “yes” means that event publish should be performed sychronously. The event detector will be notified when the Event Manager Server has completed publishing the event. The Event Manager Server will return a code that indicates whether or not the CLI command should be executed.
$_info_cli_freq_skip_[1-N]	A “yes” means that the CLI command should not be executed if the sync flag is not set.
$_info_cli_freq_occurs_[1-N]	Number of occurrences before an event is raised; if this argument is not specified an event is raised on the first occurrence.

Table 3 EEM Built-in Variables for action info Command

Built-in Variable	Description
$_info_cli_freq_period_sec_[1-N]	Number of occurrences must occur within this number of seconds in order to raise event; if not specified, does not apply.
$_info_cli_freq_period_msec_[1-N]	The number of occurrences must occur within this number of milliseconds in order to raise the event; if not specified, the period check does not apply.
action info cli history	
$_info_cli_hist_num_entries	The number of cli history entries.
$_info_cli_hist_cmd_[1-N]	The text of the CLI command.
$_info_cli_hist_time_sec_[1-N]	The time, in seconds, when the CLI command occurred.
$_info_cli_hist_time_msec_[1-N]	The time, in milliseconds, when the CLI command occurred.
action info routername	
$_info_routername	The name of the router.
action info snmp	
$_info_snmp_oid	The SNMP object ID.
$_info_snmp_value	The value string of the associated SNMP data element.
action info syslog frequency	
$_info_syslog_freq_num_entries	The number of syslog entries.
$_info_syslog_freq_pattern_[1-N]	A regular expression used to perform syslog message pattern matching.
$_info_syslog_freq_time_sec_[1-N]	The seconds in Posix timer units since January 1, 1970, which represents the time the last event was raised.
$_info_syslog_freq_time_msec_[1-N]	The milliseconds in Posix timer units since January 1, 1970, which represents the time the last event was raised.
$_info_syslog_freq_match_count_[1-N]	The number of times that a syslog message matches the pattern specified by this syslog event specification since event registration.
$_info_syslog_freq_raise_count_[1-N]	The number of times that this syslog event was raised.
$_info_syslog_freq_occurs_[1-N]	The number of occurrences needed in order to raise the event; if not specified, the event is raised on the first occurrence.
$_info_syslog_freq_period_sec_[1-N]	The number of occurrences must occur within this number of Posix timer units in order to raise the event; if not specified, the period check does not apply.
$_info_syslog_freq_period_msec_[1-N]	The number of occurrences must occur within this number of Posix timer units in order to raise the event; if not specified, the period check does not apply.

Table 3 EEM Built-in Variables for action info Command

Built-in Variable	Description
action info syslog history	
$_info_syslog_hist_num_entries	The number of syslog history entries.
$_info_syslog_hist_msg_[1-N]	The text of the syslog message.
$_info_syslog_hist_time_sec_[1-N]	The seconds since January 1, 1970 which represent the time the syslog message was logged.
$_info_syslog_hist_time_msec_[1-N]	The milliseconds since January 1, 1970 which represent the time the syslog message was logged.

Examples

The following example shows how to configure an EEM applet to intercept configuration commands that attempt to access any loopback interface. The applet also performs a **no shutdown** command on the interface that is selected, and logs a message with the number of times that any “interface loopback” has been attempted. The console output is shown with the configuration because the final line displays the log message.

Note CLI commands that are issued from within a policy do not participate in CLI event pattern matching, and this prevents recursion.

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# event manager applet cli-match
Router(config-applet)# event cli pattern ".*interface Loopback.*" sync yes
Router(config-applet)# action 1.0 cli command "enable"
Router(config-applet)# action 1.1 cli command "$_cli_msg"
Router(config-applet)# action 1.2 cli command "no shutdown"
Router(config-applet)# action 1.3 info type cli frequency
Router(config-applet)# action 1.4 syslog msg "There have been
$_info_cli_freq_match_count_1 '$_info_cli_freq_pattern_1' matches."
Router(config-applet)# set 1.5 _exit_status 0
Router(config-applet)# end
Router#

00:37:30: %SYS-5-CONFIG_I: Configured from console by console

Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# interface loopback0
Router(config)#

00:37:43: %HA_EM-6-LOG: cli-match: There have been 27 '.*interface Loopback.*' matches.
```

Related Commands

Command	Description
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

action mail

To specify the action of sending a short e-mail when an Embedded Event Manager (EEM) applet is triggered, use the **action mail** command in applet configuration mode. To remove the **action mail** command from the configuration, use the **no** form of this command.

action *label* **mail server** *server-address* **to** *to-address* **from** *from-address* [**cc** *cc-address*] **subject** *subject* **body** *body-text*

no action *label* **mail server** *server-address* **to** *to-address* **from** *from-address* [**cc** *cc-address*] **subject** *subject* **body** *body-text*

Syntax Description

label	Unique identifier that can be any string value. Actions are sorted and run in ascending alphanumeric key sequence using the label as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
server	Specifies the e-mail server to be used for forwarding the e-mail.
server-address	Fully qualified domain name of the e-mail server to be used to forward the e-mail.
to	Indicates that a recipient e-mail address is specified.
to-address	E-mail address where the e-mail is to be sent.
from	Indicates that the originating e-mail address is specified.
from-address	E-mail address from which the e-mail is sent.
cc	(Optional) Indicates that a copy e-mail address is specified.
cc-address	(Optional) E-mail address additional to the recipient listed in the *to-address* where the message is to be sent.
subject	Specifies the subject line content of the e-mail.
subject	Alphanumeric string. If the string contains embedded blanks, enclose it in double quotation marks.
body	Specifies the text content of the e-mail.
body-text	Alphanumeric string. If the string contains embedded blanks, enclose it in double quotation marks.

Command Default

No e-mails are sent.

Command Modes

Applet configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

Use the **action mail** command when an event occurs about which you want to send an e-mail message, such as informing an administrator about the event.

Examples

The following example shows how to send an e-mail when an EEM applet executes. The applet named EventInterface is triggered every time the receive_throttle counter for the Fast Ethernet interface 0/0 is incremented by 5. The polling interval to check the counter is specified to run once every 90 seconds. When the applet is triggered, a syslog message and an e-mail are sent.

```
Router(config)# event manager applet EventInterface
Router(config-applet)# event interface name FastEthernet0/0 parameter receive_throttle
entry-op ge entry-val 5 entry-val-is-increment true poll-interval 90
Router(config-applet)# action 1.0 syslog msg "Applet EventInterface"
Router(config-applet)# action 1.1 mail server mailserver.cisco.com to
engineering@cisco.com from devtest@cisco.com cc manager@cisco.com subject
"Receive_throttle counter incremented" body "Receive_throttle counter for FastEthernet0/0
interface has incremented by 5"
```

Related Commands

Command	Description
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

action policy

To specify the action of manually running an Embedded Event Manager (EEM) policy when an EEM applet is triggered, use the **action policy** command in applet configuration mode. To remove the **action policy** command from the configuration, use the **no** form of this command.

action *label* **policy** *policy-filename*

no action *label* **policy** *policy-filename*

Syntax Description

label	Unique identifier that can be any string value. Actions are sorted and run in ascending alphanumeric key sequence using the label as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
policy-filename	Name of the EEM policy to be run manually. The policy must be previously registered using the **event none** command and must not be the same as the current policy.

Command Default

No EEM policies are run.

Command Modes

Applet configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

EEM usually schedules and runs policies on the basis of an event specification that is contained within the policy itself. The **event none** command allows EEM to identify an EEM policy that can be run manually or when an EEM applet is triggered. To run the policy, use either the **action policy** command in applet configuration mode or the **event manager run** command in global configuration mode.

Examples

The following example shows how to register a policy named policy-manual to be run manually and then to execute the policy:

```
Router(config)# event manager applet policy-manual
Router(config-applet)# event none policy-manual
Router(config-applet)# action label1 policy policy-manual
```

Related Commands

Command	Description
event manager run	Manually runs a registered EEM policy.
event none	Registers an EEM applet that is to be run manually.
show event manager policy registered	Displays registered EEM policies.

action publish-event

To specify the action of publishing an application-specific event when the event specified for an Embedded Event Manager (EEM) applet is triggered, use the **action publish-event** command in applet configuration mode. To remove the action of publishing an application-specific event, use the **no** form of this command.

action *label* **publish-event sub-system** *sub-system-id* **type** *event-type* **arg1** *argument-data* [**arg2** *argument-data*] [**arg3** *argument-data*] [**arg4** *argument-data*]

no action *label* **publish-event**

Syntax Description

label	Unique identifier that can be any string value. Actions are sorted and run in ascending alphanumeric key sequence using the label as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
sub-system	Specifies an identifier for the subsystem named in the *sub-system-id* argument that will publish the application event.
sub-system-id	Identifier of the subsystem. Number in the range from 1 to 4294967295. If the event is to be published by an EEM policy, the *sub-system-id* reserved for a customer policy is 798.
type	Specifies the value of an event type within the specified event.
event-type	Event type value. Number in the range from 1 to 4294967295.
arg1	Specifies that argument data is to be passed to the application-specific event when the event is published.
argument-data	Character text, an environment variable, or a combination of the two. Optional when used with the **arg2**, **arg3**, or **arg4** keywords.
arg2 **arg3** **arg4**	(Optional) Specifies that argument data is to be passed to the application-specific event when the event is published.

Command Default

No application-specific events are published.

Command Modes

Applet configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Examples

The following example shows how a policy named EventPublish_A runs every 20 seconds and publishes an event to a well-known EEM event type numbered 1. A second policy named EventPublish_B is registered to run when the well-known EEM event type of 1 occurs. When policy EventPublish_B runs, it outputs a message to syslog containing the argument 1 argument data passed from EventPublish_A.

```
Router(config)# event manager applet EventPublish_A
Router(config-applet)# event timer watchdog time 20.0
Router(config-applet)# action 1.0 syslog msg "Applet EventPublish_A"
Router(config-applet)# action 2.0 publish-event sub-system 798 type 1 arg1 twenty
Router(config-applet)# exit
Router(config)# event manager applet EventPublish_B
Router(config-applet)# event application sub-system 798 type 1
Router(config-applet)# action 1.0 syslog msg "Applet EventPublish_B arg1
$_application_data1"
```

Related Commands

Command	Description
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

action reload

To specify the action of reloading the Cisco IOS software when an Embedded Event Manager (EEM) applet is triggered, use the **action reload** command in applet configuration mode. To remove the action of reloading the Cisco IOS software, use the **no** form of this command.

action *label* **reload**

no action *label* **reload**

Syntax Description

label	Unique identifier that can be any string value. Actions are sorted and run in ascending alphanumeric key sequence using the label as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.

Command Default

No reload of the Cisco IOS software is performed.

Command Modes

Applet configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

Before configuring the **action reload** command, you should ensure that the device is configured to reboot the software version that you are expecting. Use the **show startup-config** command and look for any **boot system** commands.

Examples

The following example shows how to reload the Cisco IOS software when the memory-fail applet is triggered:

```
Router(config)# event manager applet memory-fail
Router(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.48.1.1.1.6.1 get-type exact entry-op
lt entry-val 5120000 poll-interval 10
Router(config-applet)# action 3.0 reload
```

Related Commands

Command	Description
boot system	Configures the locations from which the router loads software when the router reboots.
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.
show startup-config	Displays the configuration to be run when the router reboots.

action snmp-trap

To specify the action of generating a Simple Network Management Protocol (SNMP) trap when an Embedded Event Manager (EEM) applet is triggered, use the **action snmp-trap** command in applet configuration mode. To remove the action of generating an SNMP trap, use the **no** form of this command.

action *label* **snmp-trap** [**intdata1** *integer*] [**intdata2** *integer*] [**strdata** *string*]

no action *label* **snmp-trap**

Syntax Description

label	Unique identifier that can be any string value. Actions are sorted and run in ascending alphanumeric key sequence using the label as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
intdata1	(Optional) Specifies an integer to be sent in the SNMP trap message to the SNMP agent.
intdata2	(Optional) Specifies a second integer to be sent in the SNMP trap message to the SNMP agent.
integer	(Optional) Integer value.
strdata	(Optional) Specifies a string to be sent in the SNMP trap message to the SNMP agent.
string	(Optional) Sequence of up to 256 characters. If the string contains embedded blanks, enclose it in double quotation marks.

Command Default

No SNMP traps are generated when an EEM applet is triggered.

Command Modes

Applet configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

Before configuring this command, you must enable the **snmp-server enable traps event-manager** command to permit SNMP traps to be sent from the Cisco IOS device to the SNMP server. Other relevant **snmp-server** commands must also be configured.

This command generates an asynchronous message that is sent from the Cisco IOS device to the SNMP agent. The SNMP agent can be coded to understand customized data such as the optional integer and string data that can be sent in the SNMP trap message.

The SNMP trap that is generated uses the EEM MIB, CISCO-EMBEDDED-EVENT-MGR-MIB.my. Details about the MIB can be found using Cisco MIB Locator at the following URL:

http://www.cisco.com/go/mibs

Examples

The following example shows an EEM applet called IPSLAping1 being registered to run when there is an exact match on the value of a specified SNMP object ID that represents a successful IP SLA ICMP echo operation (this is equivalent to a **ping** command). Four actions are triggered when the echo operation fails, and event monitoring is disabled until after the second failure. A message that the ICMP echo operation to a server failed is sent to syslog, an SNMP trap is generated, EEM publishes an application-specific event, and a counter called IPSLA1F is incremented by a value of one.

```
Router(config)# event manager applet IPSLAping1
Router(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.42.1.2.9.1.6.4 get-type exact
entry-op eq entry-val 1 exit-op eq exit-val 2 poll-interval 5
Router(config-applet)# action 1.0 syslog priority critical msg "Server IP echo failed:
OID=$_snmp_oid_val"
Router(config-applet)# action 1.1 snmp-trap strdata "EEM detected server reachability
failure to 10.1.88.9"
Router(config-applet)# action 1.2 publish-event sub-system 88000101 type 1 arg1 10.1.88.9
arg2 IPSLAEcho arg3 fail
Router(config-applet)# action 1.3 counter name _IPSLA1F value 1 op inc
```

Related Commands

Command	Description
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.
snmp-server enable traps event-manager	Permits Embedded Event Manager SNMP traps to be sent from a Cisco IOS device to the SNMP server.

action syslog

To specify the action of writing a message to syslog when an Embedded Event Manager (EEM) applet is triggered, use the **action syslog** command in applet configuration mode. To remove the syslog message event criteria, use the **no** form of this command.

action *label* **syslog** [**priority** *priority-level*] **msg** *msg-text*

no action *label* **syslog** [**priority** *priority-level*] **msg** *msg-text*

Syntax Description

label	Unique identifier that can be any string value. Actions are sorted and run in ascending alphanumeric key sequence using the label as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
priority	(Optional) Specifies the priority level of the syslog messages. If this keyword is selected, the *priority-level* argument must be defined. If this keyword is not selected, all syslog messages are set at the informational priority level.
priority-level	(Optional) Number or name of the desired priority level at which syslog messages are set. Priority levels are as follows (enter the number or the keyword): • {**0** | **emergencies**}—System is unusable. • {**1** | **alerts**}—Immediate action is needed. • {**2** | **critical**}—Critical conditions. • {**3** | **errors**}—Error conditions. • {**4** | **warnings**}—Warning conditions. • {**5** | **notifications**}—Normal but significant conditions. • {**6** | **informational**}—Informational messages. This is the default. • {**7** | **debugging**}—Debugging messages.
msg	Specifies the message to be logged.
msg-text	Character text, an environment variable, or a combination of the two. If the string contains embedded blanks, enclose it in double quotation marks. **Note** Messages written to syslog from an EEM applet are not screened for EEM syslog events, which may lead to recursive EEM syslog events. Messages sent from an EEM applet include the applet name for identification.

Command Default

No messages are written to syslog.

Command Modes

Applet configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Examples

The following example shows how to specify a message to be sent to syslog when the memory-fail applet is triggered:

```
Router(config)# event manager applet memory-fail
Router(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.48.1.1.1.6.1 get-type exact entry-op
lt entry-val 5120000 poll-interval 10
Router(config-applet)# action 4.0 syslog msg "Memory exhausted; current available memory
is $_snmp_oid_val bytes"
```

Related Commands

Command	Description
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

action track read

To specify the action of reading the state of a tracked object when an Embedded Event Manager (EEM) applet is triggered, use the **action track read** command in applet configuration mode. To remove the **action track read** command from the configuration, use the **no** form of this command.

action *label* **track read** *object-number*

no action *label* **track read** *object-number*

Syntax Description

label	Unique identifier that can be any string value. Actions are sorted and run in ascending alphanumeric key sequence using the label as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
object-number	Tracked object number in the range from 1 to 500, inclusive. The number is defined using the **track stub** command.

Command Default

The state of a tracked object is not read.

Command Modes

Applet configuration (config-applet)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(31)SB3	This command was integrated into Cisco IOS Release 12.2(31)SB3.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command generates the following result variable:

- _track_state—State of the specified tracked object. The text string returned is either up or down. If the state is up, it means that the object exists and is in an up state. If the state is down, it means that the object either does not exist or is in a down state.

This command is used to help track objects using EEM. Each tracked object is identified by a unique number that is specified on the tracking command-line interface (CLI). Client processes such as EEM use this number to track a specific object. The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to interested client processes, either immediately or after a specified delay. The object values are reported as either up or down. The enhanced object tracking event detector publishes an EEM event when the tracked object changes.

Examples

The following example shows how to specify event criteria based on a tracked object:

```
event manager applet track-ten
 event track 10 state any
 action 1.0 track set 10 state up
 action 2.0 track read 10
```

Related Commands

Command	Description
action track set	Specifies the action of setting the state of a tracked object when an EEM applet is triggered.
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.
show track	Displays tracking information.
track stub	Creates a stub object to be tracked.

action track set

To specify the action of setting the state of a tracked object when an Embedded Event Manager (EEM) applet is triggered, use the **action track set** command in applet configuration mode. To remove the **action track set** command from the configuration, use the **no** form of this command.

action *label* **track set** *object-number* **state** {**up** | **down**}

no action *label* **track set** *object-number* **state** {**up** | **down**}

Syntax Description

label	Unique identifier that can be any string value. Actions are sorted and run in ascending alphanumeric key sequence using the label as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
object-number	Tracked object number in the range from 1 to 500, inclusive. The number is defined using the **track stub** command.
state	Specifies the state to which the tracked object will be set.
up	Specifies that the state of the tracked object will be set to up.
down	Specifies that the state of the tracked object will be set to down.

Command Default

The state of a tracked object is not set.

Command Modes

Applet configuration (config-applet)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(31)SB3	This command was integrated into Cisco IOS Release 12.2(31)SB3.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command generates the following result variable:

- _track_state—State of the specified tracked object. The text string returned is either up or down. If the state is up, it means that the object exists and is in an up state. If the state is down, it means that the object either does not exist or is in a down state.

This command is used to help track objects using EEM. Each tracked object is identified by a unique number that is specified on the tracking command-line interface (CLI). Client processes such as EEM use this number to track a specific object. The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to interested client processes, either immediately or after a specified delay. The object values are reported as either up or down. The enhanced object tracking event detector publishes an EEM event when the tracked object changes.

Examples

The following example shows how to specify event criteria based on a tracked object:

```
event manager applet track-ten
 event track 10 state any
 action 1.0 track set 10 state up
 action 2.0 track read 10
```

Related Commands

Command	Description
action track read	Specifies the action of reading the state of a tracked object when an EEM applet is triggered.
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.
show track	Displays tracking information.
track stub	Creates a stub object to be tracked.

add (bulkstat object)

To add a MIB object to a 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-name* | *oid*}

no add {*object-name* | *oid*}

Syntax Description

object-name	Name of the MIB object to add to the list. Only object names from the Interfaces MIB (IF-MIB.my), Cisco Committed Access Rate MIB (CISCO-CAR-MIB.my) and the MPLS Traffic Engineering MIB (MPLS-TE-MIB.my) may be used.
oid	Object ID (OID) of the MIB object to add to the list.Only OIDs from the Interfaces MIB (IF-MIB.my), Cisco Committed Access Rate MIB (CISCO-CAR-MIB.my) and the MPLS Traffic Engineering MIB (MPLS-TE-MIB.my) may be used.

Command Default

No MIB objects are listed in the bulk statistics object list.

Command Modes

Bulk Statistics Object List configuration (config-bulk-objects)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

All the objects in an object list have to be indexed by the same MIB index, but the objects need not belong to the same MIB table. For example, it is possible to group ifInoctets and an Ether MIB object in the same schema because the containing tables are indexed by the ifIndex (in the IF-MIB).

Object names are available in the relevant MIB modules. For example, the input byte count of an interface is defined in the Interfaces Group MIB (IF-MIB.my) as ifInoctets. Complete MIB modules can be downloaded from Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Examples

In the following example, two bulk statistics object lists are configured: one for IF-MIB objects and one for CISCO-CAR-MIB objects. Because the IF-MIB objects and the CISCO-CAR-MIB objects do not have the same index, they must be defined in separate object lists.

```
Router(config)# snmp mib bulkstat object-list if-Objects
Router(config-bulk-objects)# add ifInoctets
Router(config-bulk-objects)# add ifOutoctets
Router(config-bulk-objects)# add ifInUcastPkts
Router(config-bulk-objects)# add ifInDiscards
Router(config-bulk-objects)# exit
Router(config)# snmp mib bulkstat object-list CAR-Objects
Router(config-bulk-objects)# add CcarStatSwitchedPkts
Router(config-bulk-objects)# add ccarStatSwitchedBytes
Router(config-bulk-objects)# add CcarStatFilteredBytes
Router(config-bulk-objects)# exit
Router(config)#
```

Related Commands

Command	Description
snmp mib bulkstat object-list	Names a bulk statistics object list and enters Bulk Statistics Object List configuration mode.

alias (boomerang)

To configure an alias name for a specified domain, use the **alias** command in boomerang configuration mode. To remove this 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.

alias *alias-name*

no alias *alias-name*

Syntax Description

alias-name	Alias name for a specified domain.

Command Default

No domain name alias is configured.

Command Modes

Boomerang configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **alias** command can be used only on a Director Response Protocol (DRP) agent. The boomerang client is the DRP agent.

Use the **alias** command to specify one or more alias names for an existing domain. Because the boomerang client maintains separate counters for requests received for each domain name (alias or otherwise), use the **show ip drp boomerang** command to view these counters for a specified domain name and each of its aliases.

Examples

In the following example, the domain name alias is configured for www.boom1.com. The new alias for www.boom1.com is www.boom2.com:

```
Router(config)# ip drp domain www.boom1.com
Router(config-boomerang)# alias www.boom2.com

Router# show running-config
.
.
.
ip drp domain www.boom1.com
alias www.boom2.com
```

Related Commands

Command	Description
ip drp domain	Adds a new domain to the DistributedDirector client or configures an existing domain and puts the client in boomerang configuration mode.
server (boomerang)	Configures the server address for a specified boomerang domain.
show ip drp	Displays DRP statistics on DistributedDirector or a DRP server agent.
show ip drp boomerang	Displays boomerang information on the DRP agent.
ttl dns	Configures the number of seconds for which an answer received from the boomerang client will be cached by the DNS client.
ttl ip	Configures the IP TTL value for the boomerang response packets sent from the boomerang client to the DNS client in number of hops.

announce config

To specify that an unsolicited configuration inventory is sent out by the CNS inventory agent at bootup, use the **announce config** command in CNS inventory configuration mode. To disable the sending of the configuration inventory, use the **no** form of this command.

announce config

no announce config

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

CNS inventory configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to limit inventory requests by the CNS inventory agent. When configured, the routing device details will be announced on the CNS event bus, but the routing device will not respond to any queries from the CNS event bus.

Examples

The following example shows how to configure the CNS inventory agent to send out an unsolicited configuration inventory one time only at bootup:

```
Router(config)# cns inventory
Router(cns_inv)# announce config
```

Related Commands

Command	Description
cns inventory	Enables the CNS inventory agent and enters CNS inventory configuration mode.

buffer public

To enter buffer owner configuration mode to set thresholds for buffer usage, use the **buffer public** command in resource policy node configuration mode. To exit buffer owner configuration mode, use the **no** form of this command.

buffer public

no buffer public

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Resource policy node configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command allows you to enter buffer owner configuration mode to set rising and falling values for critical, major, and minor thresholds for buffer usage.

Examples

The following example shows how to enter buffer owner configuration mode to set thresholds for buffer usage:

```
Router(config-res-policy-node)# buffer public
```

Related Commands

Command	Description
critical rising	Sets the critical level threshold values for the buffer, CPU, and memory ROs.
major rising	Sets the major level threshold values for the buffer, CPU, and memory ROs.
minor rising	Sets the minor level threshold values for the buffer, CPU, and memory ROs.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show buffer leak	Displays the buffer details.
show resource all	Displays all the resource details.
slot (ERM policy)	Configures line cards.
system (ERM policy)	Configures system level ROs.

buffer-length

To specify the maximum length of the data stream to be forwarded, use the **buffer-length** command in line configuration mode. To restore the default setting, use the **no** form of this command.

buffer-length *length*

no buffer-length

Syntax Description

length	Specifies the length of the buffer in bytes. Valid values for the *length* argument range from 16 to 1536. The default buffer length is 1536 bytes.

Defaults

1536 bytes

Command Modes

Line configuration

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **buffer-length** command configures the size of the forwarded data stream. The higher the value used for the *length* argument is, the longer the delay between data transmissions will be. Configuring a smaller buffer length can prevent connections from timing out inappropriately.

Examples

The following example configures a buffer length of 500 bytes:

```
Router(config)# line 1
Router(config-line)# buffer-length 500
```

buffers

To make adjustments to initial public buffer pool settings and to the limits at which temporary buffers are created and destroyed, use the **buffers** command in global configuration mode. To return the buffer pool settings to their default sizes, use the **no** form of this command.

buffers {{**header** | **fastswitching** | *interface number* | **small** | **middle** | **big** | **verybig** | **large** | **huge** {**initial** | **max-free** | **min-free** | **permanent**} *buffers*} | **particle-clone** *particle-clones* | **element** {**minimum** | **permanent**} *elements*}

no buffers {{**header** | **fastswitching** | *interface number* | **small** | **middle** | **big** | **verybig** | **large** | **huge** {**initial** | **max-free** | **min-free** | **permanent**} *buffers*} | **particle-clone** *particle-clones* | **element** {**minimum** | **permanent**} *elements*}

Syntax Description

header	Number of particles in the header particle pool. The range is from 256 to 65535. The defaults are min:256, max:1024, and cache:256.
fastswitching	Number of particles in the fastswitching particle pool. The range is from 512 to 65535. The defaults are min:0, max:512, and cache:512.
type number	Interface *type* and *number* of the interface buffer pool. The *type* value cannot be **fddi**.
small	Buffer size of this public buffer pool is 104 bytes.
middle	Buffer size of this public buffer pool is 600 bytes.
big	Buffer size of this public buffer pool is 1524 bytes.
verybig	Buffer size of this public buffer pool is 4520 bytes.
large	Buffer size of this public buffer pool is 5024 bytes.
huge	Public buffer pool can be configured with the **buffers huge size** command. Default buffer size of this public buffer pool, in bytes, is 18024.
initial	Number of additional temporary buffers that are to be allocated when the system is reloaded. This keyword can be used to ensure that the system has necessary buffers immediately after reloading in a high-traffic environment.
max-free	Maximum number of free or unallocated buffers in a buffer pool. The maximum number of small buffers that can be constructed in the pool is 20480.
min-free	Minimum number of free or unallocated buffers in a buffer pool.
permanent	Number of permanent buffers that the system tries to create and keep. Permanent buffers are normally not trimmed by the system.
buffers	Number of buffers to be allocated. The range is 0 to 65536.
particle-clone *particle-clone*	Number of particle clones to grow. The range is from 1024 to 65535. The default is 1024.
element	Buffer elements. The required keywords for the **element** keyword are as follows: • **permanent**—Permanent buffer elements. • **minimum**—Minimum buffer elements.
elements	Number of buffer elements. For permanent buffer elements. The range is from 500 to 65535. The default is 500. For minimum buffer elements. The range is from 500 to 65535.

Defaults

Buffers are set at default sizes that vary by hardware configuration.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.4(10)	The **minimum** keyword was added to set the minimum number of buffer elements. The **particle-clone** keyword was added to set the number of particle clones in the buffer pool. The **header** keyword was added to set the number of particles in the header particle pool. The **fastswitching** keyword was added to set the number of particles in the fastswitching particle pool.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The default number of buffers in a pool is determined by the hardware configuration and can be displayed with the **show buffers** command in user EXEC mode. Generally, buffer settings do not need to be adjusted. Consult with technical support personnel before making any changes.

Note Improper buffer settings can adversely impact system performance.

You cannot configure FDDI buffers.

Use the **element** keyword with the **permanent** *elements* keyword-argument combination to increase the number of permanent buffer elements to prevent packet loss. For example, in a multicasting environment, a higher number of buffer elements may be needed to accommodate bursts of traffic.

Use the **element** keyword with the **minimum** *elements* keyword-argument combination to set the minimum number of buffer elements.

Note It is preferable to use the **element** keyword with the **permanent** *elements* keyword-argument combination during system initialization because a higher number of permanent buffer elements will then be ready for use in case a burst of traffic occurs.

Use the **show buffers** command to display statistics such as the following:

- Free list (the total number of unallocated buffer elements)
- Max allowed (the maximum number of buffer elements that are available for allocation)
- Hits (the count of successful attempts to allocate a buffer when needed)

- Misses (the count of buffer allocation attempts that resulted in growing the buffer pool to allocate a buffer)
- Created (the count of new buffers created to satisfy buffer allocation attempts when the available buffers in the pool have already been allocated)

Note If the requested number of permanent buffer elements is fewer than the current number of permanent buffer elements, the configuration will not take effect until the next reload. Resetting the number of permanent buffer elements to the default value using the **no** form of this command will not take effect until the next reload.

Cisco 10000 Series Router

Table 4 lists the buffer sizes to configure if your network uses a RADIUS server for authentication.

Table 4 Buffer Sizes for RADIUS Authentication

Buffer	Size (in Bytes)
Small	15000
Middle	12000
Big	8000

Examples

Examples of Public Buffer Pool Tuning

The following example shows how to keep at least 50 small buffers free in the system:

```
Router(config)# buffers small min-free 50
```

The following example shows how to increase the permanent buffer pool allocation for big buffers to 200:

```
Router(config)# buffers big permanent 200
```

Example of Interface Buffer Pool Tuning

A general guideline is to display buffers with the **show buffers** command and to increase the buffer pool that is depleted.

The following example shows how to increase the permanent Ethernet interface 0 buffer pool on a Cisco 4000 router to 96 when the Ethernet 0 buffer pool is depleted:

```
Router(config)# buffers ethernet 0 permanent 96
```

Examples of Buffer Element Tuning

The following example shows how to configure the number of permanent buffer elements to 6,000:

```
Router(config)# buffers element permanent 6000
```

The following example shows how to configure the number of minimum buffer elements to 6,000:

```
Router(config)# buffers element minimum 6000
```

Related Commands

Command	Description
load-interval	Changes the length of time for which data is used to compute load statistics.
show buffers	Displays statistics for the buffer pools on the network server.

buffers huge size

To dynamically resize all huge buffers to the value you specify, use the **buffers huge size** command in global configuration mode. To restore the default buffer values, use the **no** form of this command.

buffers huge size *number-of-bytes*

no buffers huge size *number-of-bytes*

Syntax Description

number-of-bytes	Huge buffer size (in bytes). Valid range is from 18024 to 100000 bytes.

Defaults

18,024 bytes

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command only after consulting with technical support personnel. The buffer size cannot be lowered below the default.

Note Improper buffer settings can adversely impact system performance.

Examples

The following example resizes huge buffers to 20,000 bytes:

```
Router(config)# buffers huge size 20000
```

Related Commands

Command	Description
buffers	Adjusts the initial buffer pool settings and the limits at which temporary buffers are created and destroyed.
show buffers	Displays statistics for the buffer pools on the network server.

buffers tune automatic

To enable automatic tuning of buffers, use the **buffers tune automatic** command in global configuration mode. To disable automatic tuning of buffers, use the **no** form of this command.

buffers tune automatic

no buffers tune automatic

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command enables automatic tuning of buffers. Even when the command is not enabled, the parameters are computed. When you enable the command later, the buffer parameters change to the computed values.

Examples

The following example shows how to enable automatic tuning of buffers:

```
Router(config)# buffers tune automatic
```

Related Commands

Command	Description
show buffers tune	Displays the automatic buffer tune details.

buffer-size (bulkstat)

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 (config-bulk-tr)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

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.

Examples

In the following example, the bulk statistics transfer buffer size is set to 3072 bytes:

```
Router(config)# snmp mib bulkstat transfer bulkstat1
Router(config-bulk-tr)# schema ATM2/0-IFMIB
Router(config-bulk-tr)# url primary ftp://user:pswrd@host/folder/bulkstat1
Router(config-bulk-tr)# buffer-size 3072
Router(config-bulk-tr)# enable
Router(config-bulk-tr)# exit
Router(config)#
```

Related Commands

Command	Description
snmp mib bulkstat transfer	Identifies the transfer configuration with a name and enters Bulk Statistics Transfer configuration mode.

calendar set

To manually set the hardware clock (calendar), use one of the formats of the **calendar set** command in EXEC mode.

calendar set *hh***:***mm***:***ss day month year*

calendar set *hh***:***mm***:***ss month day year*

Syntax Description

*hh***:***mm***:***ss*	Current time in hours (using 24-hour notation), minutes, and seconds.
day	Current day (by date) in the month.
month	Current month (by name).
year	Current year (no abbreviation).

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Some platforms have a hardware clock that is separate from the software clock. In Cisco IOS software syntax, the hardware clock is called the "calendar." The hardware clock is a battery-powered chip that runs continuously, even if the router is powered off or rebooted. After you set the hardware clock, the software clock will be automatically set from the hardware clock when the system is restarted or when the **clock read-calendar** EXEC command is issued. The time specified in this command is relative to the configured time zone.

Examples

The following example manually sets the hardware clock to 1:32 p.m. on May 19, 2003:

```
Router# calendar set 13:32:00 May 19 2003
```

Related Commands

Command	Description
clock read-calendar	Performs a one-time update of the software clock from the hardware clock (calendar).
clock set	Sets the software clock.
clock summer-time	Configures the system time to automatically switch to summer time (daylight saving time).

Command	Description
clock timezone	Sets the time zone for display purposes.
clock update-calendar	Performs a one-time update of the hardware clock from the software clock.

cdp advertise-v2

To enable Cisco Discovery Protocol Version 2 (CDPv2) advertising functionality on a device, use the **cdp advertise-v2** command in global configuration mode. To disable advertising CDPv2 functionality, use the **no** form of the command.

cdp advertise-v2

no cdp advertise-v2

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

CDP Version 2 has three additional type-length values (TLVs): VTP Management Domain Name, Native VLAN, and full/half-Duplex.

Examples

In the following example, CDP Version 2 advertisements are disabled on the router:

```
Router# show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is  enabled
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no cdp advertise-v2
Router(config)# end
Router# show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is not enabled
Router#
```

Related Commands

Command	Description
cdp enable	Enables CDP on a supported interface.
cdp run	Reenables CDP on a Cisco device.

cdp enable

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

cdp enable

no cdp enable

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled at the global level and on all supported interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

CDP is enabled by default at the global level and on each supported interface in order to send or receive CDP information. However, some interfaces, such as ATM interfaces, do not support CDP.

Note The **cdp enable**, **cdp timer**, and **cdp run** commands affect the operation of the IP on demand routing feature (that is, the **router odr** global configuration command). For more information on the **router odr** command, see the “On-Demand Routing Commands” chapter in the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* document.

Examples

In the following example, CDP is disabled on the Ethernet 0 interface only:

```
Router# show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is  enabled
Router# config terminal
Router(config)# interface ethernet 0
Router(config-if)# no cdp enable
```

Related Commands

Command	Description
cdp run	Reenables CDP on a Cisco device.
cdp timer	Specifies how often the Cisco IOS software sends CDP updates.
router odr	Enables on-demand routing on a hub router.

cdp holdtime

To specify the amount of time the receiving device should hold a Cisco Discovery Protocol (CDP) packet from the router before discarding it, use the **cdp holdtime** command in global configuration mode. To revert to the default setting, use the **no** form of this command.

cdp holdtime *seconds*

no cdp holdtime

Syntax Description

seconds	Specifies the hold time to be sent in the CDP update packets. The default is 180 seconds.

Command Default

180 seconds

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

CDP packets are sent with a time to live, or hold time, value. The receiving device will discard the CDP information in the CDP packet after the hold time has elapsed.

You can set the hold time lower than the default setting of 180 seconds if you want the receiving devices to update their CDP information more rapidly.

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

Examples

In the following example, the CDP packets being sent from the router are configured with a hold time of 60 seconds.

```
Router(config)# cdp holdtime 60
```

Related Commands

Command	Description
cdp timer	Specifies how often the Cisco IOS software sends CDP updates.
show cdp	Displays global CDP information, including timer and hold-time information.

cdp log mismatch duplex

To display the log of duplex mismatches generated by the Cisco Discovery Protocol on Ethernet interfaces, use the **cdp log mismatch duplex** command in global configuration mode or in interface configuration mode. To disable the display of duplex messages, use the **no** form of this command.

cdp log mismatch duplex

no cdp log mismatch duplex

Syntax Description

This command has no arguments or keywords.

Command Default

Duplex mismatches are displayed for all Ethernet interfaces by default.

Command Modes

Global configuration

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Duplex mismatches can occur only on Ethernet interfaces.

When you enter the **cdp log mismatch duplex** command in global configuration mode, duplex mismatches are displayed for all Ethernet interfaces on the device. If the command is disabled in global configuration mode, the command cannot be configured in interface configuration mode. When you enter the **cdp log mismatch duplex** command in interface configuration mode, only duplex mismatches for the specified Ethernet interface are displayed.

To enable reporting of duplex mismatches, issue the **cdp log mismatch duplex** command in global configuration mode. If the command was previously disabled under a specified interface, issue the command in interface configuration mode for that interface.

To disable reporting of duplex mismatches globally, issue the **no cdp log mismatch duplex** command in global configuration mode. To disable reporting duplex mismatches for a specified Ethernet interface, use the **no cdp log mismatch duplex** command in interface configuration mode.

Examples

The following example shows how to enable the display of duplex messages from all Ethernet interfaces on a router:

```
Router(config)# cdp log mismatch duplex
```

The following example shows how to enable the display of duplex messages that may be generated from only Ethernet interface 2/1:

```
Router(config)# interface ethernet2/1
Router(config-if)# cdp log mismatch duplex
```

The following is sample output from the **show running-config** command. The bold text in the output shows that the **cdp log mismatch duplex** command is disabled globally.

```
Router# show running-config

version 12.2
hostname Router
!
interface Ethernet2/0
no ip address
duplex half
interface Ethernet2/1
no ip address
duplex half
!
no cdp log mismatch duplex
!
line con 0
line aux 0
```

The following is sample output from the **show running-config** command. The bold text in the output shows that the **cdp log mismatch duplex** command is disabled under a specific interface.

```
Router# show running-config

version 12.2
hostname Router
!
interface Ethernet2/0
no ip address
duplex half
no cdp log mismatch duplex
interface Ethernet2/1
no ip address
duplex half
!!
line con 0
line aux 0
line vty 0 4
```

Related Commands

Command	Description
cdp enable	Enables Cisco Discovery Protocol on a supported interface.
cdp run	Reenables Cisco Discovery Protocol on a Cisco device.

cdp run

To enable Cisco Discovery Protocol, use the **cdp run** command in global configuration mode. To disable Cisco Discovery Protocol, use the **no** form of this command.

cdp run

no cdp run

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled on all platforms except the Cisco 10000 Series Edge Services Router

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Cisco Discovery Protocol is enabled by default on all platforms except the Cisco 10000 Series Edge Services Router, which means Cisco IOS software receives Cisco Discovery Protocol information. Cisco Discovery Protocol also is enabled on supported interfaces by default. To disable Cisco Discovery Protocol on an interface, use the **no cdp enable** command in interface configuration mode.

The **show running-config** command lists **no cdp run** when Cisco Discovery Protocol is disabled globally, which is not the default behavior. As a result of changes made for the Cisco 10000 platform, **show running-config** will list **cdp run** when Cisco Discovery Protocol is enabled globally.

Note Because on-demand routing (ODR) uses Cisco Discovery Protocol, the **cdp enable**, **cdp timer**, and **cdp run** commands affect the operation of the **router odr** global configuration command. For more information about the **router odr** command, see the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* document.

Examples

In the following example, Cisco Discovery Protocol is disabled globally, then the user attempts to enable it on the Ethernet 0 interface:

```
Router(config)# no cdp run
Router(config)# end
Router# show cdp
```

```
% CDP is not enabled

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface ethernet0
Router(config-if)# cdp enable

% Cannot enable CDP on this interface, since CDP is not running
Router(config-if)#
```

Related Commands

Command	Description
cdp enable	Enables Cisco Discovery Protocol on a supported interface.
cdp holdtime	Specifies the amount of time a receiving device should hold a Cisco Discovery Protocol packet before discarding it.
cdp timer	Specifies how often the Cisco IOS software sends Cisco Discovery Protocol updates.
router odr	Enables ODR on the hub router.

cdp source-interface

To configure the Cisco Discovery Protocol source interface, use the **cdp source-interface** command in global configuration mode.

cdp source-interface *type number*

no cdp source-interface

Syntax Description

type	Type of interface to be configured.
number	Port, connector, or interface card number. These numbers were assigned at the time of installation or when added to a system, and can be displayed with the **show interfaces** command.

Defaults

No Cisco Discovery Protocol source-interface is specified.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use of this command ensures that Cisco Discovery Protocol packets use the IP address that has been previously assigned to an interface. Without this command, Cisco Discovery Protocol uses the IP address of the first available interface.

The conditions that an interface should satisfy to be the source interface are as follows:

- It should have an IP address.
- Its status should be UP.
- It should not be an IP unnumbered interface.

When Cisco Discovery Protocol is enabled and the Cisco Discovery Protocol source interface has not been configured, then Cisco Discovery Protocol uses the IP address of the first available interface.

Examples

The following example configures Cisco Discovery Protocol to use the IP address that has been assigned to interface loopback 1.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# cdp source-interface loopback 1
Router(config)# exit
Router#
```

Related Commands

Command	Description
cdp enable	Enables Cisco Discovery Protocol on a supported interface.
cdp run	Reenables Cisco Discovery Protocol on a Cisco device.

cdp timer

To specify how often the Cisco IOS software sends Cisco Discovery Protocol (CDP) updates, use the **cdp timer** command in global configuration mode. To revert to the default setting, use the **no** form of this command.

cdp timer *seconds*

no cdp timer

Syntax Description

seconds	Integer that specifies how often, in seconds, the Cisco IOS software sends CDP updates. The default is 60 seconds.

Command Default

The default setting is 60 seconds.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The trade-off with sending more frequent CDP updates to provide up-to-date information, is that bandwidth is used more often.

Note The **cdp enable**, **cdp timer**, and **cdp run** commands affect the operation of the IP on demand routing feature (that is, the **router odr** global configuration command). For more information on the **router odr** command, see the "On-Demand Routing Commands" chapter in the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* document.

Examples

In the following example, CDP updates are sent every 80 seconds, less frequently than the default setting of 60 seconds. You might want to make this change if you are concerned about preserving bandwidth.

```
cdp timer 80
```

Related Commands

Command	Description
cdp enable	Enables CDP on a supported interface.
cdp holdtime	Specifies the amount of time the receiving device should hold a CDP packet from your router before discarding it.
cdp timer	Specifies how often the Cisco IOS software sends CDP updates.
router odr	Enables ODR on the hub router.
show cdp	Displays global CDP information, including timer and hold-time information.

clear cdp counters

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

clear cdp counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example clears the CDP counters. The **show cdp traffic** output shows that all of the traffic counters have been reset to zero.

```
Router# clear cdp counters
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, Fragmented: 0
```

Related Commands

Command	Description
clear cdp table	Clears the table that contains CDP information about neighbors.
show cdp traffic	Displays traffic information from the CDP table.

clear cdp table

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

clear cdp table

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example clears the CDP table. The output of the **show cdp neighbors** command shows that all information has been deleted from the table.

```
Router# clear cdp table

CDP-AD: Deleted table entry for neon.cisco.com, interface Ethernet0
CDP-AD: Deleted table entry for neon.cisco.com, interface Serial0

Router# show cdp neighbors

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

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
```

Related Commands

Command	Description
show cdp neighbors	Displays information about neighbors.

clear cns config stats

To clear the statistics about the Cisco Networking Services (CNS) configuration agent, use the **clear cns config stats** command in privileged EXEC mode.

clear cns config stats

Syntax Description

This command has no arguments or keywords.

Defaults

No statistics are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **clear cns config stats** command clears all the statistics displayed by the **show cns config stats** command.

Examples

The following example shows how to clear all of the statistics for the CNS configuration agent:

```
Router# clear cns config stats
```

Related Commands

Command	Description
show cns config stats	Displays statistics about the CNS configuration agent.

clear cns counters

To clear all Cisco Networking Services (CNS) statistics, use the **clear cns counters** command in privileged EXEC mode.

clear cns counters

Syntax Description

This command has no arguments or keywords.

Defaults

No statistics are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **clear cns counters** command clears all the statistics tracked and displayed by CNS agents.

Examples

The following example shows how to clear all of the statistics used by CNS:

```
Router# clear cns counters
```

Related Commands

Command	Description
show cns config stats	Displays statistics about the CNS configuration agent.
show cns event stats	Displays statistics about the CNS event agent.
show cns image stats	Displays statistics about the CNS image agent.

clear cns event stats

To clear the statistics about the Cisco Networking Services (CNS) event agent, use the **clear cns event stats** command in privileged EXEC mode.

clear cns event stats

Syntax Description

This command has no arguments or keywords.

Defaults

No statistics are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **clear cns event stats** command clears all the statistics displayed by the **show cns event stats** command.

Examples

The following example shows how to clear all of the statistics for the CNS event agent:

```
Router# clear cns event stats
```

Related Commands

Command	Description
show cns event stats	Displays statistics about the CNS event agent.

clear cns image connections

To clear the Cisco Networking Services (CNS) image agent connections statistics, use the **clear cns image connections** command in privileged EXEC mode.

clear cns image connections

Syntax Description

This command has no arguments or keywords.

Command Default

No statistics are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **clear cns image connections** command clears all the statistics displayed by the **show cns image connections** command.

Examples

The following example shows how to clear all of the connection statistics for the CNS image agent:

```
Router# clear cns image connections
```

Related Commands

Command	Description
show cns image connections	Displays connection information for the CNS image agent.

clear cns image status

To clear the Cisco Networking Services (CNS) image agent status statistics, use the **clear cns image status** command in privileged EXEC mode.

clear cns image status

Syntax Description

This command has no arguments or keywords.

Command Default

No statistics are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **clear cns image status** command clears all the statistics displayed by the **show cns image status** command.

Examples

The following example shows how to clear all the status statistics for the CNS image agent:

```
Router# clear cns image status
```

Related Commands

Command	Description
show cns image status	Displays status information for the CNS image agent.

clear ip drp

To clear all statistics being collected on Director Response Protocol (DRP) requests and replies, use the **clear ip drp** command in privileged EXEC mode.

clear ip drp

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example clears all DRP statistics:

```
Router# clear ip drp
```

Related Commands

Command	Description
ip drp access-group	Controls the sources of DRP queries to the DRP Server Agent.
ip drp authentication key-chain	Configures authentication on the DRP Server Agent for DistributedDirector.

clear logging onboard (Cat 6K)

To clear the onboard failure logs (OBFL) on Cisco Catalyst 6000 series switches, use the **clear logging onboard** command in privileged EXEC mode.

clear logging onboard [**module** *module-number*]

Syntax Description

module *module-number*	(Optional) Specifies a particular module.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

Use this command to clear all OBFL logs or only the logs in the module specified by the **module** *module-number* option.

Note Use this command with care: Important data could be lost when the logs are cleared. Make sure the logs have been transferred to a file before using this command.

Examples

The following example shows how to clear the logs from module 2:

```
Router# clear logging onboard module 2
```

Related Commands

Command	Description
attach	Connects to a specific line card for the purpose of executing commands on that card.
copy logging onboard module (Cat 6K)	Copies OBFL data from the target OBFL-enabled module to a local or remote file system.
[**no**] **hw-module logging onboard (Cat 6K)**	Disables and enables OBFL.
show logging onboard (Cat 6K)	Displays onboard failure logs.

clear netconf

To clear network configuration protocol (NETCONF) statistics counters or NETCONF sessions and to free associated resources and locks, use the **clear netconf** command in privileged EXEC mode.

clear netconf {**counters** | **sessions**}

Syntax Description

counters	Clears the NETCONF statistics counters to zero.
sessions	Clears currently connected NETCONF sessions.

Command Default

NETCONF statistics counters are incremented and configured NETCONF sessions remain active.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to clear NETCONF statistics counters to zero, to clear all or specified NETCONF sessions and to disconnect and free associated resources and locks.

Examples

The following example shows how to clear all NETCONF counters:

```
clear netconf counters
```

Related Commands

Command	Description
debug netconf	Enables debugging of NETCONF sessions.
netconf lock-time	Specifies the maximum time a NETCONF configuration lock is in place without an intermediate operation.
netconf max-sessions	Specifies the maximum number of concurrent NETCONF sessions allowed.
netconf ssh	Enables NETCONF over SSHv2.
show netconf	Displays NETCONF statistics counters and session information.

clear xsm

To clear XML Subscription Manager (XSM) client sessions, use the **clear xsm** command in privileged EXEC mode.

clear xsm [**session** *number*]

Syntax Description

session	(Optional) Specifies an XSM client session to clear.
number	(Optional) ID number of the specific XSM client session to be cleared.

Command Default

No XSM client sessions are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command disconnects all active client sessions (such as with a VPN Device Manager [VDM]) on the XSM server, unless you state a specific session number. This command allows troubleshooting of the XSM server and its active clients by allowing individual clients to be disconnected. Use the **show xsm status** command to obtain specific session numbers.

When the optional **session** *number* keyword and argument are not used, the **clear xsm** command clears all XSM client sessions.

Examples

The following example shows how to clear all XSM client sessions:

```
Router# clear xsm
```

The following example shows how to clear XSM client session 10:

```
Router# clear xsm session 10
```

Related Commands

Command	Description
show xsm status	Displays information and status about clients subscribed to the XSM server.
xsm	Enables XSM client access to the router.

cli

To specify EXEC command-line interface (CLI) commands within a Command Scheduler policy list, use the **cli** command in kron-policy configuration mode. To delete a CLI command from the current policy list, use the **no** form of this command.

cli *command*

no cli *command*

Syntax Description

command	EXEC-mode CLI command that must not generate a prompt or allow interruption by a keystroke.

Command Default

No CLI commands are specified.

Command Modes

Kron-policy configuration (config-kron-policy)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **cli** command in conjunction with the **kron policy-list** command to create a policy list containing EXEC CLI commands to be scheduled to run on the router at a specified time. Use the **kron occurrence** and **policy-list** commands to schedule one or more policy lists to run at the same time or interval.

The Command Scheduler process is useful to automate the running of EXEC commands at recurring intervals, and it can be used in remote routers to minimize manual intervention.

Examples

The following example shows how to configure the EXEC command **cns image retrieve** within the policy list named three-day-list:

```
Router(config)# kron policy-list three-day-list
Router(config-kron-policy)# cli cns image retrieve server https://10.19.2.3/cns/image/
status https://10.19.2.3/cnsstatus/imageinfo/
```

Related Commands

Command	Description
kron occurrence	Specifies schedule parameters for a Command Scheduler occurrence and enters kron-occurrence configuration mode.
kron policy-list	Specifies a name for a Command Scheduler policy and enters kron-policy configuration mode.
policy-list	Specifies the policy list associated with a Command Scheduler occurrence.

cli (cns)

To specify the command lines of a Cisco Networking Services (CNS) connect template, use the **cli** command in CNS template connect configuration mode. To disable this configuration, use the **no** form of this command.

cli *config-text*

no cli *config-text*

Syntax Description

config-text	Command line to be included in a CNS connect template.

Command Default

No command lines are specified in the CNS connect template.

Command Modes

CNS template connect configuration

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9). The CNS connect variable **${dlci}** is not supported in this release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

First use the **cns template connect** command to enter CNS template connect configuration mode and define the name of the CNS connect template to be configured. Then use the **cli** command to specify the command lines of the CNS connect template.

Note Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), and 12.2(33)SRA the **config-cli** and **line-cli** commands are replaced by the **cli (cns)** command.

The command lines specified using the **cli** command can include CNS connect variables (see Table 5). These variables act as placeholders within the command lines of a CNS connect template. Each variable is defined by an associated **discover** command. Before a CNS connect template that contains these variables is applied to a router's configuration, the variables are replaced by the values defined by their associated **discover** command. For example, if the **discover interface serial** command was configured, and you were able to connect to the CNS configuration engine using Serial0/0, then the **cli ip route 0.0.0.0 0.0.0.0 ${interface}** command would generate the **cli ip route 0.0.0.0 0.0.0.0 serial0/0** command.

Note When creating a CNS connect template, you must enter the **exit** command to complete the configuration of the template and exit from CNS template connect configuration mode. This requirement was implemented to prevent accidentally entering a command without the **cli** command.

Table 5 Summary of the CNS Connect Variables

Variable	Description
${line}	The line type defined by the associated **discover line** *line-type* command.
${controller}	The controller type defined by the associated **discover controller** *controller-type* command.
${interface}	The interface type defined by the associated **discover interface** command.
${dlci}	The active DLCI defined by the associated **discover dlci** command.
${next-hop}	The next hop interface. This variable is identical to the **${interface}** variable unless the **discover dlci** command has been configured. In this case, the **${next-hop}** variable is identical to the **${interface}.{subinterface}** variable, where the **{subinterface}** variable is specified by the **discover dlci** command. The **${next-hop}** variable should only be used in the CNS connect templates after the last **discover** command has been entered. A typical use of this variable is to allow the default IP route to be configured to send traffic towards the CNS configuration engine. Note that the CNS configuration engine may not be on the same LAN as the router. Therefore, configuring a route to the CNS configuration engine may require deployment-specific knowledge. Common practice is to define a default route to the interface using the **ip route** command (for example, **cli ip route 0.0.0.0 0.0.0.0 ${next-hop}**).
$$	A literal substitution of the $ symbol.

Note Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), the **&** variable is replaced by the **${interface}** variable.

Examples

The following example shows how to configure a CNS connect template named template1:

```
Router(config)# cns template connect template-1
Router(config-templ-conn)# cli command-1
Router(config-templ-conn)# cli command-2
Router(config-templ-conn)# cli no command-3
Router(config-templ-conn)# exit
Router(config)#
```

When the template1 template is applied, the following commands are sent to the router's parser:

```
command-1
command-2
no command-3
```

When the template1 template is removed from the router's configuration after an unsuccessful ping attempt to the CNS configuration engine, the following commands are sent to the router's parser:

```
no command-1
no command-2
command-3
```

Related Commands

Command	Description
cns connect	Enters CNS connect configuration mode and defines the parameters of a CNS connect profile for connecting to the CNS configuration engine.
cns template connect	Enters CNS template connect configuration mode and defines the name of a CNS connect template.
discover (cns)	Defines the interface parameters within a CNS connect profile for connecting to the CNS configuration engine.
template (cns)	Specifies a list of CNS connect templates within a CNS connect profile to be applied to a router's configuration.

clock calendar-valid

To configure a system as an authoritative time source for a network based on its hardware clock (calendar), use the **clock calendar-valid** command in global configuration mode. To specify that the hardware clock is not an authoritative time source, use the **no** form of this command.

clock calendar-valid

no clock calendar-valid

Syntax Description

This command has no arguments or keywords.

Defaults

The router is not configured as a time source.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Some platforms have a hardware clock that is separate from the software clock. The hardware clock runs continuously, even if the router is powered off or rebooted. If no outside time source is available on your network, use this command to make the hardware clock an authoritative time source.

Because the hardware clock is not as accurate as other time sources, you should configure this command only when a more accurate time source (such as NTP) is not available.

Examples

The following example configures a router as the time source for a network based on its hardware clock:

```
Router(config)# clock calendar-valid
```

Related Commands

Command	Description
ntp master	Configures the Cisco IOS software as an NTP master clock to which peers synchronize themselves when an external NTP source is not available.
vines time use-system	Sets VINES network time based on the system time.

clock read-calendar

To manually read the hardware clock (calendar) settings into the software clock, use the **clock read-calendar** command in EXEC mode.

clock read-calendar

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Some platforms have a hardware clock that is separate from the software clock. The hardware clock runs continuously, even if the router is powered off or rebooted. When the router is rebooted, the hardware clock is automatically read into the software clock. However, you may use this command to manually read the hardware clock setting into the software clock. This command is useful if the **calendar set** command has been used to change the setting of the hardware clock.

Examples

The following example configures the software clock to set its date and time by the hardware clock setting:

```
Router> clock read-calendar
```

Related Commands

Command	Description
calendar set	Sets the hardware clock.
clock set	Manually sets the software clock.
clock update-calendar	Performs a one-time update of the hardware clock from the software clock.
ntp update-calendar	Periodically updates the hardware clock from the software clock.

clock save interval

To preserve recent date and time information in NVRAM for when a Cisco IOS device without a battery-backed calendar is power-cycled or reloaded, use the **clock save interval** command in global configuration mode. To return to the default disabled state, use the **no** form of this command.

clock save interval *hours*

no clock save interval *hours*

Syntax Description

hours	Interval at which the time will be stored in NVRAM. Accepted intervals range from 8 to 24 hours.

Defaults

This function is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The benefit of using this command is that upon returning from a system reload or power cycle, the system clock will be set to a time and date near the current time and date instead of being reset to the system default time and date. In the absence of better information, Cisco IOS devices will initially set their system clocks to *epoch start*, which will typically be midnight (UTC) March 1, 1993 or 2002.

When this command is entered, the date and time are saved to NVRAM at the interval specified by this command, and also during any shutdown process. When the system starts up, the system clock is set to the last time and date saved to NVRAM.

All Cisco IOS devices support Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) to learn the time from the network, and some Cisco IOS devices have built-in battery-backed clocks to maintain that time. The **clock save interval** command is for those Cisco IOS devices that do not have battery-backed clocks and need to know the time and date before they can start communicating with a network. Because the March 1 system default date will likely occur before the valid date of any recently issued certificate, communications attempted with almost any certificate will fail because it is not yet valid according to the local clock.

Saving the time at a 24-hour interval should work well for most networks, unless there is a certificate that maintains a shorter life span.

Being aware of the time and date is critical for networking devices, and it becomes an issue when communication to a network requires use of a time-based credential, such as a certificate that has start and end dates and times. NTP and SNTP are the proper ways to set the time of a network device. The **clock save interval** command is intended to complement use of NTP and SNTP, so this command is useful only when a certificate is required to initiate communication to an NTP server, and the Cisco IOS device does not have a battery-back hardware clock, but does have NVRAM.

The system time will only be saved to NVRAM when set by an authoritative source such as NTP or SNTP; the system will not save the time entered through the **set clock** command. Additionally, a clock is considered valid only when the following criteria apply:

- The clock was set by the user using the **set clock** command and declared authoritative by the **clock calendar-valid** command.
- The clock time was learned through NTP or SNTP.

Through a confluence of events, there is no means to authoritatively declare a user-entered time as valid unless the calendar (battery-backed date and time) is declared valid. Since there is no actual calendar in a system with this command, the **clock calendar-valid** command is unavailable, and therefore a user-entered time can never be considered authoritative on platforms without a battery-backed calendar. This state is intentional because a battery-backed clock continues to run, and an NVRAM clock will stay the same. And again, for these reasons the **clock save interval** command must complement the use of NTP and SNTP.

Examples

The following example shows how to configure a Cisco IOS device to save the time at 24-hour intervals:

```
Router(config)# clock save interval 24
```

clock set

To manually set the system software clock, use one of the following formats of the **clock set** command in privileged EXEC mode.

clock set *hh***:***mm***:***ss day month year*

clock set *hh***:***mm***:***ss month day year*

Syntax Description

*hh***:***mm***:***ss*	Current time in hours (24-hour format), minutes, and seconds.
day	Current day (by date) in the month.
month	Current month (by name).
year	Current year (no abbreviation).

Command Modes

Privileged EXEC mode

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Generally, if the system is synchronized by a valid outside timing mechanism, such as a Network Time Protocol (NTP) or VINES clock source, or if you have a router with a hardware clock, you need not set the software clock. Use this command if no other time sources are available. The time specified in this command is assumed to be in the time zone specified by the configuration of the **clock timezone** command.

Examples

The following example manually sets the software clock to 7:29 p.m. on May 13, 2003:

```
Router# clock set 19:29:00 13 May 2003
```

Related Commands

Command	Description
calendar set	Sets the hardware clock.
clock read-calendar	Performs a one-time update of the software clock from the hardware clock (calendar).
clock summer-time	Configures the system to automatically switch to summer time (daylight saving time).
clock timezone	Sets the time zone for display purposes.

clock summer-time

To configure the system to automatically switch to summer time (daylight saving time), use one of the formats of the **clock summer-time** command in global configuration mode. To configure the Cisco IOS software not to automatically switch to summer time, use the **no** form of this command.

clock summer-time *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]]

clock summer-time *zone* **date** *date month year hh*:*mm date month year hh*:*mm* [*offset*]

clock summer-time *zone* **date** *month date year hh*:*mm month date year hh*:*mm* [*offset*]

no clock summer-time

Syntax Description

zone	Name of the time zone (for example, "PDT" for Pacific Daylight Time) to be displayed when summer time is in effect. The length of the *zone* argument *is limited to 7 characters.*
recurring	Indicates that summer time should start and end on the corresponding specified days every year.
date	Indicates that summer time should start on the first specific date listed in the command and end on the second specific date in the command.
week	(Optional) Week of the month (1 to 5 or **last**).
day	(Optional) Day of the week (Sunday, Monday, and so on).
date	Date of the month (1 to 31).
month	(Optional) Month (January, February, and so on).
year	Year (1993 to 2035).
hh:*mm*	(Optional) Time (military format) in hours and minutes.
offset	(Optional) Number of minutes to add during summer time (default is 60).

Defaults

Summer time is disabled. If the **clock summer-time** *zone* **recurring** command is specified without parameters, the summer time rules default to United States rules. Default of the *offset* argument is 60.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command if you want to automatically switch to summer time (for display purposes only). Use the **recurring** form of the command if the local summer time rules are of this form. Use the **date** keyword to specify a start and end date for summer time if you cannot use the **recurring** keyword.

In both the **date** and **recurring** forms of the command, the first part of the command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is chronologically after the ending month, the system assumes that you are in the southern hemisphere.

Examples

The following example specifies that summer time starts on the first Sunday in April at 2 a.m. and ends on the last Sunday in October at 2 a.m.:

```
Router(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October
2:00
```

If you live in a place where summer time does not follow the pattern in the first example, you can specify the exact date and times. In the following example, daylight saving time (summer time) is configured to start on October 12, 1997 at 2 a.m., and end on April 26, 1998 at 2 a.m.:

```
Router(config)# clock summer-time date 12 October 1997 2:00 26 April 1998 2:00
```

Related Commands

Command	Description
calendar set	Sets the hardware clock.
clock timezone	Sets the time zone for display purposes.

clock timezone

To set the time zone for display purposes, use the **clock timezone** command in global configuration mode. To set the time to Coordinated Universal Time (UTC), use the **no** form of this command.

clock timezone *zone hours-offset* [*minutes-offset*]

no clock timezone

Syntax Description

zone	Name of the time zone to be displayed when standard time is in effect. The length of the *zone* argument *is limited to 7 characters.*
hours-offset	Hours difference from UTC.
minutes-offset	(Optional) Minutes difference from UTC.

Defaults

UTC

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The system internally keeps time in UTC, so this command is used only for display purposes and when the time is manually set.

Table 6 lists common time zone acronyms used for the *zone* argument.

Table 6 Common Time Zone Acronyms

Acronym	Time Zone Name and UTC Offset
Europe	
GMT	Greenwich Mean Time, as UTC
BST	British Summer Time, as UTC + 1 hour
IST	Irish Summer Time, as UTC + 1 hour
WET	Western Europe Time, as UTC
WEST	Western Europe Summer Time, as UTC + 1 hour
CET	Central Europe Time, as UTC + 1
CEST	Central Europe Summer Time, as UTC + 2

Table 6 Common Time Zone Acronyms (continued)

Acronym	Time Zone Name and UTC Offset
EET	Eastern Europe Time, as UTC + 2
EEST	Eastern Europe Summer Time, as UTC + 3
MSK	Moscow Time, as UTC + 3
MSD	Moscow Summer Time, as UTC + 4
United States and Canada	
AST	Atlantic Standard Time, as UTC –4 hours
ADT	Atlantic Daylight Time, as UTC –3 hours
ET	Eastern Time, either as EST or EDT, depending on place and time of year
EST	Eastern Standard Time, as UTC –5 hours
EDT	Eastern Daylight Saving Time, as UTC –4 hours
CT	Central Time, either as CST or CDT, depending on place and time of year
CST	Central Standard Time, as UTC –6 hours
CDT	Central Daylight Saving Time, as UTC –5 hours
MT	Mountain Time, either as MST or MDT, depending on place and time of year
MST	Mountain Standard Time, as UTC –7 hours
MDT	Mountain Daylight Saving Time, as UTC –6 hours
PT	Pacific Time, either as PST or PDT, depending on place and time of year
PST	Pacific Standard Time, as UTC –8 hours
PDT	Pacific Daylight Saving Time, as UTC –7 hours
AKST	Alaska Standard Time, as UTC –9 hours
AKDT	Alaska Standard Daylight Saving Time, as UTC –8 hours
HST	Hawaiian Standard Time, as UTC –10 hours
Australia	
WST	Western Standard Time, as UTC + 8 hours
CST	Central Standard Time, as UTC + 9.5 hours
EST	Eastern Standard/Summer Time, as UTC + 10 hours (+11 hours during summer time)

Table 7 lists an alternative method for referring to time zones, in which single letters are used to refer to the time zone difference from UTC. Using this method, the letter Z is used to indicate the zero meridian, equivalent to UTC, and the letter J (Juliet) is used to refer to the local time zone. Using this method, the International Date Line is between time zones M and Y.

Table 7 Single-Letter Time Zone Designators

Letter Designator	Word Designator	Difference from UTC
Y	Yankee	UTC –12 hours
X	Xray	UTC –11 hours
W	Whiskey	UTC –10 hours
V	Victor	UTC –9 hours
U	Uniform	UTC –8 hours
T	Tango	UTC –7 hours
S	Sierra	UTC –6 hours
R	Romeo	UTC –5 hours
Q	Quebec	UTC –4 hours
P	Papa	UTC –3 hours
O	Oscar	UTC –2 hours
N	November	UTC –1 hour
Z	Zulu	Same as UTC
A	Alpha	UTC +1 hour
B	Bravo	UTC +2 hours
C	Charlie	UTC +3 hours
D	Delta	UTC +4 hours
E	Echo	UTC +5 hours
F	Foxtrot	UTC +6 hours
G	Golf	UTC +7 hours
H	Hotel	UTC +8 hours
I	India	UTC +9 hours
K	Kilo	UTC +10 hours
L	Lima	UTC +11 hours
M	Mike	UTC +12 hours

The following example sets the time zone to Pacific Standard Time (PST), which is 8 hours behind UTC:

```
Router(config)# clock timezone PST -8
```

The following example sets the time zone to Atlantic Time (AT) for Newfoundland, Canada, which is 3.5 hours behind UTC:

```
Router(config)# clock timezone AT -3 30
```

Related Commands

Command	Description
calendar set	Sets the hardware clock.
clock set	Manually set the software clock.

Command	Description
clock summer-time	Configures the system to automatically switch to summer time (daylight saving time).
show clock	Displays the software clock.

clock update-calendar

To perform a one-time update of the hardware clock (calendar) from the software clock, use the **clock update-calendar** command in user EXEC or privileged EXEC mode.

clock update-calendar

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Some platforms have a hardware clock (calendar) in addition to a software clock. The hardware clock is battery operated, and runs continuously, even if the router is powered off or rebooted.

If the software clock and hardware clock are not synchronized, and the software clock is more accurate, use this command to update the hardware clock to the correct date and time.

Examples

The following example copies the current date and time from the software clock to the hardware clock:

```
Router> clock update-calendar
```

Related Commands

Command	Description
clock read-calendar	Performs a one-time update of the software clock from the hardware clock (calendar).
ntp update-calendar	Periodically updates the hardware clock from the software clock.

cns aaa authentication

To enable Cisco Networking Services (CNS) Authentication, Authorization, and Accounting (AAA) options, use the **cns aaa authentication** command in global configuration mode. To explicitly disable CNS AAA options, use the **no** form of this command.

cns aaa authentication *authentication-method*

no cns aaa authentication *authentication-method*

Syntax Description

authentication-method	Specifies the AAA authentication method to be used.

Command Default

AAA is enabled when using CNS by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

Use the **cns aaa authentication** command to enable AAA when using CNS. When the **cns aaa authentication** command is configured, CNS notification messages sent to the device are rejected if they do not have sender credentials. By default, no authentication is enabled. This command must be enabled to configure AAA authentication for CNS messages. Use the **no cns aaa authentication** command to explicitly disable AAA support when using CNS.

For more information about AAA authentication methods, see the "AAA Authentication Methods Configuration Task List" section in the "Configuring Authentication" chapter of the *Cisco IOS Security Configuration Guide,* Release 12.4.

Examples

The following example shows how to enable AAA authentication when using CNS:

```
cns aaa authentication method1
```

Related Commands

Command	Description
cns message format notification	Configures the message format for notification messages from a CNS device.

cns config cancel

To remove a partial Cisco Networking Services (CNS) configuration from the list of outstanding partial configurations, use the **cns config cancel** command in privileged EXEC mode.

cns config cancel *queue-id*

Syntax Description

queue-id	Indicates which partial configuration in the list of outstanding partial configurations to remove from the list. This list can be displayed by issuing the **show cns config outstanding** command in user EXEC or privileged EXEC mode.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18) ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22) S.
12.2(8)T	This command was implemented on additional platforms.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Incremental (partial) configurations take place in two steps:

1. The configuration agent receives the partial configuration. It checks the configuration commands for syntax, publishes the success or failure of the read and syntax-check operation to the sync-status subject “cisco.cns.config.sync-status,” and stores the configuration.
2. The configuration agent receives a second event message directing it to either apply or cancel the stored configuration.

Use the **cns config cancel** command in error scenarios where the second event message is not received and you need to remove the configuration from the list of outstanding configurations. Currently the maximum number of outstanding configurations is one.

Examples

The following example shows the process of checking the existing outstanding CNS configurations and canceling the configuration with the *queue-id* of 1:

```
Router# show cns config outstanding

The outstanding configuration information:
```

```
queue id   identifier       config-id
1          identifierREAD   config_idREAD

Router# cns config cancel 1

Router# show cns config outstanding

The outstanding configuration information:
queue id   identifier       config-id
```

Related Commands

Command	Description
cns config partial	Starts the CNS configuration agent, which provides CNS configuration services to Cisco IOS clients.
cns event	Configures the CNS event gateway, which provides CNS event services to Cisco IOS clients.
show cns config outstanding	Displays information about incremental CNS configurations that have started but not yet completed.
show cns event connections	Displays the status of the CNS event agent connection.

cns config connect-intf

Note Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), the **cns config connect-intf** command is replaced by the **cns connect** and **cns template connect** commands. See the **cns connect** and **cns template connect** commands for more information.

To specify the interface for connecting to the Cisco Networking Services (CNS) configuration engine, use the **cns config connect-intf** command in global configuration mode. To disable this interface for the connection, use the **no** form of this command.

cns config connect-intf *type number* [**ping-interval** *seconds*] [**retries** *number*]

no cns config connect-intf *type number*

Syntax Description

type	Type of connecting interface.
number	Number of the connecting interface.
ping-interval	(Optional) Specifies an interval between successive ping attempts.
seconds	(Optional) Interval between successive ping attempts, in seconds. Values are from 1 to 30. The default is 10.
retries	(Optional) Indicates that a ping will be retried a specified number of times.
number	(Optional) Number of times that a ping will be retried, in seconds. Values are from 1 to 30. The default is 5.

Command Default

Interfaces are not configured to connect to the CNS configuration engine.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(8)T	This command was replaced by the **cns connect** and **cns template connect** commands.
12.3(9)	This command was replaced by the **cns connect** and **cns template connect** commands.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

Use this command to connect to the CNS configuration engine using a specific type of interface. You must specify the interface type but need not specify the interface number; the router's bootstrap configuration on the router finds the connecting interface, regardless of the slot in which the card resides or the modem dialout line for the connection, by trying different candidate interfaces or lines until it successfully pings the registrar.

Use this command to enter CSN Connect-interface configuration mode (config-cns-conn-if). Then use one of the following bootstrap-configuration commands to connect to the registrar for initial configuration:

- **config-cli** followed by commands that, used as is, configure the interface.
- **line-cli** followed by a command to configure modem lines to enable dialout and, after that, commands to configure the modem dialout line.

The **config-cli** command accepts the special directive character "**&**," which acts as a placeholder for the interface name. When the configuration is applied, the **&** is replaced with the interface name. Thus, for example, if we are able to connect using FastEthernet0/0, the **config-cli ip route 0.0.0.0 0.0.0.0 &** command generates the **ip route 0.0.0.0 0.0.0.0 FastEthernet0/0** command. Similarly, the **config-virtual terminal line (vty) cns id & ipaddress** command generates the **cns id FastEthernet0/0 ipaddress** command.

Examples

In the following example, the user connects to a configuration engine using the asynch interface and issues several commands:

```
Router(config)# cns config connect-intf Async
Router(config-cns-conn-if)# config-cli encapsulation ppp
Router(config-cns-conn-if)# config-cli ip unnumbered FastEthernet0/0
Router(config-cns-conn-if)# config-cli dialer rotary-group 0
Router(config-cns-conn-if)# line-cli modem InOut
Router(config-cns-conn-if)# line-cli ...<other line commands>....
Router(config-cns-conn-if)# exit
```

These commands result in the following configuration being applied:

```
line 65
modem InOut
.
.
.
interface Async65
encapsulation ppp
dialer in-band
dialer rotary-group 0
```

Related Commands

Command	Description
cns config cancel	Cancels an incremental two-phase synchronization configuration.
cns config initial	Starts the CNS configuration agent and initiates an initial configuration.
cns config notify	Detects CNS configuration changes and sends an event containing the previous and current configuration.
cns config partial	Starts the CNS configuration agent, which provides CNS configuration services to Cisco IOS clients.

cns config initial

To enable the Cisco Networking Services (CNS) configuration agent and initiate a download of the initial configuration, use the **cns config initial** command in global configuration mode. To remove an existing **cns config initial** command from the running configuration of the routing device, use the **no** form of this command.

cns config initial {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**page** *page*] [**syntax-check**] [**no-persist**] [**source** *interface name*] [**status** *url*] [**event**] [**inventory**]

no cns config initial

Syntax Description

host-name	Hostname of the configuration server.
ip-address	IP address of the configuration server.
encrypt	(Optional) Uses a Secure Sockets Layer (SSL) encrypted link to the event gateway.
port-number	(Optional) Port number of the configuration service. The value is from 0 to 65535. The default is 80 with no encryption and 443 with encryption.
page	(Optional) Indicates that the configuration is located on a web page.
page	(Optional) Web page where the configuration is located. The default is /cns/config.asp.
syntax-check	(Optional) Turns on syntax checking.
no-persist	(Optional) Suppresses the default automatic writing to NVRAM of the configuration pulled as a result of issuing the **cns config initial** command. If not present, issuing the **cns config initial** command causes the resultant configuration to be automatically written to NVRAM.
source	(Optional) Specifies the source of CNS communications.
interface name	(Optional) Interface name of the source of CNS communications.
status *url*	(Optional) Sends an event to the specified URL via HTTP, either notifying successful completion of the configuration or warning that the configuration contained errors.
event	(Optional) Sends an event to the Event Bus notifying successful completion of the configuration or warning that the configuration contained errors. If the CNS event agent is not configured, the event will be saved until the CNS event agent is enabled. If the **event** keyword is not specified, a log message is sent to the console of the device after the configuration is complete.
inventory	(Optional) Sends an inventory of the line cards and modules in the router to the CNS configuration engine as part of the HTTP request.

Defaults

The port number defaults to 80 with no encryption and 443 with encryption.
Default web page of the initial configuration is /cns/config.asp.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(2)XB	This command was implemented on Cisco IAD2420 series Integrated Access Devices (IADs).
12.2(8)T	The **source** and **encrypt** keywords were added.
12.3(1)	The **inventory** keyword was added.
12.3(8)T	The **status** *url* keyword/argument pair was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command when a basic configuration—called a bootstrap configuration—is added to multiple routers before being deployed. When a router is initially powered (or each time a router is reloaded when the **no-persist** keyword is used) the **cns config initial** command will cause a configuration file—called an initial configuration—for the router to be downloaded from the configuration server. The initial configuration can be unique for each router.

When the configuration has been received by the router, each line of the configuration will be applied in the same order as it was received. If the Cisco IOS parser has an error with one of the lines of the configuration, then all the configuration up to this point will be applied to the router, but none of the configuration beyond the error will be applied. If an error occurs, the command will retry until it successfully completes. Once the configuration has successfully completed the **cns config initial** command will be removed from the running configuration. By default, NVRAM will be updated except when the **no-persist** keyword is configured.

When this command is used with the **event** keyword, a single message will be published on the event bus after the configuration is complete. The event bus will display one of the following status messages:

- cisco.mgmt.cns.config.complete—CNS configuration agent successfully applied the initial configuration.
- cisco.mgmt.cns.config.warning—CNS configuration agent fully applied the initial configuration but encountered possible semantic errors.

When this command is used with the **status** keyword, a single message will be published to the URL specified after the configuration is complete.

Examples

The following example shows how to enable the CNS configuration agent and initiate an initial configuration:

```
Router(config)# cns config initial 10.19.4.5 page /cns/config/first.asp
```

Related Commands

Command	Description
cns config connect-intf	Specifies the interface for connecting to the CNS configuration engine.
cns config notify	Detects CNS configuration changes and sends an event containing the previous and current configuration.

Command	Description
cns config retrieve	Enables the CNS configuration agent and initiates a download of the initial configuration.
cns event	Configures the CNS event gateway, which provides CNS event services to Cisco IOS clients.
show cns config status	Displays information about the status of the CNS configuration agent.

cns config notify

To notify Cisco Networking Services (CNS) agents of configuration changes on Cisco IOS devices, use the **cns config notify** command in global configuration mode. To disable notifications, use the **no** form of this command.

cns config notify {**all** | **diff**} [**interval** *minutes*] [**no_cns_events**] [**old-format**]

no cns config notify {**all** | **diff**} [**interval** *minutes*] [**no_cns_events**] [**old-format**]

Cisco IOS Release 12.4(9)T or Later Releases

cns config notify diff [**interval** *minutes*] [**no_cns_events**] [**qlen** *number*]

no cns config notify diff [**interval** *minutes*] [**no_cns_events**] [**qlen** *number*]

Syntax Description

all	Captures all configuration commands for the config-changed event output.
diff	Captures commands that change configuration for the config-changed event output.
interval *minutes*	(Optional) Specifies the amount of time after the last configuration change that the config-changed event is sent. The default is 5 minutes. The timer starts when you make a configuration change and you remain in configuration mode after the configuration change. If you enter the **end** command, the config-changed event is sent immediately.
no_cns_events	(Optional) Disables event notification for configurations changed through an XML file. If the configuration is changed using the command-line interface (CLI), the config-changed event will be sent.
old-format	(Optional) Provides the event notification in the old XML format for backwards compatibility. **Note** This keyword is no longer available in Cisco IOS Release 12.4(9)T or later releases.
qlen *number*	(Optional) Specifies the number of configuration changes that must occur before the CNS agent is notified of the changes. The range is 1 to 1000. The default is 100.

Command Default

CNS agents do not receive notifications.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(11)T	The **diff** keyword was removed.
12.3(1)	The **diff** and **old-format** keywords were added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(9)T	The **old-format** and **all** keywords were removed. The **qlen** *number* keyword/attribute pair were added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

When the **cns config notify** command is enabled, commands entered in configuration mode are detected. If the **all** keyword is specified, the command is stored for future notification. If the **diff** keyword is specified, the command is stored for future notification if the software determines that the command will cause a configuration change. The **diff** keyword also allows the software to store information about the command including previous configuration states, source of the change (for example, a telnet user), and the time of configuration.

The stored information is formatted in XML and sent as part of a CNS config agent change notification event. A CNS configuration agent change notification event is sent to the CNS event bus when configuration mode is exited or no activity from that source has occurred for the configured interval time.

You must enable the CNS event agent using the **cns event** command before configuring this command. If the CNS event agent is not configured, the notification event will be queued and sent when the CNS event agent is enabled. If the CNS configuration notify queue is full, subsequent events are dropped and a “lost” CNS configuration change notification is sent when the CNS event agent is enabled.

Use the **no_cns_events** for applications that already record configuration changes sent to the routing device through the CNS event bus.

Use the **old-format** keyword to generate XML output—only the entered command and previous configuration state—that is compatible with the versions of this commands when the **diff** keyword was removed.

Use the **qlen** *number* keyword/argument pair to send configuration changes to the CNS agent only after the specified number of changes has occurred.

Examples

The following example shows how to configure the CNS agent to receive configuration change notifications for all configuration commands:

```
Router(config)# cns config notify all
```

The following example shows how to configure the CNS agent to receive configuration change notifications only after 50 changes have been made:

```
Router(config)# cns config notify diff qlen 50
```

Related Commands

Command	Description
cns config cancel	Cancels an incremental two-phase synchronization configuration.
cns config connect-intf	Specifies the interface for connecting to the CNS configuration engine.
cns config initial	Starts the CNS configuration agent and initiates an initial configuration.
cns config partial	Starts the CNS configuration agent, which provides CNS configuration services to Cisco IOS clients.
cns event	Enables and configures CNS event agent services.

cns config partial

To start the Cisco Networking Services (CNS) configuration agent and accept a partial configuration, use the **cns config partial** command in global configuration mode. To shut down the CNS partial configuration agent, use the **no** form of this command.

cns config partial {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**source** *interface name*] [**inventory**]

no cns config partial

Syntax Description

host-name	Hostname of the configuration server.
ip-address	IP address of the configuration server.
encrypt	(Optional) Uses a Secure Sockets Layer (SSL) encrypted link between the router and the web server.
port-number	(Optional) Port number of the configuration service. The value is from 0 to 65535. The default is 80 with no encryption and 443 with encryption.
source	(Optional) Specifies the source of this device.
interface name	(Optional) Interface name to use as the source of this device.
inventory	(Optional) Sends an inventory of the line cards and modules in the router to the CNS configuration engine as part of the HTTP request.

Command Default

The CNS configuration agent is not enabled to accept a partial configuration and the router does not request or receive updates.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(2)XB	This command was implemented on Cisco IAD2420 series Integrated Access Devices (IADs).
12.2(8)T	The **source** keyword and **encrypt** arguments were added.
12.3(1)	The **inventory** keyword was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.4(4)T	This command was modified to include enhanced CNS error messages.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to start the CNS partial configuration agent. You must enable the CNS event agent using the **cns event** command before configuring this command. The CNS event agent sends an event with the subject "cisco.mgmt.cns.config.load" to specify whether configuration data can be pushed to the CNS partial configuration agent or pulled from a configuration server by the CNS partial configuration agent.

In the push model, the event message delivers the configuration data to the partial configuration agent.

In the pull model, the event message triggers the partial configuration agent to pull the configuration data from the CNS configuration engine. The event message contains information about the CNS configuration engine, not the actual configuration data. The host name or IP address is the address of the CNS configuration engine from which the configuration is pulled. Use the **cns trusted-server** command to specify which CNS configuration engines can be used by the CNS partial configuration agent.

When the configuration has been received by the router, each line of the configuration will be applied in the same order as it was received. If the Cisco IOS parser has an error with one of the lines of the configuration, then all the configuration up to this point will be applied to the router, but none of the configuration beyond the error will be applied. If an error occurs, the command will retry until the configuration successfully completes. In the pull mode, the command will not retry after an error. By default, NVRAM will be updated except when the **no-persist** keyword is configured.

A message will be published on the CNS event bus after the partial configuration is complete. The CNS event bus will display one of the following status messages:

- cisco.mgmt.cns.config.complete—CNS configuration agent successfully applied the partial configuration.
- cisco.mgmt.cns.config.warning—CNS configuration agent fully applied the partial configuration, but encountered possible semantic errors.
- cisco.mgmt.cns.config.failure(CLI syntax)—CNS configuration agent encountered a command line interface (CLI) syntax error and was not able to apply the partial configuration.
- cisco.mgmt.cns.config.failure(CLI semantic)—CNS configuration agent encountered a CLI semantic error and was not able to apply the partial configuration.

In Cisco IOS Releases 12.4(4)T, 12.2 (33)SRA, and later releases, a second message is sent to the subject "cisco.cns.config.results" in addition to the appropriate message above. The second message contains both overall and line-by-line information about the configuration that was sent and the result of the action requested in the original message. If the action requested was to apply the configuration, then the information in the results message is semantic in nature. If the action requested was to check syntax only, then the information in the results message is syntactical in nature.

Examples

The following example shows how to configure the CNS partial configuration agent to accept events from the event gateway at 172.28.129.22. The CNS partial configuration agent will connect to the CNS configuration server at 172.28.129.22, port number 80. The CNS partial configuration agent requests are redirected to a configuration server at 172.28.129.40, port number 80.

```
Router(config)# cns event 172.28.129.22
Router(config)# cns trusted-server config 172.28.129.40
Router(config)# cns config partial 172.28.129.22
```

The following example shows an enhanced error message sent to the subject "cisco.mgmt.cns.config.results":

```
[2005-09-08 14:30:44]: subject=cisco.mgmt.cns.config.results.dvlpr-7200-6, message=
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://www.w3.org/2003/05/soap-envelope">
<SOAP:Header>
```

```
<wsse:Security xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext"
SOAP:mustUnderstand="true">
<wsse:UsernameToken>
<wsse:Username>user1</wsse:Username>
<wsse:Password>password1</wsse:Password>
</wsse:UsernameToken>
</wsse:Security>
<CNS:cnsHeader Version="2.0" xmlns:CNS="http://www.cisco.com/management/cns/envelope">
<CNS:Agent>CNS_CONFIG</CNS:Agent>
<CNS:Response>
<CNS:correlationID>SOAP_IDENTIFIER</CNS:correlationID>
</CNS:Response>
<CNS:Time>2005-09-13T08:34:36.523Z</CNS:Time>
</CNS:cnsHeader>
</SOAP:Header>
<SOAP:Body xmlns="http://www.cisco.com/management/cns/config">
<configResults version="2.0" overall="Success">
<configId>AAA</configId>
</configResults>
</SOAP:Body>
</SOAP:Envelope>
```

Related Commands

Command	Description
cns config initial	Starts the CNS configuration agent and initiates an initial configuration.
cns event	Enables and configures CNS event agent services.
cns trusted-server	Specifies a trusted server for CNS agents.
show cns config outstanding	Displays information about incremental CNS configurations that have started but are not yet completed.

cns config retrieve

To enable the Cisco Networking Services (CNS) configuration agent and initiate a download of the initial configuration, use the **cns config retrieve** command in privileged EXEC mode.

cns config retrieve {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**page** *page*] [**overwrite-startup**] [**retry** *retries* **interval** *seconds*] [**syntax-check**] [**no-persist**] [**source** *interface name*] [**status** *url*] [**event**] [**inventory**]

Syntax Description

host-name	Hostname of the configuration server.
ip-address	IP address of the configuration server.
encrypt	(Optional) Uses a Secure Sockets Layer (SSL) encrypted link to the event gateway.
port-number	(Optional) Port number of the configuration service. The value is from 0 to 65535. The default is 80 with no encryption and 443 with encryption.
page	(Optional) Indicates that the configuration is located on a web page.
page	(Optional) Web page where the configuration is located. The default is /cns/config.asp.
overwrite-startup	(Optional) Replaces the startup configuration file. Does not apply to the running configuration file.
retry *retries*	(Optional) Specifies the retry interval. The range is 0 to 100. The default is 0.
interval *seconds*	(Optional) Specifies the time in seconds, before the next attempt to request the configuration of a device from a configuration server. The range is 1 to 3600.
syntax-check	(Optional) Turns on syntax checking.
no-persist	(Optional) Suppresses the default automatic writing to NVRAM of the configuration pulled as a result of issuing the **cns config retrieve** command. If not present, issuing the **cns config retrieve** command causes the resultant configuration to be automatically written to NVRAM.
source	(Optional) Specifies the source of CNS communications.
interface name	(Optional) Interface name of the source of the configuration.
status *url*	(Optional) Sends the configuration the specified URL via HTTP, either notifying successful completion of the configuration or warning that the configuration contained errors.
event	(Optional) Sends an event to the CNS Event Bus stating successful completion of the configuration, a warning that the configuration contained errors, or a message noting that the configuration failed. If the CNS event agent is not configured, the event will be saved until the CNS event agent is enabled. If the **event** keyword is not specified, a log message is sent to the console of the device after the configuration is complete.
inventory	(Optional) Sends an inventory of the line cards and modules in the router to the CNS configuration engine as part of the HTTP request.

Defaults

The port number defaults to 80 with no encryption and 443 with encryption.
Default web page of the initial configuration is /cns/config.asp.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.3(1)	The **inventory** keyword was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	The **retry** *retries* and **interval** *seconds* keywords and arguments were added.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to request the configuration of a device from a configuration server. Use the **cns trusted-server** command to specify which configuration server can be used (trusted).

When the configuration has been received by the router, each line of the configuration will be applied in the same order as it was received. If the Cisco IOS parser has an error with one of the lines of the configuration, then all the configuration up to this point will be applied to the router, but none of the configuration beyond the error will be applied. If an error occurs, the command will not retry.

A single message will be published on the event bus after the partial configuration is complete. The event bus will display one of the following status messages:

- cisco.mgmt.cns.config.complete—CNS configuration agent successfully applied the configuration.
- cisco.mgmt.cns.config.warning—CNS configuration agent fully applied the configuration, but encountered possible semantic errors.
- cisco.mgmt.cns.config.failure—CNS configuration agent encountered an error and was not able to apply the configuration.

The **cns config retrieve** command can be used with Command Scheduler commands (for example, **kron policy-list** and **cli** commands) in environments where it is not practical to use the CNS event agent and the **cns config partial** command. Configured within the **cli** command, the **cns config retrieve** command can be used to poll the configuration server to detect configuration changes.

You can use the optional **retry** and **interval** keywords to specify an amount of time in seconds to wait before attempting to retrieve a configuration from a trusted server. The number of retries is restricted to 100 to prevent the configuration agent from indefinitely attempting to reach an unreachable server. Use the keyboard combination **Ctrl-Shift-6** to abort this command.

Examples

The following example shows how to request a configuration from a trusted server at 10.1.1.1:

```
Router(config)# cns trusted-server all 10.1.1.1
Router(config)# exit
Router# cns config retrieve 10.1.1.1
```

The following example shows how to request a configuration from a trusted server at 10.1.1.1 and to configure a CNS configuration retrieve interval:

```
Router(config)# cns trusted-server all 10.1.1.1
Router(config)# exit
Router# cns config retrieve 10.1.1.1 retry 50 interval 1500
CNS Config Retrieve Attempt 1 out of 50 is in progress
Next cns config retrieve retry is in 1499 seconds (Ctrl-Shft-6 to abort this command).
..
00:26:40: %CNS-3-TRANSPORT: CNS_HTTP_CONNECTION_FAILED:10.1.1.1 -Process= "CNS config
retv", ipl= 0, pid= 43
00:26:40: %CNS-3-TRANSPORT: CNS_HTTP_CONNECTION_FAILED -Process= "CNS config retv", ipl=
0, pid= 43......
```

Related Commands

Command	Description
cli	Specifies EXEC CLI commands within a Command Scheduler policy list.
cns config initial	Starts the CNS configuration agent and initiates an initial configuration.
cns trusted-server	Specifies a trusted server for CNS agents.
kron policy-list	Specifies a name for a Command Scheduler policy and enters kron-policy configuration mode.
show cns config status	Displays information about the status of the CNS configuration agent.

cns connect

To enter Cisco Networking Services (CNS) connect configuration mode and define the parameters of a CNS connect profile for connecting to the CNS configuration engine, use the **cns connect** command in global configuration mode. To disable the CNS connect profile, use the **no** form of this command.

cns connect *name* [**retry-interval** *interval-seconds*] [**retries** *number-retries*] [**timeout** *timeout-seconds*] [**sleep** *sleep-seconds*]

no cns connect *name* [**retry-interval** *interval-seconds*] [**retries** *number-retries*] [**timeout** *timeout-seconds*] [**sleep** *sleep-seconds*]

Syntax Description

name	Name of the CNS connect profile to be configured.
retry-interval	(Optional) Sets the interval (in seconds) between each successive attempt to ping the CNS configuration engine. The default value is 10 seconds. The valid range is 8 to 40 seconds.
interval-seconds	(Optional) Number of seconds between each successive attempt to ping the CNS configuration engine.
retries	(Optional) Sets the number of times the CNS connect function will try to ping the CNS configuration engine. The default value is 3.
number-retries	(Optional) Number of times the CNS connect function will try to ping the CNS configuration engine.
timeout	(Optional) Sets the amount of time (in seconds) after which an interface is no longer used for ping attempts. The default value is 120 seconds.
timeout-seconds	(Optional) Number of seconds after which an interface is no longer used for ping attempts.
sleep	(Optional) Sets the amount of time (in seconds) before the first ping is attempted for each interface. This option provides time for the far end of a link to stabilize. The default value is 0 seconds.
sleep-seconds	(Optional) Number of seconds before the first ping is attempted for each interface.

Command Default

No CNS connect profiles are defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The **ping-interval** keyword was replaced by the **retry-interval** keyword.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **cns connect** command to enter CNS connect configuration mode and define the parameters of a CNS connect profile for connecting to the CNS configuration engine. Then use the following CNS connect commands to create a CNS connect profile:

- **discover**
- **template**

A CNS connect profile specifies the **discover** commands and associated **template** commands that are to be applied to a router's configuration. When multiple **discover** and **template** commands are configured in a CNS connect profile, they are processed in the order in which they are entered.

Note Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), and 12.2(33)SRA the **cns config connect-intf** command is replaced by the **cns connect** and **cns template connect** commands.

Examples

The following example shows how to create a CNS connect profile named profile-1:

```
Router(config)# cns connect profile-1
Router(config-cns-conn)# discover interface Serial
Router(config-cns-conn)# template template-1
Router(config-cns-conn)# exit
Router(config)#
```

In this example, the following sequence of events occurs for each serial interface when the **cns connect profile-1** command is processed:

1. Enter interface configuration mode and apply all commands in the template-1 template to the router's configuration.
2. Try to ping the CNS configuration engine.
3. If the ping is successful, then download pertinent configuration information from the CNS configuration engine and exit. The **cns connect profile-1** command has completed its process.
4. If the ping is unsuccessful, enter interface configuration mode and remove all commands in the template-1 template from the router's configuration. The **cns connect profile-1** command has failed to retrieve any configuration information from the CNS configuration engine.

Related Commands

Command	Description
cli (cns)	Specifies the command lines of a CNS connect template.
cns template connect	Enters CNS template connect configuration mode and defines the name of a CNS connect template.
discover (cns)	Defines the interface parameters within a CNS connect profile for connecting to the CNS configuration engine.
template (cns)	Specifies a list of CNS connect templates within a CNS connect profile to be applied to a router's configuration.

cns event

To configure the Cisco Networking Services (CNS) event gateway, which provides CNS event services to Cisco IOS clients, use the **cns event** command in global configuration mode. To remove the specified event gateway from the gateway list, use the **no** form of this command.

cns event {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**backup**] [**failover-time** *seconds*] [**keepalive** *seconds retry-count*] [**source** *interface name*] [**clock-timeout** *time*] [**reconnect** *time*]

no cns event {*host-name* | *ip-address*} [*port-number*] [**encrypt**] [**backup**] [**failover-time** *seconds*] [**keepalive** *seconds retry-count*] [**source** *interface name*] [**clock-timeout** *time*] [**reconnect** *time*]

Syntax Description

host-name	Hostname of the event gateway.
ip-address	IP address of the event gateway.
encrypt	(Optional) Uses a Secure Sockets Layer (SSL) encrypted link to the event gateway. **Note** This keyword is available only in images that support SSL.
port-number	(Optional) Port number for the event gateway. The default is 11011 with no encryption or 11012 with encryption.
backup	(Optional) Indicates a backup gateway. If omitted, indicates the primary gateway. A primary gateway must be configured before you can configure a backup gateway. Optional keywords, if omitted, are set as for the primary gateway.
failover-time *seconds*	(Optional) Specifies a time interval, in seconds, to wait for the primary gateway route after the route to the backup gateway is established. The default is 3.
keepalive *seconds retry-count*	(Optional) Specifies a keepalive timeout, in seconds, and retry count.
source *interface name*	(Optional) Indicates the interface name of the source for CNS communications.
clock-timeout *time*	(Optional) Specifies the maximum time, in minutes, that the CNS event agent will wait for the clock to be set for transports (such as SSL) that require an accurate clock. The default is 10.
reconnect *time*	(Optional) Specifies the configurable upper limit of the maximum retry timeout. The valid range is 1 through 65535. The default is 3600.

Command Default

No CNS event gateway is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into the Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(2)XB	This command was implemented on Cisco IAD2420 series Integrated Access Devices (IADs).
12.2(8)T	The **encrypt**, **init-retry**, **source**, and **force-fmt1** keywords were added.
12.3	The **reconnect-time** keyword was added.
12.3(1)	The **init-retry** keyword was replaced with the **failover-time** keyword. The **force-fmt1** keyword was removed. The **clock-timeout** keyword was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The CNS event agent must be enabled before any of the other CNS agents are configured because the CNS event agent provides a transport connection to the CNS event bus for all other CNS agents. The other CNS agents use the connection to the CNS event bus to send and receive messages. The CNS event agent does not read or modify the messages.

The **failover-time** keyword is useful if you have a backup CNS event gateway configured. If the CNS event agent is trying to connect to the gateway and it discovers that the route to the backup is available before the route to the primary gateway, the *seconds* argument specifies how long the CNS event agent will continue to search for a route to the primary gateway before attempting to link to the backup gateway.

Unless you are using a bandwidth-constrained link, you should set a keepalive timeout and retry count. Doing so allows the management network to recover gracefully should a Cisco IE2100 configuration engine ever fail. Without the keepalive data, such a failure requires manual intervention on every device. The value of the *seconds* argument multiplied by the value of the *retry-count* argument determines the length of idle time before the CNS event agent will disconnect and attempt to reconnect to the gateway. We recommend a minimum *retry-count* of two.

If the optional **source** keyword is used, the source IP address might be a secondary IP address of a specific interface to allow a management network to run on top of a production network.

If network connectivity between the Cisco IOS router running the CNS event agent and the gateway is absent, the event agent goes into an exponential backoff retry mode and gets stuck at the maximum limit (which may be hours). The **reconnect-time** keyword allows a configurable upper limit of the maximum retry timeout.

Examples

The following example shows how to set the address of the primary CNS event gateway to the configuration engine software running on IP address 10.1.2.3, port 11011, with a keepalive of 60 seconds and a retry count of 5:

```
Router(config)# cns event 10.1.2.3 11011 keepalive 60 5
```

Related Commands

Command	Description
cns id	Sets the unique event ID, config ID, or image ID used by CNS services.
show cns event status	Displays status information about the CNS event agent.

cns exec

To enable and configure the Cisco Networking Services (CNS) exec agent, which provides CNS exec agent services to Cisco IOS clients, use the **cns exec** command in global configuration mode. To disable the use of CNS exec agent services, use the **no** form of this command.

cns exec [*host-name* | *ip-address*] [**encrypt** [*enc-port-number*]] [*port-number*]
[**source** *interface name*]

no cns exec [*host-name* | *ip-address*] [**encrypt** [*enc-port-number*]] [*port-number*]
[**source** *interface name*]

Syntax Description

host-name	(Optional) Hostname of the exec server.
ip-address	(Optional) IP address of the exec server.
encrypt	(Optional) Uses a Secure Sockets Layer (SSL) encrypted link to the exec agent server. **Note** This keyword is available only in images that support SSL.
enc-port-number	(Optional) Port number for the encrypted exec server. The default is 443.
port-number	(Optional) Port number for the exec server. The default is 80.
source	(Optional) Specifies the use of an IP address defined by the *ip-address* argument as the source for CNS exec agent communications.
interface name	(Optional) Interface name.

Defaults

No CNS exec agent is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The CNS exec agent allows a remote application to execute an EXEC mode command-line interface (CLI) command on a Cisco IOS device by sending an event message containing the command. A restricted set of EXEC CLI commands—**show** commands—are supported.

In previous Cisco IOS releases, the CNS exec agent was enabled when the CNS configuration agent was enabled through the **cns config partial** command.

Examples

The following example shows how to enable the CNS exec agent with an IP address of 10.1.2.3 for the exec agent server, a port number of 93, and a source IP address of 172.17.2.2:

```
Router(config)# cns exec 10.1.2.3 93 source 172.17.2.2
```

Related Commands

Command	Description
cns event	Enables and configures CNS event agent services.
show cns event subject	Displays a list of CNS event agent subjects that are subscribed to by applications.

cns id

To set the unique event ID, config ID, or image ID used by CNS services, use the **cns id** command in global configuration mode. To set the identifier to the hostname of the Cisco IOS device, use the **no** form of this command.

If ID Choice Is an IP Address or MAC Address

cns id *type number* {**dns-reverse** | **ipaddress** | **mac-address**} [**event** | **image**]

no cns id *type number* {**dns-reverse** | **ipaddress** | **mac-address**} [**event** | **image**]

If ID Choice Is Anything Else

cns id {**hardware-serial** | **hostname** | **string** *string* | **udi**} [**event** | **image**]

no cns id {**hardware-serial** | **hostname** | **string** *string* | **udi**} [**event** | **image**]

If Using Cisco IOS Release 12.2(33)SRA

cns id *type number* {**ipaddress** | **mac-address**} [**event** | **image**]

Syntax Description

type number	Type of interface (for example, **ethernet**, **group-async**, **loopback**, or **virtual-template**) and the interface number. Indicates from which interface the IP or MAC address should be retrieved in order to define the unique ID.
dns-reverse	Uses DNS reverse lookup to retrieve the hostname of the Cisco IOS device and assign it as the unique ID.
ipaddress	Uses the IP address specified in the *type number* arguments as the unique ID.
mac-address	Uses the MAC address specified in the *type number* arguments as the unique ID.
event	(Optional) Sets this ID to be the event ID value, which is used to identify the Cisco IOS device for CNS event services. If both optional keywords are omitted, the event ID is set to the hostname of the Cisco IOS device.
image	(Optional) Sets this ID to be the image ID value, which is used to identify the Cisco IOS device for CNS image agent services. If both optional keywords are omitted, the image ID is set to the hostname of the Cisco IOS device.
hardware-serial	Uses the hardware serial number as the unique ID.
hostname	Uses the hostname as the unique ID. This is the system default.
string *string*	Uses an arbitrary text string—typically the hostname—as the unique ID.
udi	Uses the product Unique Device Identifier (UDI) as the unique ID.

Command Default

The system defaults to the hostname of the Cisco IOS device as the unique ID.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)XB	This command was introduced on Cisco IAD2420 series IADs.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.3(1)	The optional **image** keyword was added to set an image ID.
12.3(14)T	The **udi** keyword was added to use the product UDI as the unique ID.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to set the unique ID to the CNS configuration agent, which then pulls the initial configuration template to the Cisco IOS device during bootup.

You can set one or all three IDs: the config ID value for CNS configuration services, the event ID value for CNS event services, and the image ID value for CNS image agent services. To set all values, use the command three times.

To set the CNS event ID to the host name of the Cisco IOS device, use the **no** form of this command with the **event** keyword. To set the CNS config ID to the host name of the Cisco IOS device, use the **no** form of this command without the **event** keyword. To set the CNS image ID to the host name of the Cisco IOS device, use the **no** form of this command with the **image** keyword.

Unique Device Identifier

Each identifiable Cisco product is an entity, as defined by the Entity MIB (RFC-2737) and its supporting documents. Some entities, such as a chassis, will have subentities like slots. An Ethernet switch might be a member of a superentity, such as a stack. Most Cisco entities that are orderable products will leave the factory with an assigned UDI. The UDI information is printed on a label that is affixed to the physical hardware device, and it is also stored electronically on the device in order to facilitate remote retrieval. To use UDI retrieval, the Cisco product in use must be UDI-enabled.

A UDI consists of the following elements:

- Product identifier (PID)
- Version identifier (VID)
- Serial number (SN)

The PID is the name by which a product can be ordered; historically, it has been called the "Product Name" or "Part Number." This identifier is the one to use to order an exact replacement part.

The VID is the version of the product. When a product is revised, the VID is incremented according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product carries a unique serial number assigned at the factory, which cannot be changed in the field. The serial number is used to identify an individual, specific instance of a product.

Note The **udi** keyword will create an ID consisting of the PID, VID, and SN values without spaces but separated using commas. To view the UDI for this product, use the **show inventory** command. This keyword is not available in Cisco IOS Release 12.2(33)SRA.

Examples

The following example shows how to pass the hostname of the Cisco IOS device as the config ID value:

```
Router(config)# cns id hostname
```

The following example shows how to pass the hardware serial number of the Cisco IOS device as the event ID value:

```
Router(config)# cns id hardware-serial event
```

The following example shows how to pass the UDI as the event ID value:

```
Router(config)# cns id udi event
```

The following example shows how to pass the IP address of Ethernet interface 0/1 as the image ID value:

```
Router(config)# cns id ethernet 0/1 image
```

Related Commands

Command	Description
cns event	Enables the CNS event gateway, which provides CNS event services to Cisco IOS clients.
cns image	Enables the CNS image agent services to Cisco IOS clients.
show inventory	Displays the product inventory listing for all Cisco products that are installed in a networking device.

cns image

To configure the CNS image agent services, use the **cns image** command in global configuration mode. To disable the use of CNS image agent services, use the **no** form of this command.

cns image [**server** *server-url* [**status** *status-url*]]

no cns image [**server** *server-url* [**status** *status-url*]]

Syntax Description

server	(Optional) Specifies an image distribution server to contact for information about an updated image to be downloaded.
server-url	(Optional) URL used to contact an image distribution server. An IP address or domain name can be used.
status	(Optional) Specifies that any status messages generated by CNS image agent operations will be sent to the URL specified by the *status-url* argument.
status-url	(Optional) URL of a web server to which status messages are written.

Command Default

When configured, the CNS image agent always listens for image events on the CNS Event Bus server.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **cns image** command to start the CNS image agent process and to listen for image-related events on the CNS Event Bus.

If the optional server details are specified, the CNS image agent uses the server URL to contact the image management server. If no server details are specified, the URL for the image server must be supplied using one of the following three methods. The first method is to specify the image server using the server options on the **cns image retrieve** command. The second method is to use the server configured by the CNS event agent and stored as an image server event that can be received from the CNS Event Bus. The third method does not require a server URL because it uses CNS Event Bus mode.

If the optional status details are not specified, the status messages are sent as events on the CNS Event Bus.

Examples

The following example shows how to enable the CNS image agent services and configure a path to the image distribution server and a status messages server:

```
Router(config)# cns image server https://10.20.2.3:8080/cns/imageserver/ status 
https://10.20.2.3:8080/cns/imageserver/messages/
```

Related Commands

Command	Description
show cns image status	Displays information about the CNS image agent status.

cns image password

To configure a password to use with the Cisco Networking Services (CNS) image agent services, use the **cns image password** command in global configuration mode. To disable the use of a password, use the **no** form of this command.

cns image password *image-password*

no cns image password *image-password*

Syntax Description

image-password	Password to be used for CNS image agent services.

Command Default

No password is used with the CNS image agent services.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to create a password that is sent with the image ID in all CNS image agent messages. The recipient of these messages can use this information to authenticate the sending device. This password may be different from the username and password used for HTTP basic authentication configured with other CNS image agent commands.

Examples

The following example shows how to configure a password to be used for the CNS image agent services:

```
Router(config)# cns image password textabc
```

Related Commands

Command	Description
cns id	Sets the unique event ID, config ID, or image ID used by CNS services.

cns image retrieve

To contact a Cisco Networking Services (CNS) image distribution server and download a new image if a new image exists, use the **cns image retrieve** command in privileged EXEC mode.

cns image retrieve [**server** *server-url* [**status** *status-url*]]

Syntax Description

server	(Optional) Specifies an image distribution server to contact for information about an updated image to be downloaded.
server-url	(Optional) URL used to contact an image distribution server.
status	(Optional) Specifies that any status messages generated by this command will be sent to the URL specified by the *status-url* argument.
status-url	(Optional) URL of a web server to which status messages are written.

Command Default

An error occurs when a cns image server has not previously been configured in global configuration mode.

Usage Guidelines

When the **cns image retrieve** command is issued in privileged EXEC mode without the **server** keyword and *server-url* argument, an error occurs.

When a cns image server has been configured and the **cns image retrieve** command is issued with no **server** keyword and *server-url* argument, the server path configured in the **cns image** command is used.

When the **cns image** command is issued in global configuration mode with the optional **server** keyword, no keywords are required and no error occurs when you issue the **cns image retrieve** command in privileged EXEC mode.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

You must enable the CNS image agent services using the **cns image** command before configuring this command.

Use this command to poll an image distribution server and download a new image to the Cisco IOS device if a new image exists.

Examples

The following example shows how to configure the CNS image agent to access the image distribution server at 10.19.2.3 and download a new image if a new image exists:

```
Router# cns image retrieve server https://10.20.2.3:8080/cns/imageserver/ status
https://10.20.2.3:8080/cns/imageserver/messages/
```

Related Commands

Command	Description
cns image	Enables CNS image agent services.
cns trusted-server	Specifies a trusted server for CNS agents.
show cns image status	Displays information about the CNS image agent status.

cns image retry

To set the Cisco Networking Services (CNS) image upgrade retry interval, use the **cns image retry** command in global configuration mode. To restore the default value, use the **no** form of this command.

cns image retry *seconds*

no cns image retry *seconds*

Syntax Description

seconds	Integer in the range from 0 to 65535 that specifies the number of seconds in the interval. The default is 60 seconds.

Command Default

The default retry interval is 60 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to set an interval after which the CNS image agent will retry an image upgrade operation if the original upgrade attempt failed.

Examples

The following example shows how to set the CNS image upgrade interval to 240 seconds:

```
Router(config)# cns image retry 240
```

Related Commands

Command	Description
cns image	Enables CNS image agent services.

cns inventory

To enable the CNS inventory agent—that is, to send an inventory of the router's line cards and modules to the CNS configuration engine—and enter CNS inventory mode, use the **cns inventory** command in global configuration mode. To disable the CNS inventory agent, use the **no** form of this command.

cns inventory

no cns inventory

Syntax Description

This command has no arguments or keywords.

Command Default

The CNS inventory agent is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(1)	The **config**, **event**, and **notify oir** keywords were removed.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command with the **announce config** and **transport event** CNS inventory configuration mode commands to specify when to notify the CNS configuration engine of changes to the router's port-adaptor and interface inventory. A transport must be specified in CNS inventory configuration mode before any of the CNS inventory commands are executed.

Examples

The following example shows how to enable the CNS inventory agent and enter CNS inventory configuration mode:

```
Router(config)# cns inventory
Router(cns_inv)#
```

Related Commands

Command	Description
announce config	Species that an unsolicited configuration inventory is sent out by the CNS inventory agent at bootup.
cns config initial	Starts the CNS configuration agent and initiates an initial configuration.
transport event	Species that inventory events are sent out by the CNS inventory agent.

cns message format notification

To configure the message format for notification messages from a Cisco Networking Services (CNS) device, use the **cns message format notification** command in global configuration mode. To unconfigure a configured message format for notification messages from a CNS device, use the **no** form of this command.

cns message format notification {**version 1** | **version 2**}

no cns message format notification {**version 1** | **version 2**}

Syntax Description

version 1	Configures CNS notification messages to use the non- Service-Oriented Access Protocol (SOAP) format.
version 2	Configures CNS notification messages to use the SOAP format.

Command Default

Non-SOAP notification messages are used by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

Use this command to configure a CNS agent to use the SOAP format for CNS notification messages. SOAP message formats are supported by default. If the Cisco IOS device receives a request in the non-SOAP message format, the response will be sent in the non-SOAP format. If the Cisco IOS device receives a request in the SOAP format, the response will be sent in the SOAP format. By default, notification messages that are sent without any corresponding request messages will be sent in both SOAP and non-SOAP formats.

When this command is configured, received CNS notification messages that do not conform to the configured message format are rejected.

If the **cns aaa authentication notification** command is already configured, then the sender's credentials will be authenticated. If the **cns message format notification** command is configured, then the notification messages will be sent as per the configured version number. The default configuration is the legacy non-SOAP format.

Examples

The following example shows how to configure CNS notification messages to use the SOAP format:

```
cns message format notification version 2
```

Related Commands

Command	Description
cns aaa authentication	Enables CNS AAA options.

cns mib-access encapsulation

To specify whether Cisco Networking Services (CNS) should use nongranular (Simple Network Management Protocol [SNMP]) or granular (Extensible Markup Language [XML]) encapsulation to access MIBs, use the **cns mib-access encapsulation** command in global configuration mode. To disable the currently specified encapsulation, use the **no** form of this command.

cns mib-access encapsulation {**snmp** | **xml** [**size** *bytes*]}

no cns mib-access encapsulation {**snmp** | **xml**}

Syntax Description

snmp	Enables nongranular (SNMP) encapsulation for MIB access.
xml	Enables granular (XML) encapsulation for MIB access.
size *bytes*	(Optional) Maximum size in bytes for response events. The default is 3072.

Defaults

For XML encapsulation, a maximum size of 3072 bytes.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced on Cisco 2600 series and Cisco 3600 series routers.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example specifies that XML be used to access MIBs:

```
Router(config)# cns mib-access encapsulation xml
```

Related Commands

Command	Description
cns notifications encapsulation	Specifies whether CNS notifications should be sent using nongranular (SNMP) or granular (XML) encapsulation.

cns notifications encapsulation

To specify whether Cisco Networking Services (CNS) notifications should be sent using nongranular (Simple Network Management Protocol [SNMP]) or granular (Extensible Markup Language [XML]) encapsulation, use the **cns notifications encapsulation** command in global configuration mode. To disable the currently specified encapsulation, use the **no** form of this command.

cns notifications encapsulation {**snmp** | **xml**}

no cns notifications encapsulation {**snmp** | **xml**}

Syntax Description

snmp	Uses nongranular (SNMP) encapsulation to send notifications.
xml	Uses granular (XML) encapsulation to send notifications.

Command Default

CNS notifications are not sent using encapsulation.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced on Cisco 2600 series and Cisco 3600 series routers.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example shows how to specify that granular notifications should be sent:

```
Router(config)# cns notifications encapsulation xml
```

Related Commands

Command	Description
cns mib-access encapsulation	Specifies whether CNS should use granular (XML) or nongranular (SNMP) encapsulation to access MIBs.

cns template connect

To enter Cisco Networking Services (CNS) template connect configuration mode and define the name of a CNS connect template, use the **cns template connect** command in global configuration mode. To disable the CNS connect template, use the **no** form of this command.

cns template connect *name*

no cns template connect *name*

Syntax Description

name	Name of the CNS connect template to be configured.

Command Default

No CNS connect templates are defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **cns template connect** command to enter CNS template connect configuration mode and define the name of the CNS connect template to be configured. Then use the **cli** command to specify the command lines of the CNS connect template.

Note When you create a CNS connect template, you must enter the **exit** command to complete the configuration of the template and exit from CNS template connect configuration mode. This requirement was implemented to prevent accidentally entering a command without the **cli** command.

Note Effective with Cisco IOS Releases 12.3(8)T,12.3(9), and 12.2(33)SRA the **cns config connect-intf** command is replaced by the **cns connect** and **cns template connect** commands.

Examples

The following example shows how to configure a CNS connect template named template1:

```
Router(config)# cns template connect template1
Router(config-templ-conn)# cli command-1
Router(config-templ-conn)# cli command-2
Router(config-templ-conn)# cli no command-3
Router(config-templ-conn)# exit
Router(config)#
```

When the template1 template is applied, the following commands are sent to the router’s parser:

```
command-1
command-2
no command-3
```

When the template1 template is removed from the router’s configuration after an unsuccessful ping attempt to the CNS configuration engine, the following commands are sent to the router’s parser:

```
no command-1
no command-2
command-3
```

Related Commands

Command	Description
cli (cns)	Specifies the command lines of a CNS connect template.
cns connect	Enters CNS connect configuration mode and defines the parameters of a CNS connect profile for connecting to the CNS configuration engine.
discover (cns)	Defines the interface parameters within a CNS connect profile for connecting to the CNS configuration engine.
template (cns)	Specifies a list of CNS connect templates within a CNS connect profile to be applied to a router’s configuration.

cns trusted-server

To specify a trusted server for Cisco Networking Services (CNS) agents, use the **cns trusted-server** command in global configuration mode. To disable the use of a trusted server for a CNS agent, use the **no** form of this command.

cns trusted-server {**all-agents** | **config** | **event** | **exec** | **image**} *name*

no cns trusted-server {**all-agents** | **config** | **event** | **exec** | **image**} *name*

Syntax Description

all-agents	Specifies a trusted server for all CNS agents.
config	Specifies a trusted server for CNS config agent.
event	Specifies a trusted server for CNS event agent.
exec	Specifies a trusted server for CNS exec agent.
image	Specifies a trusted server for CNS image agent.
name	A string that specifies the hostname or IP address of the trusted server.

Defaults

By default, only the implicit server strings are trusted.

The configuration of the CNS event agent's server string through the command-line interface (CLI) results in an implicit trust by all CNS agents. For the other CNS agents, the configuration of a server string using the CLI results in an implicit trust of the server for the specified agent. For example, **cns exec 10.2.1.2** implies the string 10.2.1.2 is implicitly trusted by the exec agent, and specifying **cns event 10.4.2.2** implies the string 10.4.2.2 is implicitly trusted by all the CNS agents.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **cns trusted-server** command to specify a trusted server for an individual CNS agent or all the CNS agents. In previous Cisco IOS Releases, CNS agents could connect to any server and this could expose the system to security violations. An attempt to connect to a server not on the list results in an error message being displayed and an authentication failure reply extensible markup language (XML). For backwards compatibility the configuration of a server address using the configuration CLI for a CNS agent results in an implicit trust of the server for the specified agent.

Use this command when a CNS agent will redirect its response to a server address that is not explicitly configured on the command line for the specific CNS agent. For example, the CNS exec agent may have one server configured but receive a message from the CNS Event Bus that overrides the configured server. The new server address string has not been explicitly configured so the new server address is not a trusted server. An error will be generated when the CNS exec agent tries to respond to this new server address unless the **cns trusted-server** command has been configured for the new server address string.

The **cns trusted-server** command does not use Domain Name System (DNS). Instead a string comparison is done between the configured and implicit trusted servers and requested redirected server address.

Examples

The following example shows how to configure server 10.19.2.5 as a trusted server for the CNS event agent:

```
Router# cns trusted-server event 10.19.2.5
```

The following example shows how to configure server 10.2.2.8, which maps though DNS to host.somedomain.com as a trusted server for all CNS agents:

```
Router# cns trusted-server all-agents 10.2.2.8
Router# cns trusted-server all-agents host
Router# cns trusted-server all-agents host.somedomain.com
```

The following example shows how to configure the string 10.2.2.8 as an implicit trusted server for the CNS image agent:

```
Router# cns image server 10.2.2.8 status 10.2.2.8
```

Related Commands

Command	Description
cns config	Configures CNS configuration agent services.
cns event	Enables and configures CNS event agent services.
cns image	Configures CNS image agent services.

config-cli

Note Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), the **config-cli** command is replaced by the **cli (cns)** command. See the **cli (cns)** command for more information.

To connect to the Cisco Networking Services (CNS) configuration engine using a specific type of interface, use the **config-cli** command in CNS Connect-interface configuration mode.

config-cli *type* [*number*] *interface-config-cmd*

Syntax Description

type	Type of interface. Indicates from which interface the IP or MAC address should be retrieved in order to define the unique ID.
number	(Optional) Interface number. Indicates from which interface the IP or MAC address should be retrieved in order to define the unique ID.
interface-config-cmd	Command that configures the interface. The *type* argument must be configured before other interface configuration commands.

Command Default

No command lines are specified to configure the interface.

Command Modes

CNS Connect-interface configuration

Command History

Release	Modification
12.2(8)T	This command was introduced on Cisco 2600 series and Cisco 3600 series routers.
12.3(8)T	This command was replaced by the **cli (cns)** command.
12.3(9)	This command was replaced by the **cli (cns)** command.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Begin by using the **cns config connect-intf** command to enter CNS Connect-interface configuration (config-cns-conn-if) mode. Then use either this or its companion CNS bootstrap-configuration command to connect to the CNS configuration engine for initial configuration:

- **config-cli** connects to the registrar using a specific type of interface. You must specify the interface type but need not specify the interface number; the router's bootstrap configuration finds the connecting interface, regardless of the slot in which the card resides, by trying different candidate interfaces until it can ping the configuration engine.
- **line-cli** connects to the registrar using modem dialup lines.

Immediately after either of the commands, enter additional configuration commands as appropriate.

Examples

The following example enters CNS Connect-interface configuration mode, connects to a configuration engine using an asynchronous interface, and issues a number of commands:

```
Router(config)# cns config connect-intf Async
Router(config-cns-conn-if)# config-cli encapsulation ppp
Router(config-cns-conn-if)# config-cli ip unnumbered FastEthernet0/0
Router(config-cns-conn-if)# config-cli dialer rotary-group 0
Router(config-cns-conn-if)# line-cli modem InOut
Router(config-cns-conn-if)# line-cli...<other line commands>....
Router(config-cns-conn-if)# exit
```

These commands apply the following configuration:

```
line 65
modem InOut
.
.
.
interface Async65
encapsulation ppp
dialer in-band
dialer rotary-group 0
```

Related Commands

Command	Description
cns config connect-intf	Specifies the interface for connecting to the CNS configuration engine.
line-cli	Connects to the CNS configuration engine using a modem dialup line.

context

To associate a Simple Network Management Protocol (SNMP) context with a particular virtual private network (VPN) routing/forwarding instance (VRF), use the **context** command in VRF configuration mode. To disassociate an SNMP context from a VPN, use the **no** form of this command.

context *context-name*

no context *context-name*

Syntax Description

context-name	Name of the SNMP VPN context, up to 32 characters.

Command Default

No SNMP contexts are associated with VPNs.

Command Modes

VRF configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	Support for IPv6 was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before you use this command to associate an SNMP context with a VPN, you must do the following:

- Issue the **snmp-server context** command to create an SNMP context
- Associate a VPN with a context so that the specific MIB data for that VPN exists in that context.
- Associate a VPN group with the context of the VPN using the **snmp-server group** command with the **context** *context-name* keyword and argument.

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, MIB data for that VPN exists in that context. Associating a VPN with a context helps enable 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.

A route distinguisher (RD) is required when you configure an SNMP context. An RD creates routing and forwarding tables and specifies the default route distinguisher for a VPN. The RD is added to the beginning of a IPv4 prefix to make it globally unique. An RD is either ASN relative, which means it is composed of an autonomous system number and an arbitrary number, or it is IP address relative and composed of an IP address and an arbitrary number.

Examples

The following example shows how to create an SNMP context named context1 and associate the context with the VRF named vrf1:

```
Router(config)# snmp-server context1
Router(config)# ip vrf vrf1
Router(config-vrf)# rd 100:120
Router(config-vrf)# context context1
```

Related Commands

Command	Description
ip vrf	Enters VRF configuration mode for the configuration of a VRF.
snmp mib community-map	Associates an SNMP community with an SNMP context, engine ID, or security name.
snmp mib target list	Creates a list of target VRFs and hosts to associate with an SNMP v1 or v2c community.
snmp-server context	Creates an SNMP context.
snmp-server group	Configures a new SNMP group, or a table that maps SNMP users to SNMP views.
snmp-server trap authentication vrf	Controls VRF-specific SNMP authentication failure notifications.
snmp-server user	Configures a new user to an SNMP group.

copy logging onboard (Cat 6K)

To copy onboard failure logging (OBFL) data from the target OBFL-enabled module in Cisco Catalyst 6000 series switches to a local or remote file system, use the **copy logging onboard** command in privileged EXEC mode.

copy logging onboard module *module-number destination-url*

Syntax Description

module-number	Specifies the module number.
destination-url	The destination URL of the copied file or directory. The destination can be either local or remote. **Note** The exact format of the source and destination URLs varies according to the file or directory location.

Command Default

This command has no default condition.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

This command copies OBFL data from the target OBFL-enabled board to a local or remote file system. See the *Cisco IOS Configuration Fundamentals Command Reference* for more information about use of the **copy** command.

Examples

The following example shows the options for copying OBFL data:

```
Router# copy logging onboard module 2 ?

  bootflash:        Copy onboard logging to bootflash: file system
  const_nvram:      Copy onboard logging to const_nvram: file system
  dfc#2-bootflash:  Copy onboard logging to dfc#2-bootflash: file system
  dfc#4-bootflash:  Copy onboard logging to dfc#4-bootflash: file system
  disk0:            Copy onboard logging to disk0: file system
  disk1:            Copy onboard logging to disk1: file system
  ftp:              Copy onboard logging to ftp: file system
  http:             Copy onboard logging to http: file system
  https:            Copy onboard logging to https: file system
  null:             Copy onboard logging to null: file system
  nvram:            Copy onboard logging to nvram: file system
  rcp:              Copy onboard logging to rcp: file system
  scp:              Copy onboard logging to scp: file system
  sup-bootflash:    Copy onboard logging to sup-bootflash: file system
  sup-image:        Copy onboard logging to sup-image: file system
  syslog:           Copy onboard logging to syslog: file system
  system:            Copy onboard logging to system: file system
  tftp:              Copy onboard logging to tftp: file system
  tmpsys:            Copy onboard logging to tmpsys: file system
```

The following example shows how to transfer the OBFL data to a file on disk1:

```
Router# copy logging onboard module 2 disk1:tarmod2

OBFL feature copy disk1:tarmod2 2
% File transfer succeeded
```

The following example shows how to transfer the OBFL data to a file on a remote server:

```
Router# copy logging onboard module 2 tftp://server1/user1/tars/tarmod2/mod2tar

OBFL feature copy tftp://server1/user1/tars/tarmod2/mod2tar 2
% File transfer succeeded
```

Related Commands

Command	Description
attach	Connects to a specific line card for the purpose of executing commands on that card.
clear logging onboard (Cat 6K)	Clears onboard failure logs.
[**no**] **hw-module logging onboard (Cat 6K)**	Disables and enables OBFL.
show logging onboard (Cat 6K)	Displays onboard failure logs.

cpu interrupt

To enter CPU owner configuration mode to set thresholds for interrupt level CPU utilization, use the **cpu interrupt** command in resource policy node configuration mode. To exit CPU owner configuration mode, use the **no** form of this command.

cpu interrupt

no cpu interrupt

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Resource policy node configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command allows you to enter CPU owner configuration mode to set rising and falling values for critical, major, and minor thresholds for interrupt level CPU utilization.

Examples

The following example shows how to enter CPU owner configuration mode to set thresholds for interrupt level CPU utilization:

```
Router(config-res-policy-node)# cpu interrupt
```

Related Commands

Command	Description
critical rising	Sets the critical level threshold values for the buffer, CPU, and memory ROs.
major rising	Sets the major level threshold values for the buffer, CPU, and memory ROs.
minor rising	Sets the minor level threshold values for the buffer, CPU, and memory ROs.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.
slot (ERM policy)	Configures line cards.
system (ERM policy)	Configures system level ROs.

cpu process

To enter CPU owner configuration mode to set thresholds for process level CPU utilization, use the **cpu process** command in resource policy node configuration mode. To exit CPU owner configuration mode, use the **no** form of this command.

cpu process

no cpu process

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Resource policy node configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command allows you to enter CPU owner configuration mode to set rising and falling values for critical, major, and minor thresholds for process level CPU utilization.

Examples

The following example shows how to enter CPU owner configuration mode to set thresholds for process level CPU utilization:

```
Router(config-res-policy-node)# cpu process
```

Related Commands

Command	Description
critical rising	Sets the critical level threshold values for the buffer, CPU, and memory ROs.
major rising	Sets the major level threshold values for the buffer, CPU, and memory ROs.
minor rising	Sets the minor level threshold values for the buffer, CPU, and memory ROs.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.
slot (ERM policy)	Configures line cards.
system (ERM policy)	Configures system level ROs.

cpu total

To enter CPU owner configuration mode to set thresholds for total CPU utilization, use the **cpu total** command in resource policy node configuration mode. To exit CPU owner configuration mode, use the **no** form of this command.

cpu total

no cpu total

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Resource policy node configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command allows you to enter CPU owner configuration mode to set rising and falling values for critical, major, and minor thresholds for total CPU utilization.

Examples

The following example shows how to enter CPU owner configuration mode to set thresholds for total CPU utilization:

```
Router(config-res-policy-node)# cpu total
```

Related Commands

Command	Description
critical rising	Sets the critical level threshold values for the buffer, CPU, and memory ROs.
major rising	Sets the major level threshold values for the buffer, CPU, and memory ROs.
minor rising	Sets the minor level threshold values for the buffer, CPU, and memory ROs.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.
slot (ERM policy)	Configures line cards.
system (ERM policy)	Configures system level ROs.

critical rising

To set critical level threshold values for the buffer, CPU, and memory ROs, use the **critical rising** command in buffer owner configuration mode, CPU owner configuration mode, or memory owner configuration mode. To disable this function, use the **no** form of this command.

critical rising *rising-threshold-value* [**interval** *interval-value*] [**falling** *falling-threshold-value* [**interval** *interval-value*]] [**global**]

no critical rising

Syntax Description

rising-threshold-value	The rising threshold value as a percentage. Valid values are from 1 to 100.
interval	(Optional) Specifies the time, in seconds, during which the variation in rising or falling threshold values is not reported to the RU, resource groups, or resource user types. For example, if the buffer usage count remains above the configured threshold value for the configured interval, a notification is sent to the RU, resource group, or resource user types.
interval-value	The time, in seconds, during which the variation in rising or falling threshold values are not reported to the RU, resource groups, or resource user types. Valid values are from 0 to 86400. The default value is 0.
falling	(Optional) Specifies the falling threshold value as a percentage.
falling-threshold-value	(Optional) The falling threshold value as a percentage. Valid values are from 1 to 100.
global	(Optional) Configures a global threshold. The **global** keyword is optional when you set critical threshold values for public buffer, processor CPU, I/O memory, and processor memory. The **global** keyword is required when you set critical threshold values for interrupt CPU and total CPU.

Command Default

Disabled

Command Modes

Buffer owner configuration
CPU owner configuration
Memory owner configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

The interval is the dampening or observation interval time, in seconds, during which the variations in the rising and falling threshold values are not reported to the RUs. That is, the interval is the time the system waits to check whether the threshold value stabilizes. The interval is set to avoid unnecessary and unwanted threshold notifications. If not configured, the system defaults to 0 seconds.

This command allows you to configure three types of thresholding:

- System Global Thresholding
- User Local Thresholding
- Per User Global Thresholding

System Global Thresholding

System global thresholding is used when the entire resource reaches a specified value. That is, RUs are notified when the total resource utilization goes above or below a specified threshold value. The notification order is determined by the priority of the RU. The RUs with a lower priority are notified first and expected to reduce the resource utilization. This notification order prevents the sending of unwanted notifications to high-priority RUs.

You can set rising and falling threshold values. For example, if you set a total CPU utilization threshold value of 90% as the rising critical value and 20% as falling critical value, when the total CPU utilization crosses the 90% mark, a critical Up notification is sent to all the RUs and when the total CPU utilization falls below 20%, a critical Down notification is sent to all the RUs. The same criteria also apply to buffer ROs and memory ROs.

User Local Thresholding

User local thresholding is used when a specified RU exceeds the configured limits. The user local thresholding method prevents a single RU from monopolizing the resources. That is, the specified RU is notified when the resource utilization of the specified RU goes above or below a configured threshold value. For example, if you set a CPU utilization threshold value of 90% as the rising critical value and 20% as falling critical value, when the CPU utilization of the specified RU crosses the 90% mark, a critical Up notification is sent to that RU only and when the CPU utilization of the specified RU falls below 20%, a critical Down notification is sent to that RU only. The same method also applies to buffer and memory ROs.

Per User Global Thresholding

Per user global thresholding is used when the entire resource reaches a specified value. This value is unique for each RU and notification is sent only to the specified RU. User global thresholding is similar to user local thresholding, except that the global resource usage is compared against the thresholds. That is, only the specified RU is notified when the total resource utilization goes above or below a configured threshold value. For example, if you have set a CPU utilization threshold value of 90% as the rising critical value and 20% as falling critical value, when the total CPU utilization crosses the 90% mark, a critical Up notification is sent to the specified RU only and when the total CPU utilization falls below 20%, a critical Down notification is sent to the specified RU only. The same method also applies to buffer and memory ROs.

Threshold Violations

The Cisco IOS device sends out error messages when a threshold is violated. The following examples help you understand the error message pattern when different threshold violations occur in buffer, CPU, and memory ROs:

System Global Threshold Violation in Buffer RO

The threshold violation in buffer RO for a system global threshold shows the following output:

```
System global threshold-Violation (keywords Critical, Major and Minor alone will vary
accordingly)
==========================================================================================
00:15:11: %SYS-4-GLOBALBUFEXCEED: Buffer usage has gone above global buffer Critical
threshold
configured <value> Current usage :<value>
```

For example:

```
00:15:11: %SYS-4-GLOBALBUFEXCEED: Buffer usage has gone above global buffer Critical
threshold
configured 144 Current usage :145

System global threshold- Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
==========================================================================================
00:17:10: %SYS-5-GLOBALBUFRECOVER: Buffer usage has gone below global buffer Critical
threshold
configured <value> Current usage :<value>
```

For example:

```
00:17:10: %SYS-5-GLOBALBUFRECOVER: Buffer usage has gone below global buffer Critical
threshold
configured 90 Current usage :89
```

Per User Global Threshold Violation in Buffer RO

The threshold violation in buffer RO for a user global threshold shows the following output:

```
User global threshold - Violation (keywords Critical, Major and Minor alone will vary
accordingly)
==========================================================================================
00:24:04: %SYS-4-RESGLOBALBUFEXCEED: Buffer usage has gone above buffer Critical threshold
configured by resource user  <user-name>
configured 144 Current usage :145

User global threshold - Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
==========================================================================================
00:25:08: %SYS-4-RESGLOBALBUFRECOVER: Buffer usage has gone below buffer Critical
threshold configured by resource user  <user-name>
configured 126 Current usage :125
```

User Local Threshold Violation in Buffer RO

The threshold violation in buffer RO for a user local threshold shows the following output:

```
User local threshold - Violation (keywords Critical, Major and Minor alone will vary
accordingly)
=========================================================================================
00:31:15: %SYS-4-RESBUFEXCEED: Resource user  user_1 has exceeded the buffer Critical
threshold. configured 108 Current usage :109

User local threshold- Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
=========================================================================================
00:31:05: %SYS-5-RESBUFRECOVER: Resource user  user_1 has recovered after exceeding the
buffer Critical threshold. configured 90 Current usage :89
```

System Global Threshold Violation in CPU RO

The threshold violation in CPU RO for a system global threshold shows the following output:

```
System global threshold- Violation
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly )
=========================================================================================
00:19:36: %SYS-4-CPURESRISING: System is seeing global cpu util 19% at total level more
than the configured minor limit 11%

System global threshold - Recovery
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly
=========================================================================================
00:20:56: %SYS-6-CPURESFALLING: System is no longer seeing global high cpu at total level
for the configured minor limit 10%, current value 4%
```

Per User Global Threshold Violation in CPU RO

The threshold violation in CPU RO for a user global threshold shows the following output:

```
User global threshold - Violation
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly
=========================================================================================
00:14:21: %SYS-4-CPURESRISING: Resource user <user-name> is seeing global cpu util 11% at
total level more than the configured minor limit 6 %
```

For example:

```
00:14:21: %SYS-4-CPURESRISING: Resource user Test-proc-14:99s:1w:100n is seeing global cpu
util 11% at total level more than the configured minor limit 6%

User global threshold- Recovery
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly
=========================================================================================
00:14:46: %SYS-6-CPURESFALLING: Resource user <user-name> is no longer seeing global high
cpu at total level for the configured critical limit 9%, current value 4%
```

For example:

```
00:14:46: %SYS-6-CPURESFALLING: Resource user Test-proc-14:99s:1w:100n is no longer seeing
global high cpu at total level for the configured critical limit 9%, current value 4%
```

User Local Threshold Violation in CPU RO

The threshold violation in CPU RO for a user local threshold shows the following output:

```
User local threshold - Violation (keywords Critical, Major and Minor will vary accordingly
- only process level)
=========================================================================================
00:12:11: %SYS-4-CPURESRISING: Resource user <user-name> is seeing local cpu util 15% at
process level more than the configured minor limit 6%
```

For example:

```
00:12:11: %SYS-4-CPURESRISING: Resource user Test-proc-9:85s:15w:100n is seeing local cpu
util 15% at process level more than the configured minor limit 6%

User local threshold- Recovery (keywords Critical, Major and Minor will vary accordingly
- only process level)
=========================================================================================
00:13:11: %SYS-6-CPURESFALLING: Resource user <user-name> is no longer seeing local high
cpu at process level for the configured critical limit 9%, current value 3%
```

System Global Threshold Violation in Memory RO

The threshold violation in memory RO for a system global threshold shows the following output:

```
System global threshold - Violation (keywords Critical, Major and Minor alone will vary
accordingly )
(If violation happens in IO memory pool will be : I/O)
==========================================================================================
13:53:22: %SYS-5-GLOBALMEMEXCEED: Global Memory has exceeded the Minor threshold
Pool: Processor  Used: 422703520  Threshold: 373885200
```

For example:

```
13:54:03: %SYS-5-GLOBALMEMEXCEED: Global Memory has exceeded the Critical threshold
Pool: Processor  Used: 622701556  Threshold: 467356500

System global threshold - Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
(If recovery happens in IO memory pool will be : I/O)
==========================================================================================
%SYS-5-GLOBALMEMRECOVER: Global Memory has recovered  after exceeding Minor threshold
Pool: Processor  Used: 222473448  Threshold: 355190940
```

For example:

```
13:50:41: %SYS-5-GLOBALMEMRECOVER: Global Memory has recovered  after exceeding Critical
threshold
Pool: Processor  Used: 222473152  Threshold: 443988675
```

Per User Global Threshold Violation in Memory RO

The threshold violation in memory RO for a user global threshold shows the following output:

```
User global threshold - Violation (keywords Critical, Major and Minor alone will vary
accordingly)
(If violation happens in IO memory pool will be : I/O)
==========================================================================================
00:53:14: %SYS-4-RESGLOBALMEMEXCEED: Global Memory has exceeded the Minor threshold
configure by resource user <XYZ>
Pool: Processor  Used: 62273916  Threshold: 62246820

User global threshold - Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
(If recovery happens in IO memory pool will be : I/O)
==========================================================================================
00:32:56: %SYS-4-RESGLOBALMEMRECOVER: Global Memory has recovered after exceeding the
Critical threshold configure by resource user <XYZ>
Pool: Processor  Used: 329999508  Threshold: 375865440
```

User Local Threshold Violation in Memory RO

The threshold violation in memory RO for a user local threshold shows the following output:

```
User local threshold- Violation (keywords Critical, Major and Minor alone will vary
accordingly)
=========================================================================================
01:05:42: %SYS-4-RESMEMEXCEED: Resource user <XYZ> has exceeded the Critical memory
threshold
Pool: Processor Used: 103754740 Threshold: 103744700

User local threshold - Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
=========================================================================================
00:44:43: %SYS-5-RESMEMRECOVER: Resource user <XYZ> has recovered after exceeding the
Critical memory threshold
Pool: Processor Used: 328892280 Threshold :375865440
```

Examples

Configuring Critical Rising Values for System Global Thresholding

The following example shows how to configure the critical threshold values for system global thresholding with a critical rising threshold of 90% at an interval of 12 seconds and a critical falling threshold of 20% at an interval of 10 seconds:

```
Router(config-owner-cpu)# critical rising 90 interval 12 falling 20 interval 10 global
Router(config-owner-buffer)# critical rising 90 interval 12 falling 20 interval 10 global
Router(config-owner-memory)# critical rising 90 interval 12 falling 20 interval 10 global
```

Configuring Critical Rising Values for User Local Thresholding

The following example shows how to configure the critical threshold values for user local thresholding with a critical rising threshold of 90% at an interval of 12 seconds and a critical falling threshold of 20% at an interval of 10 seconds:

```
Router(config-owner-cpu)# critical rising 90 interval 12 falling 20 interval 10
Router(config-owner-buffer)# critical rising 90 interval 12 falling 20 interval 10
Router(config-owner-memory)# critical rising 90 interval 12 falling 20 interval 10
```

Configuring Critical Rising Values for Per User Global Thresholding

The following example shows how to configure the critical threshold values for per user global thresholding with a critical rising threshold of 90% at an interval of 12 seconds and a critical falling threshold of 20% at an interval of 10 seconds:

```
Router(config-owner-cpu)# critical rising 90 interval 12 falling 20 interval 10 global
Router(config-owner-buffer)# critical rising 90 interval 12 falling 20 interval 10 global
Router(config-owner-memory)# critical rising 90 interval 12 falling 20 interval 10 global
```

Related Commands

Command	Description
buffer public	Enters the buffer owner configuration mode and sets threshold values for buffer usage.
cpu interrupt	Enters the CPU owner configuration mode and sets threshold values for interrupt level CPU utilization.
cpu process	Enters the CPU owner configuration mode and sets threshold values for processor level CPU utilization.
cpu total	Enters the CPU owner configuration mode and sets threshold values for total CPU utilization.
memory io	Enters the memory owner configuration mode and sets threshold values for I/O memory.
memory processor	Enters the memory owner configuration mode and sets threshold values for processor memory.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.
slot (ERM policy)	Configures line cards.
system (ERM policy)	Configures system level ROs.

crypto mib topn

To configure TopN sampling parameters, use the **crypto mib topn** command in global configuration mode. To disable TopN sampling, use the **no** form of this command.

crypto mib topn [**interval** *seconds*] [**stop** *seconds*]

no crypto mib topn [**interval** *seconds*] [**stop** *seconds*]

Syntax Description

interval *seconds*	(Optional) Specifies the number of seconds between samples.The allowable range is from 60 to 86400 (60 seconds to 24 hours). The default is 300 (5 minutes). Defined in the MIB as TopnMinSampleInterval.
stop *seconds*	(Optional) Specifies the time, in seconds, from when this command is executed until sampling ceases. The allowable range is from 0 to 604800. A zero (0) indicates continuous sampling and is the default. For any value other than 0, the stop time value must be greater than or equal to the sampling interval value. Defined in the MIB as TopnStopTime.

Command Default

No TopN sampling parameters are configured.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to rank objects according to your chosen criteria. You will not see the stop parameter setting after enabling the **show running configuration** command if the stop parameter is set at a value greater than zero. Otherwise, the current sampling parameters are recorded in the active configuration (if sampling is enabled), and sampling occurs continuously (at the specified intervals) until, and after, the device is rebooted. This command should be disabled if your criteria queries performed by XSM clients (such as VPN Device Manager [VDM]) are not to be processed.

Crypto MIB commands apply to characteristics of the IP Security (IPSec) MIBs. TopN (**topn**) is a special subset of the IPSec MIB Export (IPSMX) interface that provides a set of queries that allows ranked reports of active Internet Key Exchange (IKE) or IPSec tunnels to be obtained depending on certain criteria. While the VPN Device Manager (VDM) application retrieves and presents the data elements defined in the IKE and IPSec MIBs, the application does not use the Simple Network Management Protocol (SNMP) interface.

Examples

The following example shows the **crypto mib topn** command being enabled with an interval frequency of 240 seconds and a designated stop time of 1200 seconds (20 minutes). At that time, the assigned sampling ceases.

```
crypto mib topn interval 240 stop 1200
```

Related Commands

Command	Description
xsm	Enables XSM client access to the router.

default-state

To set the default state for a stub object, use the **default-state** command in tracking configuration mode. To reset the default state to its internal default state, use the **no** form of this command.

default-state {**up** | **down**}

no default-state {**up** | **down**}

Syntax Description

up	Sets the current default state of a stub object to up.
down	Sets the current default state of a stub object to down.

Command Default

Internal default state is the default.

Command Modes

Tracking configuration (config-track)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(31)SB3	This command was integrated into Cisco IOS Release 12.2(31)SB3.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use the **default-state** command to set the default state of a stub object that has been created by the **track stub** command. The stub object can be tracked and manipulated by an external process, Embedded Event Manager (EEM).

EEM is a distributed, scalable, and customized approach to event detection and recovery offered directly in a Cisco IOS device. EEM offers the ability to monitor events and take informational or corrective action when the monitored events occur or when a threshold is reached. An EEM policy is an entity that defines an event and the actions to be taken when that event occurs.

Examples

The following example shows how to create a stub object and configure a default state for the stub object:

```
track 2 stub
 default-state up
```

Related Commands

Command	Description
show track	Displays tracking information.
track stub	Creates a stub object to be tracked.

discover (cns)

To define the interface parameters within a Cisco Networking Services (CNS) connect profile for connecting to the CNS configuration engine, use the **discover** command in CNS connect configuration mode. To disable this functionality, use the **no** form of this command.

discover {**line** *line-type* | **controller** *controller-type* | **interface** [*interface-type*] | **dlci** [**subinterface** *subinterface-number*]}

no discover {**line** *line-type* | **controller** *controller-type* | **interface** [*interface-type*] | **dlci** [**subinterface** *subinterface-number*]}

Syntax Description

line	Indicates that a line is used to connect to the CNS configuration engine. When the **line** *line-type* keyword and argument are specified, all the lines that create an interface that match the specified *line-type* argument are discovered. The CNS connect templates associated with the **discover line** *line-type* command are applied in line configuration mode.
line-type	Type of line used to connect to the CNS configuration engine.
controller	Indicates that a controller is used to connect to the CNS configuration engine. When the **controller** *controller-type* keyword and argument are specified, all the controllers that create an interface that match the specified *controller-type* argument are discovered. The CNS connect templates associated with the **discover controller** *controller-type* command are applied in controller configuration mode.
controller-type	Type of controller used to connect to the CNS configuration engine.
interface	Indicates that an interface is used to connect to the CNS configuration engine. If the **discover interface** *interface-type* command is the first **discover** command configured in a CNS connect profile, the interfaces that match the specified *interface-type* argument are discovered. If the **discover interface** *interface-type* command is configured after the **discover line** *line-type* or **discover controller** *controller-type* commands in a CNS connect profile, the specified *interface-type* argument is ignored. Instead, the CNS connect templates associated with the **discover interface** command are applied to all the interfaces associated with the preceding **discover line** *line-type* or **discover controller** *controller-type* commands. The CNS connect templates associated with the **discover interface** *interface-type* command are applied in interface configuration mode.
interface-type	(Optional) Type of interface used to connect to the CNS configuration engine.

dlci	Active DLCIs to be used for connecting to the CNS configuration engine. When this keyword is defined, all the active DLCIs are discovered on the interface specified by the preceding **discover interface** *interface-type* command. A Frame Relay LMI message will return a list of active DLCIs. Active DLCIs can only be discovered on interfaces configured with Frame Relay. Therefore, the location of the **discover dlci** command in a CNS connect profile is important. It must be entered after the interfaces have been configured with Frame Relay. The CNS connect templates associated with the **discover dlci** command are applied in subinterface (point-to-point) configuration mode. Defines the CNS connect variable **${dlci}** and **${next-hop}**. **Note** Any Cisco IOS command that requires knowledge of the active DLCIs must be configured after the **discover dlci** command.
subinterface	(Optional) Indicates that a point-to-point subinterface is used to perform a search for active DLCIs. If a number is not specified, the default value is 9999.
subinterface-number	(Optional) Number of the point-to-point subinterface used to perform a search for active DLCIs.

Command Default

No interface parameters within a CNS connect profile are defined.

Command Modes

CNS connect configuration

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9). The **dlci subinterface** *subinterface-number* keywords and argument and the CNS connect variable **${dlci}** are not supported in this release.

Usage Guidelines

First use the **cns connect** command to enter CNS connect configuration mode and define the parameters of a CNS connect profile for connecting to the CNS configuration engine. Then use the following CNS connect commands to create a CNS connect profile:

- **discover**
- **template**

A CNS connect profile specifies the **discover** commands and associated **template** commands to apply to a router’s configuration. The first **discover** command in a CNS connect profile defines the scope of interfaces to be searched and used to perform the ping iterations for connecting to the CNS configuration engine. Subsequent **discover** commands limit this scope.

The search is based on discovering all the interfaces that match the specified line, controller, or interface type. The search is case-insensitive and allows for abbreviations. For example, the **discover interface Serial**, **discover interface Ser**, **discover interface serial**, and **discover interface ser** commands all match the serial interface.

Each **discover** command must have at least one unique CNS connect template associated with it. Specifically, the **template** command must be configured after configuring the **discover** command. The **discover** command specifies the configuration mode in which the CNS connect templates (specified by the **template** command that is associated with the **discover** command) are to be applied. When multiple **discover** and **template** commands are configured in a CNS connect profile, they are processed in the order in which they are entered.

Table 8 provides a summary of the interface parameters that can be defined using the **discover** command.

Table 8 Summary of the discover Commands

discover Command	Description	Associated CNS Connect Variable	Configuration Mode in Which CNS Connect Templates Are Applied	Prerequisite discover Command	Required Subsequent discover Command
discover line *line-type*	Discovers all the lines that create an interface that match the specified *line-type* argument.	**${line}**	Line	—	**discover interface** *interface-type*
discover controller *controller-type*	Discovers all the controllers that create an interface that match the specified *controller-type* argument.	**${controller}**	Controller	—	**discover interface** *interface-type*
discover interface [*interface-type*]	• If this is the first **discover** command configured, then all the interfaces that match the specified *interface-type* argument are discovered. • If configured after the **discover line** *line-type* or **discover controller** *controller-type* commands, then the specified *interface-type* argument is ignored.	**${interface}** **${next-hop}**	Interface	—	—
discover dlci [**subinterface** *subinterface-number*]	Discovers all active DLCIs on the interface specified by the preceding **discover interface** command.	**${dlci}** **${next-hop}**	Subinterface (point-to-point)	**discover interface** *interface-type*	—

CNS connect variables can be used as placeholders within a CNS connect template configuration. Each variable is defined by an associated **discover** command (see Table 8 and Table 9). Before a CNS connect template that contains these variables is applied to a router's configuration, the variables are replaced by the values defined by their associated **discover** command. For example, if the **discover interface serial** command was configured, and you were able to connect to the CNS configuration engine using Serial0/0, the **cli ip route 0.0.0.0 0.0.0.0 ${interface}** command would generate the **cli ip route 0.0.0.0 0.0.0.0 serial0/0** command.

Table 9 Summary of the CNS Connect Variables

Variable	Description
${line}	The line type defined by the associated **discover line** *line-type* command.
${controller}	The controller type defined by the associated **discover controller** *controller-type* command.
${interface}	The interface type defined by the associated **discover interface** command.
${dlci}	The active DLCI defined by the associated **discover dlci** command.
${next-hop}	The next hop interface. This variable is identical to the **${interface}** variable unless the **discover dlci** command has been configured. In this case, the **${next-hop}** variable is identical to the **${interface}.{subinterface}** variable, where the **{subinterface}** variable is specified by the **discover dlci** command. The **${next-hop}** variable should only be used in the CNS connect templates after the last **discover** command has been entered. A typical use of this variable is to allow the default IP route to be configured to send traffic towards the CNS configuration engine. Note that the CNS configuration engine may not be on the same LAN as the router. Therefore, configuring a route to the CNS configuration engine may require deployment-specific knowledge. Common practice is to define a default route to the interface using the **ip route** command (for example, **cli ip route 0.0.0.0 0.0.0.0 ${next-hop}**).
$$	A literal substitution of the $ symbol.

Note Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), the **&** variable is replaced by the **${interface}** variable.

Examples

The following example shows how to create a CNS connect profile named EG:

```
Router (config)# cns connect EG
Router (config-cns-conn)# discover controller T1
Router (config-cns-conn)# template timeslot-1
Router (config-cns-conn)# discover interface
Router (config-cns-conn)# template frame
Router (config-cns-conn)# exit
Router (config)#
```

In this example, the following sequence of events occur for each T1 controller when the **cns connect EG** command is processed:

1. Enter controller configuration mode and apply all commands in the timeslot-1 template to the router's configuration.
2. For each interface associated with each T1 controller:
   a. Enter interface configuration mode and apply all commands in the frame template to the router's configuration.
   b. Try to ping the CNS configuration engine.
   c. If the ping is successful, then download pertinent configuration information from the CNS configuration engine and exit. The **cns connect EG** command has completed its process.
   d. If the ping is unsuccessful, enter interface configuration mode and remove all commands in the frame template from the router's configuration.
3. Enter controller configuration mode and remove all commands in the timeslot-1 template from the router's configuration. The **cns connect EG** command has failed to retrieve any configuration information from the CNS configuration engine.

Related Commands

Command	Description
cli (cns)	Specifies the command lines of a CNS connect template.
cns connect	Enters CNS connect configuration mode and defines the parameters of a CNS connect profile for connecting to the CNS configuration engine.
cns template connect	Enters CNS template connect configuration mode and defines the name of a CNS connect template.
template (cns)	Specifies a list of CNS connect templates within a CNS connect profile to be applied to a router's configuration.

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 arguments or keywords.

Command Default

Bulk statistics transfer is disabled.

Command Modes

Bulk Statistics Transfer configuration (config-bulk-tr)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Specific bulk statistics configurations are identified with a name, as specified in the **snmp mib bulkstat transfer** command. The **enable** command (in Bulk Statistics Transfer configuration mode) begins the periodic MIB data collection and transfer process.

Collection (and subsequent file transfer) will start only if this command is used. Conversely, the **no enable** command will stop the collection process. Subsequently, issuing the **enable** command will start 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 will immediately begin (in other words, the existing bulk statistics file will be 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.

Examples

The following example shows the bulk statistics transfer configuration named bulkstat1 as enabled:

```
Router(config)# snmp mib bulkstat transfer bulkstat1
Router(config-bulk-tr)# schema ATM2/0-IFMIB
Router(config-bulk-tr)# url primary ftp://user:pswrd@host/folder/bulkstat1
Router(config-bulk-tr)# enable
Router(config-bulk-tr)# exit
```

Related Commands

Command	Description
snmp mib bulkstat transfer	Names a bulk statistics transfer configuration and enters Bulk Statistics Transfer configuration mode.

event application

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of an event raised through the EEM Event Publish application programming interface (API), use the **event application** command in applet configuration mode. To remove the application event criteria, use the **no** form of this command.

event application subsystem *subsystem-id* **type** *event-type*

no event application subsystem *subsystem-id* **type** *event-type*

Syntax Description

subsystem	Specifies an identifier for the subsystem that will publish the application event.
subsystem-id	Number in the range from 1 to 4294967295 that identifies the subsystem. When an event is to be published by an EEM policy, the *subsystem-id* reserved for a policy is 798
type	Specifies an event type within the specified event.
event-type	Integer in the range from 1 to 4294967295.

Command Default

No EEM event criteria are specified.

Command Modes

Applet configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

An EEM event is triggered when an application calls the EEM Event Publish API with an event specification that matches the subsystem ID and application event type.

Examples

The following example shows how a policy named EventPublish_A runs every 20 seconds and publishes an event to a well-known EEM event type numbered 1. A second policy named EventPublish_B is registered to run when the well-known EEM event type of 1 occurs. When policy EventPublish_B runs, it outputs a message to syslog containing data passed as an argument from EventPublish_A.

```
Router(config)# event manager applet EventPublish_A
Router(config-applet)# event timer watchdog time 20.0
Router(config-applet)# action 1.0 syslog msg "Applet EventPublish_A"
Router(config-applet)# action 2.0 publish-event sub-system 798 type 1 arg1 twenty
Router(config-applet)# exit
Router(config)# event manager applet EventPublish_B
Router(config-applet)# event application subsystem 798 type 1
Router(config-applet)# action 1.0 syslog msg "Applet EventPublish_B arg1
$_application_data1"
```

Related Commands

Command	Description
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

event cli

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run by matching a Cisco IOS command-line interface (CLI) command, use the **event cli** command in applet configuration mode. To remove the CLI command event criteria, use the **no** form of this command.

event cli pattern *regular-expression* **sync** {**yes** | **no skip** {**yes** | **no**}} [**occurs** *num-occurrences*] [**period** *period-value*]

no event cli pattern *regular-expression* **sync** {**yes** | **no skip** {**yes** | **no**}} [**occurs** *num-occurrences*] [**period** *period-value*]

Syntax Description

pattern	Specifies the regular expression used to perform the CLI command pattern match. The CLI command must have been successfully parsed before the pattern match is attempted. The pattern match is compared with the fully expanded CLI command string.
regular-expression	Regular expression. If the expression contains embedded blanks, enclose it in double quotation marks.
sync	Indicates whether the policy should be executed synchronously before the CLI command executes. • If the **yes** keyword is specified, the policy will run synchronously with the CLI command. • If the **no** keyword is specified, the policy will run asynchronously with the CLI command.
skip	Indicates whether the CLI command should be executed. This keyword is required if the **sync** keyword is followed by the **no** keyword. If the **sync** keyword is followed by the **yes** keyword, the **skip** keyword should not be specified. • If the **yes** keyword is specified, the CLI command will not be executed. • If the **no** keyword is specified, the CLI command will be executed. This is the default. **Caution** When the **skip** keyword is followed by the **yes** keyword, unintended results may be produced if the pattern match is made for configuration commands because the CLI command that matches the regular expression will not be executed.
occurs	(Optional) Specifies the number of matching occurrences before an EEM event is triggered. When a number is not specified, an EEM event is triggered after the first match.
num-occurrences	(Optional) Integer greater than 0 that specifies the number of occurrences.

period	(Optional) Specifies the time interval during which the one or more occurrences must take place. When the keyword is not specified, no time period check is applied.
period-value	(Optional) Integer that represents seconds and optional milliseconds in the format ssssss[.mmm]. Seconds is an integer in the range from 0 to 4294967295. Milliseconds is an integer in the range from 0 to 999. When you specify milliseconds only, use the format 0.mmm.

Command Default

No EEM events are triggered on the basis of a match with a Cisco IOS CLI command.

Command Modes

Applet configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

Use the **event cli** command to set up event criteria against which CLI commands are matched. CLI commands are compared against a specified regular expression. After a specified number of matches occurs within a specified time period, an EEM event is triggered. If multiple conditions exist, the EEM event is triggered when all the conditions are met.

When the **sync** keyword is used, the event detector is notified when the policy completes running. The exit status of the policy determines whether the CLI command will be executed. If the policy exit status is zero—the policy ran successfully—the CLI command is not executed; otherwise the CLI command runs.

Examples

The following example shows how to specify an EEM applet to run when the Cisco IOS **write memory** CLI command is run. The applet provides a notification via a syslog message that this event has occurred.

```
Router(config)# event manager applet cli-match
Router(config-applet)# event cli pattern "write memory.*" sync yes
Router(config-applet)# action 1.0 syslog msg "$_cli_msg Command Executed"
Router(config-applet)# set 2.0 _exit_status 1
```

The following example shows how unintended results can be produced when using the **skip** keyword followed by the **yes** keyword. When the **skip** keyword is followed by the **yes** keyword, unintended results may be produced if the pattern match is made for configuration commands because the CLI command that matches the regular expression will not be executed. In this example, the first applet (ap1) uses the

skip keyword followed by the **yes** keyword to specify that any CLI command that contains the pattern, **show ip interface**, is not executed. This results in the second applet (ap2) being configured without an event statement because it contains the show ip interface pattern.

```
Router(config)# event manager applet ap1
Router(config-applet)# event cli pattern "show ip interface" sync no skip yes occurs 1
period 5
Router(config-applet)# action 1 syslog msg "test 1"
Router(config-applet)# exit
Router(config)# event manager applet ap2
Router(config-applet)# event cli pattern "show ip interface" sync no skip no occurs 1
period 5
Router(config-applet)# action 1 syslog msg "test 2"
Router(config-applet)# end
```

The results are displayed on the screen. Note that the second line contains a message that no event is configured for the EEM applet ap2. Use command CLI pattern matching with caution when the **skip** and **yes** keywords are specified.

```
00:00:41: %HA_EM-6-LOG: ap1: test 1
00:00:41: %HA_EM-4-FMPD_NO_EVENT: No event configured for applet ap2
router#show run | beg event event manager applet ap1 event cli pattern "show ip
interface" sync no skip yes occurs 1 period 5 action 1 syslog msg "test 1"
event manager applet ap2
 action 1 syslog msg "test 2"
!
end
```

Related Commands

Command	Description
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

event counter

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of a named counter crossing a threshold, use the **event counter** command in applet configuration mode. To remove the counter event criteria, use the **no** form of this command.

event counter name *counter-name* **entry-op** *operator* **entry-val** *entry-value* [**exit-op** *operator*] [**exit-val** *exit-value*]

no event counter name *counter-name* **entry-op** *operator* **entry-val** *entry-value* [**exit-op** *operator*] [**exit-val** *exit-value*]

Syntax Description

name	Specifies that a counter will be monitored.
counter-name	Name of the counter that will be monitored.
entry-op	Compares the contents of the current counter value with the entry value using a specified operator. If there is a match, an event is triggered and event monitoring is disabled until the exit criteria are met.
operator	Value used with the **entry-op** and **exit-op** keywords that determines how the current counter value is compared to the entry value or the exit value. Valid values are: • **gt**—Greater than. • **ge**—Greater than or equal to. • **eq**—Equal to. • **ne**—Not equal to. • **lt**—Less than. • **le**—Less than or equal to.
entry-val	Specifies the value with which the contents of the current counter are compared to decide if a counter event should be raised.
entry-value	Number in the range from –2147483648 to 2147483647, inclusive.
exit-op	(Optional) Compares the contents of the current counter with the exit value using a specified operator. If there is a match, an event is triggered and event monitoring is reenabled.
exit-val	(Optional) Specifies the value with which the contents of the current counter are compared to decide whether the exit criteria are met.
exit-value	(Optional) Number in the range from –2147483648 to 2147483647, inclusive.

Command Default

No EEM events are triggered on the basis of a named counter crossing a threshold.

Command Modes

Applet configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

An EEM event is triggered when the value of a specified counter crosses a defined threshold. Depending on the operator, the threshold may be crossed when the value is greater than the threshold or when the value is less than the threshold.

Use the **event counter** command with the **action counter** command when an event occurs periodically and you want an action to be implemented after a specified number of occurrences of the event.

Exit criteria are optional. If exit criteria are not specified, event monitoring will be reenabled immediately. If exit criteria are specified, event monitoring is not reenabled until the criteria are met.

Examples

The following example shows that policy EventCounter_A is configured to run once a minute and to increment a well-known counter called critical_errors. A second policy—EventCounter_B—is registered to be triggered when the well-known counter called critical_errors exceeds a threshold of 3. When policy EventCounter_B runs, it resets the counter to 0.

```
Router(config)# event manager applet EventCounter_A
Router(config-applet)# event timer watchdog time 60.0
Router(config-applet)# action 1.0 syslog msg "EventCounter_A"
Router(config-applet)# action 2.0 counter name critical_errors value 1 op inc
Router(config-applet)# exit
Router(config)# event manager applet EventCounter_B
Router(config-applet)# event counter name critical_errors entry-op gt entry-val 3 exit-op
lt exit-val 3
Router(config-applet)# action 1.0 syslog msg "EventCounter_B"
Router(config-applet)# action 2.0 counter name critical_errors value 0 op set
```

Related Commands

Command	Description
action counter	Sets or modifies a named counter when an Embedded Event Manager applet is triggered.
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

event gold

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of a Generic Online Diagnostic (GOLD) failure event when monitoring one or more cards and optional subcards, use the **event gold** command in applet configuration mode. To remove the report event criteria, use the **no** form of this command.

event gold card {**all** | *card-number*} [**subcard** {**all** | *subcard-number*}] [**new-failure** {**true** | **false**}] [**severity-major**] [**severity-minor**] [**severity-normal**] [**action-notify** {**true** | **false**}] [**testing-type** {**bootup** | **ondemand** | **schedule** | **monitoring**}] [**test-name** *test-name*] [**test-id** *test-id*] [**consecutive-failure** *consecutive-failure-number*] [**platform-action** *action-flag-number*] [**maxrun** *maxruntime-number*]

no event gold card {**all** | *card-number*} [**subcard** {**all** | *subcard-number*}] [**new-failure** {**true** | **false**}] [**severity-major**] [**severity-minor**] [**severity-normal**] [**action-notify** {**true** | **false**}] [**testing-type** {**bootup** | **ondemand** | **schedule** | **monitoring**}] [**test-name** *test-name*] [**test-id** *test-id*] [**consecutive-failure** *consecutive-failure-number*] [**platform-action** *action-flag-number*] [**maxrun** *maxruntime-number*]

Syntax Description

card	Specifies that all or one card must be monitored. Either **all** or *card-number* must be specified. • **all**—Specifies that all cards are to be monitored. This is the default. • *card-number*—Number of a specific card to be monitored. **Note** The **card** keyword is required to complete the **event gold** command.
subcard	(Optional) Specifies that one or more subcards are to be monitored. If the **subcard** keyword is specified, then **all** or *subcard-number* value must be specified. • **all**—Specifies that all subcards are to be monitored. • *subcard-number*—Number of a subcard to be monitored. If the **subcard** keyword is not specified, the default is **all**.
new-failure	(Optional) Specifies event criteria based on the new test failure information from GOLD. If the **new-failure** keyword is specified, then the **true** or **false** keyword must be specified. • **true**—Specifies that the event criteria for the new test failure is true from GOLD. • **false**—Specifies that the event criteria for the new test failure is false from GOLD. If the **new-failure** keyword is not specified, the new test failure information from GOLD is not considered in the event criteria.
severity-major	(Optional) Specifies that the event criteria for diagnostic result matches with diagnostic major error from GOLD.
severity-minor	(Optional) Specifies that the event criteria for diagnostic result matches with diagnostic minor error from GOLD.
severity-normal	(Optional) Specifies that the event criteria for diagnostic result matches with diagnostic normal from GOLD. This is the default.

action-notify	(Optional) Specifies the event criteria based on the action notify information from GOLD. If the **action-notify** keyword is specified, then **true** or **false** keyword must be specified. • **true**—Specifies that the event criteria for the action notify is true from GOLD. • **false**—Specifies that the event criteria for the action notify is false from GOLD. If the **action-notify** keyword is not specified, the action notify information from GOLD is not considered in the event criteria.
testing-type	(Optional) Specifies the event criteria based on the testing types of diagnostic from GOLD. If the **testing-type** keyword is specified, then **bootup**, **ondemand**, **schedule**, or **monitoring** must be specified. • **bootup**—Specifies the diagnostic tests running on system bootup. • **ondemand**—Specifies the diagnostic tests running from CLI after the card is online. • **schedule**—Specifies the scheduled diagnostic tests. • **monitoring**—Specifies the diagnostic tests that are running periodically in the background to monitor the health of the system. If the **testing-type** keyword is not specified, the testing type information from GOLD is not considered in the event criteria and the policy applies to all the diagnostic testing types.
test-name	(Optional) Specifies the event criteria based on the test name. If the **test-name** keyword is specified, then the *test-name* value must be specified. • *test-name*—Name of the test. If the **test-name** keyword is not specified, the test name information from GOLD is not considered in the event criteria.
test-id	(Optional) Specifies the event criteria based on test ID. Because the test ID can be different for the same test on different line cards, usually the **test-name** keyword should be used instead. If the test ID is specified and has conflicts with the specified test name, the test name overwrites the test ID. If the **test-id** keyword is specified, the *test-id* value must be specified. • *test-id*—ID number of the test. The limit is 65535. If the **test-id** keyword is not specified, test ID information from GOLD is not considered in the event criteria.
consecutive-failure	(Optional) Specifies the event criteria based on consecutive test failure information from GOLD. If the **consecutive-failure** keyword is specified, the c*onsecutive-failure-number* value must be specified. • *consecutive-failure-number*—Number of consecutive failures. If the **consecutive-failure** keyword is not specified, consecutive test failure information from GOLD is not considered in the event criteria.

platform-action	(Optional) Specifies whether callback to the platform is needed when all the event criteria are matched. When callback is needed, the platform needs to register a callback function through the provided registry. If the **platform-action** keyword is specified, the *action-flag-number* value must be specified. • *action-flag-number*—Number of the action flag that provides the platform with more specific information when callback is performed. The action flag is platform specific. It is up to the platform to determine what action needs to be taken based on the flag. The maximum number is 65535. If the **platform-action** keyword is not specified, there is no callback.
maxrun	(Optional) Specifies the maximum runtime of the script. If the **maxrun** keyword is specified, the *maxruntime-number* value must be specified. • *maxruntime-number*—Maximum runtime number in seconds. The maximum number is 4294967295 seconds. If the **maxrun** keyword is not specified, the default runtime is 20 seconds.

Command Default

No EEM event criteria are specified.

Command Modes

Applet configuration (config-applet)

Command History

Release	Modification
12.2(18)SXF2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	The **action-notify**, **testing-type**, **test-name**, **test-id**, **consecutive-failure**, **platform-action**, and the **maxrun** keywords were added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

You must enter the **event gold** command with the mandatory keyword **card**. For example, enter **event gold card** specifying either the **all** keyword or the *card-number* attribute; otherwise the command is incomplete. All other keywords are optional; however, once an optional keyword is specified, for example **new-failure**, its corresponding **true** or **false keyword must** be specified (the value is not optional anymore). The same principle is applicable for all other keywords that have specific values.

Examples

The following example shows how to specify that an EEM applet runs when a new GOLD failure event occurs for any card and any subcard. The applet sends a message to the CNS Event Bus to state that a GOLD failure event has occurred.

```
Router(config)# event manager applet gold-match
Router(config-applet)# event gold card all subcard all new-failure true
Router(config-applet)# action 1.0 cns-event msg "A GOLD failure event has occurred”
```

Related Commands

Command	Description
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

event interface

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of a generic interface counter crossing a threshold or reaching exit criteria, use the **event interface** command in applet configuration mode. To remove the interface event criteria, use the **no** form of this command.

event interface name *interface-type interface-number* **parameter** *counter-name* **entry-op** *operator* **entry-val** *entry-value* **entry-val-is-increment** {**true** | **false**} [**exit-comb** {**or** | **and**}] [**exit-op** *operator* **exit-val** *exit-value*] [**exit-val-is-increment** {**true** | **false**}] [**exit-time** *exit-time-value*] **poll-interval** *poll-int-value*

no event interface name *interface-type interface-number* **parameter** *counter-name* **entry-op** *operator* **entry-val** *entry-value* **entry-val-is-increment** {**true** | **false**} [**exit-comb** {**or** | **and**}] [**exit-op** *operator* **exit-val** *exit-value*] [**exit-val-is-increment** {**true** | **false**}] [**exit-time** *exit-time-value*] **poll-interval** *poll-int-value*

Syntax Description

name	Specifies the type and number of the interface to monitor.
interface-type	String that identifies the type of interface.
interface-number	Integer value that identifies the interface.
parameter	Specifies the name of the counter to monitor.
counter-name	Name of the counter. The name indicates the type of counter. Supported values for the *counter-name* argument are the following: • **input_errors**—Includes runts, giants, no buffer, cyclic redundancy checksum (CRC), frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased. Some datagrams may have more than one error. • **input_errors_crc**—Number of packets with a CRC generated by the originating LAN station or remote device that do not match the checksum calculated from the data received. • **input_errors_frame**—Number of packets received incorrectly that have a CRC error and a noninteger number of octets. • **input_errors_overrun**—Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data. • **input_packets_dropped**—Number of packets dropped because of a full input queue. • **interface_resets**—Number of times an interface has been completely reset. • **output_buffer_failures**—Number of failed buffers and number of buffers swapped out. • **output_buffer_swappedout**—Number of packets swapped to DRAM.

	• **output_errors**—Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the output errors because some datagrams may have more than one error and other datagrams may have errors that do not fall into any of the specifically tabulated categories. • **output_errors_underrun**—Number of times that the transmitter has been running faster than the router can handle. • **output_packets_dropped**—Number of packets dropped because of a full output queue. • **receive_broadcasts**—Number of broadcast or multicast packets received by the interface. • **receive_giants**—Number of packets that are discarded because they exceed the maximum packet size of the medium. • **receive_rate_bps**—Interface receive rate, in bytes per second. • **receive_rate_pps**—Interface receive rate, in packets per second. • **receive_runts**—Number of packets that are discarded because they are smaller than the minimum packet size of the medium. • **receive_throttle**—Number of times the receiver on the port was disabled, possibly because of buffer or processor overload. • **reliability**—Reliability of the interface, as a fraction of 255 (255 out of 255 is 100 percent reliability), calculated as an exponential average over 5 minutes. • **rxload**—Receive rate of the interface, as a fraction of 255 (255 out of 255 is 100 percent). • **transmit_rate_bps**—Interface transmit rate, in bytes per second. • **transmit_rate_pps**—Interface transmit rate, in packets per second. • **txload**—Transmit rate of the interface, as a fraction of 255 (255 out of 255 is 100 percent).
entry-op	Compares the current interface counter value with the entry value using the specified operator. If there is a match, an event is triggered and event monitoring is disabled until the exit criteria are met.
operator	Value used with the **entry-op** and **exit-op** keywords that determines how the current counter value is compared to the entry value or the exit value. Valid values are: • **gt**—Greater than. • **ge**—Greater than or equal to. • **eq**—Equal to. • **ne**—Not equal to. • **lt**—Less than. • **le**—Less than or equal to.
entry-val	Specifies the value with which the current interface counter value is compared to decide if the interface event should be raised.
entry-value	Number in the range from –2147483648 to 2147483647, inclusive.

entry-val-is-increment	Indicates whether the *entry-value* is an absolute or an increment value.
true	Specifies that the *entry-value* is an increment value.
false	Specifies that the *entry-value* is not an increment value.
exit-comb	(Optional) Indicates the combination of exit conditions that must be met before event monitoring is reenabled.
exit-op	(Optional) Compares the contents of the current interface counter value with the exit value using the specified operator. If there is a match, an event is triggered and event monitoring is reenabled.
exit-val	(Optional) Specifies the value with which the contents of the current interface counter value are compared to decide whether the exit criteria are met. If an exit value is specified, you must configure an exit operator.
exit-value	(Optional) Number in the range from –2147483648 to 2147483647, inclusive.
exit-val-is-increment	(Optional) Indicates whether the *exit-value* is an absolute or an increment value.
exit-time	(Optional) Specifies the time period after which the event monitoring is reenabled. The timing starts after the event is triggered.
exit-time-value	(Optional) Number that represents seconds and optional milliseconds in the format ssssss[.mmm]. The range for seconds is from 0 to 4294967295. The range for milliseconds is from 0 to 999. If using milliseconds only, specify the milliseconds in the format 0.mmm.
poll-interval	Specifies the time interval between consecutive polls.
poll-int-value	Number that represents seconds and optional milliseconds in the format ssssss[.mmm]. The range for seconds is from 60 to 4294967295. The range for milliseconds is from 0 to 999. If using milliseconds, specify the milliseconds in the format s.mmm. The minimum polling interval is 60 seconds.

Command Default

No EEM events are triggered on the basis of a generic interface counter crossing a threshold or reaching exit criteria.

Command Modes

Applet configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

An EEM event is triggered when one of the fields specified by an interface counter crosses a defined threshold.

Exit criteria are optional. If exit criteria are not specified, event monitoring will be reenabled immediately. If exit criteria are specified—on the basis of values or time periods—event monitoring is not reenabled until the criteria are met.

When the **exit-comb** keyword is used, the following criteria must be met:

- If the **or** operator is specified, an exit comparison operator and an exit object ID value, or an exit time value must exist.
- If the **and** operator is specified, an exit comparison operator, an exit object ID value, and an exit time value must exist.

When the **entry-val-is-increment** keyword is used, the following occurs:

- If the **true** keyword is specified, the *entry-value* is an increment and the interface event is raised whenever the increment value occurs.
- If the **false** keyword is specified, the *entry-value* is an absolute value and the interface event is raised whenever the absolute value occurs. This is the default.

When the optional **exit-val-is-increment** keyword is used, the following occurs:

- If the **true** keyword is specified, the *exit-value* is an increment and the event monitoring is reenabled whenever the increment value occurs.
- If the **false** keyword is specified, the *exit-value* is an absolute value and the event monitoring is reenabled whenever the absolute value occurs. This is the default.

Examples

The following example shows how a policy named EventInterface is triggered every time the receive_throttle counter for the FastEthernet 0/0 interface is incremented by 5. The polling interval to check the counter is specified to run once every 90 seconds.

```
Router(config)# event manager applet EventInterface
Router(config-applet)# event interface name FastEthernet0/0 parameter receive_throttle
entry-op ge entry-val 5 entry-val-is-increment true poll-interval 90
Router(config-applet)# action 1.0 syslog msg "Applet EventInterface"
```

Related Commands

Command	Description
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

event ioswdsysmon

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of Cisco IOS system monitor counters crossing a threshold, use the **event ioswdsysmon** command in applet configuration mode. To remove the event criteria, use the **no** form of this command.

event ioswdsysmon sub1 *subevent1* [**timewin** *timewin-value*] [**sub12-op** {**and** | **or**} **sub2** *subevent2*]

no event ioswdsysmon sub1 *subevent1* [**timewin** *timewin-value*] [**sub12-op** {**and** | **or**} **sub2** *subevent2*]

Subevent Syntax (for the *subevent1* and *subevent2* Arguments) for Cisco IOS Images

cpu-proc taskname *task-name* **op** *operator* **val** *value* [**period** *period-value*]

mem-proc taskname *task-name* **op** *operator* **val** *value* [**is-percent** {**true** | **false**}] [**period** *period-value*]

Subevent Syntax (for the *subevent1* and *subevent2* Arguments) for Cisco IOS Software Modularity Images

cpu-proc taskname *task-name* **path** *pid* **op** *operator* **val** *value* [**period** *period-value*]

mem-proc taskname *task-name* **path** *pid* **op** *operator* **val** *value* [**is-percent** {**true** | **false**}] [**period** *period-value*]

Syntax Description

sub1	Specifies the first subevent.
subevent1	First subevent. Use the syntax shown under the Subevent Syntax heading.
timewin	(Optional) Specifies the time window within which all the subevents must occur for an event to be generated.
timewin-value	(Optional) Number that represents seconds and optional milliseconds in the format ssssss[.mmm]. The range for seconds is from 0 to 4294967295. The range for milliseconds is from 0 to 999. If using milliseconds only, specify the milliseconds in the format 0.mmm.
sub12-op	(Optional) Indicates the combination operator for comparison between subevent 1 and subevent 2.
and	(Optional) Specifies that the results of both subevent 1 and subevent 2 must cross the specified thresholds.
or	(Optional) Specifies that the results of either subevent 1 or subevent 2 must cross the specified thresholds.
sub2	(Optional) Specifies the second subevent.
subevent2	(Optional) Second subevent. Use the syntax shown under the Subevent Syntax heading.
Subevent Syntax	
cpu-proc	Specifies the use of a sample collection of CPU statistics.
mem-proc	Specifies the use of a sample collection of memory statistics.

taskname	Specifies a Cisco IOS task name. **Note** In Cisco IOS Release 12.2(18)SXF4 and later releases, Software Modularity images contain POSIX processes, and Cisco IOS processes were renamed as tasks.
task-name	Name of the Cisco IOS task to be monitored. If the value of the *task-name* argument contains embedded blanks, enclose it in double quotation marks.
path	(Supported only in Software Modularity images) Specifies a Cisco IOS Software Modularity path and process name. **Note** In Cisco IOS Release 12.2(18)SXF4 and later releases, Software Modularity images contain POSIX processes, and Cisco IOS processes were renamed as tasks.
pid	(Supported only in Software Modularity images) Process ID of the Software Modularity process to be monitored.
op	Compares the collected CPU or memory usage sample with the value specified in the *value* argument.
operator	Two-character string. The *operator* argument takes one of the following values: • **gt**—Greater than • **ge**—Greater than or equal to • **eq**—Equal to • **ne**—Not equal to • **lt**—Less than • **le**—Less than or equal to
val	Specifies the value with which the collected CPU or memory usage sample is compared to decide if the subevent should be raised.
value	Number in the range from 1 to 4294967295.
period	(Optional) Specifies the elapsed time period for the collection samples to be averaged.
period-value	(Optional) Number that represents seconds and optional milliseconds in the format ssssss[.mmm]. The range for seconds is from 0 to 4294967295. The range for milliseconds is from 0 to 999. If only milliseconds are used, the format is 0.mmm. If the time period is 0, the most recent sample is used.
is-percent	(Optional) Indicates whether the *value* argument is a percentage.
true	(Optional) Specifies that the *value* argument is a percentage.
false	(Optional) Specifies that the *value* argument is not a percentage.

Command Default

No EEM events are triggered on the basis of Cisco IOS system monitor counters.

Command Modes

Applet configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	The **path** keyword and *pid* argument were added and this command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5

Usage Guidelines

An EEM event is triggered when one of the Cisco IOS system monitor counters crosses a defined threshold. Depending on the operator, the threshold may be crossed when the value exceeds the threshold or when the value is less than the threshold.

If a match is found when the **op** keyword is used, a subevent is triggered.

Examples

The following example shows how to configure a policy to trigger an applet when the total amount of memory used by the process named “IP RIB Update” has increased by more than 50 percent over the sample period of 60 seconds:

```
Router(config)# event manager applet IOSWD_Sample3
Router(config-applet)# event ioswdsysmon sub1 mem-proc taskname “IP RIB Update” op gt val 
50 is-percent true period 60
Router(config-applet)# action 1 syslog msg “IOSWD_Sample3 Policy Triggered”
```

Related Commands

Command	Description
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

event manager applet

To register an applet with the Embedded Event Manager (EEM) and to enter applet configuration mode, use the **event manager applet** command in global configuration mode. To remove the applet command from the configuration file, use the **no** form of this command.

event manager applet *applet-name*

no event manager applet *applet-name*

Syntax Description

applet-name	Name of the applet file.

Command Default

No EEM applets are registered.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

An EEM applet is a concise method for defining event screening criteria and the actions to be taken when that event occurs.

Only one event configuration command is allowed within an applet configuration. When applet configuration submode is exited and no event command is present, a warning is displayed stating that no event is associated with this applet. If no event is specified, this applet is not considered registered and the applet is not displayed. When no action is associated with this applet, events are still triggered but no actions are performed. Multiple action applet configuration commands are allowed within an applet configuration. Use the **show event manager policy registered** command to display a list of registered applets.

Before modifying an EEM applet, use the **no** form of this command to unregister the applet because the existing applet is not replaced until you exit applet configuration mode. While you are in applet configuration mode modifying the applet, the existing applet may be executing. When you exit applet configuration mode, the old applet is unregistered and the new version is registered.

Action configuration commands are uniquely identified using the *label* argument, which can be any string value. Actions are sorted in ascending alphanumeric key sequence using the *label* argument as the sort key and are run using this sequence.

The EEM schedules and runs policies on the basis of an event specification that is contained within the policy itself. When applet configuration mode is exited, EEM examines the event and action commands that are entered and registers the applet to be run when a specified event occurs.

Examples

The following example shows an EEM applet called IPSLAping1 being registered to run when there is an exact match on the value of a specified SNMP object ID that represents a successful IP SLA ICMP echo operation (this is equivalent to a **ping** command). Four actions are triggered when the echo operation fails, and event monitoring is disabled until after the second failure. A message that the ICMP echo operation to a server failed is sent to syslog, an SNMP trap is generated, EEM publishes an application-specific event, and a counter called IPSLA1F is incremented by a value of one.

```
Router(config)# event manager applet IPSLAping1
Router(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.42.1.2.9.1.6.4 get-type exact
entry-op eq entry-val 1 exit-op eq exit-val 2 poll-interval 5
Router(config-applet)# action 1.0 syslog priority critical msg "Server IP echo failed:
OID=$_snmp_oid_val"
Router(config-applet)# action 1.1 snmp-trap strdata "EEM detected server reachability
failure to 10.1.88.9"
Router(config-applet)# action 1.2 publish-event sub-system 88000101 type 1 arg1 10.1.88.9
arg2 IPSLAEcho arg3 fail
Router(config-applet)# action 1.3 counter name _IPSLA1F value 1 op inc
```

Related Commands

Command	Description
show event manager policy registered	Displays registered Embedded Event Manager policies.

event manager directory user

To specify a directory to use for storing user library files or user-defined Embedded Event Manager (EEM) policies, use the **event manager directory user** command in global configuration command. To disable use of a directory for storing user library files or user-defined EEM policies, use the **no** form of this command.

event manager directory user {**library** *path* | **policy** *path*}

no event manager directory user {**library** *path* | **policy** *path*}

Syntax Description

library	Specifies using the directory to store user library files.
policy	Specifies using the directory to store user-defined EEM policies.
path	Absolute pathname to the user directory on the flash device.

Command Default

No directory is specified for storing user library files or user-defined EEM policies.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

The user library directory is needed to store user library files associated with authoring EEM policies. If you have no plans to author EEM policies, you need not create a user library directory.

In Cisco IOS Release 12.3(14)T and later releases the software supports policy files created using the Tool Command Language (Tcl) scripting language. Tcl is provided in the Cisco IOS software image when the EEM is installed on the network device. Files with the .tcl extension can be EEM policies, Tcl library files, or a special Tcl library index file named “tclindex.” The tclindex file contains a list of user function names and the library files that contain the user functions. The EEM searches the user library directory when Tcl starts up to process the tclindex file.

To create the user library directory before identifying it to the EEM, use the **mkdir** command in privileged EXEC mode. After creating the user library directory, you can use the **copy** command to copy .tcl library files into the user library directory.

The user policy directory is needed to store user-defined policy files. If you have no plans to author EEM policies, you need not create a user policy directory. The EEM searches the user policy directory when you enter the **event manager policy** *policy-filename* **type user** command.

To create the user policy directory before identifying it to the EEM, use the **mkdir** command in privileged EXEC mode. After creating the user policy directory, you can use the **copy** command to copy policy files into the user policy directory.

Examples

The following example shows how to specify disk0:/user_library as the directory to use for storing user library files:

```
Router(config)# event manager directory user library disk0:/user_library
```

Related Commands

Command	Description
copy	Copies any file from a source to a destination.
event manager policy	Registers an EEM policy with the EEM.
mkdir	Creates a new directory in a Class C flash file system.

event manager environment

To set an Embedded Event Manager (EEM) environment variable, use the **event manager environment** command in global configuration mode. To disable an EEM environment variable, use the **no** form of this command.

event manager environment *variable-name string*

no event manager environment *variable-name*

Syntax Description

variable-name	Name assigned to the EEM environment variable.
string	Series of characters, including embedded spaces, to be placed in the environment variable *variable-name*.

Command Default

No EEM environment variables are set.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

By convention, the names of all environment variables defined by Cisco begin with an underscore character to set them apart: for example, _show_cmd.

To support embedded white spaces in the *string* argument, this command interprets everything after the *variable-name* argument to the end of the line to be part of the *string* argument.

To display the name and value of all EEM environment variables after you have configured them, use the **show event manager environment** command.

Examples

The following example of the **event manager environment** command defines a set of EEM environment variables:

```
Router(config)# event manager environment _cron_entry 0-59/2 0-23/1 * * 0-7
Router(config)# event manager environment _show_cmd show version
```

Related Commands

Command	Description
show event manager environment	Displays the name and value of all EEM environment variables.

event manager history size

To change the size of Embedded Event Manager (EEM) history tables, use the **event manager history size** command in global configuration mode. To restore the default history table size, use the **no** form of this command.

event manager history size {**events** | **traps**} [*size*]

no event manager history size {**events** | **traps**}

Syntax Description

events	Changes the size of the EEM event history table.
traps	Changes the size of the EEM Simple Network Management Protocol (SNMP) trap history table.
size	(Optional) Integer in the range from 1 to 50 that specifies the number of history table entries. Default is 50.

Command Default

The size of the history table is 50 entries.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Examples

The following example of the **event manager history size** command changes the size of the SNMP trap history table to 30 entries:

```
Router(config)# event manager history size traps 30
```

Related Commands

Command	Description
show event manager history events	Displays the EEM events that have been triggered.
show event manager history traps	Displays the EEM SNMP traps that have been sent.

event manager policy

To register an Embedded Event Manager (EEM) policy with the EEM, use the **event manager policy** command in global configuration mode. To remove the **event manager policy** command from the configuration file, use the **no** form of this command.

event manager policy *policy-filename* [**type** {**system** | **user**}] [**trap**]

no event manager policy *policy-filename*

Syntax Description

policy-filename	Name of the policy file.
type	(Optional) Specifies the type of EEM policy to be registered.
system	(Optional) Registers a Cisco-defined system policy.
user	(Optional) Registers a user-defined policy.
trap	(Optional) Generates a Simple Network Management Protocol (SNMP) trap when the policy is triggered.

Command Default

No EEM policies are registered.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	The **user** keyword was added, and this command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

The EEM schedules and runs policies on the basis of an event specification that is contained within the policy itself. When the **event manager policy** command is invoked, the EEM examines the policy and registers it to be run when the specified event occurs.

If you enter the **event manager policy** command without specifying the optional **type** keyword, the EEM first tries to locate the specified policy file in the system policy directory. If the EEM finds the file in the system policy directory, it registers the policy as a system policy. If the EEM does not find the specified policy file in the system policy directory, it looks in the user policy directory. If the EEM locates the specified file in the user policy directory, it registers the policy file as a user policy. If the EEM finds policy files with the same name in both the system policy directory and the user policy directory, the policy file in the system policy directory takes precedence and is registered as a system policy.

Examples

The following example shows how to use the **event manager policy** command to register a system-defined policy named tm_cli_cmd.tcl located in the system policy directory:

```
Router(config)# event manager policy tm_cli_cmd.tcl type system
```

The following example shows how to use the **event manager policy** command to register a user-defined policy named cron.tcl located in the user policy directory:

```
Router(config)# event manager policy cron.tcl type user
```

Related Commands

Command	Description
show event manager policy registered	Displays registered EEM policies.

event manager run

To manually run a registered Embedded Event Manager (EEM) policy, use the **event manager run** command in privileged EXEC mode.

event manager run *policy-filename*

Syntax Description

policy-filename	Name of the policy file.

Command Default

No registered EEM policies are run.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

EEM usually schedules and runs policies on the basis of an event specification that is contained within the policy itself. The **event manager run** command allows policies to be run manually. Before this command is used, the **event none** command must be configured in applet configuration for the specified policy to indicate to EEM that the policy is to be run manually.

This command does not have a **no** form.

Examples

The following example of the **event manager run** command manually runs an EEM policy named policy-manual.tcl:

```
Router# event manager run policy-manual.tcl
```

Related Commands

Command	Description
event manager applet	Registers an EEM applet with EEM and enters applet configuration mode.
event manager policy	Registers an EEM policy with EEM.

Command	Description
event none	Registers an EEM policy with EEM and indicates that the policy may be run manually.
show event manager policy registered	Displays registered EEM policies.

event manager scheduler script

To set the Embedded Event Manager (EEM) script scheduling options, use the **event manager scheduler script** command in global configuration mode. To remove the EEM script scheduling options and restore the default value, use the **no** form of this command.

event manager scheduler script thread class default number *default-number*

no event manager scheduler script thread class default number *default-number*

Syntax Description

thread class default number	Specifies the number of concurrent script execution threads. Each script execution thread is used by one EEM policy as it executes.
default-number	Number of concurrent script execution threads. The default is one script execution thread.

Command Default

Only one EEM policy can be run at a time.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

Use the **event manager scheduler script** command if you want more than one EEM policy to run concurrently.

Examples

The following example shows how to specify two script execution threads to run concurrently:

```
Router(config)# event manager scheduler script thread class default number 2
```

event manager scheduler suspend

To immediately suspend Embedded Event Manager (EEM) policy scheduling execution, use the **event manager scheduler suspend** command in global configuration mode. To resume EEM policy scheduling, use the **no** form of this command.

event manager scheduler suspend

no event manager scheduler suspend

Syntax Description

This command has no arguments or keywords.

Command Default

Policy scheduling is active.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

Use the **event manager scheduler suspend** command to suspend all policy scheduling requests and do no scheduling until you enter the **no** form of the command. The **no** form of the command resumes policy scheduling and executes any pending policies.

You might want to suspend policy execution immediately instead of unregistering policies one by one for the following reasons:

- For security—if you think the security of your system has been compromised.
- For performance—if you want to suspend policy execution temporarily to make more CPU cycles available for other functions.

Examples

The following example of the **event manager scheduler suspend** command disables policy scheduling:

```
Router(config)# event manager scheduler suspend

May 19 14:31:22.439: fm_server[12330]: %HA_EM-6-FMS_POLICY_EXEC: fh_io_msg: Policy
execution has been suspended
```

The following example of the **event manager scheduler suspend** command enables policy scheduling:

```
Router(config)# no event manager scheduler suspend

May 19 14:31:40.449: fm_server[12330]: %HA_EM-6-FMS_POLICY_EXEC: fh_io_msg: Policy
execution has been resumed
```

Related Commands

Command	Description
event manager policy	Registers an EEM policy with the EEM.

event manager session cli username

To associate a username with Embedded Event Manager (EEM) policies that use the command-line interface (CLI) library, use the **event manager session cli username** command in global configuration mode. To remove the username association with EEM policies that use the CLI library, use the **no** form of this command.

event manager session cli username *username*

no event manager session cli username *username*

Syntax Description

username	Username assigned to EEM CLI sessions that are initiated by EEM policies.

Command Default

No username is associated with EEM CLI sessions.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

Use the **event manager session cli username** command to assign a username for EEM policy CLI sessions when TACACS+ is used for command authorization.

If you are using authentication, authorization, and accounting (AAA) security and implement authorization on a command basis, you should use the **event manager session cli username** command to set a username to be associated with a Tool Command Language (Tcl) session. The username is used when a Tcl policy executes a CLI command. TACACS+ verifies each CLI command using the username associated with the Tcl session that is running the policy. Commands from Tcl policies are not usually verified because the router must be in privileged EXEC mode to register the policy.

Examples

The following example of the **event manager session cli username** command associates the username eemuser with EEM CLI sessions initiated by EEM policies:

```
Router(config)# event manager session cli username eemuser
```

Related Commands

Command	Description
show event manager session cli username	Displays the username associated with CLI sessions initiated by EEM policies that use the EEM CLI library.

event none

To specify that an Embedded Event Manager (EEM) policy is to be registered with the EEM and can be run manually, use the **event none** command in applet configuration mode. To remove the **event none** command from the configuration file, use the **no** form of this command.

event none

no event none

Syntax Description

This command has no arguments or keywords.

Command Default

No EEM policies are specified to be run manually.

Command Modes

Applet configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

EEM usually schedules and runs policies on the basis of an event specification that is contained within the policy itself. The **event none** command allows EEM to identify an EEM policy that can either be run manually or be run when an EEM applet is triggered. To run the policy, use either the **action policy** command in applet configuration mode or the **event manager run** command in global configuration mode.

Examples

The following example shows how to register a policy named manual-policy to be run manually and then how to execute the policy:

```
Router(config)# event manager applet manual-policy
Router(config-applet)# event none
Router(config-applet)# exit
Router(config)# event manager run manual-policy
```

Related Commands

Command	Description
action policy	Registers an EEM policy with EEM.
event manager applet	Registers an EEM applet with EEM and enters applet configuration mode.
event manager run	Manually runs a registered EEM policy.
show event manager policy registered	Displays registered EEM policies.

event oir

To specify that an Embedded Event Manager (EEM) applet be run on the basis of an event raised when a hardware card online insertion and removal (OIR) occurs, use the **event oir** command in applet configuration mode. To remove the **event oir** command from the configuration, use the **no** form of this command.

event oir

no event oir

Syntax Description

This command has no arguments or keywords.

Command Default

No EEM applets are run on the basis of an OIR event.

Command Modes

Applet configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Examples

The following example shows how to configure an EEM applet to be run on the basis of an OIR event:

```
Router(config)# event manager applet oir-event
Router(config-applet)# event oir
Router(config-applet)# exit
```

Related Commands

Command	Description
event manager applet	Registers an EEM applet with EEM and enters applet configuration mode.

event resource

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of an Embedded Resource Manager (ERM) event report for a specified policy, use the **event resource** command in applet configuration mode. To remove the report event criteria, use the **no** form of this command.

event [*label*] **resource policy** *policy-filename*

no event [*label*] **resource policy** *policy-filename*

Syntax Description

label	(Optional) Unique identifier that can be any string. If the string contains embedded blanks, enclose it in double quotation marks.
policy	Indicates that a specific policy is identified.
policy-filename	Policy name.

Command Default

No EEM event criteria are specified.

Command Modes

Applet configuration (config-applet)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(31)SB3	This command was integrated into Cisco IOS Release 12.2(31)SB3.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The resource event detector publishes an event when the ERM reports an event for the specified policy. The ERM infrastructure tracks resource depletion and resource dependencies across processes and within a system to handle various error conditions. The error conditions are handled by providing an equitable sharing of resources between various applications. The ERM framework provides a communication mechanism for resource entities and allows communication between these resource entities from numerous locations. The ERM framework also helps in debugging the CPU and memory-related issues. The ERM monitors system resource usage to better understand scalability needs by allowing you to configure threshold values for resources such as CPU, buffer, and memory.

Examples

The following example shows how to specify event criteria based on an ERM event report for a policy defined to report high CPU usage:

```
Router(config)# event manager applet policy-one
Router(config-applet)# event resource policy cpu-high
Router(config-applet)# action 1.0 syslog msg "CPU high at $_resource_current_value
percent"
```

Related Commands

Command	Description
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

event rf

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of Redundancy Framework (RF) state change notifications, use the **event rf** command in applet configuration mode. To remove the RF event criteria, use the **no** form of this command.

event rf event *rf-state-name*

no event rf event *rf-state-name*

Syntax Description

event	Compares the regular expression contained in the *rf-state-name* argument with an RF state change notification. If there is a match, an event is triggered. The *rf-state-name* argument takes one of the following values: • RF_EVENT_CLIENT_PROGRESSION • RF_EVENT_CONTINUE_PROGRESSION • RF_EVENT_GO_ACTIVE • RF_EVENT_GO_ACTIVE_EXTRALOAD • RF_EVENT_GO_ACTIVE_HANDBACK • RF_EVENT_GO_STANDBY • RF_EVENT_KEEP_ALIVE • RF_EVENT_KEEP_ALIVE_TMO • RF_EVENT_LOCAL_PROG_DONE • RF_EVENT_NEGOTIATE • RF_EVENT_NOTIFICATION_TMO • RF_EVENT_PEER_PROG_DONE • RF_EVENT_STANDBY_PROGRESSION • RF_EVENT_START_PROGRESSION • RF_EVENT_SWACT_INHIBIT_TMO • RF_PROG_ACTIVE • RF_PROG_ACTIVE_DRAIN • RF_PROG_ACTIVE_FAST • RF_PROG_ACTIVE_POSTCONFIG • RF_PROG_ACTIVE_PRECONFIG • RF_PROG_EXTRALOAD • RF_PROG_HANDBACK • RF_PROG_INITIALIZATION • RF_PROG_PLATFORM_SYNC

- RF_PROG_STANDBY_BULK
- RF_PROG_STANDBY_COLD
- RF_PROG_STANDBY_CONFIG
- RF_PROG_STANDBY_FILESYS
- RF_PROG_STANDBY_HOT
- RF_REGISTRATION_STATUS
- RF_STATUS_MAINTENANCE_ENABLE
- RF_STATUS_MANUAL_SWACT
- RF_STATUS_OPER_REDUNDANCY_MODE_CHANGE
- RF_STATUS_PEER_COMM
- RF_STATUS_PEER_PRESENCE
- RF_STATUS_REDUNDANCY_MODE_CHANGE
- RF_STATUS_SWACT_INHIBIT

Command Default

No EEM events are triggered.

Command Modes

Applet configuration (config-applet)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(31)SB3	This command was integrated into Cisco IOS Release 12.2(31)SB3.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

An EEM event is triggered when the expression in the *rf-state-name* argument matches an RF state change notification. The RF event detector publishes an event when one or more RF events occur during synchronization in a dual Route Processor (RP) system.

Examples

The following example shows how to specify event criteria based on an RF state change notification:

```
Router(config)# event manager applet start-rf
Router(config-applet)# event rf event rf_prog_initialization
Router(config-applet)# action 1.0 syslog msg "rf state rf_prog_initialization reached"
```

Related Commands

Command	Description
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

event snmp

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run by sampling Simple Network Management Protocol (SNMP) object identifier values, use the **event snmp** command in applet configuration mode. To remove the SNMP event criteria, use the **no** form of this command.

event snmp oid *oid-value* **get-type** {**exact** | **next**} **entry-op** *operator* **entry-val** *entry-value* [**entry-type** {**value** | **increment** | **rate**}] [**exit-comb** {**or** | **and**}] [**exit-op** *operator*] [**exit-val** *exit-value*] [**exit-type** {**value** | **increment** | **rate**}] [**exit-time** *exit-time-value*] [**exit-event** {**true** | **false**}] [**average-factor** *average-factor-value*] **poll-interval** *poll-int-value*

no event snmp oid *oid-value* **get-type** {**exact** | **next**} **entry-op** *operator* **entry-val** *entry-value* [**entry-type** {**value** | **increment** | **rate**}] [**exit-comb** {**or** | **and**}] [**exit-op** *operator*] [**exit-val** *exit-value*] [**exit-type** {**value** | **increment** | **rate**}] [**exit-time** *exit-time-value*] [**exit-event** {**true** | **false**}] [**average-factor** *average-factor-value*] **poll-interval** *poll-int-value*

Syntax Description

oid	Specifies the SNMP object identifier (object ID) values in the *oid-value* argument as the event criteria.
oid-value	Object ID value of the data element, in SNMP dotted notation. An OID is defined as a type in the associated MIB, CISCO-EMBEDDED-EVENT-MGR-MIB, and each type has an object value. Monitoring of some OID types is supported. When the **oid** keyword is used, an error message is returned if the OID is not one of the following: • INTEGER_TYPE • COUNTER_TYPE • GAUGE_TYPE • TIME_TICKS_TYPE • COUNTER_64_TYPE • OCTET_PRIM_TYPE • OPAQUE_PRIM_TYPE
get-type	Specifies the type of SNMP get operation to be applied to the object ID specified by the *oid-value* argument.
exact	Retrieves the object ID specified by the *oid-value* argument.
next	Retrieves the object ID that is the alphanumeric successor to the object ID specified by the *oid-value* argument.
entry-op	Compares the contents of the current object ID with the entry value using the specified operator. If there is a match, an event is triggered and event monitoring is disabled until the exit criteria are met.

operator	Two-character string. The *operator* argument takes one of the following values: - **gt**—Greater than. - **ge**—Greater than or equal to. - **eq**—Equal to. - **ne**—Not equal to. - **lt**—Less than. - **le**—Less than or equal to.
entry-val	Specifies the value with which the contents of the current object ID are compared to decide if an SNMP event should be raised.
entry-value	Entry object ID value of the data element.
entry-type	(Optional) Specifies a type of operation to be applied to the object ID specified by the *entry-value* argument. If not specified, the value is assumed.
value	(Optional) When used with the **entry-type** keyword, **value** specifies that an SNMP event should be raised based on a comparison of the absolute value of the *entry-value* argument. When used with the **exit-type** keyword, **value** specifies that event monitoring will be reenabled based on the absolute value of the *exit-value* argument.
increment	(Optional) When used with the **entry-type** keyword, **increment** specifies that an SNMP event should be raised base on a comparison of the incremental value of the *entry-value* argument since the last poll interval. When used with the **exit-type** keyword, **increment** specifies that event monitoring will be reenabled based on a comparison of the incremental value of the *exit-value* argument since the last poll interval.
rate	(Optional) Rate is defined as the sum of the incremental difference for the sample taken at each poll interval compared to the previous sample divided by the period. The period is defined as the average factor times the poll interval. An event is triggered or event monitoring is reenabled based on a comparison of the derived rate value. When used with the **entry-type** keyword, **rate** specifies that an SNMP event should be raised based on a comparison of the rate of change of the *entry-value* argument over a period. When used with the **exit-type** keyword, **rate** specifies that event monitoring will be reenabled based on a comparison of the rate of change of the *exit-value* argument over a period.
exit-comb	(Optional) Indicates the combination of exit conditions that must be met before event monitoring is reenabled.
or	(Optional) Specifies that an exit comparison operator and an exit object ID value or an exit time value must exist.
and	(Optional) Specifies that an exit comparison operator, an exit object ID value, and an exit time value must exist.
exit-op	(Optional) Compares the contents of the current object ID with the exit value using the specified operator. If there is a match, an event is triggered and event monitoring is reenabled.

exit-val	(Optional) Specifies the value with which the contents of the current object ID are compared to decide whether the exit criteria are met.
exit-value	(Optional) Exit object ID value of the data element.
exit-type	(Optional) Specifies a type of operation to be applied to the object ID specified by the *exit-value* argument. If not specified, the value is assumed.
exit-time	(Optional) Specifies the time period after which the event monitoring is reenabled. The timing starts after the event is triggered.
exit-time-value	(Optional) Number that represents seconds and optional milliseconds in the format ssssss[.mmm]. The range for seconds is from 0 to 4294967295. The range for milliseconds is from 0 to 999. If only milliseconds are used, the format is 0.mmm.
exit-event	(Optional) Indicates whether a separate exit event is to be triggered when event monitoring is enabled after an initial event is triggered.
true	(Optional) Specifies that a separate exit event is triggered.
false	(Optional) Specifies that a separate exit event is not triggered. This is the default.
average-factor	(Optional) Specifies a number used to calculate the period used for rate-based calculations. The *average-factor-value* is multiplied by the *poll-int-value* to derive the period in milliseconds.
average-factor-value	(Optional) Number in the range from 1 to 64. The minimum average factor value is 1.
poll-interval	Specifies the time interval between consecutive polls.
poll-int-value	Number that represents seconds and optional milliseconds in the format ssssss[.mmm]. The range for seconds is from 1 to 4294967295. The range for milliseconds is from 0 to 999. The minimum polling interval is 1 second.

Command Default

No EEM events are triggered on the basis of SNMP object identifier values.

Command Modes

Applet configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	Optional keywords to support SNMP rate-based events were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

An EEM event is triggered when one of the fields specified by an SNMP object ID crosses a defined threshold. If multiple conditions exist, the SNMP event will be triggered when all the conditions are met.

Exit criteria are optional. If exit criteria are not specified, event monitoring will be reenabled immediately. If exit criteria are specified—on the basis of values or time periods—event monitoring is not reenabled until the criteria are met.

An OID is defined as a type in the associated MIB, CISCO-EMBEDDED-EVENT-MGR-MIB, and each type has an object value. Monitoring of some OID types is supported. When the **oid** keyword is used, an error message is returned if the OID is not one of the following:

- INTEGER_TYPE
- COUNTER_TYPE
- GAUGE_TYPE
- TIME_TICKS_TYPE
- COUNTER_64_TYPE
- OCTET_PRIM_TYPE
- OPAQUE_PRIM_TYPE

When the **entry-op** keyword is used and there is a match, an event is triggered and event monitoring is disabled until the exit criteria are met.

When the **exit-op** keyword is used and there is a match, an event is triggered and event monitoring is reenabled.

The *operator* argument takes one of the following values:

- **gt**—Greater than.
- **ge**—Greater than or equal to.
- **eq**—Equal to.
- **ne**—Not equal to.
- **lt**—Less than.
- **le**—Less than or equal to.

Rate is defined as the sum of the incremental difference for the sample taken at each poll interval compared to the previous sample divided by the period. The period is defined as the average factor times the poll interval. An event is triggered or event monitoring is reenabled based on a comparison of the derived rate value.

The increment and rate types are supported only for the following OID types: INTEGER_TYPE, COUNTER_TYPE, and COUNTER_64_TYPE.

Examples

The following example shows how an EEM applet called memory-fail will run when there is an exact match on the value of a specified SNMP object ID that represents the amount of current process memory. A message saying that process memory is exhausted and noting the current available memory will be sent to syslog.

```
Router(config)# event manager applet memory-fail
Router(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.48.1.1.1.6.1 get-type exact entry-op
lt entry-val 5120000 poll-interval 10
Router(config-applet)# action 1.0 syslog msg "Memory exhausted; current available memory
is $_snmp_oid_val bytes"
```

The following example shows an EEM applet called IPSLAping1 being registered to run when there is an exact match on the value of a specified SNMP object ID that represents a successful IP SLA ICMP echo operation (this is equivalent to a **ping** command). Four actions are triggered when the echo operation fails, and event monitoring is disabled until after the second failure.

A message saying that the ICMP echo operation to a server failed is sent to syslog, an SNMP trap is generated, EEM publishes an application-specific event, and a counter called IPSLA1F is incremented by a value of one.

```
Router(config)# event manager applet IPSLAping1
Router(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.42.1.2.9.1.6.4 get-type exact
entry-op eq entry-val 1 exit-op eq exit-val 2 poll-interval 5
Router(config-applet)# action 1.0 syslog priority critical msg "Server IP echo failed:
OID=$_snmp_oid_val"
Router(config-applet)# action 1.1 snmp-trap strdata "EEM detected server reachability
failure to 10.1.88.9"
Router(config-applet)# action 1.2 publish-event sub-system 88000101 type 1 arg1 10.1.88.9
arg2 IPSLAEcho arg3 fail
```

Related Commands

Command	Description
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

event syslog

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run by matching syslog messages, use the **event syslog** command in applet configuration mode. To remove the syslog message event criteria, use the **no** form of this command.

event syslog pattern *regular-expression* [**occurs** *num-occurrences*] [**period** *period-value*] [**priority** *priority-level*] [*severity-level*]

no event syslog pattern *regular-expression* [**occurs** *num-occurrences*] [**period** *period-value*] [**priority** *priority-level*] [*severity-level*]

Syntax Description

pattern	Specifies that a regular expression is used to perform the syslog message pattern match.
regular-expression	String value that is the pattern to be matched.
occurs	(Optional) Specifies the number of matching occurrences before an EEM event is triggered. If a number is not specified, an EEM event is triggered after the first match.
num-occurrences	(Optional) Integer in the range of 1 to 32, inclusive.
period	(Optional) Specifies the time interval during which the one or more occurrences must take place. If the **period** keyword is not specified, no time-period check is applied.
period-value	(Optional) Number that represents seconds and optional milliseconds in the format ssssss[.mmm]. The range for seconds is from 0 to 4294967295. The range for milliseconds is from 0 to 999. If using milliseconds only, specify the milliseconds in the format 0.mmm.
priority	(Optional) Specifies the priority level of the syslog messages to be screened. If this keyword is selected, the *priority-level* argument must be defined. If this keyword is not specified, the software will use the default of **priority all**, and all priorities will be considered when log messages are screened.
priority-level	(Optional) Number or name of the desired priority level against which syslog messages are matched. Messages at or numerically lower than the specified level are matched. Valid levels for the *priority-level* argument are as follows (enter the keyword or number, if available): • **all**—All priorities are considered when log messages are screened. • {**0** | **emergencies**}—System is unusable. • {**1** | **alerts**}—Immediate action is needed. • {**2** | **critical**}—Critical conditions. • {**3** | **errors**}—Error conditions.

	• {**4** | **warnings**}—Warning conditions. • {**5** | **notifications**}—Normal but significant conditions. • {**6** | **informational**}—Informational messages. • {**7** | **debugging**}—Debugging messages.
severity-level	(Optional) Specifies the severity level of the syslog messages to be screened. If no severity level is specified, the software will not use any severity filtering and all events will be considered when log messages are screened. The *severity-level* argument may be one or more of the following keywords: • **severity-critical**—Critical conditions. • **severity-debugging**—Debugging messages. • **severity-fatal**—Fatal conditions. • **severity-major**—Major conditions. • **severity-minor**—Minor conditions. • **severity-normal**—Normal conditions. • **severity-notification**—Significant conditions. • **severity-warning**—Warning conditions.

Command Default

No EEM events are triggered on the basis of matches with syslog messages.

Command Modes

Applet configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	Optional severity-level keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

Use the **event syslog** command to set up event criteria against which syslog messages are matched. Syslog messages are compared against a specified regular expression. After a specified number of matches occurs within a specified time period, an EEM event is triggered. If multiple conditions exist, the EEM event is triggered when all the conditions are met.

Valid levels for the *priority-level* argument are as follows (enter the keyword or number, if available):

- **all**—All priorities are considered when log messages are screened.
- {**0** | **emergencies**}—System is unusable.
- {**1** | **alerts**}—Immediate action is needed.
- {**2** | **critical**}—Critical conditions.
- {**3** | **errors**}—Error conditions.
- {**4** | **warnings**}—Warning conditions.
- {**5** | **notifications**}—Normal but significant conditions.
- {**6** | **informational**}—Informational messages.
- {**7** | **debugging**}—Debugging messages.

The *severity-level* argument may be one or more of the following keywords:

- **severity-critical**—Critical conditions.
- **severity-debugging**—Debugging messages.
- **severity-fatal**—Fatal conditions.
- **severity-major**—Major conditions.
- **severity-minor**—Minor conditions.
- **severity-normal**—Normal conditions.
- **severity-notification**—Significant conditions.
- **severity-warning**—Warning conditions.

Examples

The following example shows how to specify an EEM applet to run when syslog identifies that Ethernet interface 1/0 is down. The applet sends a message about the interface to syslog.

```
Router(config)# event manager applet interface-down
Router(config-applet)# event syslog pattern {.*UPDOWN.*Ethernet1/0.*} occurs 4
```

Related Commands

Command	Description
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

event timer

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of time-specific events, use the **event timer** command in applet configuration mode. To remove the time-specific event criteria, use the **no** form of this command.

event timer {**absolute time** *time-value* | **countdown time** *time-value* | **cron cron-entry** *cron-entry* | **watchdog time** *time-value*} [**name** *timer-name*]

no event timer {**absolute time** *time-value* | **countdown time** *time-value* | **cron cron-entry** *cron-entry* | **watchdog time** *time-value*} [**name** *timer-name*]

Syntax Description

absolute	Specifies that an event is triggered when the specified absolute time of day occurs.
time	Specifies the time interval during which the event must take place.
time-value	Integer that specifies, in seconds and optional milliseconds, the time interval during which the event must take place. The range for seconds is from 0 to 4294967295 and the range for milliseconds is from 0 to 999. The format is ssssss[.mmm]. When only milliseconds are specified, use the format 0.mmm.
countdown	Specifies that an event is triggered when the specified time counts down to zero. The timer does not reset.
cron	Specifies that an event is triggered when the CRON string specification matches the current time.
cron-entry	Specifies the first five fields of a UNIX crontab entry as used with the UNIX CRON daemon.
cron-entry	Text string that consists of five fields separated by spaces. The fields represent the times and dates when CRON timer events will be triggered. Fields and corresponding values are as follows: – *minute*—A number in the range from 0 to 59 that specifies when a CRON timer event is triggered. – *hour*—A number in the range from 0 to 23 that specifies when a CRON timer event is triggered. – *day-of-month*—A number in the range from 1 to 31 that specifies the day of the month when a CRON timer event is triggered. – *month*—A number in the range from 1 to 12 or the first three letters (not case-sensitive) of the name of the month in which a CRON timer event is triggered. – *day-of-week*—A number in the range from 0 to 6 (Sunday is 0) or the first three letters (not case-sensitive) of the name of the day when a CRON timer event is triggered. Instead of the first five fields, special strings can be entered. See the “Usage Guidelines” section for details.
watchdog	Specifies that an event is triggered when the specified time counts down to zero. The timer automatically resets to the initial value and continues to count down.

name	(Optional) Specifies that the timer is named.
timer-name	(Optional) Name of the timer.

Command Default

No EEM events are triggered on the basis of time-specific events.

Command Modes

Applet configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

For the *cron-entry* argument, the following special strings also are allowed in syntax:

- Range of numbers—The specified range is inclusive, and a hyphen separates the numbers. For example, 8-11 after the hour field specifies execution of a CRON timer event at hours 8, 9, 10, and 11.
- Asterisk (*)—Indicates that a field is not specified and can be any value.
- List—A list is a set of numbers or ranges separated by a comma but no space. For example, 1,2,5,9 or 0-4,8-12.
- Step value in conjunction with a range—Following a range with /*number* specifies skips of the *number* value through the range. For example, 0-23/2 in the hour field specifies that an event is triggered every second hour. Steps are permitted after an asterisk, for example */2 means every two hours.

Instead of the five fields of a UNIX crontab entry for the *cron-entry* argument, one of the following seven special strings can be entered:

- **@yearly**—An event is triggered once a year. This is the equivalent of specifying 0 0 1 1 * for the first five fields.
- **@annually**—Same as **@yearly**.
- **@monthly**—An event is triggered once a month. This is the equivalent of specifying 0 0 1 * * for the first five fields.
- **@weekly**—An event is triggered once a week. This is the equivalent of specifying 0 0 * * 0 for the first five fields.
- **@daily**—An event is triggered once a day. This is the equivalent of specifying 0 0 * * * for the first five fields.

- **@midnight**—Same as **@daily**.
- **@hourly**—An event is triggered once an hour. This is the equivalent of specifying 0 * * * * for the first five fields.

A CRON timer may not produce the intended result if the time-of-day clock is not set to the correct time. Network Time Protocol (NTP) services can be used to facilitate keeping an accurate time-of-day clock setting. For more details on NTP configuration, see the "Performing Basic System Management" chapter of the *Cisco IOS Network Management Configuration Guide*, Release 12.4.

Examples

The following example shows how to specify that an event is triggered one time after 5 hours:

```
Router(config)# event manager applet timer-absolute
Router(config-applet)# event timer absolute time 18000
```

The following example shows how to specify that an event is triggered once after 6 minutes and 6 milliseconds:

```
Router(config)# event manager applet timer-set
Router(config-applet)# event timer countdown time 360.006 name six-minutes
```

The following example shows how to specify that an event is triggered at 1:01 a.m. on January 1 each year:

```
Router(config)# event manager applet timer-cron1
Router(config-applet)# event timer cron cron-entry 1 1 1 1 * name Jan1
```

The following example shows how to specify that an event is triggered at noon on Monday through Friday of every week:

```
Router(config)# event manager applet timer-cron2
Router(config-applet)# event timer cron cron-entry 0 12 * * 1-5 name MonFri
```

The following example shows how to specify that an event is triggered at midnight on Sunday every week:

```
Router(config)# event manager applet timer-cron3
Router(config-applet)# event timer cron cron-entry @weekly name Sunday
```

The following example shows how to specify that an event is triggered every 5 hours:

```
Router(config)# event manager applet timer-watch
Router(config-applet)# event timer watchdog time 18000
```

Related Commands

Command	Description
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

event track

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of a Cisco IOS Object Tracking subsystem report for the specified object number, use the **event track** command in applet configuration mode. To remove the report event criteria, use the **no** form of this command.

event [*label*] **track** *object-number* [**state** {**up** | **down** | **any**}]

no event [*label*] **track** *object-number* [**state** {**up** | **down** | **any**}]

Syntax Description

label	(Optional) Unique identifier that can be any string. If the string contains embedded blanks, enclose it in double quotation marks.
object-number	Tracked object number in the range from 1 to 500, inclusive. The number is defined using the **track stub** command.
state	(Optional) Specifies that the tracked object transition will cause an event to be raised.
up	(Optional) Specifies that an event will be raised when the tracked object transitions from a down state to an up state.
down	(Optional) Specifies that an event will be raised when the tracked object transitions from an up state to a down state.
any	(Optional) Specifies that an event will be raised when the tracked object transitions to or from any state. This is the default.

Command Default

No EEM event criteria are specified.

Command Modes

Applet configuration (config-applet)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(31)SB3	This command was integrated into Cisco IOS Release 12.2(31)SB3.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

There are two entry variables associated with this command:

- _track_number—Number of the tracked object that caused the event to be triggered.
- _track_state—State of the tracked object when the event was triggered; valid states are “up” or “down.”

This command is used to help track objects using EEM. Each tracked object is identified by a unique number that is specified on the tracking command-line interface (CLI). Client processes such as EEM use this number to track a specific object. The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to interested client processes, either immediately or after a specified delay. The object values are reported as either up or down.

Examples

The following example shows how to specify event criteria based on a tracked object:

```
event manager applet track-ten
 event track 10 state any
 action 1.0 track set 10 state up
 action 2.0 track read 10
```

Related Commands

Command	Description
action track read	Specifies the action of reading the state of a tracked object when an EEM applet is triggered.
action track set	Specifies the action of setting the state of a tracked object when an EEM applet is triggered.
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.
show track	Displays tracking information.
track stub	Creates a stub object to be tracked.

exception core-file

To specify the name of the core dump file in Cisco IOS or Cisco IOS Software Modularity software, use the **exception core-file** command in global configuration mode. To return to the default core filename, use the **no** form of this command.

Cisco IOS Software

exception core-file *filename*

no exception core-file

Cisco IOS Software Modularity

exception core-file [*filename*] [**limit** *upper-limit*] [**compress**] [**timestamp**]

no exception core-file

Syntax Description

filename	Name of the core dump file saved on the server. (Optional) In Software Modularity images, if this argument is not specified, the default core file is named using the name of the process that is being dumped. For example, if the raw_ip.proc is the process that is being dumped, then the default core file is named raw_ip.proc.
limit	(Optional) For Cisco IOS Software Modularity images only. Specifies an upper limit of a range so that core dumps of more than one process can be created without overwriting the previous core dump.
upper-limit	(Optional) For Cisco IOS Software Modularity images only. Number, in the range from 1 to 64, that represents the upper limit.
compress	(Optional) For Cisco IOS Software Modularity images only. Turns on dump file compression. By default, compression is turned off.
timestamp	(Optional) For Cisco IOS Software Modularity images only. Adds a time stamp to the core dump file.

Command Default

Cisco IOS Software: The core file is named *hostname*-core, where *hostname* is the name of the router.
Cisco IOS Software Modularity: The core file is named using the name of the process that is being dumped.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.2	This command was introduced.
12.2(18)SXF4	The **limit**, **compress**, and **timestamp** keywords were added to support Software Modularity images.

Usage Guidelines

If you use TFTP to dump the core file to a server, the router will only dump the first 16 MB of the core file. If the router's memory is larger than 16 MB, the whole core file will not be copied to the server. Therefore, use rcp or FTP to dump the core file. The network dump is not supported in Software Modularity images.

Caution This command is of use only to Cisco technical support representatives in analyzing system failures in the field. Under normal circumstances, there should be no reason to change the default core filename. For that reason, this command should be used only by Cisco Certified Internetwork Experts (CCIEs) or under the direction of Cisco Technical Assistance Center (TAC) personnel.

Examples

Cisco IOS Software

In the following example, the router is configured to use FTP to dump a core file named dumpfile to the FTP server at 172.17.92.2 when the router crashes:

```
ip ftp username red
ip ftp password blue
exception protocol ftp
exception dump 172.17.92.2
exception core-file dumpfile
```

Cisco IOS Software Modularity

In the following example, the router is configured to dump the main memory used by the TCP process to a file named dump-tcp when the TCP process crashes. The dump file is configured with an upper limit of 20, to be compressed, and to have a time stamp applied.

```
exception core tcp.proc mainmem
exception core-file dump-tcp limit 20 compress timestamp
```

Note The **exception protocol** and **exception dump** commands are not supported in Software Modularity images.

Related Commands

Command	Description
exception core	Sets or changes the core dump options for a Cisco IOS Software Modularity process.
exception dump	Causes the router to dump a core file to a particular server when the router crashes.
exception memory	Causes the router to create a core dump and reboot when certain memory size parameters are violated.
exception protocol	Configures the protocol used for core dumps.
exception spurious-interrupt	Causes the router to create a core dump and reload after a specified number of spurious interrupts.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the username for FTP connections.

exception crashinfo buffersize

To change the size of the buffer used for crash info files, use the **exception crashinfo buffersize** command in global configuration mode. To revert to the default buffer size, use the **no** form of this command.

exception crashinfo buffersize *kilobytes*

no exception crashinfo buffersize *kilobytes*

Syntax Description

kilobytes	Buffer size, in kilobytes (KB). Range is 32 to 256. Default is 32.

Command Default

Crashinfo buffer is 32 KB.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)T, 12.2(11)	This command was introduced for the Cisco 3600 series only (3620, 3640, and 3660 platforms).
12.2(13)T	This command was implemented in 6400-NSP images.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.2(18)SXF4	This command was integrated into Release 12.2(18)SXF4 to support Software Modularity images.

Usage Guidelines

The crash info file saves information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). The device writes the crash information to the console at the time of the failure, and the file is created the next time you boot the Cisco IOS image after the failure (instead of while the system is failing).

Note If you are running a Software Modularity image, setting the crash info buffer size to the default of 32 KB does not limit the crash info buffer size. The crash info file size is limited to the value set if the value is set to anything other than the default 32 KB.

Examples

In the following example, the crash info buffer is set to 100 KB:

```
Router(config)# exception crashinfo buffersize 100
```

Related Commands

Command	Description
exception crashinfo file	Enables the creation of a diagnostic file at the time of unexpected system shutdowns.

exception crashinfo dump

To specify the type of output information to be written to the crashinfo file, use the **exception crashinfo dump** command in global configuration mode. To remove this information from the crashinfo file, use the **no** form of this command.

exception crashinfo dump {**command** *cli* | **garbage-detector**}

no exception crashinfo dump {**command** *cli* | **garbage-detector**}

Syntax Description

command *cli*	Indicates the Cisco IOS command for which you want the output information written to the crashinfo file.
garbage-detector	If a router crashes due to low memory, specifies that the output from the **show memory debug leaks summary** command should be written to the crashinfo file.

Command Default

This command is disabled by default.

If a router crashes due to low memory, the output from the following Cisco IOS commands is written to the crashinfo file by default:

- **show process memory**
- **show processes cpu**
- **show memory summary**
- **show buffers**

If the **exception crashinfo dump garbage-detector** command is enabled, the output from the **show memory debug leaks summary** command is also written to the crashinfo file by default.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

A benefit for using the **exception crashinfo dump** command is that it allows users to customize the crashinfo file to contain information that is relevant to their troubleshooting situation.

Examples

The following example shows how to specify that the output from the **show interfaces** command should be written to the crashinfo file:

```
exception crashinfo dump command show interfaces
```

Related Commands

Command	Description
exception memory	Sets free memory and memory block size threshold parameters.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

exception crashinfo file

To enable the creation of a diagnostic file at the time of unexpected system shutdowns, use the **exception crashinfo file** command in global configuration mode. To disable the creation of crashinfo files, use the **no** form of this command.

exception crashinfo file *device*:*filename*

no exception crashinfo file *device*:*filename*

Syntax Description

device:filename	Specifies the flash device and file name to be used for storing the diagnostic information. The file name can be up to 38 characters. The colon is required.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T, 12.2(11)	This command was introduced for the Cisco 3600 series only.
12.2(13)T	This command was implemented in 6400-NSP images.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The “crashinfo” file saves information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). The switch writes the crash information to the console at the time of the failure, and the file is created the next time you boot the IOS image after the failure (instead of while the system is failing). The filename will be *filename_yyyymmdd-hhmmss*, where *y* is year, *m* is month, *d* is date, *h* is hour, and *s* is seconds.

Examples

In the following example, a crashinfo file called “crashdata” will be created in the default flash memory device if a system crash occurs:

```
Router(config)# exception crashinfo file flash:crashinfo
```

Related Commands

Command	Description
exception crashinfo buffersize	Changes the size of the crashinfo buffer.

exception crashinfo maximum files

To enable a Cisco IOS device to automatically delete old crashinfo files to help create space for the writing of new crashinfo files when a system crashes, use the **exception crashinfo maximum files** command in global configuration mode. To disable automatic deletion of crashinfo files, use the **no** form of this command.

exception crashinfo maximum files *file-numbers*

no exception crashinfo maximum files *file-numbers*

Syntax Description

file-numbers	The number of most recent crashinfo files across all file systems in the device to be saved when crashinfo files are deleted automatically. Valid values are from 0 to 32.

Command Default

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(33)SRA	This feature was integrated in Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is effective only when a device crashes. If the value of the *file-numbers* argument is given as zero (0), all old crashinfo files across all file systems are deleted when the crashinfo files are deleted automatically.

While booting a device, the default file location is bootflash.

If the file system does not have free space equivalent to or more than 250 KB, the system displays a warning. You can verify the available disk space and create free space for writing the crashinfo files.

Examples

The following example shows how to enable a Cisco IOS device to automatically delete old crashinfo files if the device needs space for writing new crashinfo files when a system crashes. In this example, the device is configured to preserve the 22 latest crashinfo files from previous crashinfo collections.

```
configure terminal
!
exception crashinfo maximum files 22
```

Related Commands

Command	Description
exception crashinfo buffersize	Changes the size of the crashinfo buffer.
exception crashinfo file	Creates a diagnostic file at the time of unexpected system shutdown.

exception dump

To configure the router to dump a core file to a particular server when the router crashes, use the **exception dump** command in global configuration mode. To disable core dumps, use the **no** form of this command.

exception dump *ip-address*

no exception dump

Syntax Description

ip-address	IP address of the server that stores the core dump file.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Caution Use the **exception dump** command only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

If you use TFTP to dump the core file to a server, the router will only dump the first 16 MB of the core file. If the router's memory is larger than 16 MB, the whole core file will not be copied to the server. Therefore, use rcp or FTP to dump the core file.

The core dump is written to a file named *hostname*-core on your server, where *hostname* is the name of the router. You can change the name of the core file by configuring the **exception core-file** command.

This procedure can fail for certain types of system crashes. However, if successful, the core dump file will be the size of the memory available on the processor (for example, 16 MB for a CSC/4).

Examples

In the following example, a user configures a router to use FTP to dump a core file to the FTP server at 172.17.92.2 when it crashes:

```
Router(config)# ip ftp username red
Router(config)# ip ftp password blue
Router(config)# exception protocol ftp
Router(config)# exception dump 172.17.92.2
Router(config)# exception core-file dumpfile
```

Related Commands

Command	Description
exception core-file	Specifies the name of the core dump file.
exception memory	Causes the router to create a core dump and reboot when certain memory size parameters are violated.
exception protocol	Configures the protocol used for core dumps.
exception spurious-interrupt	Causes the router to create a core dump and reload after a specified number of spurious interrupts.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the username for FTP connections.
ip rcmd remote-username	Configures the remote username to be used when requesting a remote copy using rcp.

exception linecard

To enable storing of crash information for a line card and optionally specify the type and amount of information stored, use the **exception linecard** command in global configuration mode. To disable the storing of crash information for the line card, use the **no** form of this command.

exception linecard {**all** | **slot** *slot-number*} [**corefile** *filename* | **main-memory** *size* [**k** | **m**] | **queue-ram** *size* [**k** | **m**] | **rx-buffer** *size* [**k** | **m**] | **sqe-register-rx** | **sqe-register-tx** | **tx-buffer** *size* [**k** | **m**]]

no exception linecard

Syntax Description

all	Stores crash information for all line cards.
slot *slot-number*	Stores crash information for the line card in the specified slot. Slot numbers range from 0 to 11 for the Cisco 12012 and 0 to 7 for the Cisco 12008 router.
corefile *filename*	(Optional) Stores the crash information in the specified file in NVRAM. The default filename is *hostname*-**core-***slot-number* (for example, c12012-core-8).
main-memory *size*	(Optional) Stores the crash information for the main memory on the line card and specifies the size of the crash information. Size of the memory to store is 0 to 268435456.
queue-ram *size*	(Optional) Stores the crash information for the queue RAM memory on the line card and specifies the size of the crash information. Size of the memory to store can be from 0 to 1048576.
rx-buffer *size* **tx-buffer** *size*	(Optional) Stores the crash information for the receive and transmit buffer on the line card and specifies the size of the crash information. Size of the memory to store can be from 0 to 67108864.
sqe-register-rx **sqe-register-tx**	(Optional) Stores crash information for the receive or transmit silicon queueing engine registers on the line card.
k **m**	(Optional) The **k** option multiplies the specified *size* by 1K (1024), and the **m** option multiplies the specified *size* by 1M (1024*1024).

Defaults

No crash information is stored for the line card.

If enabled with no options, the default is to store 256 MB of main memory.

Command Modes

Global configuration

Command History

Release	Modification
11.2 GS	This command was introduced for Cisco 12000 series Gigabit Switch Routers (GSRs).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use caution when enabling the **exception linecard** global configuration command. Enabling all options could cause a large amount (150 to 250 MB) of crash information to be sent to the server.

Caution Use the **exception linecard** global configuration command only when directed by a technical support representative. Only enable options that the technical support representative requests you to enable. Technical support representatives need to be able to look at the crash information from the line card to troubleshoot serious problems on the line card. The crash information contains all the line card memory information including the main memory and transmit and receive buffer information. .

Examples

In the following example, the user enables the storing of crash information for line card 8. By default, 256 MB of main memory is stored.

```
Router(config)# exception linecard slot 8
```

exception memory

To set free memory and memory block size threshold parameters, use the **exception memory** command in global configuration mode. To disable this functionality, use the **no** form of this command.

exception memory {**fragment** | **minimum**} [**processor** | **io**] *size* [**interval 1**] [**reboot**]

no exception memory {**fragment** | **minimum**} [**processor** | **io**] *size* [**interval 1**] [**reboot**]

Syntax Description

fragment *size*	Sets the minimum contiguous block of memory in the free pool, in bytes.
minimum *size*	Sets the minimum size of the free memory pool, in bytes.
processor	(Optional) Specifies processor memory.
io	(Optional) Specifies I/O memory.
interval 1	(Optional) Checks the largest memory block size every 1 second. If the **interval 1** keyword is not configured, the memory block size is checked every 60 seconds (1 minute) by default.
reboot	(Optional) Reloads the router when a memory size threshold is violated. If the **reboot** keyword is not configured, the router will not reload when a memory size threshold is violated.

Command Default

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.3(11)T	The **processor**, **io**, **interval 1**, and **reboot** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command is used to troubleshoot memory leaks and memory fragmentation issues.

The free memory size is checked for every memory allocation. The largest memory block size is checked every 60 seconds by default. If the **interval 1** keyword is configured, the largest memory block size is checked every 1 second.

When a memory size threshold is violated, the router will display an error message and create a crashinfo file. A core dump file will also be created if the **exception dump** command is configured. The router will not reload unless the **reboot** keyword is configured.

Caution Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

Examples

In the following example, the user configures the router to monitor the free memory. If the amount of free memory falls below 250,000 bytes, the router will create a crashinfo file and core dump file and reload.

```
configure terminal
!
exception dump 131.108.92.2
exception core-file memory.overrun
exception memory minimum 250000 reboot
```

Related Commands

Command	Description
exception core-file	Specifies the name of the core dump file.
exception crashinfo dump	Specifies the type of output information to be written to the crashinfo file.
exception dump	Configures the router to dump a core file to a particular server when the router crashes.
exception protocol	Configures the protocol used for core dumps.
exception region-size	Specifies the size of the region for the exception-time memory pool.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the username for FTP connections.

exception memory ignore overflow

To configure the Cisco IOS software to correct corruption in memory block headers and allow a router to continue its normal operation, use the **exception memory ignore overflow** command in global configuration mode. To disable memory overflow correction, use the **no** form of this command.

exception memory ignore overflow {**io** | **processor**} [**frequency** *seconds*] [**maxcount** *corrections*]

no exception memory ignore overflow {**io** | **processor**} [**frequency** *seconds*] [**maxcount** *corrections*]

Syntax Description

io	Selects input/output (also called packet) memory.
processor	Selects processor memory.
frequency *seconds*	(Optional) Specifies the minimum time gap between two memory block header corrections, in the range from 1 to 600 seconds. The default is once every 10 seconds.
maxcount *corrections*	(Optional) Specifies the maximum number of memory block header corrections allowed, in the range from 1 to 1000. The default is 0, which sets an unlimited number of corrections.

Command Default

The default is to allow the memory overflow correction once every 10 seconds, and for memory overflow corrections to happen an unlimited number of times.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to improve device availability when software faults are detected in the network. You can configure the frequency and the maximum number of memory overflow corrections. If overflow correction is required more often than the configured value, a software forced reload is triggered because a severe system problem is indicated.

Examples

The following example shows how to set a maximum of five processor memory block header corruption corrections to occur every 30 seconds:

```
configure terminal
!
exception memory ignore overflow processor frequency 30 maxcount 5
end
```

Related Commands

Command	Description
show memory overflow	Displays the details of a memory block header corruption correction.

exception protocol

To configure the protocol used for core dumps, use the **exception protocol** command in global configuration mode. To configure the router to use the default protocol, use the **no** form of this command.

exception protocol {**ftp** | **rcp** | **tftp**}

no exception protocol

Syntax Description

ftp	Uses FTP for core dumps.
rcp	Uses rcp for core dumps.
tftp	Uses TFTP for core dumps. This is the default.

Defaults

TFTP

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Caution Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

If you use TFTP to dump the core file to a server, the router will only dump the first 16 MB of the core file. If the router’s memory is larger than 16 MB, the whole core file will not be copied to the server. Therefore, use rcp or FTP to dump the core file.

Examples

In the following example, the user configures a router to use FTP to dump a core file to the FTP server at 172.17.92.2 when it crashes:

```
Router(config)# ip ftp username red
Router(config)# ip ftp password blue
Router(config)# exception protocol ftp
Router(config)# exception dump 172.17.92.2
```

Related Commands

Command	Description
exception core-file	Specifies the name of the core dump file.
exception dump	Causes the router to dump a core file to a particular server when the router crashes.
exception memory	Causes the router to create a core dump and reboot when certain memory size parameters are violated.
exception spurious-interrupt	Causes the router to create a core dump and reload after a specified number of spurious interrupts.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the username for FTP connections.

exception region-size

To specify the size of the region for the exception-time memory pool, use the **exception region-size** command in global configuration mode. To use the default region size, use the **no** form of this command.

exception region-size *size*

no exception region-size

Syntax Description

size	The size of the region for the exception-time memory pool.

Defaults

16,384 bytes

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Caution Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

The **exception region-size** command is used to define a small amount of memory to serve as a fallback pool when the processor memory pool is marked corrupt. The **exception memory** command must be used to allocate memory to perform a core dump.

Examples

In the following example, the region size is set at 1024:

```
Router(config)# exception region-size 1024
```

Related Commands

Command	Description
exception core-file	Specifies the name of the core dump file.
exception dump	Configures the router to dump a core file to a particular server when the router crashes.
exception memory	Causes the router to create a core dump and reboot when certain memory size parameters are violated.
exception protocol	Configures the protocol used for core dumps.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the username for FTP connections.

exception spurious-interrupt

To configure the router to create a core dump and reload after a specified number of spurious interrupts, use the **exception spurious-interrupt** command in global configuration mode. To disable the core dump and reload, use the **no** form of this command.

exception spurious-interrupt [*number*]

no exception spurious-interrupt

Syntax Description

number	(Optional) A number from 1 to 4294967295 that indicates the maximum number of spurious interrupts to include in the core dump before reloading.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Caution Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

If you use TFTP to dump the core dump file to a server, the router will only dump the first 16 MB of the file. If the router's memory is larger than 16 MB, the whole core file will not be copied to the server. Therefore, use rcp or FTP to dump the core file.

Examples

In the following example, the user configures a router to create a core dump with a limit of two spurious interrupts:

```
Router(config)# exception spurious-interrupt 2
```

Related Commands

Command	Description
exception core-file	Specifies the name of the core dump file.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the user name for FTP connections.

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 (human-readable) format.
schemaASCII	ASCII format with 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 (config-bulk-tr)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Note In Cisco IOS Release 12.0(24)S, only the schemaASCII format is supported. This command will not change the file format in that release.

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.

For the bulkASCII and bulkBinary formats, periodic polling enables data for a single data group (object list) to be collected more than once in the same VFile. Each such instance of a data group can be treated as a different “table” type.

Every object and table tag contains an additional sysUpTime field. Similarly each row tag contains the value of the sysUpTime when the data for that row was collected. The sysUpTime provides a time stamp for the data.

For additional information about the structures of the bulk statistics data file formats, see the definitions in the CISCO-DATA-COLLECTION-MIB.

Examples

In the following example, the bulk statistics data file is set to schemaASCII:

```
Router(config)# snmp mib bulkstat transfer bulkstat1
Router(config-bulk-tr)# schema ATM2/0-IFMIB
Router(config-bulk-tr)# url primary ftp://user:pswrd@host/folder/bulkstat1
Router(config-bulk-tr)# format schemaASCII
Router(config-bulk-tr)# exit
```

Related Commands

Command	Description
snmp mib bulkstat transfer	Names a bulk statistics transfer configuration and enters Bulk Statistics Transfer configuration mode.

hw-module logging onboard (Cat 6K)

To re-enable onboard failure logging (OBFL) on Cisco Catalyst 6000 series switches if logging has been disabled, use the **hw-module logging onboard** command in global configuration mode. To disable OBFL (not recommended), use the **no** form of this command.

hw-module switch *switch-number* **module** *module-number* **logging onboard** [**message level** {**1-7**}]

no hw-module switch *switch-number* **module** *module-number* **logging onboard** [**message level** {**1-7**}]

Syntax Description

switch *switch-number*	Specifies the switch number.
module *module-number*	Specifies the module number.
message level {**1-7**}	(Optional) Specifies the level of severity for system messages that will be logged in OBFL files, as follows: Level 1—Alert (immediate action needed) Level 2—Critical condition Level 3—Error condition Level 4—Warning condition Level 5—Notification (significant condition) Level 6—Informational message only Level 7—Debugging (appears during debugging only)

Command Default

Enabled in all hardware and is the recommended state; all levels of system messages are logged.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

This command enables operating temperatures, hardware uptime, interrupts, and other important events and messages to be recorded in files stored in nonvolatile memory, so that the data can be used to diagnose problems with hardware cards installed in a Cisco router or switch. When the onboard hardware is started up, a first record is made for each area monitored and becomes a base value for subsequent records. This command provides a circular updating scheme for collecting continuous records and archiving older (historical) records, ensuring accurate data about the hardware. Data is recorded in one of two formats: continuous information that displays a snapshot of data in a continuous file, and summary information that provides details about the data being collected. Use the **show logging onboard** privileged EXEC command to see reports of current and historical data.

This configuration command is applicable to the module inserted in a device. When the module is removed and inserted into a new device, the configuration of this command follows the module to the new device.

This command is normally accessed through the route processor or supervisor command line interface; however, some system images do not provide full support for client remote terminal access. When using these images, use the **attach** command to connect to the console on the line card.

Examples

The following example shows how to configure OBFL message logging at level 7 (debugging):

```
Router> enable
Router# configure terminal
Router(config)# hw-module switch 2 module 1 logging onboard message level 7
Router(config)# end
```

Related Commands

Command	Description
attach	Connects to a specific line card for the purpose of executing commands on that card.
clear logging onboard (Cat 6K)	Clears onboard failure logs.
copy logging onboard (Cat 6K)	Copies OBFL data from the target OBFL-enabled module to a local or remote file system.
show logging onboard (Cat 6K)	Displays onboard failure logs.

instance (MIB)

To configure the MIB object instances to be used in a bulk statistics schema, use the **instance** command in Bulk Statistics Schema configuration mode. To remove a Simple Network Management Protocol (SNMP) bulk statistics object list, use the **no** form of this command.

instance {**exact** | **wild**} {**interface** *interface-id* [**sub-if**] | **controller** *controller-id* [**sub-if**] | **oid** *oid*}

no instance {**exact** | **wild**} {**interface** *interface-id* [**sub-if**] | **controller** *controller-id* [**sub-if**] | **oid** *oid*}

Syntax Description

exact	Indicates that the specified instance (interface, controller, or object identifier [OID]), when appended to the object list, is the complete OID to be used in this schema.
wild	Indicates that all instances that fall within the specified interface, controller, or OID range should be included in this schema.
interface	Specifies a specific interface or group of interfaces for the schema.
interface-id	Interface name and number for a specific interface or group of interfaces.
sub-if	(Optional) Specifies that the object instances should be polled for all subinterfaces of the specified interface or controller in addition to the object instances for the main interface.
controller	Indicates that a controller or group of controllers is specified for the schema.
controller-id	Controller ID for a specific controller or group of controllers.
oid	Indicates that an OID is specified.
oid	Object ID that, when appended to the object list, specifies the complete (or wildcarded) OID for the objects to be monitored.

Command Default

If the **sub-if** keyword is not used, the subinterfaces of the interface or controller will not be polled.

Command Modes

Bulk Statistics Schema configuration (config-bulk-sc)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **instance** command specifies the instance information for objects in the schema being configured. 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 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. In other words, the **wild** keyword allows you to specify a partial, wildcarded instance.

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, Ethernet 0) instead of specifying the ifIndex OID for the interface. Similarly, the **controller** *controller-id* syntax allows you to specify a controller interface.

The optional **sub-if** keyword, when added after specifying an interface or controller, includes the ifIndexes for all subinterfaces of the interface you specified.

Only one **instance** command can be configured per schema.

Examples

The following example shows how to configure the router to collect bulk statistics for the ifInOctets object (from the IF-MIB) for the Ethernet interface 3/0. In this example, 3 is the ifIndex instance for interface Ethernet3/0. The instance (3) when combined with the object list (ifIndex; 1.3.6.1.2.1.2.2.1.1) translates to the OID 1.3.6.1.2.1.2.2.1.1.3.

```
Router# configure terminal
Router(config)# snmp mib bulkstat object-list E0InOctets
! The following command specifies the object 1.3.6.1.2.1.2.2.1.1.3 (ifIndex)
Router(config-bulk-objects)# add ifIndex
Router(config-bulk-objects)# exit
Router(config)# snmp mib bulkstat schema E0
Router(config-bulk-sc)# object-list EOInOctets
! The following command is equivalent to "instance exact oid 3".
Router(config-bulk-sc)# instance exact interface Ethernet 3/0
Router(config-bulk-sc)# exit
Router(config)# snmp mib bulkstat transfer bulkstat1
Router(config-bulk-tr)# schema E0
Router(config-bulk-tr)# url primary ftp://user:password@host/ftp/user/bulkstat1
Router(config-bulk-tr)# url secondary tftp://user@host/tftp/user/bulkstat1
Router(config-bulk-tr)# format schemaASCII
Router(config-bulk-tr)# transfer-interval 30
Router(config-bulk-tr)# retry 5
Router(config-bulk-tr)# enable
Router(config-bulk-tr)# exit
Router(config)# do copy running-config startup-config
```

Related Commands

Command	Description
object-list	Configures the bulk statistics object list to be used in the bulk statistics schema.
snmp mib bulkstat schema	Names an SNMP bulk statistics schema and enters Bulk Statistics Schema configuration mode.

instance (resource group)

To add request/response units (RUs) to a specified resource group, use the **instance** command in resource group configuration mode. To disable this function, use the **no** form of this command.

instance *instance-name*

no instance *instance-name*

Syntax Description

instance-name	Name of the RU you want to add to the resource group (for example, **http**, **snmp**).

Command Default

Disabled

Command Modes

Resource group configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Before adding RUs to a resource group, you must create a resource group using the **user group** *resource-group-name* **type** *resource-user-type* command in ERM configuration mode.

For example, you have a resource group named lowPrioUsers with a type of iosprocess. You have low-priority RUs or tasks such as HTTP and Simple Network Management Protocol (SNMP), and you want to set a threshold for all the low-priority RUs as a group. You must add the RUs to the resource group using the **instance** *instance-name* command and then apply a resource policy.

If the resource policy you applied sets a minor rising threshold value of 10 percent for the resource group, when the accumulated usage of both HTTP and SNMP RUs crosses 10 percent a notification is sent to the RUs in the resource group lowPrioUsers. For example, if HTTP usage is 4 percent and SNMP usage is 7 percent, a notification is sent to the resource group.

Examples

The following example shows how to add an HTTP RU to a resource group named lowPrioUsers:

```
Router(config-erm)# user group lowPrioUsers type iosprocess
Router(config-res-group)# instance http
```

Related Commands

Command	Description
policy (resource group)	Applies a policy to all the RUs in the resource group.
user (ERM)	Creates a resource group.

instance range

To specify the range of instances to collect for a given data group, use the **instance range** command in global configuration mode. To delete a previously configured instance range, use the **no** form of this command.

instance range start *oid* **end** *oid*

no instance range start *oid* **end** *oid*

Syntax Description

start	Indicates the beginning of the range.
oid	The object ID to be monitored for the specific range.
end	Indicates the end of the range.

Command Default

No instance range is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

When used in conjunction with the **snmp mib bulkstat schema** command, the **instance range** command can be used to configure a range of instances on which to collect data.

Examples

The following example shows the collection of data for all instances starting with instance 1 and ending with instance 2:

```
snmp mib bulkstat object-list ifmib
  add ifInOctets
  add ifOutOctets
  exit
!
snmp mib bulkstat schema IFMIB
 object-list ifmib
 poll-interval 1
 instance range start 1 end 2
 exit
!
snmp mib bulkstat transfer bulkstat1
 schema IFMIB
 url primary tftp://202.153.144.25/pcn/bulkstat1
 format schemaASCII
 transfer-interval 5
 retry 5
 buffer-size 1024
```

```
retain 30
enable
end
```

Related Commands

Command	Description
instance	Specifies the instance that, when appended to the object list, gives the OID of the object instance to be monitored in the bulk statistics schema.
snmp mib bulkstat schema	Names a bulk statistics schema and enters Bulk Statistics Schema configuration mode.

instance repetition

To configure 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 global 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 repetition *oid-instance*

Syntax Description

oid-instance	Object ID of the instance to be monitored.
max *repeat-number*	Number of times the instance should repeat.

Command Default

No instance repetition is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

When used in conjunction with the **snmp mib bulkstat schema** command, the **instance repetition** command can be used to configure data collection to repeat for a certain number of instances of a MIB object.

Examples

The following example shows how to start data collection at the first instance and repeat for four instances of the indicated MIB object:

```
snmp mib bulkstat object-list ifmib
 add ifOutOctets
 add ifInOctets
snmp mib bulkstat schema IFMIB
 object-list ifmib
 poll-interval 1
 instance repetition 1 max 4
snmp mib bulkstat transfer bulkstat1
 schema IFMIB
 transfer-interval 5
 retain 30
 retry 5
 buffer-size 1024
 enable
```

Related Commands

Command	Description
instance	Specifies the instance that, when appended to the object list, gives the OID of the object instance to be monitored in the bulk statistics schema.
snmp mib bulkstat schema	Names a bulk statistics schema and enters Bulk Statistics Schema configuration mode.

ip address dynamic

To discover a customer premises equipment (CPE) router's IP address dynamically based on an aggregator router's IP address, use the **ip address dynamic** command in Frame Relay DLCI interface configuration mode. To disable this request, use the **no** form of this command.

ip address dynamic

no ip address dynamic

Syntax Description

This command has no arguments or keywords.

Command Default

No IP address discovery request is made.

Command Modes

Frame Relay DLCI interface configuration

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.

Usage Guidelines

When you enter the **ip address dynamic** command, the CPE router sends an Inverse Address Resolution Protocol (ARP) request to the aggregator router asking for the IP address of its interface. The aggregator router replies with its own subinterface's IP address. The CPE router then calculates a valid IP address and a suitable netmask for its subinterface based on the data received from the aggregator router. The aggregator router is polled at regular intervals. If the IP address on the aggregator router's interface changes, the CPE router's IP address will adjust as necessary.

You can check the assigned IP address by entering the **show interface** command and specifying the subinterface being configured.

Note The **ip address dynamic** command is only applicable for Frame Relay point-to-point subinterfaces.

Examples

The following example shows how to configure serial interface 1 to run Frame Relay. Its subinterface is then configured to discover the IP address using the **ip address dynamic** command.

```
interface Serial 1
 encapsulation frame
interface serial 1.1 point-to-point
 frame-relay interface-dlci 100
 ip address dynamic
```

Related Commands

Command	Description
frame-relay interface-dlci	Assigns a data link connection identifier (DLCI) to a specified Frame Relay subinterface on the router or access server, and enters Frame Relay DLCI interface configuration mode.

ip director access-group local

To configure the DistributedDirector to process only Domain Name System (DNS) queries for hostnames that are configured directly through command-line interface (CLI) commands or text (TXT) resource records, use the **ip director access-group local** command in global configuration mode. To turn off this configuration, use the **no** form of this command.

ip director access-group local

no ip director access-group local

Syntax Description

This command has no arguments or keywords.

Command Default

All DNS queries are processed by the director code.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the primary director agent is considered the official name server for the entire domain, the **ip director access-group local** command should be used to allow the DistributedDirector to directly handle only the configured hostnames.

Examples

The following example shows how to configure the DistributedDirector to process only DNS queries for hostnames that are configured directly through CLI commands or TXT resource records:

```
Router(config)# ip director access-group local
```

ip director cache refresh

To enable the DistributedDirector Cache Auto Refresh function, use the **ip director cache refresh** command in global configuration mode. To disable automatic background refresh, use the **no** form of this command.

ip director cache refresh

no ip director cache refresh

Syntax Description

This command has no keywords or arguments.

Command Default

Automatic background refresh is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The sorting cache on DistributedDirector must be enabled before you can use the **ip director cache refresh** command. To enable the sorting cache, use the **ip director cache** command.

Once automatic background refresh for the DistributedDirector cache is enabled, the cache will actively and continuously update every expired entry by processing a fake Domain Name System (DNS) request. The cache accumulates and updates answers to all past DNS queries received since cache auto refresh was initiated. Any repeat DNS request is always serviced directly from the cache.

Examples

The following example enables automatic background refresh for the DistributedDirector cache:

```
Router(config)# ip director cache
Router(config)# ip director cache refresh

Router# show running-config

ip host myhost 172.2.2.10 172.2.2.20 172.2.2.30
.
.
.
ip director cache refresh
```

ip director cache size

To configure the variable size of the DistributedDirector cache, use the **ip director cache size** command in global configuration mode. To remove this 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.

ip director cache size *entries*

no ip director cache size *entries*

Syntax Description

entries	An integer in the range from 1 to 4294967295 that specifies the maximum number of cache entries.

Command Default

Maximum number of cache entries: 2000

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use the **ip director cache size** command to configure the maximum number of cache entries that the DistributedDirector system will retain in its cache. This cache size is the maximum number of cache entries that are displayed when the user enters the **show ip director cache** command.

Examples

The following example configures the maximum number of cache entries:

```
Router(config)# ip director cache size 1500
Cache size shrinked to 1500

Router# show ip director cache
Director cache is on
Cache current size = 0 maximum size = 1500
Cache time for sort cache entries: 60 secs
Director sort cache hits = 0
```

Related Commands

Command	Description
ip director cache	Enables the sorting cache on DistributedDirector.
ip director cache time	Configures how long the DistributedDirector system will retain per-client sorting information.

ip director cache time

To configure how long the DistributedDirector system will retain per-client sorting information, use the **ip director cache time** command in global configuration mode. To remove this 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.

ip director cache time *seconds*

no ip director cache time *seconds*

Syntax Description

seconds	An integer in the range from 1 to 2147483 that specifies, in seconds, the amount of time the per-client sorting information is retained. The default is 60 seconds.

Command Default

The default is 60 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use the **ip director cache time** command to specify how long the DistributedDirector system will retain per-client sorting in its cache. This cache time is the maximum amount of cache time displayed when the user enters the **show ip director cache** command.

Examples

The following example configures how long the DistributedDirector system will retain per-client sorting information:

```
Router(config)# ip director cache time 100

Router# show ip director cache
Director cache is on
Cache current size = 0 maximum size = 2000
Cache time for sort cache entries: 100 secs
Director sort cache hits = 0
```

Related Commands

Command	Description
ip director cache	Enables the sorting cache on DistributedDirector.
ip director cache size	Configures the variable size of the DistributedDirector cache.

ip director default priorities

To set a default priority for a specific metric on the DistributedDirector, use the **ip director default priorities** command in global configuration mode. To remove a default priority for a metric, use the **no** form of this command.

ip director default priorities [**drp-int** *number*] [**drp-ext** *number*] [**drp-ser** *number*] [**random** *number*] [**admin** *number*] [**drp-rtt** *number*] [**portion** *number*] [**availability** *number*] [**route-map** *number*] [**boomerang** *number*]

no ip director default priorities [**drp-int** *number*] [**drp-ext** *number*] [**drp-ser** *number*] [**random** *number*] [**admin** *number*] [**drp-rtt** *number*] [**portion** *number*] [**availability** *number*] [**route-map** *number*] [**boomerang** *number*]

Syntax Description

drp-int	(Optional) DRP internal metric.
number	(Optional) Numeric value of a priority level for a given metric. Range is from 1 to 100.
drp-ext	(Optional) DRP external metric.
drp-ser	(Optional) DRP server metric.
random	(Optional) Random metric.
admin	(Optional) Administrative metric.
drp-rtt	(Optional) DRP round-trip time metric.
portion	(Optional) Portion metric.
availability	(Optional) Availability metric.
route-map	(Optional) Route-map metric.
boomerang	(Optional) Boomerang metric.

Command Default

No default priorities are specified.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(8)T	The boomerang metric was added.

Usage Guidelines

Not all of the metrics need to be specified, but at least one must be specified. If the boomerang metric is specified for a given host name, then all metrics of lower priority (that is, having a higher priority number) than boomerang are always ignored.

The default priorities specified will take effect if no priorities are specified in the **ip director host priority** command or in the corresponding Domain Name System (DNS) text record for the host.

To set the default priority for several metrics, enter the metric keywords and values to be configured on the same line as the **ip director default priorities** command.

Examples

In the following example, the boomerang metric is selected as the default priority:

```
Router(config)# ip director default priorities boomerang 1

Router# show running-config

ip host boom1 172.2.2.10 172.2.2.20 172.2.2.30
ip director server 172.2.2.20 drp-association 172.4.4.2
ip director server 172.2.2.30 drp-association 172.4.4.3
ip director server 172.2.2.10 drp-association 172.4.4.1
ip director host boom1
no ip director cache
ip dns primary boom1 soa boom1 boom1@com
ip director host boom1 priority boomerang 1
no ip director drp synchronized
```

Related Commands

Command	Description
ip director access-list	Defines an access list for DistributedDirector that specifies which subdomain names and host names should be sorted.
ip director cache	Enables the sorting cache on DistributedDirector.
ip director default priorities	Sets a default priority for a specific metric on DistributedDirector.
ip director default weights	Configures default weight metrics for DistributedDirector.
ip director host priority	Configures the order in which DistributedDirector considers metrics when picking a server.
ip director host weights	Sets host-specific weights for the metrics that DistributedDirector uses to determine the best server within a specific host name.
ip director server admin-pref	Configures a per-service administrative preference value.
ip director server portion	Sets the portion value for a specific server.
ip director server preference	Specifies DistributedDirector preference of one server over others or takes a server out of service.
show ip director default priority	Verifies the default configurations of DistributedDirector metrics.
show ip director default weights	Shows DistributedDirector default weights.
show ip director servers	Displays DistributedDirector server preference information.

ip director default weights

To configure default weight metrics for DistributedDirector, use the **ip director default weights** command in global configuration mode. To set the defaults to zero, use the **no** form of this command.

ip director default weights {[**drp-int** *number*] [**drp-ext** *number*] [**drp-ser** *number*] [**drp-rtt** *number*] [**random** *number*] [**admin** *number*] [**portion** *number*] [**availability** *avail-number*] [**route-map** *number*]}

no ip director default weights {[**drp-int** *number*] [**drp-ext** *number*] [**drp-ser** *number*] [**drp-rtt** *number*] [**random** *number*] [**admin** *number*] [**portion** *number*] [**availability** *avail-number*] [**route-map** *number*]}

Syntax Description

drp-int	(Optional) Sends a Director Response Protocol (DRP) request to all DRP server agents, asking them for the distance from themselves to the edge of their Border Gateway Protocol (BGP) autonomous system in the direction of the client originating the Domain Name System (DNS) query.
drp-ext	(Optional) Sends a DRP request to all DRP server agents, asking them for the BGP distance between them and the client originating the DNS query.
drp-ser	(Optional) Sends a DRP request to all DRP server agents, asking them for the IGP route metric between them and the distributed servers that they support.
drp-rtt	(Optional) Sends a DRP request to all DRP server agents, asking them for the round-trip time between the DRP agent and the client originating the DNS query.
random	(Optional) Selects a random number for each distributed server and defines the “best” server as the one with the smallest random number assignment.
admin	(Optional) Specifies a simple preference of one server over another. If this administrative metric has been explicitly set to zero, the Director will not consider the server, so the server is taken out of service.
portion	(Optional) Assigns a load “portion” to each server such that servers with a higher portion value will receive a larger percentage of connections at any one time.
availability	(Optional) Specifies the load information for the DistributedDirector. The default value is 65535.
avail-number	(Optional) Integer in the range of 1 to 65535, inclusive.
route-map	(Optional) Specifies whether a server should be offered to a client.
number	(Optional) Integer in the range of 1 to 100, inclusive.

Command Default

No default weights are specified.

The availability default value is 65535.

Command Modes

Global configuration

Command History

Release	Modification
11.1(18)IA	This command was introduced.
12.1(5)T	The availability and route-map metrics were added.
12.2(4)T	The command name was changed slightly: **default weights** replaced **default-weights**.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Not all the metrics need to be configured; however, at least one metric must be configured when this command is used.

Default weights are used for all host names sorted by the DistributedDirector. To override default weights for a certain host, specify host-specific weights in the private DNS server configuration.

When the associated metric is referenced in the sorting decision, it will always be multiplied by the appropriate metric weight. In this way, you can specify that some metrics be weighted more than others. You may determine the weights that you want to use through experimentation. The weights given do not need to total 100.

The distance specified with the **drp-int** keyword can be used with the DRP external metric (**drp-ext**) to help determine the distance between the router and the client originating the DNS query.

If the client and the DRP server agent are in the same autonomous system, this metric returns the Interior Gateway Protocol (IGP) cost metric between the client and the DRP server agent.

The distance learned through the **drp-ext** keyword represents the number of BGP hops between the autonomous system of the DRP server agent and the autonomous system of the client originating the DNS query. Because this is BGP information, the DRP server agents need to have access to full Internet BGP information for this metric to be useful.

The distance learned through the **drp-ser** keyword can be used with the DRP internal metric (**drp-int**) to get a finer distance calculation between the distributed servers and the edge of the BGP autonomous system in the direction of the client originating the DistributedDirector query.

If a true BGP border router is used as a DRP server agent, the DRP server metric will return the IGP route metric between the distributed server and the BGP border router (autonomous system edge). Because DRP server metrics should not change frequently, DistributedDirector issues DRP server queries (and caches the results) every 10 minutes.

Using the **random** keyword alone results in random redirection of clients to the distributed servers. Because this metric requires no routing table information, it does not trigger DRP requests to the DRP server agents.

The new availability metric allows the DistributedDirector to attempt to create a TCP connection to each distributed server on a configured port over a configurable time interval.

Examples

The following command shows how to configure default weights for the internal and external metrics:

```
Router(config)# ip director default weights drp-int 10 drp-ext 90
```

Related Commands

Command	Description
debug ip director parse	Shows debugging information for DistributedDirector parsing of TXT information.
debug ip director sort	Shows debugging information for DistributedDirector IP address sorting.
ip director access-list	Defines an access list for the DistributedDirector that specifies which subdomain names and host names should be sorted.
ip director cache	Enables the sorting cache on the DistributedDirector.
ip director default priorities	Sets default priorities for a specific metric on the DistributedDirector.
ip director drp rttprobe	Sets the protocol used by DRP agents for RTT probing in DistributedDirector.
ip director host priority	Configures the order in which the DistributedDirector considers metrics when selecting a server.
ip director host weights	Sets host-specific weights for the metrics that the DistributedDirector uses to determine the best server within a specific host name.
ip director server admin-pref	Configures a per-service administrative preference value.
ip director server portion	Sets the portion value for a specific server.
ip director server preference	Specifies DistributedDirector preference of one server over others or takes a server out of service.
show ip director default priority	Verifies the default configurations of DistributedDirector metrics.
show ip director default weights	Shows the DistributedDirector default weights.
show ip director servers	Displays the DistributedDirector server preference information.

ip director dfp

To configure the DistributedDirector Dynamic Feedback Protocol (DFP) agent with which the DistributedDirector should communicate, use the **ip director dfp** command in global configuration mode. To turn off the DFP agent, use the **no** form of this command.

ip director dfp *ip-address* [*port*] [**retry** *number*] [**attempts** *seconds*] [**timeout** *seconds*]

no ip director dfp *ip-address* [*port*] [**retry** *number*] [**attempts** *seconds*] [**timeout** *seconds*]

Syntax Description

ip-address	IP address.
port	(Optional) Port number to which the distributed servers are configured. The default value is 8080.
retry *number*	(Optional) Specifies the number of times a connection will be attempted. The default value is 5.
attempts *seconds*	(Optional) Specifies the delay, in seconds, between each connection attempt. The default value is 10000.
timeout *seconds*	(Optional) Specifies the maximum amount of time, in seconds, for which DFP information is assumed valid. The default value is 10000.

Command Default

The port default value is 8080.

The retry default value is 5.

The attempts default value is 10000.

The timeout default value is 10000.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A connection is attempted a specified number of times with a delay of a specified number of seconds between each attempt. When a connection is established, the DFP protocol runs. If a time interval update has not occurred for this DFP session, the connection breaks and is reestablished as previously described.

Examples

The following example shows how to configure the DistributedDirector to communicate with a specified DFP agent:

```
ip director dfp 10.0.0.1 retry 3 attempts 60 timeout 6000
```

ip director dfp security

To configure a security key for use when connecting to the Dynamic Feedback Protocol (DFP) client named, use the **ip director dfp security** command in global configuration mode. To turn off the security key, use the **no** form of this command.

ip director dfp security *ip-address* **md5** *string* [*timeout*]

no ip director dfp security *ip-address* **md5** *string* [*timeout*]

Syntax Description

ip-address	IP address for the service.
md5	Message Digest 5 (MD5) security data authentication.
string	Security key.
timeout	(Optional) Amount of time, in seconds, during which DistributedDirector will continue to accept a previously defined security key. The default value is 0 seconds.

Command Default

The default timeout value is 0 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ip director dfp security** command should be entered before configuring the **ip director dfp** command, resulting in a connection being made, but it can be entered independently of making a connection.

DFP allows servers to take themselves Out-of-Service and place themselves back In-Service. This function could result in a security risk because a network that is hacked could be shut down even though all the servers are still performing. An optional security vector is included in DFP to allow each message to be verified. The security vector is used to describe the security algorithm being used and to provide the data for that algorithm. The security vector itself is also extensible in that it specifies which security algorithm is being used. This specification allows different levels of security from MD5 to Data Encryption Standard (DES) to be used without overhauling the protocol and disrupting an installed base of equipment. If a receiving unit is configured for the specified security type, all DFP packets must contain that security vector or they are ignored. If a receiving unit is not configured for any security type, the security vector does not have to be present, and if it is present, it is ignored while the rest of the message is processed normally.

Examples

The following example shows how to configure the security key hello:

```
ip director dfp security 10.0.0.1 md5 hello 60
```

Related Commands

Command	Purpose
ip director dfp	Configures the DistributedDirector DFP agent with which the DistributedDirector should communicate.

ip director drp retries

To configure the maximum number of Director Response Protocol (DRP) query retries for the DistributedDirector, use the **ip director drp retries** command in global configuration mode. To restore the default, use the **no** form of this command.

ip director drp retries *attempts*

no ip director drp retries *attempts*

Syntax Description

attempts	Integer in the range of 0 to 1000 that specifies the number of retry attempts. The default is 2.

Command Default

No retries are attempted.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When a DistributedDirector is slow in determining if a DRP agent is not responding, the **ip director drp retries** command can be used to limit the number of retry attempts to each DRP agent so that the DistributedDirector can respond faster to clients.

Examples

The following example shows how to configure one DRP query retry for a DistributedDirector:

```
Router(config)# ip director drp retries 1
```

ip director drp rttprobe

To set the protocol used by Director Response Protocol (DRP) agents for round-trip time (RTT) probing in DistributedDirector, use the **ip director drp rttprobe** command in global configuration mode. To disable the use of a protocol, use the **no** form of the command.

ip director drp rttprobe [**tcp** | **icmp**]

no ip director drp rttprobe [**tcp** | **icmp**]

Syntax Description

tcp	(Optional) Transmission Control Protocol. This is the default.
icmp	(Optional) Internet Control Message Protocol.

Command Default

TCP is the default protocol.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

Both protocols can be activated, in which case DistributedDirector will instruct DRP agents to return the RTT collected from either the TCP or Internet Control Message Protocol (ICMP) protocol, whichever becomes available first. At any time, at least one of the protocols must be active.

To use only one protocol, enable the protocol you want to use, and then disable the protocol that was already configured.

```
Router(config)# ip director drp rttprobe icmp
Router(config)# no ip director drp rttprobe tcp
```

Examples

The following example shows that ICMP is configured for use by DRP agents for RTT probing:

```
Router(config)# ip director drp rttprobe icmp
```

Related Commands

Command	Description
ip director access-list	Defines an access list for the DistributedDirector that specifies which subdomain names and host names should be sorted.
ip director cache	Enables the sorting cache on the DistributedDirector.
ip director default priorities	Sets default priorities for a specific metric on the DistributedDirector.
ip director default weights	Configures default weight metrics for the DistributedDirector.

Command	Description
ip director host priority	Configures the order in which the DistributedDirector considers metrics when selecting a server.
ip director host weights	Sets host-specific weights for the metrics that the DistributedDirector uses to determine the best server within a specific host name.
ip director server admin-pref	Configures a per-service administrative preference value.
ip director server portion	Sets the portion value for a specific server.
ip director server preference	Specifies DistributedDirector preference of one server over others or takes a server out of service.
show ip director default priority	Verifies the default configurations of DistributedDirector metrics.
show ip director default weights	Shows the DistributedDirector default weights.
show ip director servers	Displays the DistributedDirector server preference information.

ip director drp synchronized

To activate clock synchronization between DistributedDirector and Director Response Protocol (DRP), use the **ip director drp synchronized** command in global configuration mode. To deactivate synchronization between the clocks in DistributedDirector and the DRPs, use the **no** form of this command.

ip director drp synchronized

no ip director drp synchronized

Syntax Description

This command has no arguments or keywords.

Command Default

Clock synchronization is deactivated.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

This command is used in conjunction with boomerang racing.

When the **ip dir drp synchronized** command is configured, DistributedDirector specifies an absolute time at which the DRP agent should respond to the DNS client.

When **no ip director drp synchronized** is configured (which is the default), DistributedDirector specifies a relative time (based on the delay measured between DistributedDirector and the DRP agent) at which the DRP agent should respond to the Domain Name Service (DNS) client.

Examples

In the following example, DistributedDirector and DRP clock synchronization are activated:

```
Router(config)# ip director drp synchronized

Router(config)# show running-config

ip host boom1 172.2.2.10 172.2.2.20 172.2.2.30
ip director server 172.2.2.20 drp-association 172.4.4.2
ip director server 172.2.2.30 drp-association 172.4.4.3
ip director server 172.2.2.10 drp-association 172.4.4.1
ip director host boom1
.
.
ip director drp synchronized
```

ip director drp timeout

To configure a DistributedDirector with a Director Response Protocol (DRP) query timeout period, use the **ip director drp timeout** command in global configuration mode. To reset each DRP query timeout to the default value, use the **no** form of this command.

ip director drp timeout *seconds*

no ip director drp timeout *seconds*

Syntax Description

seconds	Integer in the range of 1 to 3600 that specifies the time, in seconds, of the DRP query timeout.

Command Default

When this command is not issued, the lookup query timeout default is 1 second and the measure query timeout default is 4 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When a DistributedDirector is not detecting that a DRP agent is unresponsive, the **ip director drp timeout** command can be used to shorten the timeout period so that the DistributedDirector can respond to its clients faster.

Note If the time interval for a DRP query is too short, there is a risk that the DistributedDirector can miss a response from a DRP agent. The time set for a measure query timeout period should be longer than for a lookup query timeout period.

Examples

The following example shows how to configure a disconnection time interval of 3 seconds for all DFP queries:

```
Router(config)# ip director drp timeout 3
```

Related Commands

Command	Description
ip director drp timeout lookup	Configures the maximum amount of time that a DistributedDirector waits to resend a DRP lookup query.
ip director drp timeout measure	Configures the maximum amount of time that a DistributedDirector waits to resend a DRP measure query.

ip director drp timeout lookup

To configure the maximum amount of time that a DistributedDirector waits to resend a Director Response Protocol (DRP) lookup query, use the **ip director drp timeout lookup** command in global configuration mode. To restore the DRP lookup default, use the **no** form of this command.

ip director drp timeout lookup *seconds*

no ip director drp timeout lookup *seconds*

Syntax Description

seconds	Integer in the range of 1 to 3600 that specifies the number of seconds a DistributedDirector waits before resending a DRP lookup query. The default is 1.

Command Default

DRP lookup queries are resent every 1 second.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A DRP agent looks in existing internal tables and immediately answers the lookup query.

Examples

The following example shows how to configure a DistributedDirector to wait 3 seconds before resending a DRP lookup query:

```
Router(config)# ip director drp timeout lookup 3
```

Related Commands

Command	Description
ip director drp timeout	Configures a DistributedDirector to set a disconnection time interval for all DRP queries.
ip director drp timeout measure	Configures the maximum amount of time that a DistributedDirector waits to resend a DRP measure query.

ip director drp timeout measure

To configure the maximum amount of time that a DistributedDirector waits to resend a Director Response Protocol (DRP) measure query, use the **ip director drp timeout measure** command in global configuration mode. To restore the default, use the **no** form of this command.

ip director drp timeout measure *seconds*

no ip director drp timeout measure *seconds*

Syntax Description

seconds	Integer in the range of 1 to 3600 that specifies the number of seconds a DistributedDirector waits before resending a DRP measure query. The default is 4.

Command Default

DRP measure queries are resent every 4 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A timeout measure query allows a DRP agent to return extended external information. When extended external information is returned, delays can result.

Note The measure query timeout period should be longer than the lookup query timeout period. If the time interval for the measure query timeout is too short, the DistributedDirector can miss responses from the DRP agent.

Examples

The following example shows how to configure a DistributedDirector to wait 2 seconds before resending a DRP measure query:

```
Router(config)# ip director drp timeout measure 2
```

Related Commands

Command	Description
ip director drp timeout	Configures a DistributedDirector to set a disconnection time interval for all DRP queries.
ip director drp timeout lookup	Configures the maximum amount of time that a DistributedDirector waits to resend a DRP lookup query.

ip director host active-close

To direct a DistributedDirector to close a TCP connection using the standard TCP close procedure, use the **ip director host active-close** command in global configuration mode. To restore this command to its default, use the **no** form of this command.

ip director host [*hostname*] [*query-type*] **active-close**

no ip director host [*hostname*] [*query-type*] **active-close**

Syntax Description

hostname	(Optional) Name of the host that maps to one or more IP addresses. Do not use an IP address.
query-type	(Optional) Type of query. Two values are valid: • **a** indicates that the configuration is used for processing Domain Name System (DNS) address queries for the specified hostname. This is the default • **mx** indicates that the configuration is used for processing Mail eXchange (MX) queries for the specified hostname.

Command Default

TCP connections are reset.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

DistributedDirector resets TCP connections when it performs connection tests because a standard TCP close can consume excessive memory resources. The **ip director host active-close** command overrides this behavior, resulting in a standard TCP close rather than a TCP reset.

Examples

The following example shows how to set the connection test interval to 5 minutes for the distributed servers on port 80, for host www.xyz.com. The TCP connection is specified as closed using the standard TCP close procedure.

```
Router(config)# ip director host www.xyz.com connect 80 5
Router(config)# ip director host www.xyz.com active-close
```

Related Commands

Command	Description
ip director host connect	Enables DistributedDirector to verify that a server is available.
ip director server connect-interval	Configures a per-service TCP connection interval.

ip director host connect

To enable a DistributedDirector to verify that a server is available, use the **ip director host connect** command in global configuration mode. To turn off connection parameters, use the **no** form of this command.

ip director host *hostname* [*query-type*] **connect** *port* [*minutes* | **interval** *seconds*]

no ip director host *hostname* [*query-type*] **connect**

Syntax Description

hostname	Name of the host that maps to one or more IP addresses. Do not use an IP address.
query-type	(Optional) Type of query. Two values are valid: • **a** indicates that the configuration is used for processing Domain Name System (DNS) address queries for the specified hostname. This is the default. • **mx** indicates that the configuration is used for processing Mail eXchange (MX) queries for the specified hostname.
port	Integer in the range of 1 to 65535 that specifies the port to which the distributed servers are connected.
minutes	(Optional) Integer in the range of 10 to 65535 that specifies the time, in minutes, between availability checks.
interval	(Optional) Configures a connection-time interval in seconds instead of minutes.
seconds	(Optional) Integer in the range of 10 to 65535 that specifies the time, in seconds, between availability checks.

Command Default

No connection parameter is set.

Command Modes

Global configuration

Command History

Release	Modification
11.1(1)IA	This command was introduced.
11.1(25)IA	The *query-type* argument with **a** and **mx** keywords was added to Cisco IOS Release 11.2(25)IA.
11.1(28)IA	The Enhanced Server Verification with Multiple Port Connect Tests functionality was added to Cisco IOS Release 11.1(28)IA.
12.0(5)T	The *query-type* argument with **a** and **mx** keywords was integrated into Cisco IOS Release 12.0(5)T.
12.1(5)T	The Enhanced Server Verification with Multiple Port Connect Tests functionality was integrated into Cisco IOS Release 12.1(5)T.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The DistributedDirector redirects clients only to servers that are responsive.

When you enter several **ip director host connect** commands for the same hostname but with different port numbers, the DistributedDirector verifies that all the ports are accessible. The DistributedDirector considers the server accessible only if all the ports are accessible.

Examples

The following example shows how to set the time to 5 minutes for the distributed servers on port 80 and on port 90. The distributed servers are considered accessible only if both port 80 and port 90 are accessible.

```
Router(config)# ip director host www.xyz.com connect 80 5
Router(config)# ip director host www.xyz.com connect 90 5
```

ip director host logging

To configure a DistributedDirector to log events to syslog, use the **ip director host logging** command in global configuration mode. To turn off logging, use the **no** form of this command.

ip director host *hostname* [*query-type*] **logging**

no ip director host *hostname* [*query-type*] **logging**

Syntax Description

hostname	Name of the host that maps to one or more IP addresses. Do not use an IP address.
query-type	(Optional) Type of query. Two values are valid: • **a** indicates that the configuration is used for processing Domain Name System (DNS) address queries for the specified hostname. This is the default. • **mx** indicates that the configuration is used for processing Mail eXchange (MX) queries for the specified hostname.

Command Default

Logging is disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.1(28)IA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Event Recording with Syslog feature provides the capability to examine DNS traffic and the way in which servers are chosen. The server state is logged by default, providing a useful log of when servers are up or down. Additionally, the server selection process may be logged. In both cases, the logging priority level is informational.

Caution Extensive syslog output is generated when a server selection is logged. This feature should not be used when a heavy request load is expected.

Examples

Before a DistributedDirector is configured to log events about DNS address queries on a specific resource record, the following command must be typed on the command line:

```
Router(config)# logging 172.21.34.2
Router(config)# logging trap informational
```

Note The IP address specified in this section is the IP address of the log server in which the syslog messages are recorded.

The following examples show how to configure a DistributedDirector to log events about DNS address queries on a resource record for hostname www.xyz.com, DNS address queries on a resource record for hostname alias.xyz.com, and DNS requests on MX hostname mail.xyz.com:

```
Router(config)# ip director host www.xyz.com logging
Router(config)# ip director host alias.xyz.com a logging
Router(config)# ip director host mail.xyz.com mx logging
```

Related Commands

Command	Description
logging	Logs messages to a syslog server host,

ip director host multiple

To configure the number of resource records that a DistributedDirector returns for each Domain Name System (DNS) response, use the **ip director host multiple** command in global configuration mode. To configure a DistributedDirector to return only the best resource record for each DNS response, use the **no** form of this command.

ip director host *hostname* [*query-type*] **multiple** *integer*

no ip director host *hostname* [*query-type*] **multiple**

Syntax Description

hostname	Name of the host that maps to one or more IP addresses. Do not use an IP address.
query-type	(Optional) Type of query. Two values are valid: • **a** indicates that the configuration is used for processing DNS address queries for the specified hostname. This is the default. • **mx** indicates that the configuration is used for processing Mail eXchange (MX) queries for the specified hostname.
integer	Integer in the range of 1 to 65535 that indicates the number of servers returned.

Command Default

Only the best resource record for each DNS response is returned.

Command Modes

Global configuration

Command History

Release	Modification
11.1(28)IA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configuring a DistributedDirector to return a large volume of records may reduce the benefit of using a DistributedDirector to select the best server.

Examples

The following examples show how to configure a DistributedDirector to return the three best servers for a DNS resource record on hostname www.xyz.com, the two best servers for a DNS resource record on hostname alias.xyz.com, and the two best servers for MX resource mail.xyz.com:

```
Router(config)# ip director host www.xyz.com multiple 3
Router(config)# ip director host alias.xyz.com a multiple 2
Router(config)# ip director host mail.xyz.com mx multiple 2
```

ip director host priority

To configure the order in which the DistributedDirector considers metrics when picking a server, use the **ip director host priority** command in global configuration mode. To turn off metric priorities, use the **no** form of this command.

ip director host *host-name* **priority** {[**drp-int** *number*] [**drp-ext** *number*] [**drp-ser** *number*] [**drp-rtt** *number*] [**random** *number*] [**admin** *number*] [**portion** *number*] [**availability** *avail-number*] [**route-map** *number*]}

no ip director host *host-name* **priority** {[**drp-int** *number*] [**drp-ext** *number*] [**drp-ser** *number*] [**drp-rtt** *number*] [**random** *number*] [**admin** *number*] [**portion** *number*] [**availability** *avail-number*] [**route-map** *number*]}

host-name	Name of the host that maps to one or more IP addresses. The *host-name* argument is not an IP address.
drp-int	(Optional) Sends a Director Response Protocol (DRP) request to all DRP server agents, asking them for the distance from themselves to the edge of their Border Gateway Protocol (BGP) autonomous system in the direction of the client originating the Domain Name System (DNS) query.
drp-ext	(Optional) Sends a DRP request to all DRP server agents, asking them for the BGP distance between them and the client originating the DNS query.
drp-ser	(Optional) Sends a DRP request to all DRP server agents, asking them for the IGP route metric between them and the distributed servers that they support.
drp-rtt	(Optional) Sends a DRP request to all DRP server agents, asking them for the round-trip time between the DRP agent and the client originating the DNS query.
random	(Optional) Selects a random number for each distributed server and defines the "best" server as the one with the smallest random number assignment.
admin	(Optional) Specifies a simple preference of one server over another. If this administrative metric has been explicitly set to zero, the Director will not consider the server, so the server is taken out of service.
portion	(Optional) Assigns a load "portion" to each server such that servers with a higher portion value will receive a larger percentage of connections at any one time.
availability	(Optional) Specifies the load information for the DistributedDirector. The default value is 65535.
avail-number	(Optional) Integer in the range of 1 to 65535, inclusive.
route-map	(Optional) Specifies whether a server should be offered to a client.
number	(Optional) Integer in the range of 1 to 100, inclusive.

Command Default

The availability default value is 65535.

Command Modes

Global configuration

Command History

Release	Modification
11.1(18)IA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1 T. The **availability** and **route-map** metrics were added.
12.2(8)T	The **boomerang** metric was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Not all of the metrics need to be specified, but at least one must be specified. If the boomerang metric is specified at a given priority level, then all other metrics of lower priority (that is, having a higher priority number) for that host name are ignored. If the boomerang metric is being considered, then it is the final step in determining the best server.

The distance specified with the **drp-int** keyword can be used with the DRP external metric (**drp-ext**) to help determine the distance between the router and the client originating the DNS query.

If the client and the DRP server agent are in the same autonomous system, this metric returns the Interior Gateway Protocol (IGP) cost metric between the client and the DRP server agent.

The distance learned through the **drp-ext** keyword represents the number of BGP hops between the autonomous system of the DRP server agent and the autonomous system of the client originating the DNS query. Because this is BGP information, the DRP server agents need to have access to full Internet BGP information for this metric to be useful.

The distance learned through the **drp-ser** keyword can be used with the DRP internal metric (**drp-int**) to get a finer distance calculation between the distributed servers and the edge of the BGP autonomous system in the direction of the client originating the DistributedDirector query.

If a true BGP border router is used as a DRP server agent, the DRP server metric will return the IGP route metric between the distributed server and the BGP border router (autonomous system edge). Because DRP server metrics should not change frequently, DistributedDirector issues DRP server queries (and caches the results) every 10 minutes.

Using the **random** keyword alone results in random redirection of clients to the distributed servers. Because this metric requires no routing table information, it does not trigger DRP requests to the DRP server agents.

The **availability** keyword allows the DistributedDirector to attempt to create a TCP connection to each distributed server on a configured port over a configurable time interval.

If multiple servers end up with the same metric value, the next metric is considered to determine the “best” server. If multiple metrics have the same priority value, the metrics are added to obtain a *composite metric*. For example, if two metrics have the same priority value, they are first multiplied by their weight values (if specified) and then added together to form the composite metric.

If you do not specify weights for a group of distributed servers, there are no default weights for the Director, and if you have specified priority values, the weight values are set to 1.

Any metrics that have a nonzero weight and that are assigned no priority value are set to a priority value of 101. They are considered after all other metrics that have priority values. As a result, if no priority values are specified for any metric, metrics are treated additively to form one composite metric.

If you do not use priority and multiple servers have the same metric value, the server whose last IP address was looked at will be returned as the "best" server. If you want to return a random IP address in the case of a tie, use metric priority with the **random** metric as the last criterion.

To turn off all priorities on all metrics associated with the defined host name, use the **no ip director host priority** command. You can turn off the priority for a specific metric or metrics using the **no ip director host** *host-name* **priority** [**drp-int** *number*] [**drp-ext** *number*] [**drp-ser** *number*] [**drp-rtt** *number*] [**random** *number*] [**admin** *number*] [**portion** *number*] [**availability** *number*] [**route-map** *number*] command.

Examples

The following example sets the external metric as the first priority and the administrative metric as the second priority:

```
Router(config)# ip director host www.xyz.com priority drp-ext 1 admin 2
```

The following example specifies the per-host priority of the metric, with a host named boom1, where the DRP internal metric is specified with a priority number of 1 and boomerang is specified with a priority number of 2:

```
Router(config)# ip director host BOOM1 priority drp-int 1 boomerang 2

Router(config)# do show running-config

ip host BOOM1 172.2.2.10 172.2.2.20 172.2.2.30
.
.
.
ip director host BOOM1
no ip director cache
ip dns primary boom1 soa boom1 boom1@com
ip director host boom1 priority drp-int 1 boomerang 2
```

Related Commands

Command	Description
ip director default priorities	Sets a default priority for a specific metric on DistributedDirector.
ip director default weights	Configures default weight metrics for DistributedDirector.
ip director host connect	Enables the DistributedDirector to verify that a server is available.
ip director host weights	Sets host-specific weights for the metrics that DistributedDirector uses to determine the best server within a specific host name.
show ip director default priority	Verifies the default configurations of DistributedDirector metrics.
show ip director default weights	Shows DistributedDirector default weights.
show ip director hosts	Displays DistributedDirector host information.

ip director host tolerance

To associate a tolerance for a specified load range with a specified priority level, use the **ip director host tolerance** command in global configuration mode. To turn off tolerance, use the **no** form of this command.

ip director host *hostname* **tolerance** *priority-level percentage*

no ip director host *hostname* **tolerance** *priority-level percentage*

Syntax Description

hostname	Domain Name Server (DNS) name.
priority-level	Integer in the range of 0 to 65535 that sets the order of importance that a DistributedDirector uses when it selects the best server for a hostname.
percentage	Percentage of tolerance. The range is 1 to 100.

Command Default

No tolerance level is specified.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If two or more remote servers have metrics at the same priority level and the levels are within a specified load range of each other, consider them to be at the same level. In this case, a DistributedDirector uses the next highest priority level to select the best server.

Examples

The following example shows how to configure a DistributedDirector to be directed to the closest server farm (measured using the round-trip time metric) if the loads on the server farms are within 20 percent of each other.

```
Router(config)# ip director host www.xyz.com priority availability 1 drp-rtt 2
Router(config)# ip director host www.xyz.com port 80
Router(config)# ip director host www.xyz.com tolerance 1 20
```

ip director host verify-url

To configure a DistributedDirector to search for a URL string at a specific time interval, use the **ip director host verify-url** command in global configuration mode. To turn off this URL search, use the **no** form of this command.

ip director host *hostname* **verify-url** *url* **connection-interval** *seconds*

no ip director host *hostname* **verify-url** *url* **connection-interval** *seconds*

Syntax Description

hostname	Domain Name Server (DNS) name.
url	URL for verification.
connection-interval	Specifies that a search is performed at a specific time interval.
seconds	Integer in the range of 10 to 32767 that specifies the time, in seconds, between searches.

Command Default

No URL search is specified.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If a URL is found and an HTTP reply code is received, the DistributedDirector marks all servers associated with the hostname as being up. If an error code is received, the DistributedDirector marks all servers associated with the hostname as being down. Servers that are in a down state cannot be selected.

If verification URLs have been configured for both a hostname and a specific server, the status returned from the connection on behalf of the specific server overrides the configuration because the status is considered more specific than a single hostname. The same URL may be specified for verifying multiple pairs, in which case the smallest configured availability checks will be used for all pairs and one connection will be made to verify all pairs.

Using the **ip director host verify-url** command in conjunction with the **ip director host connect** command causes a DistributedDirector to simultaneously run one instance of each keepalive process. Using these two commands together may cause IP address availability to flap if the **ip director host connect** probe succeeds and the **ip director host verify-url** probe fails or vice versa. Running both of these probes for the same domain is not recommended.

Examples

The following example shows how to configure a DistributedDirector to search for the URL string http://www.xyz.com/index.html every 120 seconds:

```
Router(config)# ip director host www.xyz.com port-service 80
Router(config)# ip director host www.xyz.com verify-url http://www.xyz.com/index.html
connection-interval 120
```

Related Commands

Command	Description
ip director host connect	Enables a DistributedDirector to verify that a server is available.

ip director host weights

To set host-specific weights for the metrics that the DistributedDirector uses to determine the best server within a specific host name, use the **ip director host weights** command in global configuration mode. To turn off weights for a host, use the **no** form of this command.

ip director host *host-name* **weights** {[**drp-int** *number*] [**drp-ext** *number*] [**drp-ser** *number*] [**drp-rtt** *number*] [**random** *number*] [**admin** *number*] [**portion** *number*] [**availability** *avail-number*] [**route-map** *number*]}

no ip director host *host-name* **weights** {[**drp-int** *number*] [**drp-ext** *number*] [**drp-ser** *number*] [**drp-rtt** *number*] [**random** *number*] [**admin** *number*] [**portion** *number*] [**availability** *avail-number*] [**route-map** *number*]}

Syntax Description

host-name	Name of the host that maps to one or more IP addresses. The *host-name* argument is not an IP address.
drp-int	(Optional) Sends a Director Response Protocol (DRP) request to all DRP server agents, asking them for the distance from themselves to the edge of their Border Gateway Protocol (BGP) autonomous system in the direction of the client originating the Domain Name System (DNS) query.
drp-ext	(Optional) Sends a DRP request to all DRP server agents, asking them for the BGP distance between them and the client originating the DNS query.
drp-ser	(Optional) Sends a DRP request to all DRP server agents, asking them for the IGP route metric between them and the distributed servers that they support.
drp-rtt	(Optional) Sends a DRP request to all DRP server agents, asking them for the round-trip time between the DRP agent and the client originating the DNS query.
random	(Optional) Selects a random number for each distributed server and defines the "best" server as the one with the smallest random number assignment.
admin	(Optional) Specifies a simple preference of one server over another. If this administrative metric has been explicitly set to zero, the Director will not consider the server, so the server is taken out of service.
portion	(Optional) Assigns a load "portion" to each server such that servers with a higher portion value will receive a larger percentage of connections at any one time.
availability	(Optional) Specifies the load information for the DistributedDirector. The default value is 65535.
avail-number	(Optional) Integer in the range of 1 to 65535, inclusive.
route-map	(Optional) Specifies whether a server should be offered to a client.
number	(Optional) Integer in the range of 1 to 100, inclusive.

Note No host weights are set. If the **ip director default-weights** command is configured, the configured weights are the default.

Command Default

The availability default value is 65535.

Command Modes

Global configuration

Command History

Release	Modification
11.1(25)IA	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.1(5)T	The **availability** and **route-map** metrics were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use host-specific weights when you want to use different metric weights for different virtual host names (for example, www.xyz.com and ftp.xyz.com).

The distance specified with the **drp-int** keyword can be used with the DRP external metric (**drp-ext**) to help determine the distance between the router and the client originating the DNS query.

If the client and the DRP server agent are in the same autonomous system, this metric returns the Interior Gateway Protocol (IGP) cost metric between the client and the DRP server agent.

The distance learned through the **drp-ext** keyword represents the number of BGP hops between the autonomous system of the DRP server agent and the autonomous system of the client originating the DNS query. Because this is BGP information, the DRP server agents need to have access to full Internet BGP information for this metric to be useful.

The distance learned through the **drp-ser** keyword can be used with the DRP internal metric (**drp-int**) to get a finer distance calculation between the distributed servers and the edge of the BGP autonomous system in the direction of the client originating the DistributedDirector query.

If a true BGP border router is used as a DRP server agent, the DRP server metric will return the IGP route metric between the distributed server and the BGP border router (autonomous system edge). Because DRP server metrics should not change frequently, DistributedDirector issues DRP server queries (and caches the results) every 10 minutes.

Using the **random** keyword alone results in random redirection of clients to the distributed servers. Because this metric requires no routing table information, it does not trigger DRP requests to the DRP server agents.

The new availability metric allows the DistributedDirector to attempt to create a TCP connection to each distributed server on a configured port over a configurable time interval.

If desired, host-specific weights can instead be configured on the DistributedDirector default DNS server.

For example, you could configure host-specific weights with the following DNS TXT record:

```
hostname in txt "ciscoDD: weights {[drp-int number] [drp-ext number] [drp-ser number]
[random number] [admin number]}"
```

To use the default weights for all metrics associated with this host name, use the **no ip director host weights** command. To use the default weights for a specific metric or metrics, use the **no ip director host** *host-name* **weights** [**drp-int** *number*] [**drp-ext** *number*] [**drp-ser** *number*] [**drp-rtt** *number*] [**random** *number*] [**admin** *number*] [**portion** *number*] [**availability** *number*] [**route-map** *number*] command.

Examples

The following example shows how to set the DRP internal metric to 4:

```
Router(config)# ip director host www.xyz.com weights drp-int 4
```

Related Commands

Command	Description
ip director default-weights	Configures default weight metrics for the DistributedDirector.
show ip director dfp	Displays information about the current status of the DistributedDirector connections with a particular DFP agent.

ip director server availability

To configure a default availability value for all ports on a server, use the **ip director server availability** command in global configuration mode. To restore the default, use the **no** form of this command.

ip director server *ip-address* **availability** {*availability-value* | **dfp** [*availability-value*]}

no ip director server *ip-address* **availability** {*availability-value* | **dfp** [*availability-value*]}

Syntax Description

ip-address	IP address of the IP director server.
availability-value	Integer in the range from 0 to 65535 that specifies the availability value as it would be represented on the DistributedDirector system. (Optional) When used with the **dfp** keyword, the availability value is for the LocalDirector system.
dfp	Specifies that Dynamic Feedback Protocol is configured.

Command Default

The availability default value is 65535.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

There are two methods for specifying a default availability value. These two methods exist because the LocalDirector and the DistributedDirector deal with values in two different ways. All metrics for the DistributedDirector are arranged such that lower is better; however the LocalDirector load information is calculated such that higher is better. Thus, the DistributedDirector translates the metric value upon receipt from the LocalDirector by subtracting the availability from the maximum possible value of 65535.

Examples

To configure a default availability to be used if there is no other valid availability information, the following configuration would suffice. The following example shows how to specify the LocalDirector load and DistributedDirector availability, respectively:

```
Router(config)# ip director server 10.0.0.1 availability dfp 1
Router(config)# ip director server 10.0.0.1 availability 65534
```

To make the availability clear and to allow for specifying numbers in both schemes easily, there are two methods of specifying availability information. If the servers are running multiple serves, it may be necessary to configure the default availability value on a per-port basis by using the **ip director server port availability** command.

```
Router(config)# ip director server 10.0.0.1 port availability dfp 65535
Router(config)# ip director server 10.0.0.20 port availability dfp 65535
```

Related Commands

Command	Description
ip director server port availability	Configures a default availability value for a specific port on a server.

ip director server port availability

To configure a default availability value for a specific port on a server, use the **ip director server port availability** command in global configuration mode. To restore the default, use the **no** form of this command.

ip director server *ip-address* **port availability** {*availability-value* | **dfp** [*availability-value*]}

no ip director server *ip-address* **port availability** {*availability-value* | **dfp** [*availability-value*]}

Syntax Description

ip-address	IP address of the IP director server.
availability-value	Integer in the range from 0 to 65535 that specifies the availability value as it would be represented on the DistributedDirector system. (Optional) When used with the **dfp** keyword, the availability value is for the LocalDirector system.
dfp	Specifies that Dynamic Feedback Protocol is configured.

Command Default

The availability default value is 65535.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Two methods are available for specifying a default availability value because the LocalDirector and the DistributedDirector process these values differently. All metrics for the DistributedDirector are arranged such that a lower value is better. The LocalDirector load information is calculated such that a higher value is better. As a result, the DistributedDirector translates the metric value upon receipt from the LocalDirector by subtracting the availability from the maximum possible value of availability value.

Examples

The following examples show how to make the availability clear and how to specify numbers in both methods.

If the servers are running multiple serves, it may be necessary to configure the default availability value on a per-port basis by using the **ip director server port availability** command.

```
Router(config)# ip director server 10.0.0.1 port availability dfp 65535
Router(config)# ip director server 10.0.0.20 port availability dfp 65535
```

The following example shows how to configure the LocalDirector load and DistributedDirector availability, respectively, when there is no other valid availability information.

```
Router(config)# ip director server 10.0.0.1 availability dfp 1
Router(config)# ip director server 10.0.0.1 availability 65534
```

Related Commands

Command	Description
ip director server availability	Configures a default availability value for all ports on a server.

ip director server reinstatement

To configure a DistributedDirector to automatically detect when a server is running and mark it as available, use the **ip director server reinstatement** command in global configuration mode. To restore the default, use the **no** form of this command.

ip director server *ip-address* **reinstatement**

no ip director server *ip-address* **reinstatement**

Syntax Description

ip-address	IP address of the server.

Command Default

Automatic server reinstatement is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If a DistributedDirector detects that a server is unavailable and the DistributedDirector has enabled that server to be restored to its previous effective state, the **ip director server reinstatement** command must be issued to bring the server up again.

When a DistributedDirector detects that a server is unavailable, it stops attempting to create a TCP connection to that server. The exception is when the DistributedDirector was configured by a user to continue connection attempts.

Examples

The following example shows how to configure a DistributedDirector to automatically detect if server 10.0.0.1 is running. If server 10.0.0.1 is not running, traffic is redirected to server 10.0.0.2.

```
Router(config)# ip director server 10.0.0.1 reinstatement
Router(config)# ip director server 10.0.0.2 reinstatement
```

ip director server route-map

To configure a DistributedDirector to use the source autonomous systems identifier as a server-selection criterion, use the **ip director server route-map** command in global configuration mode. To restore the default, use the **no** form of this command.

ip director server *ip-address* **route-map** *map-name*

no ip director server *ip-address* **route-map** *map-name*

Syntax Description

ip-address	IP address of the server.
map-name	Name of the route map.

Command Default

Use of the autonomous systems identifier as a selection criterion is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Each autonomous system that makes up the Internet has a numeric identifier that routing protocols use. The **ip director server route-map** command provides a way for a DistributedDirector to use the source autonomous system (the autonomous system in which the client resides) identifier as a server-selection criterion.

The route-map mechanism is normally used in Cisco IOS software to map or associate routes from one routing protocol to another. For example, a route learned via Open Shortest Path First (OSPF) could be passed or mapped to Routing Information Protocol (RIP). The **ip director server route-map** command uses the existing route-map infrastructure to access routing data.

For the route-map mechanism to run correctly, the **ip host**, **ip dns primary**, and **ip director host** commands must be configured before issuing the **ip director server route-map** command.

Examples

The following example shows how to configure a DistributedDirector to have all clients using autonomous system 200 use server 10.0.0.2 and all other clients use server 10.0.0.1:

```
Router(config)# ip host www.xyz.com 10.0.0.1 10.0.0.2
Router(config)# ip dns primary www.xyz.com soa ns.xyz.com blank.com
Router(config)# ip director host www.xyz.com priority route-map 1
Router(config)# ip director server 10.0.0.1 route-map block200
Router(config)# ip director server 10.0.0.2 route-map allow200
Router(config)# ip as-path access-list 100 permit 200
Router(config)# ip as-path access-list 101 deny 200
Router(config)# route-map allow 200 permit 1
Router(config)# match as-path 100
Router(config)# route-map block200 permit 1
Router(config)# match as-path 101
```

Related Commands

Command	Description
ip director host	Defines the virtual hostname to be used for the distributed servers.
ip dns primary	Identifies the DistributedDirector as the primary DNS name server for a domain and as the statement-of-authority record source.
ip host	Defines a static hostname-to-address mapping in the host cache.

ip director server verify-url

To configure a DistributedDirector to search for a URL string with a specified server and at a specific time interval, use the **ip director server verify-url** command in global configuration mode. To turn off this URL search, use the **no** form of this command.

ip director server *ip-address port* **verify-url** *string* **connection-interval** *seconds*

no ip director server *ip-address port* **verify-url** *string* **connection-interval** *seconds*

Syntax Description

ip-address	IP address of the server.
port	Port number to be associated with the host.
string	Full URL or pathname.
connection-interval	Specifies a time between availability checks.
seconds	Time, in seconds, between availability checks.

Command Default

No URL search is specified.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If a URL is found and an HTTP reply code is received, the DistributedDirector marks all servers associated with the hostname as being up. If an error code is received, the DistributedDirector marks all servers associated with the hostname as being down. Servers that are in a down state cannot be selected.

If verification URLs have been configured for both a hostname and a specific server, the status returned from the connection on behalf of the specific server overrides the configuration because the status is considered more specific than a single hostname. The same URL may be specified for verifying multiple pairs, in which case the smallest configured availability checks are used for all pairs and one connection is made to verify all pairs.

Examples

The following example shows how to configure a DistributedDirector to search the server with IP address 10.0.0.1, port 80, for the URL string http://www.xyz.com/index.html every 120 seconds:

```
Router(config)# ip director server 10.0.0.1 80 verify-url http://www.xyz.com/index.html
connection-interval 120
```

ip director server weights

To configure a "per-service per-metric" weight, use the **ip director server weights** command in global configuration mode. To turn off a metric weight configuration, use the **no** form of this command.

ip director server *ip-address port* **weights** *metric-name metric-weight*

no ip director server *ip-address port* **weights** *metric-name metric-weight*

Syntax Description

ip-address	IP address of the server.
port	Port number to be associated with the host.
metric-name	Name of the metric used.
metric-weight	Weight of the metric used.

Command Default

No per-service-per-metric weight is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the metric name is referenced with respect to this server and port, the value of the metric is multiplied by the metric weight.

Examples

The following example shows how to configure a DistributedDirector to check port 80 for an availability metric of 3.

```
Router(config)# ip director server 10.0.0.1 80 weights availability 3
```

ip dns server

To enable the Domain Name System (DNS) server on a router, use the **ip dns server** command in global configuration mode. To disable the DNS server, use the **no** form of the command.

ip dns server

no ip dns server

Syntax Description

This command has no arguments or keywords.

Command Default

The DNS server is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

Use this command to enable the DNS server as needed.

Examples

In the following example, the DNS server is enabled:

```
Router(config)# ip dns server
```

ip drp access-group

To control the sources of Director Response Protocol (DRP) queries to the DRP server agent, use the **ip drp access-group** command in global configuration mode. To remove the access list, use the **no** form of this command.

ip drp access-group *access-list-number*

no ip drp access-group *access-list-number*

Syntax Description

access-list-number	Number of a standard IP access list in the range from 1 to 99 or from 1300 to 1999.

Defaults

The DRP server agent will answer all queries.

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies an access list to the interface, thereby controlling which devices can send queries to the DRP Server Agent.

If both an authentication key chain and an access group have been specified, both security measures must permit access before a request is processed.

Examples

The following example configures access list 1, which permits only queries from the host at 10.45.12.4:

```
Router(config)# access-list 1 permit 10.45.12.4
Router(config)# ip drp access-group 1
```

Related Commands

Command	Description
ip drp authentication key-chain	Configures authentication on the DRP Server Agent for DistributedDirector.
show ip drp	Displays information about the DRP Server Agent for DistributedDirector.

ip drp authentication key-chain

To configure authentication on the Director Response Protocol (DRP) Server Agent for DistributedDirector, use the **ip drp authentication key-chain** command in global configuration mode. To remove the key chain, use the **no** form of this command.

ip drp authentication key-chain *name-of-chain*

no ip drp authentication key-chain *name-of-chain*

Syntax Description

name-of-chain	Name of the key chain containing one or more authentication keys.

Defaults

No authentication is configured for the DRP Server Agent.

Command Modes

Global configuration

Command History

Release	Modification
11.2F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When a key chain and key are configured, the key is used to authenticate all DRP requests and responses. The active key on the DRP Server Agent must match the active key on the primary agent. Use the **key** and **key-string** commands to configure the key.

Examples

The following example configures a key chain named *ddchain*:

```
Router(config)# ip drp authentication key-chain ddchain
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ip drp access-group	Controls the sources of DRP queries to the DRP Server Agent.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

Command	Description
show ip drp	Displays information about the DRP Server Agent for DistributedDirector.
show key chain	Displays authentication key information.

ip drp domain

To add a new domain to the DistributedDirector client or to configure an existing domain, use the **ip drp domain** command in global configuration mode. To remove this 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.

ip drp domain *domain-name*

no ip drp domain *domain-name*

Syntax Description

domain-name	The specified domain name.

Command Default

No default domain is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ip drp domain** command can be used only on a Director Response Protocol (DRP) agent. The boomerang client is the DRP agent.

Enabling this command puts the client in boomerang configuration mode.

Use the **ip drp domain** command to enter a new or existing domain name. Entering a new domain name creates a new domain, and entering an existing domain name allows the user to configure the specified domain. When a domain name is configured on the boomerang client, the user can configure specific parameters, such as server address, aliases, and time to live (TTL) values, for that domain.

When a Director Response Protocol (DRP) agent receives a Domain Name System (DNS) racing message from boomerang servers such as DistributedDirector, the DRP agent extracts the specified domain name (for example, www.cisco.com) in the DNS message.

Examples

In the following example, a domain named "www.boom1.com" is added on the boomerang client:

```
Router(config)# ip drp domain www.boom1.com

Router# show running-config
.
.
.
ip drp domain www.boom1.com
```

Related Commands

Command	Description
alias (boomerang)	Configures an alias name for a specified domain.
server (boomerang)	Configures the server address for a specified boomerang domain.
show ip drp	Displays DRP statistics on DistributedDirector or a DRP server agent.
show ip drp boomerang	Displays boomerang information on the DRP agent.
ttl dns	Configures the number of seconds for which an answer received from the boomerang client will be cached by the DNS client.
ttl ip	Configures the IP TTL value for the boomerang response packets sent from the boomerang client to the DNS client in number of hops.

ip drp server

To enable the Director Response Protocol (DRP) Server Agent that works with DistributedDirector, use the **ip drp server** command in global configuration mode. To disable the DRP Server Agent, use the **no** form of this command.

ip drp server

no ip drp server

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example enables the DRP Server Agent:

```
Router(config)# ip drp server
```

Related Commands

Command	Description
ip drp access-group	Controls the sources of DRP queries to the DRP Server Agent.
ip drp authentication key-chain	Configures authentication on the DRP Server Agent for DistributedDirector.
show ip drp	Displays information about the DRP Server Agent for DistributedDirector.

ip host ns

To create a name server (NS) resource record to be returned when a Domain Name System (DNS) server is queried for the associated domain, use the **ip host ns** command in global configuration mode. To remove the NS records, use the **no** form of this command.

ip host *domain-name* **ns** *server-name*

no ip host *domain-name* **ns** *server-name*

Syntax Description

domain-name	Name of the authority that is delegated to another NS, such as a second-level DistributedDirector.
server-name	Name of the second-level DNS server.

Command Default

None.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

The **ip host ns** command allows a DistributedDirector to distribute the server selection process to multiple DistributedDirectors, providing greater scalability and better administrative control.

A DNS server can delegate responsibility for a domain to another DNS server by returning an NS record when queried. This task is especially useful to a DistributedDirector because determining the best DNS reply may be time consuming. To expedite replies, a DistributedDirector can return an NS record, delegating authority for the requested data to one or more second-level DistributedDirectors.

Examples

The following example shows a top-level DistributedDirector that uses the low-cost metric random to distribute its load over second-level DistributedDirectors:

Top-Level DistributedDirector

```
Router(config)# ip host www.xyz.com ns ns.xyz.com
Router(config)# ip host ns2.xyz.com 10.0.0.1 10.0.0.2 10.0.0.3
Router(config)# ip director host ns.xyz.com priority random 1
Router(config)# ip dns primary www.xyz.com soa ns2.xyz.com
```

The following example shows second-level DistributedDirectors that use more expensive metrics such as drp-ext and drp-rtt to perform precise server selection.

Second-Level DistributedDirector

```
Router(config)# ip host www.xyz.com 10.0.0.4 10.0.0.5 10.0.0.6
Router(config)# ip director host www.xyz.com priority drp-ext 1
Router(config)# ip director host www.xyz.com priority drp-rtt 2
Router(config)# ip director server 10.0.0.4 drp-association 10.0.0.7
Router(config)# ip director server 10.0.0.5 drp-association 10.0.0.8
Router(config)# ip director server 10.0.0.6 drp-association 10.0.0.9
```

ip http access-class

To specify the access list that should be used to restrict access to the HTTP server, use the **ip http access-class** command in global configuration mode. To remove a previously configured access list association, use the **no** form of this command.

ip http access-class *access-list-number*

no ip http access-class *access-list-number*

Syntax Description

access-list-number	Standard IP access list number in the range 0 to 99, as configured by the **access-list** global configuration command.

Command Default

No access list is applied to the HTTP server.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

If this command is configured, the specified access list is assigned to the HTTP server. Before the HTTP server accepts a connection, it checks the access list. If the check fails, the HTTP server does not accept the request for a connection.

Examples

The following example shows how to define an access list as 20 and assign it to the HTTP server:

```
Router(config)# ip access-list standard 20
Router(config-std-nacl)# permit 209.165.202.130 0.0.0.255
Router(config-std-nacl)# permit 209.165.201.1 0.0.255.255
Router(config-std-nacl)# permit 209.165.200.225 0.255.255.255
! (Note: all other access implicitly denied)
Router(config-std-nacl)# exit
Router(config)# ip http access-class 20
```

Related Commands

Command	Description
ip access-list	Assigns an ID to an access list and enters access list configuration mode.
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

ip http accounting commands

To specify a particular command accounting method for HTTP server users, use the **ip http accounting commands** command in global configuration mode. To disable a configured command accounting method, use the **no** form of this command.

ip http accounting commands *level* {**default** | *named-accounting-method-list*}

no ip http accounting commands *level*

level	Indicates a privilege value from 0 to 15. By default, there are the following three command privilege levels on the router: • 0—Includes the **disable**, **enable**, **exit**, **help**, and **logout** commands. • 1—Includes all user-level commands at the router prompt (>). • 15—Includes all enable-level commands at the router prompt (>).
default	Indicates the **default** accounting method list configured by the **aaa accounting** commands CLI.
named-accounting-method-list	Indicates the name of the predefined command accounting method list.

Command Default

Command accounting for HTTP and HTTP over Secure Socket Layer (HTTPS) is automatically enabled when authentication, authorization, and accounting (AAA) is configured on the device. It is not possible to dissable accounting for HTTP and HTTPS. HTTP and HTTPS will default to using the global AAA default method list for accounting. The CLI can be used to configure HTTP and HTTPS to use any predefined AAA method list.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **ip http accounting commands** command is used to specify a particular command accounting method for HTTP server users.

Command accounting provides information about the commands for a specified privilege level that are being executed on a device. Each command accounting record corresponds to one IOS command executed at its respective privilege level, as well as the date and time the command was executed, and the user who executed it. Command accounting will be implemented for HTTP and HTTPS. A stop accounting record will be generated for any CLI execution/configuration done by a user via HTTP and HTTPS.

If this command is not configured, HTTP and HTTPS will use the default AAA accounting list whenever AAA is turned-on using **aaa new-model** configuration CLI. If the default method-list doesn't exist, no accounting records will be generated. Whenever AAA is not turned-on, again no accounting records will be generated.

Note The above behavior is essential to maintain consistency of HTTP and HTTPS accounting CLI with their counterparts available for Telnet/SSH in the IOS line configuration mode.

Examples

The following example shows how to configure HTTP and HTTPS to allow AAA accounting support:

```
Router(config)# ip http accounting commands 1 oneacct
```

Related Commands

Command	Description
aaa authentication login	Specifies the login authentication method to be used by the AAA service.
aaa authorization	Sets parameters that restrict user access to a network.
aaa new-model	Enables the AAA access control model.
ip http authentication aaa	Specifies a particular authentication method for HTTP server users.
ip http server	Enables the HTTP server.

ip http active-session-modules

To selectively enable HTTP applications that will service incoming HTTP requests from remote clients, use the **ip http active-session-modules** command in global configuration mode. Use the **no** form of this command to return to the default, for which all HTTP services will be enabled.

ip http active-session-modules {*listname* | **none** | **all**}

no ip http active-session-modules {*listname*}

Syntax Description

listname	Enables only those HTTP services configured in the list identified by the **ip http session-module-list** command to serve HTTP requests. All other HTTP or HTTPS applications on the router or switch will be disabled.
none	Disables all HTTP services.
all	Enables all HTTP applications to service incoming HTTP requests from remote clients.

Defaults

If no arguments or keywords are specified, all HTTP services will be enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Use the **ip http active-session-modules** command to selectively enable HTTP applications, for servicing incoming HTTP requests from remote clients. With this command, a selected list of applications can be enabled. All the applications can be enabled or none of the applications can be enabled, in other words, all disabled. Use the **ip http session-module-list** command to define a list of HTTP or secure HTTP (HTTPS) application names to be enabled. If an HTTP request is made for a service that is disabled, a 404 error message is displayed in the remote client browser.

Note The HTTPS server is not supported in Cisco IOS Release 12.2(31)SB.

Examples

The following example shows how to configure a different set of services to be available for HTTP and HTTPS requests. In this example, all HTTP applications are enabled for providing services to remote clients, but for HTTPS services, only the HTTPS applications defined in list1 (Simple Certificate Enrollment Protocol [SCEP] and HOME_PAGE) are enabled.

```
ip http session-module-list list1 SCEP,HOME_PAGE
ip http active-session-modules all
ip http server
ip http secure-server
ip http secure-active-session-modules list1
```

Related Commands

Command	Description
ip http secure-active-session-modules	Selectively enables HTTPS applications that will service incoming HTTPS requests from remote clients.
ip http session-module-list	Defines a list of HTTP or HTTPS application names.
show ip http server	Displays details about the current configuration of the HTTP server.

ip http authentication

To specify a particular authentication method for HTTP server users, use the **ip http authentication** command in global configuration mode. To disable a configured authentication method, use the **no** form of this command.

ip http authentication {**aaa** {**command-authorization** *level listname* | **exec-authorization** *listname* | **login-authentication** *listname*} | **enable** | **local** | **tacacs**}

no ip http authentication {**aaa** {**command-authorization** *level listname* | **exec-authorization** *listname* | **login-authentication** *listname*} | **enable** | **local** | **tacacs**}

Syntax Description

aaa	Indicates that the authentication method used for the authentication, authorization, and accounting (AAA) login service should be used for authentication. The AAA login authentication method is specified by the **aaa authentication login default** command, unless otherwise specified by the **login-authentication** *listname* keyword and argument.
command-authorization	Sets the authorization method list for commands at the specified privilege level.
level	Indicates a privilege value from 0 through 15. By default, there are the following three command privilege levels on the router: • 0—Includes the **disable**, **enable**, **exit**, **help**, and **logout** commands. • 1—Includes all user-level commands at the router prompt (>). • 15—Includes all enable-level commands at the router prompt (>).
listname	Sets the name of the method list.
exec-authorization	Sets the method list for EXEC authorization, which applies authorization for starting an EXEC session.
login-authentication	Sets the method list for login authentication, which enables AAA authentication for logins.
enable	Indicates that the "enable" password should be used for authentication. (This is the default method.)
local	Indicates that the login user name, password and privilege level access combination specified in the local system configuration (by the **username** global configuration command) should be used for authentication and authorization.
tacacs	Indicates that the TACACS (or XTACACS) server should be used for authentication.

Defaults

The "enable" password is required when users (clients) connect to the HTTP server.
Three command privilege levels exist on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2 F	This command was introduced.
12.3(8)T	The **tacacs** keyword was removed. The **command-authorization**, **exec-authorization**, and **login-authentication** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

The **ip http authentication** command specifies the authentication method to be used for login when a client connects to the HTTP server. Use of the **aaa** option is recommended. The **enable**, **local**, and **tacacs** methods should be specified using the **aaa authentication login** command.

The “enable” password method is the default HTTP server authentication method. If the enable password is used as the HTTP server login authentication method, the client connects to the HTTP server with a default privilege level of 15.

Note When the “enable” password is used as the HTTP server login authentication method, any username entered will be ignored; the server will only verify the “enable” password. This may make it easier for an attacker to access the router. Because a username and password pair is more secure than using only a password for authentication, using only “enable” password for authentication is strongly discouraged. Instead, use of the **local** or **tacacs** authentication options, configured as part of a global AAA framework, is recommended.
To configure HTTP access as part of a AAA policy, use the **aaa** command option. The **local**, **tacacs**, or **enable** authentication methods should then be configured using the **aaa authentication login** command.

Examples

The following example shows how to specify that AAA should be used for authentication for HTTP server users. The AAA login method is configured as the “local” username/password authentication method. This example also shows how to specify using the local username database for login authentication and EXEC authorization of HTTP sessions:

```
Router(config)# aaa authentication login LOCALDB local
Router(config)# aaa authorization exec LOCALDB local
Router(config)# ip http authentication aaa login-authentication LOCALDB
Router(config)# ip http authentication aaa exec-authorization LOCALDB
```

Related Commands

Command	Description
aaa authentication login	Specifies the login authentication method to be used by the AAA service.
aaa authorization	Sets parameters that restrict user access to a network.
ip http server	Enables the HTTP server.

ip http client cache

To configure the HTTP client cache, use the **ip http client cache** command in global configuration mode. To remove the specification of a value configured for the HTTP client cache, use the **no** form of this command.

ip http client cache {**ager interval** *minutes* | **memory** {**file** *file-size-limit* | **pool** *pool-size-limit*}

no ip http client cache {**ager interval** | **memory** {**file** | **pool**}}

Syntax Description

ager	Specifies a cache ager interval time
interval	Specifies an interval, in minutes.
minutes	Frequency, in minutes, at which the router removes expired cached responses from the HTTP client cache pool. The range is from 0 to 60. The default is 5. **Note** The explicit expiration time for a cached response can be provided by the origin server. If this information is not configured, the HTTP cache uses heuristic calculations to determine a plausible expiration time for the cached response.
memory	Specifies the maximum memory allowed for HTTP client cache.
file	Specifies the maximum file size allowed for caching.
file-size-limit	Maximum file size, in kilobytes, supported by the HTTP client cache. The range is from 1 to10, and the default is 2.
pool	Specifies the maximum memory pool allowed for HTTP cache.
pool-size-limit	Maximum memory pool size, in kilobytes. The range is from 0 to 100. The default is 100.

Command Default

5 second ager interval for the HTTP client cache memory pool
2 KB maximum file size supported by the HTTP client cache
100 KB maximum memory pool size for the HTTP client cache

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to specify the HTTP client cache ager interval, maximum file size, or maximum memory pool size.

To display the values configured by this command, use the **show ip http client cache** command.

Examples

The following example shows how to specify an HTTP client cache ager interval of 10 minutes:

```
Router(config)# ip http client cache ager interval 10
```

The following example shows how to specify an HTTP client cache maximum file size of 7 KB:

```
Router(config)# ip http client cache memory file 7
```

The following example shows how to specify an HTTP client cache maximum memory pool size of 55 KB:

```
Router(config)# ip http client cache memory pool 55
```

Related Commands

Command	Description
copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
debug ip http client	Enables debugging output for the HTTP client.
ip http client connection	Configures the HTTP client connection.
ip http client password	Configures a password for all HTTP client connections.
ip http client proxy-server	Configures an HTTP proxy server.
ip http client response	Configures HTTP client characteristics for managing HTTP server responses to request messages.
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.
show ip http client	Displays a report about the HTTP client.

ip http client connection

To configure characteristics for HTTP client connections to a remote HTTP server for all file transfers, use the **ip http client connection** command in global configuration mode. To remove the specification of a value configured for a connection characteristic, use the **no** form of this command.

ip http client connection {**forceclose** | **idle timeout** *seconds* | **retry** *count* | **timeout** *seconds*}

no ip http client connection {**forceclose** | **idle** | **retry** | **timeout**}

Syntax Description

forceclose	Disables a persistent connection. Enabled by default.
idle timeout	Sets the period of time allowed for an idle connection between an HTTP client and server before the connection is closed.
seconds	Integer in the range of 1 to 60 that specifies the number of seconds allowed for an idle connection before the connection is closed. The default is 30.
retry	Sets the connection establishment timeout. Accepted range is from 1 to 5 retries, and the default is 1.
count	Number of connection attempts, in the range of 1 to 5. The default is 1.
timeout	Sets the maximum time an HTTP client will wait for a connection.
seconds	Maximum time, in seconds, that an HTTP client will wait for a connection. Accepted range is from 1 to 60 seconds, and the default is 10.

Defaults

Persistent connection maintenance is enabled.
30-second idle timeout
1 retry attempt
10-second maximum timeout

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to change or remove the specification of a value configured as a characteristics for establishing an HTTP client connection to a remove HTTP server for all file transfers.

Examples

The following example shows how to configure the default HTTP client persistent connection for a 15-second idle connection period. The maximum time the HTTP client will wait for a connection is 10 seconds.

```
Router(config)# ip http client connection idle timeout 15
```

Related Commands

Command	Description
copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
debug ip http client	Enables debugging output for the HTTP client.
ip http client cache	Configures the HTTP client cache.
ip http client password	Configures a password for all HTTP client connections.
ip http client proxy-server	Configures an HTTP proxy server.
ip http client response	Configures HTTP client characteristics for managing HTTP server responses to request messages.
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.
show ip http client	Displays a report about the HTTP client.

iip http client password

To configure the default password used for connections to remote HTTP servers, use the **ip http client password** command in global configuration mode. To remove a configured default password from the configuration, use the **no** form of this command.

ip http client password *password*

no ip http client password

Syntax Description

password	The password string to be used in HTTP client connection requests sent to remote HTTP servers.

Defaults

No default password exists for the HTTP connections.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command is used to configure a default password before a file is downloaded from a remote web server using the **copy http://** or **copy https://** command. The default password will be overridden by a password specified in the URL of the **copy** command.

The password is encrypted in the configuration files.

Note The secure HTTP (HTTPS) client is not supported in Cisco IOS Release 12.2(31)SB.

Examples

In the following example, the default HTTP password is configured as Secret and the default HTTP username is configured as User2 for connections to remote HTTP or HTTPS servers:

```
Router(config)# ip http client password Secret
Router(config)# ip http client username User2
Router(config)# do show running-config | include ip http client
```

Related Commands

Command	Description
copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
debug ip http client	Enables debugging output for the HTTP client.
ip http client cache	Configures the HTTP client cache.
ip http client connection	Configures the HTTP client connection.
ip http client proxy-server	Configures an HTTP proxy server.
ip http client response	Configures HTTP client characteristics for managing HTTP server responses to request messages.
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.
show ip http client	Displays a report about the HTTP client.

ip http client proxy-server

To configure an HTTP proxy server, use the **ip http client proxy-server** command in global configuration mode. To disable or change the proxy server, use the **no** form of this command.

ip http client proxy-server *proxy-name* **proxy-port** *port-number*]

no ip http client proxy-server

Syntax Description

proxy-name	Name of the proxy server.
proxy-port	Specifies a proxy port for HTTP file system client connections.
port-number	Integer in the range of 1 to 65535 that specifies a port number on the remote proxy server.

Defaults

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command configures the HTTP client to connect to a remote proxy server for HTTP file system client connections.

Examples

The following example shows how to configure the HTTP proxy server named edge2 at port 29:

```
Router(config)# ip http client proxy-server edge2 proxy-port 29
```

Related Commands

Command	Description
copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
debug ip http client	Enables debugging output for the HTTP client.
ip http client cache	Configures the HTTP client cache.
ip http client connection	Configures the HTTP client connection.

Command	Description
ip http client password	Configures a password for all HTTP client connections.
ip http client response	Configures HTTP client characteristics for managing HTTP server responses to request messages.
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.
show ip http client	Displays a report about the HTTP client.

ip http client response

To configure the number of seconds that the HTTP client waits for a response from the server for a request message, use the **ip http client response** command in global configuration mode. To remove the specified number of seconds that the HTTP client waits for a response, use the **no** form of this command.

ip http client response timeout *seconds*

no ip http client response timeout

Syntax Description

timeout	Specifies a response timeout period.
seconds	The amount of time, in seconds, to wait for a response to a domain name system (DNS) query. The range is from 1 to 300.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to specify the response timeout value.

Examples

The following example shows how to specify a response timeout of 180 seconds:

```
Router(config)# ip http client response timeout 180
```

Related Commands

Command	Description
copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
debug ip http client	Enables debugging output for the HTTP client.
ip http client cache	Configures the HTTP client cache.
ip http client connection	Configures the HTTP client connection.
ip http client password	Configures a password for all HTTP client connections.

Command	Description
ip http client proxy-server	Configures an HTTP proxy server.
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.
show ip http client	Displays a report about the HTTP client.

ip http client secure-ciphersuite

To specify the CipherSuite that should be used for encryption over the secure HTTP connection from the client to a remote server, use the **ip http client secure-ciphersuite** command in global configuration mode. To remove a previously configured CipherSuite specification for the client, use the **no** form of this command.

ip http client secure-ciphersuite [**3des-ede-cbc-sha**] [**rc4-128-sha**] [**rc4-128-md5**] [**des-cbc-sha**]

no ip http client secure-ciphersuite

Syntax Description

3des-ede-cbc-sha	SSL_RSA_WITH_3DES_EDE_CBC_SHA—Rivest, Shamir, and Adleman (RSA) key exchange with 3DES and DES-EDE3-CBC for message encryption and Secure Hash Algorithm (SHA) for message digest.
rc4-128-sha	SSL_RSA_WITH_RC4_128_SHA—RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and SHA for message digest.
rc4-128-md5	SSL_RSA_WITH_RC4_128_MD5—RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and Message Digest 5 (MD5) for message digest.
des-cbc-sha	SSL_RSA_WITH_DES_CBC_SHA—RSA key exchange with DES-CBC for message encryption and SHA for message digest.

Command Default

The client and server negotiate the best CipherSuite that they both support from the list of available CipherSuites.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command allows you to restrict the list of CipherSuites (encryption algorithms) that the client offers when connecting to a secure HTTP server. For example, you may want to allow only the most secure CipherSuites to be used.

Unless you have a reason to specify the CipherSuites that should be used, or you are unfamiliar with the details of these CipherSuites, you should leave this command unconfigured and let the server and client negotiate the CipherSuite that they both support (this is the default). The **no** form of this command returns the list of available CipherSuites to the default (that is, all CipherSuites supported on your device are available for negotiation).

Examples

The following example shows how to configure the HTTPS client to use only the SSL_RSA_WITH_3DES_EDE_CBC_SHA CipherSuite:

```
Router(config)# ip http client secure-ciphersuite 3des-ede-cbc-sha
```

Related Commands

Command	Description
show ip http client secure status	Displays the configuration status of the secure HTTP client.

ip http client secure-trustpoint

To specify the remote certificate authority (CA) trustpoint that should be used if certification is needed for the secure HTTP client, use the **ip http client secure-trustpoint** command in global configuration mode. To remove a client trustpoint from the configuration, use the **no** form of this command.

ip http client secure-trustpoint *trustpoint-name*

no ip http client secure-trustpoint *trustpoint-name*

Syntax Description

trustpoint-name	Name of a configured trustpoint. Use the same trustpoint name that was used in the associated **crypto ca trustpoint** command.

Command Default

If the remote HTTPS server requests client certification, the secure HTTP client will use the trustpoint configured using the **primary** command in the CA trustpoint configuration. If a trustpoint is not configured, client certification will fail.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command specifies that the secure HTTP client should use the certificate associated with the trustpoint indicated by the *trustpoint-name* argument. Use the same trustpoint name that you used in the associated **crypto ca trustpoint** command.

The specified X.509v3 security certificate will be used by the HTTPS client for cases when the remote HTTPS server requires client authorization.

Use this command only if you have already declared a CA trustpoint using the **crypto ca trustpoint** command and associated submode commands. If the remote HTTPS server requires client authorization and a trustpoint is not configured for the client, the remote HTTPS server will reject the connection.

If this command is not used, the client attempts to use the certificate associated with the primary trustpoint. The primary trustpoint is configured using the **primary** command.

Examples

In the following example, the CA trustpoint is configured and referenced in the secure HTTP server configuration:

```
!The following commands specify a CA trustpoint that can be used
!to obtain a X.509v3 security certificate.
```

```
Router(config)# crypto ca trustpoint tp1
Router(config-ca)# enrollment url http://host1:80
Router(config-ca)# exit
!The following command is used to actually obtain the security certificate.
!A trustpoint NAME is used because there could be multiple trust points
!configured for the router.

Router(config)# crypto ca enrollment TP1

!The following command specifies that the secure HTTP client
!should use the certificate associated with the TP1 trustpoint for HTTPS connections.
Router(config)# ip http client secure-trustpoint tp1
```

Related Commands

Command	Description
crypto ca trustpoint	Specifies a name for a certificate authority trustpoint and enters CA trustpoint configuration mode.
primary	Indicates that the CA trustpoint being configured should be used as the primary (default) trustpoint.

iip http client source-interface

To configure a source interface for the HTTP client, use the **ip http client source-interface** command in global configuration mode. To change or disable the source interface, use the **no** form of this command.

ip http client source-interface *type number*

no ip http client source-interface

Syntax Description

type	Name of the source interface.
number	Number of the source interface.

Defaults

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to specify a source interface to use for HTTP connections.

Examples

The following example shows how to configure the source interface as Ethernet 0/1:

```
Router(config)# ip http client source-interface Ethernet 0/1
```

Related Commands

Command	Description
copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
debug ip http client	Enables debugging output for the HTTP client.
ip http client cache	Configures the HTTP client cache.
ip http client connection	Configures the HTTP client connection.
ip http client password	Configures a password for all HTTP client connections.

Command	Description
ip http client proxy-server	Configures an HTTP proxy server.
ip http client response	Configures HTTP client characteristics for managing HTTP server responses to request messages.
ip http client username	Configures a login name for all HTTP client connections.
show ip http client	Displays a report about the HTTP client.

ip http client username

To configure the default username used for connections to remote HTTP servers, use the **ip http client username** command in global configuration mode. To remove a configured default HTTP username from the configuration, use the **no** form of this command.

ip http client username *username*

no ip http client username

Syntax Description

username	String that is the username (login name) to be used in HTTP client connection requests sent to remote HTTP servers.

Defaults

No default username exists for the HTTP connections.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command is used to configure a default username before a file is copied to or from a remote web server using the **copy http://** or **copy https://** command. The default username will be overridden by a username specified in the URL of the **copy** command.

Note The secure HTTP (HTTPS) client is not supported in Cisco IOS Release 12.2(31)SB.

Examples

In the following example, the default HTTP password is configured as Secret and the default HTTP username is configured as User1 for connections to remote HTTP or HTTPS servers:

```
Router(config)# ip http client password Secret
Router(config)# ip http client username User1
```

Related Commands

Command	Description
copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
debug ip http client	Enables debugging output for the HTTP client.

Command	Description
ip http client cache	Configures the HTTP client cache.
ip http client connection	Configures the HTTP client connection.
ip http client password	Configures a password for all HTTP client connections.
ip http client proxy-server	Configures an HTTP proxy server.
ip http client response	Configures HTTP client characteristics for managing HTTP server responses to request messages.
ip http client source-interface	Configures a source interface for the HTTP client.
show ip http client	Displays a report about the HTTP client.

ip http help-path

To configure the help root used to locate help files for use by the user's current GUI screen, use the **ip http help-path** command in global configuration mode.

ip http help-path *url*

Syntax Description

url	Uniform Resource Locator (URL) specifying the root for the location of help files used by the user's GUI screens. The currently configured complete path of the location of specific help files can be obtained from the output of the **show ip http help-path** user EXEC command.

Command Default

No URL is specified.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

The URL specified in this command must be populated with 'help' files with read access that are appropriate for the application that will be using the URL.

Examples

In the following example, the HTML files are located in the specified location on the system:

```
Router(config)# ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/ivory/1100
```

Related Commands

Command	Description
ip http server	Enables the HTTP server, including the Cisco web browser user interface.
show ip http-help path	Displays the IP HTTP help-path URL.

ip http max-connections

To configure the maximum number of concurrent connections allowed for the HTTP server, use the **ip http max-connections** command in global configuration mode. To return the maximum connection value to the default, use the **no** form of this command.

ip http max-connections *value*

no ip http max-connections

Syntax Description

value	An integer in the range from 1 to 16 that specifies the maximum number of concurrent HTTP connections. The default is 5.

Command Default

Five concurrent HTTP connections is the default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Platform-specific implementations can supersede the upper range limit of 16.

If a new value is configured that is less than the previously configured value while the current number of connections exceeds the new maximum value, the HTTP server will not abort any of the current connections. However, the server will not accept new connections until the current number of connections falls below the new configured value.

Examples

The following example shows how to configure the HTTP server to allow up to 10 simultaneous connections:

```
Router(config)# ip http server
Router(config)# ip http max-connections 10
```

Related Commands

Command	Description
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

ip http path

To specify the base path used to locate files for use by the HTTP server, use the **ip http path** command in global configuration mode. To remove the base path specification, use the **no** form of this command.

ip http path *url*

no ip http path

Syntax Description

url	Cisco IOS File System (IFS) URL specifying the location of the HTML files used by the HTTP server.

Command Default

The HTTP server is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

After enabling the HTTP server, you should set the base path by specifying the location of the HTML files to be served. HTML files used by the HTTP web server typically reside in system flash memory.

Remote URLs can be specified using this command, but use of remote path names (for example, where HTML files are located on a remote TFTP server) is not recommended.

Examples

In the following example, the HTML files are located in the default flash location on the system:

```
Router(config)# ip http path flash:
```

In the following example, the HTML files are located in the directory named web on the flash memory card inserted in slot 0:

```
Router(config)# ip http path slot0:web
```

Related Commands

Command	Description
ip http server	Enables the HTTP server, including the Cisco web browser user interface.

ip http port

To specify the port number to be used by the HTTP server, use the **ip http port** command in global configuration mode. To return the port number to the default, use the **no** form of this command.

ip http port *port-number*

no ip http port

Syntax Description

port-number	The integer 80 or any integer in the range from 1025 to 65535 that specifies the port number to be used for the HTTP server. The default is 80.

Command Default

The HTTP server uses port 80.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.2(15)T	This command was modified to restrict port numbers. The port number 443 is now reserved for secure HTTP (HTTPS) connections.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

HTTP port 80 is the standard port used by web servers.

Note The secure HTTP (HTTPS) server is not supported in Cisco IOS Release 12.2(31)SB.

Examples

The following example shows how to change the HTTP server port to port 8080:

```
Router(config)# ip http server
Router(config)# ip http port 8080
```

Related Commands

Command	Description
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

iip http secure-ciphersuite

To specify the CipherSuites that should be used by the secure HTTP server when negotiating a connection with a remote client, use the **ip http secure-ciphersuite** command in global configuration mode. To return the configuration to the default set of CipherSuites, use the **no** form of this command.

ip http secure-ciphersuite [**3des-ede-cbc-sha**] [**rc4-128-sha**] [**rc4-128-md5**] [**des-cbc-sha**]

no ip http secure-ciphersuite

Syntax Description

3des-ede-cbc-sha	SSL_RSA_WITH_3DES_EDE_CBC_SHA—Rivest, Shamir, and Adleman (RSA) key exchange with 3DES and DES-EDE3-CBC for message encryption and Secure Hash Algorithm (SHA) for message digest.
rc4-128-sha	SSL_RSA_WITH_RC4_128_SHA —RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and SHA for message digest.
rc4-128-md5	SSL_RSA_WITH_RC4_128_MD5 —RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and Message Digest 5 (MD5) for message digest.
des-cbc-sha	SSL_RSA_WITH_DES_CBC_SHA—RSA key exchange with DES-CBC for message encryption and SHA for message digest.

Command Default

The HTTPS server negotiates the best CipherSuite using the list received from the connecting client.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command is used to restrict the list of CipherSuites (encryption algorithms) that should be used for encryption over the HTTPS connection. For example, you may want to allow only the most secure CipherSuites to be used.

Unless you have a reason to specify the CipherSuites that should be used, or you are unfamiliar with the details of these CipherSuites, you should leave this command unconfigured and let the server and client negotiate the CipherSuite that they both support (this is the default).

The supported CipherSuites vary by Cisco IOS software image. For example, “IP Sec56” (“k8”) images support only the SSL_RSA_WITH_DES_CBC_SHA CipherSuite in Cisco IOS Release 12.2(15)T.

In terms of router processing load (speed), the following list ranks the CipherSuites from fastest to slowest (slightly more processing time is required for the more secure and more complex CipherSuites):

1. SSL_RSA_WITH_DES_CBC_SHA
2. SSL_RSA_WITH_RC4_128_MD5
3. SSL_RSA_WITH_RC4_128_SHA
4. SSL_RSA_WITH_3DES_EDE_CBC_SHA

Additional information about these CipherSuites can be found online from sources that document the Secure Sockets Layer (SSL) 3.0 protocol.

Examples

The following exampleshows how to restrictsthe CipherSuites offered to a connecting secure web client:

```
Router(config)# ip http secure-ciphersuite rc4-128-sha rc4-128-md5
```

Related Commands

Command	Description
ip http secure-server	Enables the HTTPS server.
show ip http server secure status	Displays the configuration status of the secure HTTP server.

ip http secure-client-auth

To configure the secure HTTP server to authenticate connecting clients, use the **ip http secure-client-auth** command in global configuration mode. To remove the requirement for client authorization, use the **no** form of this command.

ip http secure-client-auth

no ip http secure-client-auth

Syntax Description

This command has no arguments or keywords.

Command Default

Client authentication is not required for connections to the secure HTTP server.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command configures the HTTP server to request an X.509v3 certificate from the client in order to authenticate the client during the connection process.

In the default connection and authentication process, the client requests a certificate from the HTTP server, but the server does not attempt to authenticate the client. Authenticating the client provides more security than server authentication by itself, but not all web clients may be configured for certificate authority (CA) authentication.

Examples

In the following example the secure web server is enabled and the server is configured to accept connections only from clients with a signed security certificate:

```
Router(config)# no ip http server
Router(config)# ip http secure-server
Router(config)# ip http secure-client-auth
```

Related Commands

Command	Description
ip http secure-server	Enables the HTTPS server.
show ip http server secure status	Displays the configuration status of the secure HTTP server.

iip http secure-port

To set the secure HTTP (HTTPS) server port number for listening, use the **ip http secure-port** command in global configuration mode. To return the HTTPS server port number to the default, use the **no** form of this command.

ip http secure-port *port-number*

no ip http secure-port

Syntax Description

port-number	Integer in the range of 0 to 65535 is accepted, but the port number must be higher than 1024 unless the default is used. The default is 443.

Command Default

The HTTPS server port number is not set for listening.

Command Modes

Global configuration

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

An HTTP server and an HTTPS server cannot use the same port. If you try to configure both on the same port, the following message is displayed:

```
% Port port_number in use by HTTP.
```

where port_number is the port number that is already assigned to the HTTP server.

If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format:

https://device:port_number

where port_number is the HTTPS port number.

Examples

The following example shows how to assign port 1025 for HTTPS server connections:

```
Router(config)# ip http secure-port 1025
```

Related Commands

Command	Description
ip http secure-server	Enables an HTTPS server.

ip http secure-server

To enable a secure HTTP (HTTPS) server, use the **ip http secure-server** command in global configuration mode. To disable an HTTPS server, use the **no** form of this command.

ip http secure-server

no ip http secure-server

Syntax Description

This command has no arguments or keywords.

Command Default

The HTTPS server is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The HTTPS server uses the Secure Sockets Layer (SSL) version 3.0 protocol.

Note When enabling an HTTPS server, you should always disable the standard HTTP server to prevent unsecured connections to the same services. Disable the standard HTTP server using the **no ip http server** command in global configuration mode (this step is precautionary; typically, the HTTP server is disabled by default).

If a certificate authority (CA) is used for certification, you should declare the CA trustpoint on the routing device before enabling the HTTPS server.

Examples

In the following example the HTTPS server is enabled, and the (previously configured) CA trustpoint CA-trust-local is specified:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# ip http secure-server
Router(config)# ip http secure-trustpoint CA-trust-local
Router(config)# end
```

```
Router# show ip http server secure status

HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint: CA-trust-local
```

Related Commands

Command	Description
ip http secure-trustpoint	Specifies the CA trustpoint that should be used for obtaining signed certificates for the HTTPS server.
ip http server	Enables the HTTP server on an IP or IPv6 system, including the Cisco web browser user interface.
show ip http server secure status	Displays the configuration status of the HTTPS server.

ip http secure-trustpoint

To specify the certificate authority (CA) trustpoint that should be used for obtaining signed certificates for a secure HTTP (HTTPS) server, use the **ip http secure-trustpoint** command in global configuration mode. To remove a previously specified CA trustpoint, use the **no** form of this command.

ip http secure-trustpoint *trustpoint-name*

no ip http secure-trustpoint *trustpoint-name*

Syntax Description

trustpoint-name	Name of a configured trustpoint. Use the same trustpoint name that was used in the associated **crypto ca trustpoint** command.

Command Default

The HTTPS server uses the trustpoint configured when you use the **primary** command. If a trustpoint is not configured, the HTTPS server uses a self-signed certificate.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command specifies that the HTTPS server should use the X.509v3 certificate associated with the trustpoint indicated by the *trustpoint-name* argument. Use the same trustpoint name that you used in the associated **crypto ca trustpoint** command.

The specified X.509v3 security certificate will be used to authenticate the server to connecting clients, and, if remote client authentication is enabled, to authenticate the connecting clients.

Use this command only if you have already declared a CA trustpoint using the **crypto ca trustpoint** command and associated submode commands. If a trustpoint is not configured, the HTTPS server will use a self-signed certificate.

If this command is not used, the server will attempt to use the certificate associated with the primary trustpoint. The primary trustpoint is configured using the **primary** command.

Examples

In the following example, the CA trustpoint is configured, a certificate is obtained, and the certificate is referenced in the HTTPS server configuration:

```
!The following commands specifies a CA trustpoint that can be used
!to obtain a X.509v3 security certificate.
!A trustpoint NAME is used because there could be multiple trustpoints
!configured for the router.
```

```
Router(config)# crypto ca trustpoint tp1
Router(config-ca)# enrollment url http://host1:80
Router(config-ca)# exit
Router(config)# crypto ca authenticate tp1

!The following command is used to actually obtain the security certificate.

Router(config)# crypto ca enrollment tp1
Router(config)# ip http secure-server

!The following command specifies that the secure HTTP server
!should use a certificate associated with the TP1 trustpoint for HTTPS connections.
Router(config)# ip http secure-trustpoint tp1
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your routing device should use.
ip http secure-server	Enables the HTTPS server.
primary	Assigns a specified trustpoint as the primary trustpoint of the router.
show ip http server secure status	Displays the configuration status of the secure HTTP server.

ip http server

To enable the HTTP server on your IP or IPv6 system, including the Cisco web browser user interface, use the **ip http server** command in global configuration mode. To disable the HTTP server, use the **no** form of this command.

ip http server

no ip http server

Syntax Description

This command has no arguments or keywords.

Command Default

The HTTP server is disabled on the Cisco Catalyst 4000 series switch. The HTTP server is enabled for clustering on the following Cisco switches: Catalyst 3700 series, Catalyst 3750 series, Catalyst 3550 series, Catalyst 3560 series, and Catalyst 2950 series.

The HTTP server uses the standard port 80 by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.2(2)T	IPv6 support was added.
12.2(15)T	The HTTP 1.0 implementation was replaced by the HTTP 1.1 implementation. The secure HTTP server feature was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

With IPv6 support added in Cisco IOS Release 12.2(2)T, the **ip http server** command simultaneously enables and disables both IP and IPv6 access to the HTTP server. However, an access list configured with the **ip http access-class** command will only be applied to IPv4 traffic. IPv6 traffic filtering is not supported.

Caution The standard HTTP server and the secure HTTP (HTTPS) server can run on a system at the same time. If you enable the HTTPS server using the **ip http secure-server** command, disable the standard HTTP server using the **no ip http server** command to ensure that secure data cannot be accessed through the standard HTTP connection.

Examples

The following example shows how to enable the HTTP server on both IP and IPv6 systems:

```
Router(config)# ip http server
Router(config)# ip http path flash:
```

Related Commands

Command	Description
ip http access-class	Specifies the access list that should be used to restrict access to the HTTP server.
ip http path	Specifies the base path used to locate files for use by the HTTP server.
ip http secure-server	Enables the HTTPS server.

ip http session-module-list

To define a list of HTTP or secure HTTP (HTTPS) application names, use the **ip http session-module-list** command in global configuration mode. To remove the defined list, use the **no** form of this command.

ip http session-module-list *listname prefix1* [*prefix2,...,prefixn*]

no ip http session-module-list *listname prefix1* [*prefix2,...,prefixn*]

Syntax Description

listname	Name of the list.
prefix1	Associated HTTP or HTTPS application names. Prefix strings represent the names of applications, for example, SCEP, WEB_EXEC or HOME_PAGE.
prefix2,...,prefixn	(Optional) Additional associated HTTP or HTTPS application names. Each application is separated by a comma.

Defaults

No list of HTTP or HTTPS application names is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Use this command to define a list of HTTP or HTTPS application names. The defined list can then be used by the **ip http active-session-modules** or **ip http secure-active-session-modules** commands to selectively enable HTTP or HTTPS applications, respectively, for servicing incoming HTTP and HTTPS requests from remote clients.

When defining a list of HTTP or HTTPS application names, use the following guidelines:

- A maximum of four lists can be defined on a router or switch. Attempts to define more than four lists will fail and an error message will be displayed stating the limit restrictions.
- An existing list can be removed using the **no ip http session-module-list** command.
- You cannot reconfigure an existing list. Instead of reconfiguring an existing list, remove the existing list and create a new list with the same name.
- There is no limit to how many application names can be in the list. However, the maximum number of sessions that can be registered with the Cisco IOS HTTP or HTTPS server is 32.

Note The HTTPS server is not supported in Cisco IOS Release 12.2(31)SB.

Examples

The following example shows how to configure a different set of services to be available for HTTP and HTTPS requests. In this example, all HTTP applications are enabled for providing services to remote clients, but for HTTPS services, only the HTTPS applications defined in list1 (Simple Certificate Enrollment Protocol [SCEP] and HOME_PAGE) are enabled.

```
ip http session-module-list list1 SCEP,HOME_PAGE
ip http active-session-modules all
ip http server
ip http secure-server
ip http secure-active-session-modules list1
```

Related Commands

Command	Description
ip http active-session-modules	Selectively enables HTTP applications that will service incoming HTTP requests from remote clients.
ip http secure-active-session-modules	Selectively enables HTTPS applications that will service incoming HTTPS requests from remote clients.
show ip http server	Displays details about the current configuration of the HTTP server.

ip http timeout-policy

To configure the parameters for closing connections to the local HTTP server, use the **ip http timeout-policy** command in global configuration mode. To return the parameters to their defaults, use the **no** form of this command.

ip http timeout-policy idle *seconds* **life** *seconds* **requests** *value*

no ip http timeout-policy

Syntax Description

idle	Specifies the maximum number of seconds that a connection will be kept open if no data is received or response data cannot be sent out.
life	Specifies the maximum number of seconds that a connection will be kept open from the time the connection is established.
seconds	When used with the **idle** keyword, an integer in the range of 1 to 600 that specifies the number of seconds (10 minutes maximum). The default is 180 (3 minutes). When used with the **life** keyword, an integer in the range of 1 to 86400 that specifies the number of seconds (24 hours maximum). The default is 180 (3 minutes).
requests	Specifies that a maximum limit is set on the number of requests processed on a persistent connection before it is closed.
value	Integer in the range from 1 to 86400. The default is 1.

Defaults

HTTP server connection idle time: 180 seconds (3 minutes)

HTTP server connection life time: 180 seconds (3 minutes)

HTTP server connection maximum requests: 1

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command sets the characteristics that determine how long a connection to the HTTP server should remain open.

This command may not take effect immediately on any HTTP connections that are open at the time you use this command. In other words, new values for idle time, life time, and maximum requests will apply only to connections made to the HTTP server after this command is issued.

A connection may be closed sooner than the configured idle time if the server is too busy or the limit on the life time or the number of requests is reached.

Also, since the server will not close a connection while actively processing a request, the connection may remain open longer than the specified life time if processing is occurring when the life maximum is reached. In this case, the connection will be closed when processing finishes.

A connection may be closed before the maximum number of requests are processed if the server is too busy or the limit on the idle time or life time is reached.

The **ip http timeout-policy** command allows you to specify a general access policy to the HTTP server by adjusting the connection timeout values. For example, if you want to maximize throughput for HTTP connections, you should configure a policy that minimizes connection overhead. You can do this by specifying large values for the **life** and **requests** options so that each connection stays open longer and more requests are processed for each connection.

Another example would be to configure a policy that minimizes the response time for new connections. You can do this by specifying small values for the **life** and **requests** options so that the connections are quickly released to serve new clients.

A throughput policy would be better for HTTP sessions with dedicated management applications, as it would allow the application to send more requests before the connection is closed, while a response time policy would be better for interactive HTTP sessions, as it would allow more people to connect to the server at the same time without having to wait for connections to become available.

In general, you should configure these options as appropriate for your environment. The value for the **idle** option should be balanced so that it is large enough not to cause an unwanted request or response timeout on the connection, but small enough that it does not hold a connection open longer than necessary.

Examples

In the following example, a Throughput timeout policy is applied. This configuration would allow each connection to be idle for a maximum of 30 seconds (approximately). Each connection will remain open (be “alive”) until either the HTTP server has been busy processing requests for approximately 2 minutes (120 seconds) or until approximately 100 requests have been processed.

```
Router(config)# ip http timeout-policy idle 30 life 120 requests 100
```

In the following example, a Response Time timeout policy is applied. This configuration would allow each connection to be idle for a maximum of 30 seconds (approximately). Each connection will be closed as soon as the first request has been processed.

```
Router(config)# ip http timeout-policy idle 30 life 30 requests 1
```

Related Commands

Command	Description
ip http server	Enables the HTTP server, including the Cisco web browser user interface.

kron occurrence

To specify schedule parameters for a Command Scheduler occurrence and enter kron-occurrence configuration mode, use the **kron occurrence** command in global configuration mode. To delete a Command Scheduler occurrence, use the **no** form of this command.

kron occurrence *occurrence-name* [**user** *username*] {**in** [[*numdays*:] *numhours*:] *nummin* | **at** *hours*:*min* [[*month*] *day-of-month*] [*day-of-week*]} {**oneshot** | **recurring** | **system-startup**}

no kron occurrence *occurrence-name* [**user** *username*] {**in** [[*numdays*:] *numhours*:] *nummin* | **at** *hours*:*min* [[*month*] *day-of-month*] [*day-of-week*]} {**oneshot** | **recurring** | **system-startup**}

Syntax Description

occurrence-name	Name of the occurrence. The length of *occurrence-name* is from 1 to 31 characters. If the *occurrence-name* is new, an occurrence structure will be created. If the *occurrence-name* is not new, the existing occurrence will be edited.
user	(Optional) Identifies a particular user.
username	(Optional) Name of the user.
in	Indicates that the occurrence is to run after a specified time interval. The timer starts when the occurrence is configured.
numdays:	(Optional) Number of days. If used, add a colon after the number.
numhours:	(Optional) Number of hours. If used, add a colon after the number.
nummin	Number of minutes.
at	Indicates that the occurrence is to run at a specified calendar date and time.
hours:	Hour as a number using the twenty-four hour clock. Add a colon after the number.
min	Minute as a number.
month	(Optional) Month name. If used, you must also specify *day-of-month*.
day-of-month	(Optional) Day of month as a number.
day-of-week	(Optional) Day of week name.
oneshot	Indicates that the occurrence is to run only one time. After the occurrence has run, the configuration is removed.
recurring	Indicates that the occurrence is to run on a recurring basis.
system-startup	Indicates that the occurrence is to run on system startup, in addition to the **recurring** or **oneshot** occurrences.

Command Default

No schedule parameters are specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	The **system-startup** keyword was added. The **user** keyword and *username* argument were removed from this command in Cisco IOS Release 12.4(15)T.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Prior to Cisco IOS Release 12.4, when you configured a kron occurrence for a calendar time when the system clock was not set, you received a printf message stating that the clock was not set and the occurrence would not be scheduled until it was set.

Beginning in Cisco IOS Release 12.4, when you configure a kron occurrence for a calendar time when the system clock is not set, the occurrence is scheduled but a printf message appears stating that the clock is not set and that it currently reads <current clock time>.

If you set the clock, the schedule of the occurrence is affected in one of the following ways:

- A new clock time set for less than 3 hours after the occurrence is scheduled to happen causes the occurrence to happen immediately.
- A new clock time set for less than 3 hours before the occurrence is scheduled to happen causes the occurrence to happen as scheduled.
- A new clock time set for more than 3 hours after the occurrence is scheduled to happen causes the occurrence to be rescheduled for the next regular calendar time.
- A new clock time set for more than 3 hours before the occurrence is scheduled to happen causes the occurrence to be rescheduled for the previous regular calendar time.

Use the **kron occurrence** and **policy-list** commands to schedule one or more policy lists to run at the same time or interval.

Use the **kron policy-list** command in conjunction with the **cli** command to create a Command Scheduler policy containing EXEC command-line interface (CLI) commands to be scheduled to run on the router at a specified time.

Use the **show kron schedule** command to display the name of each configured occurrence and when it will next run.

The Command Scheduler process is useful to automate the running of EXEC commands at recurring intervals, and it can be used in remote routers to minimize manual intervention.

Examples

The following example shows how to create a Command Scheduler occurrence named info-three and schedule it to run every three days, 10 hours, and 50 minutes. The EXEC CLI in the policy named three-day-list is configured to run as part of occurrence info-three.

```
Router(config)# kron occurrence info-three user IT2 in 3:10:50 recurring
Router(config-kron-occurrence)# policy-list three-day-list
```

The following example shows how to create a Command Scheduler occurrence named auto-mkt and schedule it to run once on June 4 at 5:30 a.m. The EXEC CLI in the policies named mkt-list and mkt-list2 are configured to run as part of occurrence auto-mkt.

```
Router(config)# kron occurrence auto-mkt user marketing at 5:30 jun 4 oneshot
Router(config-kron-occurrence)# policy-list mkt-list
Router(config-kron-occurrence)# policy-list mkt-list2
```

Related Commands

Command	Description
cli	Specifies EXEC CLI commands within a Command Scheduler policy list.
kron policy-list	Specifies a name for a Command Scheduler policy and enters kron-policy configuration mode.
policy-list	Specifies the policy list associated with a Command Scheduler occurrence.
show kron schedule	Displays the status and schedule information for Command Scheduler occurrences.

kron policy-list

To specify a name for a Command Scheduler policy and enter kron-policy configuration mode, use the **kron policy-list** command in global configuration mode. To delete the policy list, use the **no** form of this command.

kron policy-list *list-name*

no kron policy-list *list-name*

Syntax Description

list-name	String from 1 to 31 characters that specifies the name of the policy.

Command Default

If the specified list name does not exist, a new policy list is created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **kron policy-list** command in conjunction with the **cli** command to create a Command Scheduler policy containing EXEC command-line interface (CLI) commands to be scheduled to run on the router at a specified time. Use the **kron occurrence** and **policy-list** commands to schedule one or more policy lists to run at the same time or interval.

When the *list-name* is new, a policy list structure is created. When the *list-name* is not new, the existing policy list is edited.

The Command Scheduler process is useful to automate the running of EXEC commands at recurring intervals, and it can be used in remote routers to minimize manual intervention.

Examples

The following example shows how to create a policy named sales-may and configure EXEC CLI commands to run the CNS command that retrieves an image from a server:

```
Router(config)# kron policy-list sales-may
Router(config-kron-policy)# cli cns image retrieve server https://10.21.2.3/imgsvr/ status
https://10.21.2.5/status/
```

Related Commands

Command	Description
cli	Specifies EXEC CLI commands within a Command Scheduler policy list.
kron occurrence	Specifies schedule parameters for a Command Scheduler occurrence and enters kron-occurrence configuration mode.
policy-list	Specifies the policy list associated with a Command Scheduler occurrence.

line-cli

Note Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), the **line-cli** command is replaced by the **cli (cns)** command. See the **cli (cns)** command for more information.

To connect to the Cisco Networking Services (CNS) configuration engine using a modem dialup line, use the **line-cli** command in CNS Connect-interface configuration mode.

line-cli {*modem-cmd* | *line-config-cmd*}

Syntax Description

modem-cmd	Modem line command that enables dialout. Indicates from which line or interface the IP or MAC address should be retrieved in order to define the unique ID.
line-config-cmd	Command that configures the line. The *modem-cmd* argument must be configured before other line configuration commands.

Command Default

No command lines are specified to configure modem lines.

Command Modes

CNS Connect-interface configuration

Command History

Release	Modification
12.2(8)T	This command was introduced on Cisco 2600 series and Cisco 3600 series routers.
12.3(8)T	This command was replaced by the **cli (cns)** command.
12.3(9)	This command was replaced by the **cli (cns)** command.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to connect to the CNS configuration engine using a modem dialout line. The bootstrap configuration on the router finds the connecting interface, regardless of the slot in which the card resides or the modem dialout line for the connection, by trying different candidate interfaces or lines until it successfully pings the registrar.

Enter this command to enter CNS Connect-interface configuration (config-cns-conn-if) mode. Then use one of the following bootstrap-configuration commands to connect to the registrar for initial configuration:

- **config-cli** followed by commands that, used as is, configure the interface.
- **line-cli** followed by a command to configure modem lines to enable dialout and, after that, commands to configure the modem dialout line.

The **config-cli** command accepts the special directive character "**&**," which acts as a placeholder for the interface name. When the configuration is applied, the **&** is replaced with the interface name. Thus, for example, if we are able to connect using FastEthernet0/0, the following is the case:

- The **config-cli ip route 0.0.0.0 0.0.0.0 &** command generates the **config ip route 0.0.0.0 0.0.0.0 FastEthernet0/0** command.
- The **cns id & ipaddress** command generates the **cns id FastEthernet0/0 ipaddress** command.

Examples

The following example enters CNS Connect-interface configuration mode, connects to a configuration engine using an asynchronous interface, and issues a number of commands:

```
Router(config)# cns config connect-intf Async
Router(config-cns-conn-if)# config-cli encapsulation ppp
Router(config-cns-conn-if)# config-cli ip unnumbered FastEthernet0/0
Router(config-cns-conn-if)# config-cli dialer rotart-group 0
Router(config-cns-conn-if)# line-cli modem InOut
Router(config-cns-conn-if)# line-cli...<other line commands>...
Router(config-cns-conn-if)# exit
```

These commands apply the following configuration:

```
line 65
modem InOut
.
.
.
interface Async65
encapsulation ppp
dialer in-band
dialer rotary-group 0
```

Related Commands

Command	Description
cns config connect-intf	Specifies the interface for connecting to the CNS configuration engine.
config-cli	Connects to the CNS configuration engine using a specific type of interface.

logging buffered

To enable system message logging to a local buffer, use the **logging buffered** command in global configuration mode. To cancel the use of the buffer, use the **no** form of this command. To return the buffer size to its default value, use the default form of this command.

logging buffered [*buffer-size* | *severity-level* | **discriminator** *discr-name* [*severity-level*]]

no logging buffered

default logging buffered

Syntax Description

buffer-size	(Optional) Size of the buffer, in bytes. The range is 4096 to 4294967295. The default size varies by platform.
severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): [**0** | **emergencies**]—System is unusable [**1** | **alerts**]—Immediate action needed [**2** | **critical**]—Critical conditions [**3** | **errors**]—Error conditions [**4** | **warnings**]—Warning conditions [**5** | **notifications**]—Normal but significant conditions [**6** | **informational**]—Informational messages [**7** | **debugging**]—Debugging messages The default logging level varies by platform but is generally 7. Level 7 means that messages at all levels (0–7) are logged to the buffer.
discriminator	(Optional) Specifies a user-defined filter, via the logging discriminator, for syslog messages.
discr-name	(Optional) String of a maximum of 8 alphanumeric, case-sensitive characters. Blank spaces between characters are not allowed.

Command Default

Varies by platform. For most platforms, logging to the buffer is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.1(17)T	The *severity-level* argument was added in Cisco IOS Release 11.1(17)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.4(11)T	The **discriminator** keyword and *discr-name* argument were added in Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command copies logging messages to an internal buffer. The buffer is circular in nature, so newer messages overwrite older messages after the buffer is filled.

Specifying a severity-level causes messages at that level and numerically lower levels to be logged in an internal buffer.

The optional **discriminator** keyword and *discr-name* argument provide another layer of filtering that you can use to control the type and number of syslog messages that you want to receive.

When you resize the logging buffer, the existing buffer is freed and a new buffer is allocated. To prevent the router from running out of memory, do not make the buffer size too large. You can use the **show memory** EXEC command to view the free processor memory on the router; however, the memory value shown is the maximum available and should not be approached. The **default logging buffered** command resets the buffer size to the default for the platform.

To display messages that are logged in the buffer, use the **show logging** command. The first message displayed is the oldest message in the buffer.

The **show logging** command displays the addresses and levels associated with the current logging setup and other logging statistics.

Table 10 shows a list of levels and corresponding syslog definitions.

Table 10 Error Message Logging Priorities and Corresponding Syslog Definitions

Level	Level Keyword	Syslog Definition
0	**emergencies**	LOG_EMERG
1	**alerts**	LOG_ALERT
2	**critical**	LOG_CRIT
3	**errors**	LOG_ERR
4	**warnings**	LOG_WARNING
5	**notifications**	LOG_NOTICE
6	**informational**	LOG_INFO
7	**debugging**	LOG_DEBUG

Examples

The following example shows how to enable standard system logging to the local syslog buffer:

```
Router(config)# logging buffered
```

The following example shows how to use a message discriminator named buffer1 to filter critical messages, meaning that messages at levels 0, 1, and 2 are filtered:

```
Router(config)# logging buffered discriminator buffer1 critical
```

Related Commands

Command	Description
clear logging	Clears messages from the logging buffer.
logging buffered xml	Enables system message logging (syslog) and sends XML-formatted logging messages to the XML-specific system buffer.
show logging	Displays the syslog.

logging buffered filtered

To enable Embedded Syslog Manager (ESM) filtered system message logging to the standard syslog buffer, use the **logging buffered filtered** command in global configuration mode. To disable all logging to the buffer and return the size of the buffer to the default, use the **no** form of this command.

logging buffered filtered [*severity-level*]

no logging buffered filtered

Syntax Description

severity-level	(Optional) Limits messages sent to the buffer to those messages at or numerically lower than the specified value. For example, if level **1** is specified, only messages at level 1 (alerts) or level 0 (emergencies) will be sent to the specified target. Severity levels are specified as a number or a keyword: {**0** | **emergencies**}—System is unusable {**1** | **alerts**}—Immediate action needed {**2** | **critical**}—Critical conditions {**3** | **errors**}—Error conditions {**4** | **warnings**}—Warning conditions {**5** | **notifications**}—Normal but significant conditions {**6** | **informational**}—Informational messages {**7** | **debugging**}—Debugging messages The default severity level varies by platform but is generally level 7 (“debugging”), meaning that messages at all severity levels (0 through 7) are logged.

Command Default

Logging to the buffer is enabled.

ESM filtering of system logging messages sent to the buffer is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

If standard logging has been disabled on your system (using the **no logging on** command), standard logging must be reenabled using the **logging on** command before using the **logging buffered filtered** command.

Standard logging is enabled by default, but filtering by the ESM is disabled by default.

ESM uses syslog filter modules, which are Tcl script files stored locally or on a remote device. The syslog filter modules must be configured using the **logging filter** command before filtered output can be sent to the buffer.

When ESM filtering is enabled, all messages sent to the buffer have the configured syslog filter modules applied. To return to standard logging to the buffer, use the plain form of the **logging buffered** command (without the **filtered** keyword). To disabled all logging to the buffer, use the **no logging buffered** command, with or without the **filtered** keyword.

The buffer is circular, so newer messages overwrite older messages as the buffer is filled. To change the size of the buffer, use the **logging buffered** *buffer-size* command, then issue the **logging buffered filtered** command to start (or restart) filtered logging.

To display the messages that are logged in the buffer, use the **show logging** command in EXEC mode. The first message displayed is the oldest message in the buffer.

Examples

In the following example, the user enables ESM filtered logging to the buffer:

```
Router(config)# logging filter tftp://209.165.200.225/ESM/escalate.tcl
Router(config)# logging filter slot0:/email.tcl user@example.com
Router(config)# logging buffer filtered
```

Related Commands

Command	Description
clear logging	Clears all messages from the system message logging (syslog) buffer.
logging buffered	Enables standard system message logging (syslog) to a local buffer and sets the severity level and buffer size for the logging buffer.
logging filter	Specifies the name and location of a syslog filter module to be applied to generated system logging messages.
logging on	Globally controls (enables or disables) system message logging.
show logging	Displays the state of system message logging, followed by the contents of the logging buffer.

logging buffered xml

To enable system message logging (syslog) and send XML-formatted logging messages to the XML-specific system buffer, use the **logging buffered xml** command in global configuration mode. To disable the XML syslog buffer and return the size of the buffer to the default, use the **no** form of this command.

logging buffered xml [*xml-buffer-size*]

no logging buffered xml [*xml-buffer-size*]

Syntax Description

xml-buffer-size	(Optional) Size of the buffer, from 4,096 to 4,294,967,295 bytes (4 kilobytes to 2 gigabytes). The default size varies by platform. This value is ignored if entered as part of the **no** form of this command.

Defaults

XML formatting of system logging messages is disabled.

The default XML syslog buffer size is the same size as the standard syslog buffer.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Standard logging is enabled by default, but XML-formatted system message logging is disabled by default. If standard logging has been disabled on your system (using the **no logging on** command), standard logging must be reenabled using the **logging on** command before using the **logging buffered xml** command.

The **logging buffered xml** command copies logging messages to an internal XML buffer. The XML syslog buffer is separate from the standard syslog buffer (created using the **logging buffered** command).

The buffer is circular, so newer messages overwrite older messages as the buffer is filled.

The severity level for logged messages is determined by the setting of the **logging buffered** command. If the **logging buffered** command has not been used, the default severity level for that command is used. The default severity level varies by platform, but is generally level 7 (“debugging”), meaning that messages at all severity levels (0 through 7) are logged. For more information on severity levels, see the documentation of the **logging buffered** command.

When you resize the logging buffer, the existing buffer is freed and a new buffer is allocated. Do not make the buffer size too large because the router could run out of memory for other tasks. You can use the **show memory** command in EXEC mode to view the free processor memory on the router; however, this value is the maximum available and should not be approached.

To return the size of the XML logging buffer to the default, use the **no logging buffered xml** command.

To display the messages that are logged in the buffer, use the **show logging xml** command in EXEC mode. The first message displayed is the oldest message in the buffer.

Examples

In the following example, the user enables logging to the XML syslog buffer and sets the XML syslog buffer size to 14 kilobytes:

```
Router(config)# logging buffered xml 14336
```

Related Commands

Command	Description
clear logging xml	Clears all messages from the XML-specific system message logging (syslog) buffer.
logging buffered	Enables standard system message logging (syslog) to a local buffer and sets the severity level and buffer size for the logging buffer.
logging on	Globally controls (enables or disables) system message logging.
show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML-specific buffer.

logging cns-events

To enable extensible markup language (XML)-formatted system event message logging to be sent through the Cisco Networking Services (CNS) event bus, use the **logging cns-events** command in global configuration mode. To disable the ability to send system logging event messages through the CNS event bus, use the **no** form of this command.

logging cns-events [*severity-level*]

no logging cns-events

Syntax Description

severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): {**0** | **emergencies**}— System is unusable {**1** | **alerts**}—Immediate action needed {**2** | **critical**}—Critical conditions {**3** | **errors**}—Error conditions {**4** | **warnings**}—Warning conditions {**5** | **notifications**}—Normal but significant conditions {**6** | **informational**}—Informational messages {**7** | **debugging**}— Debugging messages

Defaults

Level 7: debugging

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Before you configure this command you must enable the CNS event agent with the **cns event** command because the CNS event agent sends out the CNS event logging messages. The generation of many CNS event logging messages can negatively impact the publishing time of standard CNS event messages that must be sent to the network.

If the **debug cns event** command is active when the **logging cns-events** command is configured, the logging of CNS events is disabled.

Examples

In the following example, the user enables XML-formatted CNS system error message logging to the CNS event bus for messages at levels 0 through 4:

```
Router(config)# logging cns-events 4
```

Related Commands

Command	Description
cns event	Configures CNS event gateway, which provides CNS event services to Cisco IOS clients.
debug cns event	Displays CNS event agent debugging messages.

logging console

To send system logging (syslog) messages to all available TTY lines and limit messages based on severity, use the **logging console** command in global configuration mode. To disable logging to the console terminal, use the **no** form of this command.

logging console [*severity-level* | **discriminator** *discr-name* [*severity-level*]]

no logging console

Syntax Description

severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): [**0** | **emergencies**]—System is unusable [**1** | **alerts**]—Immediate action needed [**2** | **critical**]—Critical conditions [**3** | **errors**]—Error conditions [**4** | **warnings**]—Warning conditions [**5** | **notifications**]—Normal but significant conditions [**6** | **informational**]—Informational messages [**7** | **debugging**]—Debugging messages Level 7 is the default.
discriminator	(Optional) Specifies a user-defined filter, via the logging discriminator, for syslog messages.
discr-name	(Optional) String of a maximum of 8 alphanumeric, case-sensitive characters. Blank spaces between characters are not allowed.

Command Default

The default varies by platform. In general, the default is to log all messages.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **discriminator** keyword and *discr-name* argument were added in Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **logging console** command includes all the TTY lines in the device, not only the console TTY. For example, if you are running the **debug ip rip** command from a Telnet session to a VTY TTY on a router and you configure **no logging console**, the debugging messages will not appear in your Telnet command-line interface (CLI) session.

Specifying a level causes messages at that level and numerically lower levels to be sent to the console (TTY lines).

The optional **discriminator** keyword and *discr-name* argument provide another layer of filtering that you can use to control the type and number of syslog messages that you want to receive.

Caution The console is a slow display device. In message storms some logging messages may be silently dropped when the console queue becomes full. Set severity levels accordingly.

The **show logging** EXEC command displays the addresses and levels associated with the current logging setup and other logging statistics.

Table 11 shows a list of levels and corresponding syslog definitions.

Table 11 Error Message Logging Priorities and Corresponding Syslog Definitions

Level	Level Keyword	Syslog Definition
0	**emergencies**	LOG_EMERG
1	**alerts**	LOG_ALERT
2	**critical**	LOG_CRIT
3	**errors**	LOG_ERR
4	**warnings**	LOG_WARNING
5	**notifications**	LOG_NOTICE
6	**informational**	LOG_INFO
7	**debugging**	LOG_DEBUG

Note The behavior of the **log** keyword that is supported by some access lists such as IP extended, IP expanded, and IPX extended depends on the setting of the **logging console** command. The **log** keyword takes effect only if the logging console level is set to 6 or 7. If you change the default to a level lower than 6 and specify the **log** keyword with the **IP access list** (extended) command, no information is logged or displayed.

Examples

The following example shows how to change the level of messages sent to the console terminal (TTY lines) to **alerts**, meaning that messages at levels 0 and 1 are sent:

```
Router(config)# logging console alerts
```

The following example shows how to use a discriminator named msglog1 to filter alerts, meaning that messages at levels 0 and 1 are filtered:

```
Router(config)# logging console discriminator msglog1 alerts
```

Related Commands

Command	Description
access-list (extended)	Defines an extended XNS access list.
logging facility	Configures the syslog facility in which error messages are sent.

logging console filtered

To enable Embedded Syslog Monitor (ESM) filtered system message logging to the console connections, use the **logging console filtered** command in global configuration mode. To disable all logging to the console connections, use the **no** form of this command.

logging console filtered [*severity-level*]

no logging console

Syntax Description

severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): {**0** | **emergencies**}—System is unusable {**1** | **alerts**}—Immediate action needed {**2** | **critical**}—Critical conditions {**3** | **errors**}—Error conditions {**4** | **warnings**}—Warning conditions {**5** | **notifications**}—Normal but significant conditions {**6** | **informational**}—Informational messages {**7** | **debugging**}—Debugging messages The default severity level varies by platform, but is generally level 7 (messages at levels 0 through 7 are logged).

Command Default

Logging to the console is enabled.

ESM filtering of system logging messages sent to the console is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

If standard logging has been disabled on your system (using the **no logging on** command), standard logging must be re-enabled using the **logging on** command before using the **logging console filtered** command.

Standard logging is enabled by default, but filtering by the ESM is disabled by default.

ESM uses syslog filter modules, which are Tcl script files stored locally or on a remote device. The syslog filter modules must be configured using the **logging filter** command before system logging messages can be filtered.

When ESM filtering is enabled, all messages sent to the console have the configured syslog filter modules applied. To disable filtered logging to the console and return to standard logging, use the standard **logging console** command (without the **filtered** keyword). To disable all logging to the console, use the **no logging console** command, with or without the **filtered** keyword.

Examples

The following example shows how to enable ESM filtered logging to the console for severity levels 0 through 3:

```
Router(config)# logging filter tftp://209.165.200.225/ESM/escalate.tcl
Router(config)# logging filter slot0:/email.tcl user@example.com
Router(config)# logging console filtered 3
```

Related Commands

Command	Description
logging console	Enables standard system message logging (syslog) to all console (CTY) connections and sets the severity level.
logging filter	Specifies the name and location of a syslog filter module to be applied to generated system logging messages.
logging on	Globally controls (enables or disables) system message logging.
show logging	Displays the state of system message logging, followed by the contents of the logging buffer.

logging console xml

To enable XML-formatted system message logging to the console connections, use the **logging console xml** command in global configuration mode. To disable all logging to the console connections, use the **no** form of this command.

logging console xml [*severity-level*]

no logging console xml

Syntax Description

severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): {**0** | **emergencies**}— System is unusable {**1** | **alerts**}—Immediate action needed {**2** | **critical**}—Critical conditions {**3** | **errors**}—Error conditions {**4** | **warnings**}—Warning conditions {**5** | **notifications**}—Normal but significant conditions {**6** | **informational**}—Informational messages {**7** | **debugging**}— Debugging messages

Defaults

Logging to the console is enabled.

XML-formatted logging to the console is disabled.

The default severity level varies by platform, but is generally level 7 (messages at levels 0 through 7 are logged).

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To return system logging messages to standard text (without XML formatting), issue the standard **logging console** command (without the **xml** keyword extension).

Examples

In the following example, the user enables XML-formatted system message logging to the console for messages at levels 0 through 4:

```
Router(config)# logging console xml 4
```

Related Commands

Command	Description
show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML syslog buffer.

logging count

To enable the error log count capability, use the **logging count** command in global configuration mode. To disable the error log count capability, use the **no** form of this command.

logging count

no logging count

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **logging count** command counts every syslog message and time-stamps the occurrence of each message.

Examples

In the following example, syslog messages are logged to the system buffer and the logging count capability is enabled:

```
Router(config)# logging buffered notifications
Router(config)# logging count
Router(config)# end
Router# show logging count

Facility       Message Name                     Sev Occur   Last Time

=============================================================================
SYS            BOOTTIME                          6    1     00:00:12
SYS            RESTART                           5    1     00:00:11
SYS            CONFIG_I                          5    3     1d00h
-------------  -------------------------------  -----------------------------
SYS TOTAL                                              5

LINEPROTO      UPDOWN                             5   13 00:00:19
-------------  -------------------------------  -----------------------------
LINEPROTO TOTAL                                       13
```

```
LINK           UPDOWN                             3    1 00:00:18
LINK           CHANGED                            5   12 00:00:09
-------------  -------------------------------  -----------------------------
LINK TOTAL                                            13

SNMP           COLDSTART                          5    1 00:00:11
-------------  -------------------------------  -----------------------------
SNMP TOTAL
```

Related Commands

Command	Description
show logging	Displays the state of system logging (syslog).

logging discriminator

To create a syslog message discriminator, use the **logging discriminator** command in global configuration mode. To turn off the syslog message discriminator, use the **no** form of this command.

logging discriminator *discr-name* [[[**facility** | **mnemonics** | **msg-body**] {**drops** | **includes**} *string*] | **severity** {**drops** | **includes**} *sev-num* | **rate-limit** *msglimit*]

no logging discriminator *discr-name*

Syntax Description

discr-name	String of a maximum of 8 alphanumeric, case-sensitive characters. Blank spaces between characters are not allowed.
facility	(Optional) Message subfilter for the facility pattern in an event message.
mnemonics	(Optional) Message subfilter for the mnemonic pattern in an event message.
msg-body	(Optional) Message subfilter for the msg-body pattern in an event message.
drops	Drops messages that do not match the pattern, including the specified regular expression.
includes	Delivers messages that match the pattern, including the specified regular expression string.
string	(Optional) Expression used for message filtering.
severity	(Optional) Message subfilter by severity level or group.
sev-num	(Optional) Integer that identifies the severity level or multiple levels. Multiple levels must be separated with a comma (,).
rate-limit	(Optional) Specifies a number of messages to be processed within a unit of time.
msglimit	(Optional) Integer in the range of 1 to 1000 that identifies the number of messages not to be exceeded.

Command Default

The logging discriminator function is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

If you enter a discriminator name that was previously specified, your entry is treated as a modification to the discriminator. The modification becomes effective when the configuration is completed. All associated sessions will use the modified value. When you remove a discriminator, the associations of all entries in the logging host list are removed.

When you issue the **no logging discriminator** command and the discriminator name is not found, an error message is generated. If the discriminator name is valid and actively associated with syslog sessions, the effect is immediate; the next syslog message to be processed will go through.

Subfilters are checked in the following order. If a message is dropped by any of the subfilters, the remaining checks are skipped.

1. Severity level or levels specified
2. Facility within the message body that matches a regular expression
3. Mnemonic that matches a regular expression
4. Part of the body of a message that matches a regular expression
5. Rate-limit

Examples

The following example shows how to enable the logging discriminator named msglog01 to filter messages with a severity level of 5.

```
Router(config)# logging discriminator msglog01 severity includes 5
```

Related Commands

Command	Description
logging monitor	Enables system message logging to the terminal lines (monitor connections)

logging facility

To configure the syslog facility in which error messages are sent, use the **logging facility** command in global configuration mode. To revert to the default of **local7**, use the **no** form of this command.

logging facility *facility-type*

no logging facility

Syntax Description

facility-type	Syslog facility. See the "Usage Guidelines" section of this command reference entry for descriptions of acceptable keywords.

Defaults

local7

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Table 12 describes the acceptable keywords for the *facility-type* argument.

Table 12 logging facility facility-type Argument

Facility-type keyword	Description
auth	Authorization system
cron	Cron facility
daemon	System daemon
kern	Kernel
local0–7	Reserved for locally defined messages
lpr	Line printer system
mail	Mail system
news	USENET news
sys9	System use
sys10	System use
sys11	System use

Table 12 logging facility facility-type Argument (continued)

Facility-type keyword	Description
sys12	System use
sys13	System use
sys14	System use
syslog	System log
user	User process
uucp	UNIX-to-UNIX copy system

Examples

In the following example, the user configures the syslog facility to the kernel facility type:

```
Router(config)# logging facility kern
```

Related Commands

Command	Description
logging console	Limits messages logged to the console based on severity.

logging filter

To specify a syslog filter module to be used by the Embedded Syslog Manager (ESM), use the **logging filter** command in global configuration mode. To remove a module from the filter chain, use the **no** form of this command.

logging filter *filter-url* [*position*] [**args** *filter-arguments*]

no logging filter *filter-url*

Syntax Description

filter-url	Specifies the location of the syslog filter module (script file), using the standard Cisco IOS File System URL syntax. • The location can be a local memory location, such as **flash:** or **slot0:**, or a remote file server system, such as **tftp:**, **ftp:**, or **rcp:**. • The *filter-url* should include the name of the syslog filter module, such as email.tcl or email.txt.
position	(Optional) An integer that specifies the order in which the syslog filter modules should be executed. The valid value for this argument is N + 1, where N is the current number of configured filters. • If this argument is omitted, the specified module will be positioned as the last module in the chain (the Nth+1 position).
args *filter-arguments*	(Optional) Any arguments you wish to pass to the ESM file chain can be added using this syntax. The ESM filter modules will determine what arguments you should use.

Command Default

No ESM filters are applied to system logging messages.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to enable the Embedded Syslog Manager by specifying the filter that should be applied to logging messages generated by the system. Repeat this command for each syslog filter module that should be used.

Syslog filter modules are Tcl script files. These files can be stored as plain text files (.txt) or as precompiled Tcl scripts (.tcl). When positioning (ordering) the modules, keep in mind that the output of each filter module is used as input for the next filter module in the chain.

By default, syslog filter modules are executed in the order in which they appear in the system configuration file. The *position* argument can be used to order the filter modules manually. Filter modules can also be reordered at any time by reentering the **logging filter** command and specifying a different position for a given filter module.

The optional **args** *filter-arguments* syntax can be added to pass arguments to the specified filter. Multiple arguments can be specified. The number and type of arguments should be defined in the syslog filter module. For example, if the syslog filter module is designed to accept a specific e-mail address as an argument, you could pass the e-mail address using the **args user@host.com** syntax. Multiple arguments are typically delimited by spaces.

To remove a module from the list of modules to be executed, use the **no** form of this command. Modules not referenced in the configuration will not be executed, regardless of their "position" number.

Examples

The following example shows how to enable ESM filtered logging to the console for severity levels 0 through 3:

```
Router(config)# logging filter tftp://209.165.200.225/ESM/escalate.tcl
Router(config)# logging filter slot0:/email.tcl user@example.com
Router(config)# logging filter slot0:/email_guts.tcl
Router(config)# logging console filtered 3
```

Related Commands

Command	Description
logging buffer filtered	Enables ESM filtered system message logging to the system logging buffer.
logging console filtered	Enables ESM filtered system message logging to all console connections.
logging host	Enables system message logging to a remote host (syslog collector).
logging monitor filtered	Enables ESM filtered system message logging to all monitor (TTY) connections.
show logging	Displays the status of system message logging, followed by the contents of the logging buffer.

logging history

To limit syslog messages sent to the router's history table and to an SNMP network management station based on severity, use the **logging history** command in global configuration mode. To return the logging of syslog messages to the default level, use the **no** form of this command with the previously configured severity level argument.

logging history [*severity-level-name* | *severity-level-number*]

no logging history [*severity-level-name* | *severity-level-number*]

Syntax Description

severity-level-name	Name of the severity level. Specifies the lowest severity level for system error message logging. See the "Usage Guidelines" section of this command for available keywords.
severity-level-number	Number of the severity level. Specifies the lowest severity level for system error message logging. See the "Usage Guidelines" section of this command for available keywords.

Defaults

Logging of error messages of severity levels 0 through 4 (emergency, alert, critical, error, and warning levels); in other words, "saving level warnings or higher."

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The sending of syslog messages to an SNMP network management station (NMS) occurs when you enable syslog traps with the **snmp-server enable traps syslog** global configuration mode command.

Because SNMP traps are potentially unreliable, at least one syslog message, the most recent message, is stored in a history table on the router. The history table, which contains table size, message status, and message text data, can be viewed using the **show logging history** command. The number of messages stored in the table is governed by the **logging history size** global configuration mode command.

Severity levels are numbered 0 through 7, with 0 being the highest severity level and 7 being the lowest severity level (that is, the lower the number, the more critical the message). Specifying a *level* causes messages at that severity level and numerically lower levels to be stored in the router's history table and sent to the SNMP network management station. For example, specifying the level **critical** causes messages as the critical (3), alert (2), and emergency (1) levles to be saved to the logging history table.

Table 13 provides a description of logging severity levels, listed from higest severity to lowest severity, and the arguments used in the **logging history** command syntax. Note that you can use the level name or the level number as the *level* argument in this command.

Table 13 Syslog Error Message Severity Levels

Severity Level Name	Severity Level Number	Description	Syslog Definition
emergencies	**0**	System unusable	LOG_EMERG
alerts	**1**	Immediate action needed	LOG_ALERT
critical	**2**	Critical conditions	LOG_CRIT
errors	**3**	Error conditions	LOG_ERR
warnings	**4**	Warning conditions	LOG_WARNING
notifications	**5**	Normal but significant condition	LOG_NOTICE
informational	**6**	Informational messages only	LOG_INFO
debugging	**7**	Debugging messages	LOG_DEBUG

Examples

In the following example, the system is initially configured to the default of saving severity level 4 or higher. The **logging history 1** command is used to configure the system to save only level 1 (alert) and level 0 (emergency) messages to the logging history table, and, by extension, to send only these levels in the SNMP notifications. The configuration is then confirmed using the **show logging history** command.

```
Router# show logging history
Syslog History Table:10 maximum table entries,
! The following line shows that system-error-message-logging is set to the
! default level of “warnings” (4).
saving level warnings or higher
 23 messages ignored, 0 dropped, 0 recursion drops
 1 table entries flushed
 SNMP notifications not enabled
   entry number 2 : LINK-3-UPDOWN
    Interface FastEthernet0, changed state to up
    timestamp: 2766
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# logging history 1
Router(config)# snmp-server enable traps syslog
Router(config)# end
Router#
4w0d: %SYS-5-CONFIG_I: Configured from console by console
Router# show logging history
Syslog History Table:1 maximum table entries,
! The following line indicates that ‘logging history level 1’ (alerts) is configured.
saving level alerts or higher
 18 messages ignored, 0 dropped, 0 recursion drops
 1 table entries flushed
 SNMP notifications enabled, 0 notifications sent
   entry number 2 : LINK-3-UPDOWN
    Interface FastEthernet0, changed state to up
    timestamp: 2766
Router#
```

Related Commands

Command	Description
logging history size	Sets the maximum number of syslog messages that can be stored in the router's syslog history table.
logging on	Controls (enables or disables) the logging of error messages.
show logging	Displays the state of system logging (syslog) and contents of the local logging buffer.
show logging history	Displays information about the system logging history table.
snmp-server enable traps syslog	Controls (enables or disables) the sending of SYSLOG MIB notifications.
snmp-server host	Specifies the recipient of an SNMP notification operation.

logging history size

To change the number of syslog messages stored in the router’s history table, use the **logging history size** command in global configuration mode. To return the number of messages to the default value, use the **no** form of this command.

logging history size *number*

no logging history size

Syntax Description

number	Number from 1 to 500 that indicates the maximum number of messages stored in the history table. The default is one message.

Defaults

One message

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the history table is full (that is, it contains the maximum number of message entries specified with the **logging history size** command), the oldest message entry is deleted from the table to allow the new message entry to be stored.

Examples

In the following example, the user sets the number of messages stored in the history table to 20:

```
logging history size 20
```

Related Commands

Command	Description
logging history	Limits syslog messages sent to the router’s history table and the SNMP network management station based on severity.
show logging	Displays the state of logging (syslog).

logging host

To log system messages and debug output to a remote host, use the **logging host** command in global configuration mode. To remove a specified logging host from the configuration, use the **no** form of this command.

logging host {{*ip-address* | *hostname*} [**vrf** *vrf-name*] | **ipv6** {*ipv6-address* | *hostname*}} [**discriminator** *discr-name* | [[**filtered** [**stream** *stream-id*] | **xml**]] [**transport** {[**beep** [**audit**] [**channel** *chnl-number*] [**sasl** *profile-name*] [**tls cipher** [*cipher-num*] **trustpoint** *trustpt-name*]]] | **tcp** [**audit**] | **udp**} [**port** *port-num*]] [**sequence-num-session**] [**session-id**]

no logging host {*ip-address* | *hostname*} | **ipv6** {*ipv6-address* | *hostname*}

Syntax Description

ip-address	IP address of the host that will receive the system logging (syslog) messages.
hostname	Name of the IP or IPv6 host that will receive the syslog messages.
vrf	(Optional) Specifies a virtual private network (VPN) routing and forwarding instance (VRF) that connects to the syslog server host.
vrf-name	(Optional) Name of the VRF that connects to the syslog server host.
ipv6	Indicates that an IPv6 address will be used for a host that will receive the syslog messages.
ipv6-address	IPv6 address of the host that will receive the syslog messages.
discriminator	(Optional) Specifies a message discriminator for the session.
discr-name	(Optional) Name of the message discriminator.
filtered	(Optional) Specifies that logging messages sent to this host should first be filtered by the Embedded Syslog Manager (ESM) syslog filter modules specified in the **logging filter** commands.
stream	(Optional) Specifies that only ESM filtered messages with the stream identification number specified in the *stream-id* argument should be sent to this host.
stream-id	(Optional) Number from 10 to 65535 that identifies the message stream.
xml	(Optional) Specifies that the logging output should be tagged using the Extensible Markup Language (XML) tags defined by Cisco.
transport	(Optional) Method of transport to be used. UDP is the default.
beep	(Optional) Specifies that the Blocks Extensible Exchange Protocol (BEEP) transport will be used.
audit	(Optional) Available only for BEEP and TCP. When the **audit** keyword is used, the specified host is identified for firewall audit logging.
channel	(Optional) Specifies the BEEP channel number to use.
chnl-number	(Optional) Number of the BEEP channel. Valid values are 1, 3, 5, 7, 9, 11, 13, and 15. The default is 1.
sasl	(Optional) Applies the Simple Authentication and Security Layer BEEP profile.
profile-name	(Optional) Name of the SASL profile.
tls cipher	(Optional) Specifies the cipher suites to be used for a connection. Cipher suites are referred to by mask values. Multiple cipher suites can be chosen by adding the mask values. The **tls cipher** *cipher-num* keyword and argument pair is available only in crypto images.

cipher-num	(Optional) Integer from 32 to 224 that is the mask value of a cipher suite (sum of up to three numbers: 32, 64, and 128) and refers to the following: ENC_FLAG_TLS_RSA_WITH_NULL_SHA – 32 ENC_FLAG_TLS_RSA_WITH_RC4_128_MD5 – 64 ENC_FLAG_TLS_RSA_WITH_AES_128_CBC_SHA – 128 The **tls cipher** *cipher-num* keyword and argument pair is available only in crypto images.
trustpoint	(Optional) Specifies a trustpoint for identity information and certificates. The **trustpoint** *trustpt-name* keyword and argument pair is available only in crypto images.
trustpt-name	(Optional) Name of the trustpoint. If you previously declared the trustpoint and want only to update its characteristics, specify the name you previously created. The **trustpoint** *trustpt-name* keyword and argument pair is available only in crypto images.
tcp	(Optional) Specifies that TCP transport will be used.
udp	(Optional) Specifies that the User Datagram Protocol (UDP) transport will be used.
port	(Optional) Specifies a port will be used.
port-number	(Optional) Integer from 1 through 65535 that defines the port. If a port number is not specified, the standard Cisco default port number for TCP is 601, for BEEP is 601, and for UDP is 514.
sequence-num-session	(Optional) Includes a session sequence number tag in the syslog message.
session-id	(Optional) Specifies syslog message session ID tagging

Command Default

System logging messages are not sent to any remote host.
When this command is entered without the **xml** or **filtered** keyword, messages are sent in the standard format.

Command Modes

Global configuration

Command History

Release	Modification
10.0	The **logging** command was introduced.
12.0(14)S	The **logging host** command replaced the **logging** command.
12.0(14)ST	The **logging host** command replaced the **logging** command.
12.2(15)T	The **logging host** command replaced the **logging** command. The **xml** keyword was added.
12.3(2)T	The **filtered** [**stream** *stream-id*] syntax was added as part of the ESM feature.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.

Release	Modification
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S and the **vrf** *vrf-name* keyword-argument pair was added.
12.4(4)T	The **ipv6** *ipv6-address* and **vrf** *vrf-name* keyword-argument pairs were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	Support for BEEP and the **discriminator** keyword and *discr-name* argument were added in Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was implemented on the Cisco 10000 series routers.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Standard system logging is enabled by default. If logging is disabled on your system (using the **no logging on** command), you must enter the **logging on** command to reenable logging before you can use the **logging host** command.

The **logging host** command identifies a remote host (usually a device serving as a syslog server) to receive logging messages. By issuing this command more than once, you can build a list of hosts that receive logging messages.

To specify the severity level for logging to all hosts, use the **logging trap** command.

Use the **vrf** *vrf-name* keyword and argument to enable a syslog client (a provider edge [PE] router) to send syslog messages to a syslog server host connected through a VRF interface. To delete the configuration of the syslog server host from the VRF, use the **no logging host** command with the **vrf** *vrf-name* keyword and argument.

When XML-formatted syslog is enabled using the **logging host** command with the **xml** keyword, messages are sent to the specified host with the system-defined XML tags. These tags are predefined and cannot be configured by a user. XML formatting is not applied to debug output.

If you are using the ESM feature, you can enable ESM-filtered syslog messages to be sent to one or more hosts using the **logging host filtered** command. To use the ESM feature, you must first specify the syslog filter modules that should be applied to the messages using the **logging filter** command. See the description of the **logging filter** command for more information about the ESM feature.

Note ESM and message discriminator usage are mutually exclusive on a given syslog session.

Using the BEEP transport protocol, you can have reliable and secure delivery for syslog messages and configure multiple sessions over 8 BEEP channels. The **sasl** *profile-name*, **tls cipher** *cipher-num,* **trustpoint** *trustpt-name* keywords and arguments are available only in crypto images.

To configure standard logging to a specific host after configuring XML-formatted or ESM-filtered logging to that host, use the **logging host** command without the **xml** or **filtered** keyword. Issuing the standard **logging host** command replaces an XML- or ESM- filtered **logging host** command, and vice versa, if the same host is specified.

You can configure the system to send standard messages to one or more hosts, XML-formatted messages to one or more hosts, and ESM-filtered messages to one or more hosts by repeating this command as many times as desired with the appropriate syntax. (See the "Examples" section.)

When the **no logging host** command is issued with or without the optional keywords, all logging to the specified host is disabled.

Examples

In the following example, messages at severity levels 0 (emergencies) through 5 (notifications) (**logging trap** command severity levels) are logged to a host at 192.168.202.169:

```
Router(config)# logging host 192.168.202.169
Router(config)# logging trap 5
```

In the following example, standard system logging messages are sent to the host at 192.168.200.225, XML-formatted system logging messages are sent to the host at 192.168.200.226, ESM-filtered logging messages with the stream 10 value are sent to the host at 192.168.200.227, and ESM-filtered logging messages with the stream 20 value are sent to host at 192.168.202.129:

```
Router(config)# logging host 192.168.200.225
Router(config)# logging host 192.168.200.226 xml
Router(config)# logging host 192.168.200.227 filtered stream 10
Router(config)# logging host 192.168.202.129 filtered stream 20
```

In the following example, messages are logged to a host with an IP address of 172.16.150.63 connected through a VRF named vpn1:

```
Router(config)# logging host 172.16.150.63 vrf vpn1
```

In the following example, the default UDP on an IPv6 server is set because no port number is specified. The default port number of 514 is used:

```
Router(config)# logging host ipv6 AAAA:BBBB:CCCC:DDDD::FFFF
```

In the following example, TCP port 1774 on an IPv6 server is set:

```
Router(config)# logging host ipv6 BBBB:CCCC:DDDD:FFFF::1234 transport tcp port 1774
```

In the following example, the UDP port default is used on an IPv6 server with a hostname of v6-hostname:

```
Router(config)# logging host ipv6 v6-hostname transport udp port 514
```

In the following example, a message discriminator named fltr1 is specified as well as the BEEP protocol for port 600 and channel 3.

```
Router(config)# logging host host2 transport beep channel 3 port 600
```

Related Commands

Command	Description
logging filter	Specifies a syslog filter module to be used by the ESM.
logging on	Globally controls (enables or disables) system message logging.
logging trap	Limits messages sent to the syslog servers based on severity level.
show logging	Displays the state of system message logging, followed by the contents of the standard syslog buffer.
show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML syslog buffer.

logging linecard

To log messages to an internal buffer on a line card, use the **logging linecard** command in global configuration mode. To cancel the use of the internal buffer on the line cards, use the **no** form of this command.

logging linecard [*size* | *level*]

no logging linecard

Syntax Description

size	(Optional) Size of the buffer used for each line card. The range is from 4096 to 65,536 bytes. The default is 8 KB.
level	(Optional) Limits the logging of messages displayed on the console terminal to a specified level. The message level can be one of the following: • **alerts**—Immediate action needed • **critical**—Critical conditions • **debugging**—Debugging messages • **emergencies**—System is unusable • **errors**—Error conditions • **informational**—Informational messages • **notifications**—Normal but significant conditions • **warnings**—Warning conditions

Defaults

The Cisco IOS software logs messages to the internal buffer on the GRP card.

Command Modes

Global configuration

Command History

Release	Modification
11.2GS	This command was added to support the Cisco 12000 series Gigabit Switch Routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Specifying a message level causes messages at that level and numerically lower levels to be stored in the internal buffer on the line cards.

Table 14 lists the message levels and associated numerical level. For example, if you specify a message level of critical, all critical, alert, and emergency messages will be logged.

Table 14 Message Levels

Level Keyword	Level
emergencies	0
alerts	1
critical	2
errors	3
warnings	4
notifications	5
informational	6
debugging	7

To display the messages that are logged in the buffer, use the **show logging slot** EXEC command. The first message displayed is the oldest message in the buffer.

Do not make the buffer size too large because the router could run out of memory for other tasks. You can use the **show memory** EXEC command to view the free processor memory on the router; however, this is the maximum available and should not be approached.

Examples

The following example enables logging to an internal buffer on the line cards using the default buffer size and logging warning, error, critical, alert, and emergency messages:

```
Router(config)# logging linecard warnings
```

Related Commands

Command	Description
clear logging	Clears messages from the logging buffer.
show logging	Displays the state of logging (syslog).

logging message-counter

To enable logging of debug, log, or syslog messages, use the **logging message-counter** command in global configuration mode. To turn off logging for these message types, use the **no** form of this command.

logging message-counter {**debug** | **log** | **syslog**}

no logging message-counter {**debug** | **log** | **syslog**}

Syntax Description

debug	Enables the debug information message counter, which is a counter of accumulated debug information messages received by the logger.
log	Enables all message counters of accumulated logging messages received by the logger.
syslog	Enables the syslog message counter, which is a counter of current lines of syslog messages sent. This counter is enabled by default.

Command Default

The logging message counter function is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to help identify where event messages are being dropped because of rate limiting or to exclude the syslog counter from a syslog message.

Examples

The following example shows how to enable the syslog message counter:

```
Router(config)# logging message-counter syslog
```

logging monitor

To enable system message logging to the terminal lines (monitor connections), use the **logging monitor** command in global configuration mode. To disable logging to terminal lines other than the console line, use the **no** form of this command.

logging monitor [*severity-level* | **discriminator** *discr-name* [*severity-level*]]

no logging monitor

Syntax Description

severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): {**0** | **emergencies**}—System is unusable {**1** | **alerts**}—Immediate action needed {**2** | **critical**}—Critical conditions {**3** | **errors**}—Error conditions {**4** | **warnings**}—Warning conditions {**5** | **notifications**}—Normal but significant conditions {**6** | **informational**}—Informational messages {**7** | **debugging**}— Debugging messages Level 7 is the default.
discriminator	(Optional) Specifies a user-defined filter, via the logging discriminator, for syslog messages.
discr-name	(Optional) String of a maximum of 8 alphanumeric, case-sensitive characters. Blank spaces between characters are not allowed.

Command Default

The logging monitor function is disabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **discriminator** keyword and *discr-name* argument were added in Cisco IOS Release 12.4(11)T.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Specifying a severity-level causes messages both at that level and at numerically lower levels to be displayed to the monitor. Table 15 shows a list of levels and corresponding syslog definitions.

Table 15 Error Message Logging Priorities and Corresponding Syslog Definitions

Level	Level Keyword	Syslog Definition
0	**emergencies**	LOG_EMERG
1	**alerts**	LOG_ALERT
2	**critical**	LOG_CRIT
3	**errors**	LOG_ERR
4	**warnings**	LOG_WARNING
5	**notifications**	LOG_NOTICE
6	**informational**	LOG_INFO
7	**debugging**	LOG_DEBUG

Examples

The following example shows how to specify that messages at levels 3 (errors), 2 (critical), 1 (alerts), and 0 (emergencies) be logged to monitor connections:

```
Router(config)# logging monitor 3
```

The following example shows how to use a discriminator named monitor1 to filter critical messages, meaning that messages at levels 0, 1, and 2 are filtered:

```
Router(config)# logging monitor discriminator monitor1 critical
```

Related Commands

Command	Description
logging monitor filtered	Enables ESM filtered system message logging to monitor connections.
logging monitor xml	Applies XML formatting to messages logged to the monitor connections.
terminal monitor	Displays **debug** command output and system error messages for the current terminal and session.

logging monitor filtered

To enable Embedded Syslog Manager (ESM) filtered system message logging to monitor connections, use the **logging monitor filtered** command in global configuration mode. To disable all logging to the monitor connections, use the **no** form of this command.

logging monitor filtered [*severity-level*]

no logging monitor filtered

Syntax Description

severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): {**0** | **emergencies**}—System is unusable {**1** | **alerts**}—Immediate action needed {**2** | **critical**}—Critical conditions {**3** | **errors**}—Error conditions {**4** | **warnings**}—Warning conditions {**5** | **notifications**}—Normal but significant conditions {**6** | **informational**}—Informational messages {**7** | **debugging**}—Debugging messages The default severity level varies by platform, but is generally level 7 (messages at levels 0 through 7 are logged).

Command Default

Logging to monitor connections is enabled.

ESM filtering of system logging messages sent to the monitor connections is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **monitor** keyword specifies the TTY (TeleTYpe) line connections at all line ports. TTY lines (also called ports) communicate with peripheral devices such as terminals, modems, and serial printers. An example of a TTY connection is a PC with a terminal emulation program connected to the device using a dial-up modem, or a Telnet connection.

Standard logging is enabled by default, but filtering by the ESM is disabled by default. If standard logging has been disabled on your system (using the **no logging on** command), standard logging must be re-enabled using the **logging on** command before using the **logging monitor filtered** command.

ESM uses syslog filter modules, which are Tcl script files stored locally or on a remote device. The syslog filter modules must be configured using the **logging filter** command before system logging messages can be filtered.

When ESM filtering is enabled, all messages sent to the monitor have the configured syslog filter modules applied. To disable filtered logging to the monitor and return to standard logging, issue the standard **logging monitor** command (without the **filtered** keyword). To disable all logging to the monitor connections, use the **no logging monitor** command, with or without the **filtered** keyword.

Examples

The following example shows how to enable ESM filtered logging to the monitor connections:

```
Router(config)# logging filter tftp://209.165.200.225/ESM/escalate.tcl
Router(config)# logging filter slot0:/email.tcl user@example.com
Router(config)# logging monitor filtered
```

Related Commands

Command	Description
logging monitor	Enables standard system message logging to all monitor (TTY) connections.
show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML syslog buffer.

logging monitor xml

To enable XML-formatted system message logging to monitor connections, use the **logging console xml** command in global configuration mode. To disable all logging to the monitor connections, use the **no** form of this command.

logging monitor xml [*severity-level*]

no logging monitor xml

Syntax Description

severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): {**0** | **emergencies**}— System is unusable {**1** | **alerts**}—Immediate action needed {**2** | **critical**}—Critical conditions {**3** | **errors**}—Error conditions {**4** | **warnings**}—Warning conditions {**5** | **notifications**}—Normal but significant conditions {**6** | **informational**}—Informational messages {**7** | **debugging**}— Debugging messages

Defaults

Logging to monitor connections is enabled.

XML-formatted logging to monitor connections is disabled.

The default severity level varies by platform, but is generally level 7 (messages at levels 0 through 7 are logged).

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **monitor** keyword specifies the tty line connections at all line ports. The tty lines (also called ports) communicate with peripheral devices such as terminals, modems, and serial printers. An example of a tty connection is a PC with a terminal emulation program connected to the device using a dial-up modem, or a Telnet connection.

To return system logging messages to standard text (without XML formatting), issue the standard **logging monitor** command (without the **xml** keyword extension).

Examples

In the following example, the user enables XML-formatted system message logging to the console for messages at levels 0 through 4 and XML-formatted system message logging to tty line connections at the default severity level:

```
Router(config)# logging console xml 4
Router(config)# logging monitor xml
```

Related Commands

Command	Description
logging monitor	Enables system message logging in standard (plain text) format to all monitor (TTY) connections.
show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML syslog buffer.

logging on

To enable logging of system messages, use the **logging on** command in global configuration mode. This command sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages. To disable the logging process, use the **no** form of this command.

logging on

no logging on

Syntax Description

This command has no arguments or keywords.

Defaults

The Cisco IOS software sends messages to the asynchronous logging process.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, terminal lines, or syslog server. System logging messages are also known as system error messages. You can turn logging on and off for these destinations individually using the **logging buffered**, **logging monitor**, and **logging** global configuration commands. However, if the **logging on** command is disabled, no messages will be sent to these destinations. Only the console will receive messages.

Additionally, the logging process logs messages to the console and the various destinations after the processes that generated them have completed. When the logging process is disabled, messages are displayed on the console as soon as they are produced, often appearing in the middle of command output.

⚠ **Caution** Disabling the **logging on** command may substantially slow down the router. Any process generating debug or error messages will wait until the messages have been displayed on the console before continuing.

The **logging synchronous** line configuration command also affects the displaying of messages to the console. When the **logging synchronous** command is enabled, messages will appear only after the user types a carriage return.

Examples

The following example shows command output and message output when logging is enabled. The ping process finishes before any of the logging information is printed to the console (or any other destination).

```
Router(config)# logging on
Router(config)# end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router# ping dirt

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.129, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
Router#
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
```

In the following example, logging is disabled. The message output is displayed as messages are generated, causing the debug messages to be interspersed with the message “Type escape sequence to abort.”

```
Router(config)# no logging on
Router(config)# end

%SYS-5-CONFIG_I: Configured from console by console
Router#
Router# ping dirt

IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sendingTyp
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1e
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending esc
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sendingape
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sendingse
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sendingquen
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1ce to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.129, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 152/152/156 ms
Router#
```

Related Commands

Command	Description
logging host	Logs messages to a syslog server host.
logging buffered	Logs messages to an internal buffer.
logging console	Logs messages to console connections.

Command	Description
logging monitor	Limits messages logged to the terminal lines (monitors) based on severity.
logging synchronous	Synchronizes unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty.

logging origin-id

To add an origin identifier to system logging messages sent to remote hosts, use the **logging origin-id** command in global configuration mode. To disable the origin identifier, use the **no** form of this command.

logging origin-id {**hostname** | **ip** | **ipv6** | **string** *user-defined-id*}

no logging origin-id

Syntax Description

hostname	Specifies that the hostname will be used as the message origin identifier.
ip	Specifies that the IP address of the sending interface will be used as the message origin identifier.
ipv6	Specifies that the IPv6 address of the sending interface will be used as the message origin identifier.
string *user-defined-id*	Allows you to enter your own identifying description. The *user-defined-id* argument is a string you specify. • You can enter a string with no spaces or use delimiting quotation marks to enclose a string with spaces.

Command Default

This feature is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(1)	The **string** *user-defined-id* syntax was added.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.4(4)T	The **ipv6** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The origin identifier is added to the beginning of all system logging (syslog) messages sent to remote hosts. The identifier can be the hostname, the IP address, the IPv6 address, or any text that you specify. The origin identifier is not added to messages sent to local destinations (the console, monitor, or buffer).

The origin identifier is useful for identifying the source of system logging messages in cases where you send syslog output from multiple devices to a single syslog host.

When you specify your own identification string using the **logging origin-id string** *user-defined-id* command, the system expects a string without spaces. For example:

```
Router(config)# logging origin-id string Cisco_Systems
```

To uses spaces (multiple words) or additional syntax, enclose the string with quotes. For example:

```
Router(config)# logging origin-id string "Cisco Systems, Inc."
```

Examples

In the following example, the origin identifier "Domain 1, router B" will be added to the beginning of all system logging messages sent to remote hosts:

```
Router(config)# logging origin-id string Domain 1, router B
```

In the following example, all logging messages sent to remote hosts will have the IP address configured for the serial 1 interface added to the beginning of the message:

```
Router(config)# logging host 209.165.200.225
Router(config)# logging trap 5
Router(config)# logging source-interface serial 1
Router(config)# logging origin-id ip
```

Related Commands

Command	Description
logging host	Enables system message logging to a remote host.
logging source-interface	Forces logging messages to be sent from a specified interface, instead of any available interface.
logging trap	Configures the severity level at or numerically below which logging messages should be sent to a remote host.

logging persistent

To enable the storage of logging messages on the router's advanced technology attachment (ATA) disk, use the **logging persistent** command in global configuration mode. To disable logging message storage on the ATA disk, use the **no** form of this command.

logging persistent [**url** {**disk0:/***directory* | **disk1:/***directory*}] [**size** *filesystem-size*] [**filesize** *logging-file-size*]

no logging persistent

Syntax Description

url	(Optional) Any supported local Cisco IOS file system location. The default URL is disk0:/syslog.
disk0:/*directory*	Directory on disk 0 where syslog messages are saved.
disk1:/*directory*	Directory on disk 1 where syslog messages are saved.
size *filesystem-size*	(Optional) Amount of disk space allocated to syslog messages in bytes. • Minimum value is 16384. • Maximum value is the total amount of available disk space. • Default value is 10% of total disk space.
filesize *logging-file-size*	(Optional) Size of individual logging files in bytes. • Minimum value is 8192. • Maximum value is the total amount of available disk space. • Default value is 262144.

Command Default

The logging messages are not stored in the router's ATA memory.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

The **logging persistent** command enables the storage of syslog data on the router's ATA Flash disk. Because the syslog data must be copied from the router's internal memory buffer, you must enable the **logging buffered** command prior to enabling the **logging persistent** command.

Note Any filtering of syslog messages written to the router's internal memory buffer results in filtering of syslog messages written to the router's ATA Flash disk.

Examples

The following example shows how to write up to 134217728 bytes (128 MB) of logging messages to the syslog directory of disk 0, with a file size of 16384 bytes:

```
Router(config)# logging buffered
Router(config)# logging persistent url disk0:/syslog size 134217728 filesize 16384
```

Related Commands

Command	Description
logging buffered	Saves syslog messages in router memory.

logging queue-limit

To control how much system memory may be used for queued log messages, use the **logging queue-limit** command in global configuration mode. To permit unlimited use of memory for queued log messages, use the **no** form of this command.

logging queue-limit [*queuesize* | **trap** *queuesize* | **esm** *queuesize*]

no logging queue-limit

Syntax Description

queuesize	(Optional) The number of messages in the logger queue. The valid range is 100 to 2147483647. The default is 100.
trap	(Optional) Specifies the limit for the number of log messages that may be queued for a remote system logging (syslog) server and sends the messages to a trap.
esm	(Optional) Specifies the limit for the number of log messages that may be queued for the Embedded Syslog Manager (ESM) subsystem. The size change to the ESM queue will take effect only if the ESM feature is supported in the image and an ESM filter has been configured.

Command Default

100 messages

Note The default logger queue size varies depending on the hardware platform and is set up by an internal function at run time. The default queue sizes in Cisco IOS Release 12.4(8) are listed as follows. These sizes are subject to change.

- Cisco Catalyst 6500 series switches—256 messages
- Cisco 7200 platform—250 messages
- Cisco AS5400 platform—200 messages
- All other Cisco platforms—100 messages

Command Modes

Global configuration

Command History

Release	Modification
12.4(8)	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

The size of the logging queue affects system memory. In the logging queue, each message has its own memory object. The more messages being queued, the less memory is available for other components of the system to share.

Tuning the queue size is sometimes required when Cisco technical support staff needs to reduce the possibility that logging messages are dropped because the event messages are bursty. The **logging queue-limit** command is meant for use by Cisco technical support staff assisting on a field-critical case to ensure critical messages are not dropped because of a smaller default queue size.

Customers are discouraged from tuning the message queue size if they have not first contacted the Cisco Technical Support Center (TAC).

Caution When you are tuning the queue size to a larger value, no messages will be dropped. When you relax or remove limits on logger queueing, it is possible to adversely impact the system due to memory, CPU, or network exhaustion.

When the **logging queue-limit** command is used to reset the logging queue to the default size, it also resets the trap and ESM queues to their default sizes.

Examples

The following example sets the logging queue to the system default size:

```
Router(config)# logging queue-limit
```

The following example sets the logging queue to 1000 queue entries:

```
Router(config)# logging queue-limit 1000
```

The following example removes all logging queue limits:

```
Router(config)# no logging queue-limit
```

The following example sets the logging queue size at 1000 for messages sent to the ESM:

```
Router(config)# logging queue-limit esm 1000
```

The following example sets the logging queue size to 1000 for messages sent to an external syslog:

```
Router(config)# logging queue-limit trap 1000
```

Related Commands

Command	Description
logging rate-limit	Limits the rate of messages logged per second.
logging synchronous	Synchronizes unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty.
logging trap	Limits messages logged to the syslog servers based on severity.
show logging	Displays the state of the syslog and the contents of the standard system logging buffer.

logging rate-limit

To limit the rate of messages logged per second, use the **logging rate-limit** command in global configuration mode. To disable the limit, use the **no** form of this command.

logging rate-limit {*number* | **all** *number* | **console** {*number* | **all** *number*}} [**except** *severity*]

no logging rate-limit

Syntax Description

number	Number of messages to be logged per second. Valid values are 1 to 10000. The default is 10.
all	Sets the rate limit for all error and debug messages displayed at the console and printer.
console	Sets the rate limit for error and debug messages displayed at the console.
except *severity*	(Optional) Excludes messages of this severity level and lower. Valid levels are 0 to 7. Severity decreases as the number increases; therefore, severity level 1 indicates a problem more serious than a severity level 3.

Command Default

The default is 10 messages logged per second.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.3	This command was integrated into Cisco IOS Release 12.3.
12.3T	This command was integrated into Cisco IOS Release 12.3T.
12.4	This command was integrated into Cisco IOS Release 12.4.
12.4T	This command was integrated into Cisco IOS Release 12.4T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **logging rate-limit** command controls the output of messages from the system. Use this command to avoid a flood of output messages. You can select the severity of the output messages and the output rate by using the **logging rate-limit** command. You can issue the **logging rate-limit** command at any time. System performance is not negatively affected and may improve when severities and rates of output messages are specified.

You can use **logging rate-limit** command with or without the **logging synchronous** line configuration command. For example, if you want to see all severity 0, 1, and 2 messages, use the **no logging synchronous** command and specify **logging rate-limit 10 except 2**. By using the two commands together, you cause all messages of 0, 1, and 2 severity to print and limit the less severe ones (higher number than 2) to only 10 per second.

Table 16 shows the numeric severity level, equivalent meaning in text, and a description for error messages.

Table 16 Error Message Severity Levels, Equivalent Text, and Descriptions

Numeric Severity Level	Equivalent Word	Description
0	**emergencies**	System unusable
1	**alerts**	Immediate action needed
2	**critical**	Critical conditions
3	**errors**	Error conditions
4	**warnings**	Warning conditions
5	**notifications**	Normal but significant condition
6	**informational**	Informational messages only
7	**debugging**	Debugging messages

Cisco 10000 Series Router

To avoid CPU overload and router instability, use the **logging rate-limit** command to limit the rate at which the Cisco 10000 series router logs system messages. To increase the Point-to-Point Protocol call rate, you can turn off console logging completely using the **no logging console** command.

Examples

The following example shows how to limit message output to 200 per second:

```
Router(config)# logging rate-limit 200
```

Related Commands

Command	Description
logging synchronous	Synchronizes unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty.
no logging console	Disables syslog message logging to the console terminal.

logging source-interface

To specify the source IP or IPv6 address of system logging packets, use the **logging source-interface** command in global configuration mode. To remove the source designation, use the **no** form of this command.

logging source-interface *interface-type interface-number*

no logging source-interface

Syntax Description

interface-type	Interface type.
interface-number	Interface number.

Command Default

No interface is specified.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.4(4)T	IPv6 support was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Normally, a syslog message contains the IP or IPv6 address of the interface it uses to leave the router. The **logging source-interface** command specifies that syslog packets contain the IP or IPv6 address of a particular interface, regardless of which interface the packet uses to exit the router.

When no specific interface is configured, a wildcard interface address of 0.0.0.0 (for IPv4) or :: (for IPv6) is used, and the IP socket selects the best outbound interface.

Examples

In the following example, the user specifies that the IP address for Ethernet interface 0 is the source IP address for all syslog messages:

```
Router(config)# logging source-interface ethernet 0
```

The following example specifies that the IP address for Ethernet interface 2/1 on a Cisco 7000 series router is the source IP address for all syslog messages:

```
Router(config)# logging source-interface ethernet 2/1
```

Related Commands

Command	Description
logging	Logs messages to a syslog server host.

logging trap

To limit messages logged to the syslog servers based on severity, use the **logging trap** command in global configuration mode. To return the logging to remote hosts to the default level, use the **no** form of this command.

logging trap *level*

no logging trap

Syntax Description

severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): {**0** | **emergencies**}— System is unusable {**1** | **alerts**}—Immediate action needed {**2** | **critical**}—Critical conditions {**3** | **errors**}—Error conditions {**4** | **warnings**}—Warning conditions {**5** | **notifications**}—Normal but significant conditions {**6** | **informational**}—Informational messages {**7** | **debugging**}— Debugging messages

Defaults

Syslog messages at level 0 to level 6 are generated, but will only be sent to a remote host if the **logging host** command is configured.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A trap is an unsolicited message sent to a remote network management host. Logging traps should not be confused with SNMP traps (SNMP logging traps require the use of the CISCO -SYSLOG-MIB, are enabled using the **snmp-server enable traps syslog** command, and are sent using the Simple Network Management Protocol.)

The **show logging** EXEC command displays the addresses and levels associated with the current logging setup. The status of logging to remote hosts appears in the command output as “trap logging”.

Table 17 lists the syslog definitions that correspond to the debugging message levels. Additionally, four categories of messages are generated by the software, as follows:

- Error messages about software or hardware malfunctions at the LOG_ERR level.
- Output for the debug commands at the LOG_WARNING level.
- Interface up/down transitions and system restarts at the LOG_NOTICE level.
- Reload requests and low process stacks at the LOG_INFO level.

Use the **logging host** and **logging trap** commands to send messages to a remote syslog server.

Table 17 logging trap Error Message Logging Priorities

Level Arguments	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Examples

In the following example, system messages of levels 0 (emergencies) through 5 (notifications) are sent to the host at 209.165.200.225:

```
Router(config)# logging host 209.165.200.225
Router(config)# logging trap notifications
Router(config)# end
Router# show logging
Syslog logging: enabled (0 messages dropped, 1 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)
    Console logging: level emergencies, 0 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging: level debugging, 67 messages logged, xml disabled,
                    filtering disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: enabled
    Trap logging: level notifications, 71 message lines logged

Log Buffer (4096 bytes):
00:00:20: %SYS-5-CONFIG_I: Configured from memory by console
 .
 .
 .
```

Related Commands

Command	Description
logging host	Enables remote logging of system logging messages and specifies the syslog server host that messages should be sent to.

logging userinfo

To enable logging user information use the **logging userinfo** command in global configuration mode. To cancel the logging of user information, use the **no** form of this command.

logging userinfo

no logging userinfo

Syntax Description

This command has no arguments or keywords.

Command Default

User information logging is disabled by default.

Command Modes

Global configuration mode

Command History

Release	Modification
12.0S	This command was introduced.
12.3T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **logging userinfo** global configuration command allows the logging of user information when the user invokes the enable privilege mode or when the user changes the privilege level. Information logged includes “username”, “line” (i.e. Console, vty0, etc.) and “privileged level” (i.e. 0 - 15).

Note When a username is not available, “unknown” is displayed as the username.

Examples

The following example enables user information logging.

```
Router# configure terminal
Router(config)# logging userinfo
Router(config)# exit
```

The following are 2 examples of user information logging.

```
Router> enable
Password:
Router#
*Feb 26 17:11:15.398: %SYS-5-PRIV_AUTH_PASS: Privilege level set to 15 by cisco)
Router# disable 6
Router#
*Feb 26 17:12:28.922: %SYS-5-PRIV_AUTH_PASS: Privilege level set to 6 by cisco)
```

```
Router# enable 15
Password:
Router#
*Feb 26 17:15:48.022: %SYS-5-PRIV_AUTH_PASS: Privilege level set to 15 by cisco)
Router#
```

Related Commands

Command	Description
disable	Exits from privileged EXEC mode to user EXEC mode, or, if privilege levels are set, to the specified privilege level.
enable	Enables higher privilege level access, such as privileged EXEC mode.
privilege level (global)	Sets a privilege level for a command.
privilege level (line)	Sets a privilege level for a command for a specific line.

major rising

To set major level threshold values for the buffer, CPU, and memory resource owners (ROs), use the **major rising** command in buffer owner configuration mode, CPU owner configuration mode, or memory owner configuration mode. To disable this function, use the **no** form of this command.

major rising *rising-threshold-value* [**interval** *interval-value*] [**falling** *falling-threshold-value* [**interval** *interval-value*]] [**global**]

no major rising

Syntax Description

rising-threshold-value	The rising threshold value as a percentage. Valid values are from 1 to 100.
interval	(Optional) Specifies the time, in seconds, during which the variation in rising or falling threshold values are not reported to the request/response unit (RU), resource group, or resource user types. For example, if the buffer usage count remains above the configured threshold value for the configured interval, a notification is sent to the RU, resource group, or resource user types.
interval-value	The time, in seconds, during which the variation in rising or falling threshold values is not reported to the RU, resource group, or resource user types. Valid values are from 0 to 86400. The default value is 0.
falling	(Optional) Specifies the falling threshold value as a percentage.
falling-threshold-value	(Optional) The falling threshold value. Valid values are from 1 to 100.
global	(Optional) Configures a global threshold. The **global** keyword is optional when you set major threshold values for public buffer, processor CPU, I/O memory, and processor memory. The **global** keyword is required when you set major threshold values for interrupt CPU and total CPU.

Command Default

Disabled

Command Modes

Buffer owner configuration
CPU owner configuration
Memory owner configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

The interval is the dampening or observation interval time, in seconds, during which the variations in the rising and falling threshold values are not notified to the ROs or RUs. That is, the interval is the time the system waits to check whether the threshold value stabilizes. The interval is set to avoid unnecessary and unwanted threshold notifications. If not configured, the system defaults to 0 seconds.

This command allows you to configure three types of thresholding:

- System Global Thresholding
- User Local Thresholding
- Per User Global Thresholding

System Global Thresholding

System global thresholding is used when the entire resource reaches a specified value. That is, RUs are notified when the total resource utilization goes above or below a specified threshold value. The notification order is determined by the priority of the RU. The RUs with a lower priority are notified first, and are expected to reduce the resource utilization. This notification order prevents the high-priority RUs from being sent unwanted notifications.

You can set rising and falling threshold values. For example, if you have set a total CPU utilization threshold value of 70% as the rising major value and 15% as the falling major value, when the total CPU utilization crosses the 70% mark, a major Up notification is sent to all the RUs and when the total CPU utilization falls below 15%, a major Down notification is sent to all the RUs. The same criteria apply to buffer ROs and memory ROs.

User Local Thresholding

User local thresholding is used when a specified RU exceeds the configured limits. The user local thresholding method prevents a single RU from monopolizing resources. That is, the specified RU is notified when its resource utilization exceeds or falls below a configured threshold value. For example, if you set a CPU utilization threshold value of 70% as the rising major value and 15% as the falling major value, when the CPU utilization of the specified RU crosses the 70% mark, a major Up notification is sent to that RU only and when the CPU utilization of the specified RU falls below 15%, a major Down notification is sent to only that RU. The same method also applies to buffer and memory ROs.

Per User Global Thresholding

Per user global thresholding is used when the entire resource reaches a specified value. This value is unique for each RU and notification is sent only to the specified RU. User global thresholding is similar to user local thresholding, except that the global resource usage is compared against the thresholds. That is, only the specified RU is notified when the total resource utilization exceeds or falls below a configured threshold value. For example, if you set a CPU utilization threshold value of 70% as the rising major value and 15% as the falling major value, when the total CPU utilization crosses the 70% mark, a major Up notification is sent to only the specified RU and when the total CPU utilization falls below 15%, a major Down notification is sent to only the specified RU. The same method also applies to buffer and memory ROs.

Threshold Violations

The Cisco IOS device sends out error messages when a threshold is violated. The following examples help you understand the error message pattern when different threshold violations occur in buffer, CPU, and memory ROs:

System Global Threshold Violation in Buffer RO

The threshold violation in buffer RO for a system global threshold shows the following output:

```
System global threshold-Violation (keywords Critical, Major and Minor alone will vary
accordingly)
=========================================================================================
00:15:11: %SYS-4-GLOBALBUFEXCEED: Buffer usage has gone above global buffer Major
threshold
configured <value> Current usage :<value>
```

For example:

```
00:15:11: %SYS-4-GLOBALBUFEXCEED: Buffer usage has gone above global buffer Major 
threshold
configured 100 Current usage :101

System global threshold- Recovery (keywords Critical, Major and Minor alone will vary 
accordingly)
==========================================================================================
00:17:10: %SYS-5-GLOBALBUFRECOVER: Buffer usage has gone below global buffer Major 
threshold
configured <value> Current usage :<value>
```

For example:

```
00:17:10: %SYS-5-GLOBALBUFRECOVER: Buffer usage has gone below global buffer Critical 
threshold
configured 70 Current usage :69
```

Per User Global Threshold Violation in Buffer RO

The threshold violation in buffer RO for a user global threshold shows the following output:

```
User global threshold - Violation (keywords Critical, Major and Minor alone will vary 
accordingly)
==========================================================================================
00:24:04: %SYS-4-RESGLOBALBUFEXCEED: Buffer usage has gone above buffer Major threshold 
configured by resource user  <user-name>
 configured 100 Current usage :101

User global threshold - Recovery (keywords Critical, Major and Minor alone will vary 
accordingly)
==========================================================================================
00:25:08: %SYS-4-RESGLOBALBUFRECOVER: Buffer usage has gone below buffer Major threshold 
configured by resource user  <user-name>
configured 76 Current usage :75
```

User Local Threshold Violation in Buffer RO

The threshold violation in buffer RO for a user local threshold shows the following output:

```
User local threshold - Violation (keywords Critical, Major and Minor alone will vary 
accordingly)
=========================================================================================
00:31:15: %SYS-4-RESBUFEXCEED: Resource user  user_1 has exceeded the buffer Major 
threshold. configured 108 Current usage :109

User local threshold- Recovery (keywords Critical, Major and Minor alone will vary 
accordingly)
=========================================================================================
00:31:05: %SYS-5-RESBUFRECOVER: Resource user  user_1 has recovered after exceeding the 
buffer Major threshold. configured 90 Current usage :89
```

System Global Threshold Violation in CPU RO

The threshold violation in CPU RO for a system global threshold shows the following output:

```
System global threshold- Violation
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly )
==========================================================================================
00:19:36: %SYS-4-CPURESRISING: System is seeing global cpu util 19% at total level more 
than the configured major limit 11%
System global threshold - Recovery
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly )
```

```
==========================================================================================
00:20:56: %SYS-6-CPURESFALLING: System is no longer seeing global high cpu at total level
for the configured major limit 10%, current value 4%
```

Per User Global Threshold Violation in CPU RO

The threshold violation in CPU RO for a user global threshold shows the following output:

```
User global threshold - Violation
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly )
==========================================================================================
00:14:21: %SYS-4-CPURESRISING: Resource user <user-name> is seeing global cpu util 11% at
total level more than the configured major limit 6%
```

For example:

```
00:14:21: %SYS-4-CPURESRISING: Resource user Test-proc-14:99s:1w:100n is seeing global cpu
util 11% at total level more than the configured major limit 6%

User global threshold- Recovery
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly )
==========================================================================================
00:14:46: %SYS-6-CPURESFALLING: Resource user <user-name> is no longer seeing global high
cpu at total level for the configured critical limit 9%, current value 4%
```

For example:

```
00:14:46: %SYS-6-CPURESFALLING: Resource user Test-proc-14:99s:1w:100n is no longer seeing
global high cpu at total level for the configured critical limit 9%, current value 4%
```

User Local Threshold Violation in CPU RO

The threshold violation in CPU RO for a user local threshold shows the following output:

```
User local threshold - Violation (keywords Critical, Major and Minor will vary accordingly
- only process level)
==========================================================================================
00:12:11: %SYS-4-CPURESRISING: Resource user <user-name> is seeing local cpu util 15% at
process level more than the configured minor limit 6 %
```

For example:

```
00:12:11: %SYS-4-CPURESRISING: Resource user Test-proc-9:85s:15w:100n is seeing local cpu
util 15% at process level more than the configured minor limit 6%

User local threshold- Recovery (keywords Critical, Major and Minor will vary accordingly
- only process level)
==========================================================================================
00:13:11: %SYS-6-CPURESFALLING: Resource user <user-name> is no longer seeing local high
cpu at process level for the configured critical limit 9%, current value 3%
```

System Global Threshold Violation in Memory RO

The threshold violation in memory RO for a system global threshold shows the following output:

```
System global threshold - Violation (keywords Critical, Major and Minor alone will vary
accordingly)
(If violation happens in IO memory pool will be : I/O)
==========================================================================================


13:53:22: %SYS-5-GLOBALMEMEXCEED: Global Memory has exceeded the Minor threshold
Pool: Processor  Used: 422703520  Threshold: 373885200
```

For example:

```
13:54:03: %SYS-5-GLOBALMEMEXCEED: Global Memory has exceeded the Critical threshold
Pool: Processor  Used: 622701556  Threshold: 467356500

System global threshold - Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
(If recovery happens in IO memory pool will be : I/O)
==========================================================================================
%SYS-5-GLOBALMEMRECOVER: Global Memory has recovered  after exceeding Minor threshold
Pool: Processor  Used: 222473448  Threshold: 355190940
```

For example:

```
13:50:41: %SYS-5-GLOBALMEMRECOVER: Global Memory has recovered  after exceeding Critical
threshold
Pool: Processor  Used: 222473152  Threshold: 443988675
```

Per User Global Threshold Violation in Memory RO

The threshold violation in memory RO for a user global threshold shows the following output:

```
User global threshold - Violation (keywords Critical, Major and Minor alone will vary
accordingly)
(If violation happens in IO memory pool will be : I/O)
==========================================================================================
00:53:14: %SYS-4-RESGLOBALMEMEXCEED: Global Memory has exceeded the Minor threshold
configure by resource user <XYZ>
Pool: Processor  Used: 62273916  Threshold: 62246820

User global threshold - Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
(If recovery happens in IO memory pool will be : I/O)
==========================================================================================
00:32:56: %SYS-4-RESGLOBALMEMRECOVER: Global Memory has recovered after exceeding the
Critical threshold configure by resource user <XYZ>
Pool: Processor  Used: 329999508  Threshold: 375865440
```

User Local Threshold Violation in Memory RO

The threshold violation in memory RO for a user local threshold shows the following output:

```
User local threshold- Violation (keywords Critical, Major and Minor alone will vary
accordingly)
=========================================================================================
01:05:42: %SYS-4-RESMEMEXCEED: Resource user <XYZ> has exceeded the Critical memory
threshold
Pool: Processor Used: 103754740 Threshold: 103744700

User local threshold - Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
=========================================================================================
00:44:43: %SYS-5-RESMEMRECOVER: Resource user <XYZ> has recovered after exceeding the
Critical memory threshold
Pool: Processor Used: 328892280 Threshold :375865440
```

Examples

Configuring Major Rising Values for System Global Thresholding

The following example shows how to configure the major threshold values for system global thresholding with a major rising threshold of 70% at an interval of 12 seconds and a major falling threshold of 15% at an interval of 10 seconds:

```
Router(config-owner-cpu)# major rising 70 interval 12 falling 15 interval 10 global
Router(config-owner-buffer)# major rising 70 interval 12 falling 15 interval 10 global
Router(config-owner-memory)# major rising 70 interval 12 falling 15 interval 10 global
```

Configuring Major Rising Values for User Local Thresholding

The following example shows how to configure the major threshold values for user local thresholding with a major rising threshold of 70% at an interval of 12 seconds and a major falling threshold of 15% at an interval of 10 seconds:

```
Router(config-owner-cpu)# major rising 70 interval 12 falling 15 interval 10
Router(config-owner-buffer)# major rising 70 interval 12 falling 15 interval 10
Router(config-owner-memory)# major rising 70 interval 12 falling 15 interval 10
```

Configuring Major Rising Values for Per User Global Thresholding

The following example shows how to configure the major threshold values for per user global thresholding with a major rising threshold of 70% at an interval of 12 seconds and a major falling threshold of 15% at an interval of 10 seconds:

```
Router(config-owner-cpu)# major rising 70 interval 12 falling 15 interval 10 global
Router(config-owner-buffer)# major rising 70 interval 12 falling 15 interval 10 global
Router(config-owner-memory)# major rising 70 interval 12 falling 15 interval 10 global
```

Related Commands

Command	Description
buffer public	Enters the buffer owner configuration mode and sets threshold values for buffer usage.
cpu interrupt	Enters the CPU owner configuration mode and sets threshold values for interrupt level CPU utilization.
cpu process	Enters the CPU owner configuration mode and sets threshold values for processor level CPU utilization.
cpu total	Enters the CPU owner configuration mode and sets threshold values for total CPU utilization.
memory io	Enters the memory owner configuration mode and sets threshold values for I/O memory.
memory processor	Enters the memory owner configuration mode and sets threshold values for processor memory.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.
slot (ERM policy)	Configures line cards.
system (ERM policy)	Configures system level ROs.

memory io

To enter memory owner configuration mode to set threshold values for I/O memory, use the **memory io** command in resource policy node configuration mode. To exit memory owner configuration mode, use the **no** form of this command.

memory io

no memory io

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Resource policy node configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command allows you to enter memory owner configuration mode to set rising and falling values for critical, major, and minor thresholds for I/O memory.

Examples

The following example shows how to enter memory owner configuration mode to set threshold values for I/O memory:

```
Router(config-res-policy-node)# memory io
```

Related Commands

Command	Description
critical rising	Sets the critical level threshold values for the buffer, CPU, and memory ROs.
major rising	Sets the major level threshold values for the buffer, CPU, and memory ROs.
minor rising	Sets the minor level threshold values for the buffer, CPU, and memory ROs.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.
slot (ERM policy)	Configures line cards.
system (ERM policy)	Configures system level ROs.

memory processor

To enter memory owner configuration mode to set the threshold values for the processor memory, use the **memory processor** command in resource policy node configuration mode. To exit memory owner configuration mode, use the **no** form of this command.

memory processor

no memory processor

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Resource policy node configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command allows you to enter memory owner configuration mode to set rising and falling values for critical, major, and minor thresholds for the processor memory.

Examples

The following example shows how to enter memory owner configuration mode to set the threshold values for the processor memory:

```
Router(config-res-policy-node)# memory processor
```

Related Commands

Command	Description
critical rising	Sets the critical level threshold values for the buffer, CPU, and memory ROs.
major rising	Sets the major level threshold values for the buffer, CPU, and memory ROs.
minor rising	Sets the minor level threshold values for the buffer, CPU, and memory ROs.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.
slot (ERM policy)	Configures line cards.
system (ERM policy)	Configures system level ROs.

memory statistics history table

To change the number of hours for which the memory log is maintained, use the **memory statistics history table** command in global configuration mode. To return the logging to its default values, use the **no** form of this command.

memory statistics history table *number-of-hours*

no memory statistics history table *number-of-hours*

Syntax Description

number-of-hours	Number of hours of history for which the log is maintained. Valid values are from 12 to 72. The default value is 24.

Command Default

The memory log is maintained for 24 hours.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command allows you to change the number of hours for which the memory log is maintained. You cannot disable this command. The **no** form of the command only returns the logging to its default value.

Examples

The following example shows how to change the memory log time to 48 hours of history:

```
Router(config)# memory statistics history table 48
```

Related Commands

Command	Description
show memory statistics history table	Displays the history of memory consumption on the Cisco IOS router over a specified period of time.

minor rising

To set minor level threshold values for the buffer, CPU, and memory resource owners (ROs), use the **minor rising** command in buffer owner configuration mode, CPU owner configuration mode, or memory owner configuration mode. To disable this function, use the **no** form of this command.

minor rising *rising-threshold-value* [**interval** *interval-value*] [**falling** *falling-threshold-value* [**interval** *interval-value*]] [**global**]

no minor rising

Syntax Description

rising-threshold-value	The rising threshold value as a percentage. Valid values are from 1 to 100.
interval	(Optional) Specifies the time, in seconds, during which the variation in rising or falling threshold values are not reported to the request/response unit (RU), resource group, or resource user types. For example, if the buffer usage count has gone above the configured threshold value and if it remains longer than the configured interval, a notification is sent to the RU, resource group, or resource user types.
interval-value	(Optional) The time, in seconds, during which the variation in rising or falling threshold values are not reported to the RU, resource group, or resource user types. Valid values are from 0 to 86400. The default value is 0.
falling	(Optional) Specifies the falling threshold value as a percentage.
falling-threshold-value	(Optional) The falling threshold value as a percentage. Valid values are from 1 to 100.
global	(Optional) Configures a global threshold. The **global** keyword is optional when you set major threshold values for public buffer, processor CPU, I/O memory, and processor memory. The **global** keyword is required when you set major threshold values for interrupt CPU and total CPU.

Command Default

Disabled by default.

Command Modes

Buffer owner configuration
CPU owner configuration
Memory owner configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

The interval is the dampening or observation interval time in seconds during which the variations in the rising and falling threshold values are not notified to the ROs or RUs. That is, the interval is the time the system waits to check whether the threshold value stabilizes or not. The interval is set to avoid unnecessary and unwanted threshold notifications. If not configured, the system defaults to 0 seconds.

This command allows you to configure three types of thresholding:

- System Global Thresholding
- User Local Thresholding
- Per User Global Thresholding

System Global Thresholding

System global thresholding is used when the entire resource reaches a specified value. That is, RUs are notified when the total resource utilization goes above or below a specified threshold value. The notification order is determined by the priority of the RU. The RUs with a lower priority will be notified first, so that these low-priority RUs are expected to reduce the resource utilization. This order prevents the high-priority RUs from getting affected with unwanted notifications.

You can set rising and falling threshold values. For example, if you have set a total CPU utilization threshold value of 60% as the rising minor value and 5% as falling minor value, then when the total CPU utilization crosses the 60% mark, a minor Up notification is sent to all the RUs and when the total CPU utilization falls below 5%, a minor Down notification is sent to all the RUs. The same criteria apply to buffer ROs and memory ROs.

User Local Thresholding

User local thresholding is used when a specified RU exceeds the configured limits. The user local thresholding method prevents a single RU from monopolizing the resources. That is, the specified RU is notified when the resource utilization of the specified RU goes above or below a configured threshold value. For example, if you have set a CPU utilization threshold value of 60% as the rising minor value and 5% as the falling minor value, when the CPU utilization of the specified RU crosses the 60% mark, a minor Up notification is sent to only that RU and when the CPU utilization of the specified RU falls below 5%, a minor Down notification is sent to only that RU. The same method also applies to buffer and memory ROs.

Per User Global Thresholding

Per user global thresholding is used when the entire resource reaches a specified value. This value is unique for each RU and notification is sent only to the specified RU. User global thresholding is similar to user local thresholding, except that the global resource usage is compared against the thresholds. That is, only the specified RU is notified when the total resource utilization exceeds or falls below a configured threshold value. For example, if you have set a CPU utilization threshold value of 60% as the rising minor value and 5% as the falling minor value, when the total CPU utilization crosses the 60% mark, a minor Up notification is sent to only the specified RU and when the total CPU utilization falls below 5%, a minor Down notification is sent to only the specified RU. The same criteria also apply to buffer and memory ROs.

Threshold Violations

The Cisco IOS device sends out error messages when a threshold is violated. The following examples help you understand the error message pattern when different threshold violations occur in buffer, CPU, and memory ROs:

System Global Threshold Violation in Buffer RO

The threshold violation in buffer RO for a system global threshold shows the following output:

```
System global threshold-Violation (keywords Critical, Major and Minor alone will vary 
accordingly)
==========================================================================================
00:15:11: %SYS-4-GLOBALBUFEXCEED: Buffer usage has gone above global buffer Critical 
threshold
configured <value> Current usage :<value>
```

For example:

```
00:15:11: %SYS-4-GLOBALBUFEXCEED: Buffer usage has gone above global buffer Critical 
threshold
configured 144 Current usage :145

System global threshold- Recovery (keywords Critical, Major and Minor alone will vary 
accordingly)
==========================================================================================
00:17:10: %SYS-5-GLOBALBUFRECOVER: Buffer usage has gone below global buffer Critical 
threshold
configured <value> Current usage :<value>
```

For example:

```
00:17:10: %SYS-5-GLOBALBUFRECOVER: Buffer usage has gone below global buffer Critical 
threshold
configured 90 Current usage :89
```

Per User Global Threshold Violation in Buffer RO

The threshold violation in buffer RO for a user global threshold shows the following output:

```
User global threshold - Violation (keywords Critical, Major and Minor alone will vary 
accordingly)
==========================================================================================
00:24:04: %SYS-4-RESGLOBALBUFEXCEED: Buffer usage has gone above buffer Critical threshold
configured by resource user  <user-name>
configured 144 Current usage :145

User global threshold - Recovery (keywords Critical, Major and Minor alone will vary 
accordingly)
==========================================================================================
00:25:08: %SYS-4-RESGLOBALBUFRECOVER: Buffer usage has gone below buffer Critical 
threshold configured by resource user <user-name>
configured 126 Current usage :125
```

User Local Threshold Violation in Buffer RO

The threshold violation in buffer RO for a user local threshold shows the following output:

```
User local threshold - Violation (keywords Critical, Major and Minor alone will vary 
accordingly)
=========================================================================================
00:31:15: %SYS-4-RESBUFEXCEED: Resource user  user_1 has exceeded the buffer Critical 
threshold. configured 108 Current usage :109

User local threshold- Recovery (keywords Critical, Major and Minor alone will vary 
accordingly)
=========================================================================================
00:31:05: %SYS-5-RESBUFRECOVER: Resource user  user_1 has recovered after exceeding the 
buffer Critical threshold. configured 90 Current usage :89
```

System Global Threshold Violation in CPU RO

The threshold violation in CPU RO for a system global threshold shows the following output:

```
System global threshold- Violation
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly
===========================================================================================
00:19:36: %SYS-4-CPURESRISING: System is seeing global cpu util 19% at total level more
than the configured minor limit 11%

System global threshold - Recovery
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly
===========================================================================================
00:20:56: %SYS-6-CPURESFALLING: System is no longer seeing global high cpu at total level
for the configured minor limit 10%, current value 4%
```

Per User Global Threshold Violation in CPU RO

The threshold violation in CPU RO for a user global threshold shows the following output:

```
User global threshold - Violation
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly
===========================================================================================
00:14:21: %SYS-4-CPURESRISING: Resource user <user-name> is seeing global cpu util 11% at
total level more than the configured minor limit 6 %
```

For example:

```
00:14:21: %SYS-4-CPURESRISING: Resource user Test-proc-14:99s:1w:100n is seeing global cpu
util 11% at total level more than the configured minor limit 6%

User global threshold- Recovery
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly
===========================================================================================
00:14:46: %SYS-6-CPURESFALLING: Resource user <user-name> is no longer seeing global high
cpu at total level for the configured critical limit 9%, current value 4%
```

For example:

```
00:14:46: %SYS-6-CPURESFALLING: Resource user Test-proc-14:99s:1w:100n is no longer seeing
global high cpu at total level for the configured critical limit 9%, current value 4%
```

User Local Threshold Violation in CPU RO

The threshold violation in CPU RO for a user local threshold shows the following output:

```
User local threshold - Violation (keywords Critical, Major and Minor will vary accordingly
- only process level)
===========================================================================================
00:12:11: %SYS-4-CPURESRISING: Resource user <user-name> is seeing local cpu util 15% at
process level more than the configured minor limit 6%
```

For example:

```
00:12:11: %SYS-4-CPURESRISING: Resource user Test-proc-9:85s:15w:100n is seeing local cpu
util 15% at process level more than the configured minor limit 6%

User local threshold- Recovery (keywords Critical, Major and Minor will vary accordingly
- only process level)
===========================================================================================
00:13:11: %SYS-6-CPURESFALLING: Resource user <user-name> is no longer seeing local high
cpu at process level for the configured critical limit 9%, current value 3%
```

System Global Threshold Violation in Memory RO

The threshold violation in memory RO for a system global threshold shows the following output:

```
System global threshold - Violation (keywords Critical, Major and Minor alone will vary
accordingly)
(If violation happens in IO memory pool will be : I/O)
==========================================================================================
13:53:22: %SYS-5-GLOBALMEMEXCEED: Global Memory has exceeded the Minor threshold
Pool: Processor  Used: 422703520  Threshold: 373885200
```

For example:

```
13:54:03: %SYS-5-GLOBALMEMEXCEED: Global Memory has exceeded the Critical threshold
Pool: Processor  Used: 622701556  Threshold: 467356500

System global threshold - Recovery ( keywords Critical, Major and Minor alone will vary
accordingly )
(If recovery happens in IO memory pool will be : I/O)
==========================================================================================
%SYS-5-GLOBALMEMRECOVER: Global Memory has recovered after exceeding Minor threshold
Pool: Processor  Used: 222473448  Threshold: 355190940
```

For example:

```
13:50:41: %SYS-5-GLOBALMEMRECOVER: Global Memory has recovered after exceeding Critical
threshold
Pool: Processor  Used: 222473152  Threshold: 443988675
```

Per User Global Threshold Violation in Memory RO

The threshold violation in memory RO for a user global threshold shows the following output:

```
User global threshold - Violation (keywords Critical, Major and Minor alone will vary
accordingly)
(If violation happens in IO memory pool will be : I/O)
==========================================================================================
00:53:14: %SYS-4-RESGLOBALMEMEXCEED: Global Memory has exceeded the Minor threshold
configure by resource user <XYZ>
Pool: Processor  Used: 62273916  Threshold: 62246820

User global threshold - Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
(If recovery happens in IO memory pool will be : I/O)
==========================================================================================
00:32:56: %SYS-4-RESGLOBALMEMRECOVER: Global Memory has recovered after exceeding the
Critical threshold configure by resource user <XYZ>
Pool: Processor  Used: 329999508  Threshold: 375865440
```

User Local Threshold Violation in Memory RO

The threshold violation in memory RO for a user local threshold shows the following output:

```
User local threshold- Violation (keywords Critical, Major and Minor alone will vary
accordingly)
=========================================================================================
01:05:42: %SYS-4-RESMEMEXCEED: Resource user <XYZ> has exceeded the Critical memory
threshold
Pool: Processor Used: 103754740 Threshold: 103744700

User local threshold - Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
=========================================================================================
00:44:43: %SYS-5-RESMEMRECOVER: Resource user <XYZ> has recovered after exceeding the
Critical memory threshold
Pool: Processor Used: 328892280 Threshold :375865440
```

Examples

Configuring Minor Rising Values for System Global Thresholding

The following example shows how to configure the minor threshold values for the system global thresholding with a minor rising threshold of 60% at an interval of 12 seconds and a minor falling threshold of 5% at an interval of 10 seconds:

```
Router(config-owner-cpu)# minor rising 60 interval 12 falling 5 interval 10 global
Router(config-owner-buffer)# minor rising 60 interval 12 falling 5 interval 10 global
Router(config-owner-memory)# minor rising 60 interval 12 falling 5 interval 10 global
```

Configuring Minor Rising Values for User Local Thresholding

The following example shows how to configure the minor threshold values for user local thresholding with a minor rising threshold of 60% at an interval of 12 seconds and a minor falling threshold of 5% at an interval of 10 seconds:

```
Router(config-owner-cpu)# minor rising 60 interval 12 falling 5 interval 10
Router(config-owner-buffer)# minor rising 60 interval 12 falling 5 interval 10
Router(config-owner-memory)# minor rising 60 interval 12 falling 5 interval 10
```

Configuring Minor Rising Values for Per User Global Thresholding

The following example shows how to configure the minor threshold values for per user global thresholding with a minor rising threshold of 60% at an interval of 12 seconds and a minor falling threshold of 5% at an interval of 10 seconds:

```
Router(config-owner-cpu)# minor rising 60 interval 12 falling 5 interval 10 global
Router(config-owner-buffer)# minor rising 60 interval 12 falling 5 interval 10 global
Router(config-owner-memory)# minor rising 60 interval 12 falling 5 interval 10 global
```

Related Commands

Command	Description
buffer public	Enters the buffer owner configuration mode and sets threshold values for buffer usage.
cpu interrupt	Enters the CPU owner configuration mode and sets threshold values for interrupt level CPU utilization.
cpu process	Enters the CPU owner configuration mode and sets threshold values for processor level CPU utilization.
cpu total	Enters the CPU owner configuration mode and sets threshold values for total CPU utilization.
memory io	Enters the memory owner configuration mode and sets threshold values for I/O memory.
memory processor	Enters the memory owner configuration mode and sets threshold values for processor memory.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.
slot (ERM policy)	Configures line cards.
system (ERM policy)	Configures system level ROs.

monitor event-trace cpu-report (EXEC)

To monitor the event tracing of the CPU reports, use the **monitor event-trace cpu-report** command in user EXEC or privileged EXEC mode.

monitor event-trace cpu-report {**clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **one-shot**}

Syntax Description

clear	Clears the event tracing.
continuous	Displays continuously the latest event trace entries.
cancel	(Optional) Cancels the continuous display of the latest event trace entries.
disable	Disables event tracing.
dump	Dumps the event buffer into a file.
pretty	(Optional) Dumps the event buffer into a file in ASCII format.
enable	Enables the event tracing.
one-shot	Indicates that first clears the event trace, sets running, and then disables at wrap point.

Command Default

Disabled

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Examples

The following example shows how to enable event tracing of the CPU reports:

```
Router# monitor event-trace cpu-report enable
```

The following example shows how to enable continuous event tracing of the CPU reports:

```
Router# monitor event-trace cpu-report continuous
```

The following example shows how to dump the event tracing information into a file in ASCII format:

```
Router# monitor event-trace cpu-report dump pretty
```

The following example shows how to clear the event tracing information:

```
Router# monitor event-trace cpu-report clear
```

Related Commands

Command	Description
show monitor event-trace cpu-report	Displays the CPU report details for event tracing on a networking device.

monitor event-trace cpu-report (global)

To monitor the collection of CPU report traces, use the **monitor event-trace cpu-report** command in global configuration mode.

monitor event-trace cpu-report {**disable** | **dump-file** *location* | **enable** | **size** | **stacktrace**}

Syntax Description

disable	Disables event tracing.
dump-file	Dumps the event buffer into a file.
location	The URL at which the file is stored.
enable	Enables the event tracing.
size	Sets the size of event trace. Valid values are from 1 to 1000000.
stacktrace	Clears the trace buffer first and then traces the call stack at tracepoints. Valid values for the depth of stack traces stored are from 1 to 16.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Examples

The following example shows how to enable event tracing of the CPU reports:

```
Router(config)# monitor event-trace cpu-report enable
```

The following example shows how to dump the event tracing information into a file at http:\\www.cisco.com location:

```
Router# monitor event-trace cpu-report dump-file http:\\www.cisco.com
```

The following example shows how to disable the event tracing information:

```
Router# monitor event-trace cpu-report disable
```

The following example shows how to first clear the event tracing and then trace the call stacks at the tracepoints 4:

```
Router# monitor event-trace cpu-report stacktrace 4
```

Related Commands

Command	Description
show monitor event-trace cpu-report	Displays the CPU report details for event tracing on a networking device.

monitor platform command

To monitor the output of a **show** command by watching the output continually appear on the console, enter the **monitor platform command** command in priviliged EXEC or diagnostic mode.

monitor platform command show *show-command-option*

Syntax Description

show *show-command-option*	A **show** command option from an existing **show** command.

Command Modes

Diagnostic Mode (diag)

Privileged EXEC (#)

Command Default

No default behavior or values.

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.

Usage Guidelines

When the **monitor platform command** command is entered, a monitor function that continually displays the output of the specified **show** *show-command-option* will appear on the console. Enter **Ctrl-C** or **q** at any time while the monitor is running to return to the command-line interface prompt.

Once the monitor is running, the following options, which can be seen at any time by entering **h** or **?**, are available:

- **d**—toggle continuous diff mode. In continuous diff mode, the monitor will display the changes that have occurred inbetween display intervals.
- **D**—toggle fixed diff mode. In fixed diff mode, the monitor will display all changes made after entering fixed diff mode in each line of output.
- **h**—help. Displays the menu options available while the monitor is running.
- **q**—quit. Quits the monitor and returns to the command-line interface prompt.
- **r**—set a refresh time. Takes user to a prompt where the refresh time can be specified in seconds.
- **s**—set a sort column. Takes user to a prompt where the sorting of tabular output can be set.
- **?**—help. Displays the menu options available while the monitor is running.

To see the *show-command-options* that can be used with this command, enter **monitor platform command show ?** and continue to navigate the CLI using the **?** help function.

The output of a **show** command specified using the **show** *show-command-option* within this command-line is identical to the output that would be displayed if the **show** command was entered once without using the **monitor platform command** function. For information on the output of a particular **show** command, see the command reference for that specified **show** command.

Examples

In the following example, the **monitor platform command** command is used to repeatedly show the output of the **show rom-monitor r0** command. Note that Ctrl-Z is used to stop the output display and return to the command-line prompt.

```
Router# monitor platform command show rom-monitor r0

System Bootstrap, Version 12.2(20070807:170946) [asr1000_rommon_rel_1_22 101], DEVELOPMENT
SOFTWARE
Copyright (c) 1994-2006 by cisco Systems, Inc.

System Bootstrap, Version 12.2(20070807:170946) [asr1000_rommon_rel_1_22 101], DEVELOPMENT
SOFTWARE
Copyright (c) 1994-2006 by cisco Systems, Inc.

System Bootstrap, Version 12.2(20070807:170946) [asr1000_rommon_rel_1_22 101], DEVELOPMENT
SOFTWARE
Copyright (c) 1994-2006 by cisco Systems, Inc.

System Bootstrap, Version 12.2(20070807:170946) [asr1000_rommon_rel_1_22 101], DEVELOPMENT
SOFTWARE
Copyright (c) 1994-2006 by cisco Systems, Inc.

System Bootstrap, Version 12.2(20070807:170946) [asr1000_rommon_rel_1_22 101], DEVELOPMENT
SOFTWARE
Copyright (c) 1994-2006 by cisco Systems, Inc.

System Bootstrap, Version 12.2(20070807:170946) [asr1000_rommon_rel_1_22 101], DEVELOPMENT
SOFTWARE
Copyright (c) 1994-2006 by cisco Systems, Inc.

System Bootstrap, Version 12.2(20070807:170946) [asr1000_rommon_rel_1_22 101], DEVELOPMENT
SOFTWARE
Copyright (c) 1994-2006 by cisco Systems, Inc.

q

Router#
```

monitor platform software process

To monitor software processes on the Cisco ASR 1000 Series Routers, enter the **monitor platform software process** command in priviliged EXEC or diagnostic mode.

monitor platform software process [*slot*]

Syntax Description

slot	Specifies the slot of the *hardware-module*. Options include: • *number*—the number of the SIP slot. For instance, if you wanted to specify the SIP in SIP slot 2 of the router, enter 2 as the *number*. • **f0**—the ESP in ESP slot 0. • **f1**—the ESP in ESP slot 1 • **fp active**—the active ESP. • **fp standby**—the standby ESP. • **r0**—the RP in RP slot 0. • **r1**—the RP in RP slot 1. • **rp active**—the active RP. • **rp standby**—the standby RP.

Command Modes

Diagnostic Mode (diag)

Privileged EXEC (#)

Command Default

No default behavior or values.

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.

Usage Guidelines

When the **monitor platform software process** command is entered, a monitor function that shows memory-related data about the router by process will appear on the console. This monitor function will continue to update itself until **Ctrl-C** or **q** is entered to return to the command-line interface prompt.

Many options are available while the monitor is running. To view these options, enter **h** or **?** while the monitor is running.

If this command is entered without a *slot* specification, the output will reflect all processes on the active RP.

This command is particularly useful for monitoring cpu and memory usage by process.

Examples

In the following example, the **monitor platform software process** command is entered to monitor all processes on a Cisco ASR 1000 Series Router.

```
Router# monitor platform software process
top - 18:29:08 up 1 day,  1:36,  0 users,  load average: 0.00, 0.00, 0.00
Tasks: 138 total,   3 running, 135 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.7% us,  0.0% sy,  0.0% ni, 99.3% id,  0.0% wa,  0.0% hi,  0.0% si
Mem:   3941456k total,  1076004k used,  2865452k free,    59904k buffers
Swap:        0k total,        0k used,        0k free,   673648k cached

  PID USER     PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 9429 root     20   0 42224  21m  18m S  0.3  0.5   1:54.54 imand
10126 root     20   0 1886m 259m  79m R  0.3  6.7   4:02.15 ppc_linux_iosd-
27897 binos    20   0  2352 1212  932 R  0.3  0.0   0:00.02 top
    1 root     20   0  1928  576  500 S  0.0  0.0   0:11.48 init
    2 root     39  19     0    0    0 S  0.0  0.0   0:00.06 ksoftirqd/0
    3 root     15  -5     0    0    0 S  0.0  0.0   0:00.00 events/0
    4 root     15  -5     0    0    0 S  0.0  0.0   0:00.01 khelper
    5 root     15  -5     0    0    0 S  0.0  0.0   0:00.00 kthread
   26 root     15  -5     0    0    0 S  0.0  0.0   0:00.00 kblockd/0
   30 root     15  -5     0    0    0 S  0.0  0.0   0:00.23 khubd
   66 root     20   0     0    0    0 S  0.0  0.0   0:00.00 pdflush
   67 root     20   0     0    0    0 S  0.0  0.0   0:00.02 pdflush
   68 root     15  -5     0    0    0 S  0.0  0.0   0:00.01 kswapd0
   69 root     15  -5     0    0    0 S  0.0  0.0   0:00.00 aio/0
   70 root     15  -5     0    0    0 S  0.0  0.0   0:00.00 xfslogd/0
   71 root     15  -5     0    0    0 S  0.0  0.0   0:00.00 xfsdatad/0
  677 root     20   0     0    0    0 S  0.0  0.0   0:00.11 mtdblockd
  736 root     15  -5     0    0    0 S  0.0  0.0   0:00.00 scsi_eh_0
  737 root     15  -5     0    0    0 S  0.0  0.0   0:00.00 usb-storage
  740 root     15  -5     0    0    0 S  0.0  0.0   0:00.00 scsi_eh_1
  741 root     15  -5     0    0    0 S  0.0  0.0   0:00.05 usb-storage
  766 root     15  -5     0    0    0 S  0.0  0.0   0:00.00 scsi_eh_2
  767 root     15  -5     0    0    0 S  0.0  0.0   0:00.00 scsi_eh_3
  768 root     15  -5     0    0    0 S  0.0  0.0   0:00.00 scsi_eh_4
  769 root     15  -5     0    0    0 S  0.0  0.0   0:00.00 scsi_eh_5
  782 root     15  -5     0    0    0 S  0.0  0.0   0:00.00 mcp-rtc-wq
 1617 root      0 -20     0    0    0 S  0.0  0.0   0:00.00 loop0
 1708 bin      20   0  2028  628  524 S  0.0  0.0   0:00.00 portmap
 1710 bin      20   0  2028  604  512 S  0.0  0.0   0:00.00 portmap
 1764 root      0 -20     0    0    0 S  0.0  0.0   0:00.01 loop1
 1798 root      0 -20     0    0    0 S  0.0  0.0   0:00.12 loop2
 1832 root      0 -20     0    0    0 S  0.0  0.0   0:00.19 loop3
 1866 root      0 -20     0    0    0 S  0.0  0.0   0:00.01 loop4
 1956 root      0 -20     0    0    0 S  0.0  0.0   0:00.05 loop5
 1990 root      0 -20     0    0    0 S  0.0  0.0   0:00.04 loop6
 2031 root      0 -20     0    0    0 S  0.0  0.0   0:00.06 loop7
 2898 root     16  -4  1928  456  344 S  0.0  0.0   0:00.23 udevd
 3762 root     30  10     0    0    0 S  0.0  0.0   0:00.00 jffs2_gcd_mtd1
  4179 root      20   0  2924 1356 1148 S  0.0  0.0   0:00.00 auxinit.sh
q
Router#
```

monitor processes cpu extended

To configure a process or processes to be included in the extended load monitor report, use the **monitor processes cpu extended** command in user EXEC or privileged EXEC mode. To disable this function, use the **no** form of this command.

monitor processes cpu extended *process-id-list*

no monitor processes cpu extended *process-id-list*

Syntax Description

process-id-list	The list of process identifiers (PIDs). You can specify a maximum of eight processes. Valid values range from 1 to 2147483647.

Command Default

Disabled by default.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command marks a process or processes to be monitored for extended CPU load. You can specify a maximum of eight processes to be monitored using this command. This command is used to forcibly put a process in the latency report generated by the extended load monitor.

Examples

The following example shows how to enable extended CPU load monitor for the process with PID 2:

```
Router# monitor processes cpu extended 2
```

Related Commands

Command	Description
show processes cpu extended	Displays an extended CPU load report.

netconf beep initiator

To configure Blocks Extensible Exchange Protocol (BEEP) as the transport protocol for Network Configuration Protocol (NETCONF) and to configure a peer as the BEEP initiator, use the **netconf beep initiator** command in global configuration mode. To disable the BEEP initiator, use the **no** form of this command.

netconf beep initiator {*hostname* | *ip-address*} *port-number* **user** *sasl-user* **password** *sasl-password* [**encrypt** *trustpoint*] [**reconnect-time** *seconds*]

no netconf beep initiator {*hostname* | *ip-address*} *port-number*

Syntax Description

hostname	Hostname of the remote device.
ip-address	IP address of the remote device.
port-number	Specifies the BEEP port to use. The valid range is 1 to 65535.
user *sasl-user*	Specifies the Simple Authentication and Security Layer (SASL) user on the far end for this NETCONF session.
password *sasl-password*	Sets the password for the SASL user on the far end.
encrypt *trustpoint*	(Optional) Configures transport layer security (TLS) on this NETCONF session.
reconnect-time *seconds*	(Optional) Specifies the retry timeout for the NETCONF session. The range is 3 to 3600 seconds.

Command Default

BEEP is not enabled as the transport protocol for NETCONF sessions.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **netconf beep initiator** command to specify BEEP as the transport protocol for NETCONF sessions and to specify a peer as the BEEP initiator.

BEEP is a peer-to-peer client-server protocol. Each peer is labeled in the context of the role it plays at a given time. When a BEEP session is established, the peer that awaits new connections is the BEEP listener. The other peer, which establishes a connection to the listener, is the BEEP initiator. The BEEP peer that starts an exchange is the client; similarly, the other BEEP peer is the server. Typically, a BEEP peer that acts in the server role also performs in the listening role. However, because BEEP is a peer-to-peer protocol, the BEEP peer that acts in the server role is not required to also perform in the listening role.

Use the optional **encrypt** keyword to configure BEEP to use TLS to provide simple security for NETCONF sessions.

Examples

The following example shows how to enable NETCONF over BEEP and to configure a BEEP peer as the BEEP initiator:

```
Router(config)# netconf beep initiator host1 25 user user1 password password1 encrypt 23
reconnect-time 60
```

Related Commands

Command	Description
netconf beep listener	Configures BEEP as the transport protocol for NETCONF and configures a peer as the BEEP listener.

netconf beep listener

To configure Blocks Extensible Exchange Protocol (BEEP) as the transport protocol for Network Configuration Protocol (NETCONF) and to configure a peer as the BEEP listener, use the **netconf beep listener** command in global configuration mode. To disable the BEEP listener, use the **no** form of this command.

netconf beep listener [*port-number*] [**acl** *access-list-number*] [**sasl** *sasl-profile*]
[**encrypt** *trustpoint*]

no netconf beep listener

Syntax Description

port-number	(Optional) Specifies which BEEP port on which to listen.
acl *access-list-number*	(Optional) Specifies the access control list to be applied to restrict incoming client connections.
sasl *sasl-profile*	(Optional) Configures a Simple Authentication and Security Layer (SASL) profile to use during session establishment.
encrypt *trustpoint*	(Optional) Configures transport layer security (TLS) on a NETCONF session.

Command Default

BEEP is not enabled as the transport protocol for NETCONF sessions.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **netconf beep listener** command to specify BEEP as the transport protocol for NETCONF sessions and to specify a peer as the BEEP listener.

BEEP is a peer-to-peer client-server protocol. Each peer is labeled in the context of the role it plays at a given time. When a BEEP session is established, the peer that awaits new connections is the BEEP listener. The other peer, which establishes a connection to the listener, is the BEEP initiator. The BEEP peer that starts an exchange is the client; similarly, the other BEEP peer is the server. Typically, a BEEP peer that acts in the server role also performs in the listening role. However, because BEEP is a peer-to-peer protocol, the BEEP peer that acts in the server role is not required to also perform in the listening role.

You must configure a SASL profile before you can configure NETCONF over BEEP to use SASL during session establishment.

Examples

The following example shows how to configure NETCONF over BEEP and to specify a peer as the BEEP listener:

```
Router(config)# sasl profile beep
 mechanism digest-md5
 server user user1 password password1
 exit
Router(config)# netconf beep listener 23 acl 1 sasl beep encrypt 25
```

Related Commands

Command	Description
netconf beep initiator	Configures BEEP as the transport protocol for NETCONF and configures a peer as the BEEP initiator.

netconf lock-time

To specify the maximum time a network configuration protocol (NETCONF) configuration lock is in place without an intermediate operation, use the **netconf lock-time** command in global configuration mode. To set the NETCONF configuration lock time to the default value, use the **no** form of this command.

netconf lock-time *seconds*

no netconf lock-time

Syntax Description

seconds	Maximum NETCONF session time in seconds. The valid range is 1 to 300 seconds. The default is 10 seconds.

Command Default

The maximum lock time for a NETCONF session is 10 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

NETCONF enables you to set a configuration lock. Setting a configuration lock allows you to have exclusive rights to the configuration in order to apply configuration changes. Other users will not have access to the console during the lock time. If the user who has enabled the configuration lock is inactive, the lock timer expires and the session is ejected, preventing the configuration from being locked out if the user loses network connectivity while they have the configuration locked.

Examples

The following example shows how to limit a NETCONF configuration lock to 60 seconds:

```
netconf lock-time 60
```

Related Commands

Command	Description
clear netconf	Clears NETCONF statistics counters, NETCONF sessions, and frees associated resources and locks.
debug netconf	Enables debugging of NETCONF sessions.
netconf max-sessions	Specifies the maximum number of concurrent NETCONF sessions allowed.
netconf ssh	Enables NETCONF over SSHv2.
show netconf	Displays NETCONF statistics counters and session information.

netconf max-sessions

To specify the maximum number of concurrent network configuration protocol (NETCONF) sessions allowed, use the **netconf max-sessions** command in global configuration mode. To reset the number of concurrent NETCONF sessions allowed to the default value of four sessions, use the **no** form of this command.

netconf max-sessions *session*

no netconf max-sessions

Syntax Description

session	Specifies the total number of concurrent NETCONF sessions allowed. The default is 4. The range is 4 to 16.

Command Default

Four concurrent NETCONF sessions are allowed.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

You can have multiple NETCONF Network Managers concurrently connected. The **netconf max-sessions** command allows the maximum number of concurrent NETCONF sessions. The number of NETCONF sessions is also limited by the amount of available of vty line configured.

Note There must be at least as many vty lines configured as there are concurrent NETCONF sessions.

Extra NETCONF sessions beyond the maximum are not accepted.

Examples

The following example allows a maximum of five concurrent NETCONF sessions:

```
Router(config)# netconf max-sessions 5
```

Related Commands

Command	Description
clear netconf	Clears NETCONF statistics counters, NETCONF sessions, and frees associated resources and locks.
debug netconf	Enables debugging of NETCONF sessions.

Command	Description
netconf lock-time	Specifies the maximum time a NETCONF configuration lock is in place without an intermediate operation.
netconf ssh	Enables NETCONF over SSHv2.
show netconf	Displays NETCONF statistics counters and session information.

netconf ssh

To enable Network Configuration Protocol (NETCONF) over Secure Shell Version 2 (SSHv2), use the **netconf ssh** command in global configuration mode. To disable NETCONF over SSHv2, use the **no** form of this command.

netconf ssh [**acl** *access-list-number*]

no netconf ssh

Syntax Description

acl	(Optional) Specifies an access list to use during NETCONF sessions.
access-list-number	Number of the access list to use during NETCONF sessions.

Command Default

NETCONF over SSHv2 is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

NETCONF is supported only on SSHv2.

Examples

The following example shows how to enable NETCONF over SSHv2 and apply access list 1 to NETCONF sessions:

```
Router(config)# netconf ssh acl 1
```

Related Commands

Command	Description
clear netconf	Clears NETCONF statistics counters, NETCONF sessions, and frees associated resources and locks.
debug netconf	Enables debugging of NETCONF sessions.
netconf lock-time	Specifies the maximum time a NETCONF configuration lock is in place without an intermediate operation.
netconf max-sessions	Specifies the maximum number of concurrent NETCONF sessions allowed.
show netconf	Displays NETCONF statistics counters and session information.

no snmp-server

To disable Simple Network Management Protocol (SNMP) agent operation, use the **no snmp-server** command in global configuration mode.

no snmp-server

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command disables all running versions of SNMP (SNMPv1, SNMPv2C, and SNMPv3) on the device.

Examples

The following example disables the current running version of SNMP:

```
Router(config)# no snmp-server
```

ntp access-group

To control access to the Network Time Protocol (NTP) services on the system, use the **ntp access-group** command in global configuration mode. To remove access control to the NTP services, use the **no** form of this command.

ntp access-group {**query-only** | **serve-only** | **serve** | **peer**} *access-list-number*

no ntp [**access-group** {**query-only** | **serve-only** | **serve** | **peer**}

Syntax Description

query-only	Allows only NTP control queries. See RFC 1305 (NTP version 3).
serve-only	Allows only time requests. **Note** You must configure the **ntp server** *ip-address* command before you can use the **serve-only** keyword.
serve	Allows time requests and NTP control queries, but does not allow the system to synchronize to the remote system.
peer	Allows time requests and NTP control queries and allows the system to synchronize to the remote system.
access-list-number	Number (from 1 to 99) of a standard IP access list.

Defaults

No access control (full access granted to all systems)

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The access group options are scanned in the following order from least restrictive to most restrictive:

1. **peer**
2. **serve**
3. **serve-only**
4. **query-only**

Access is granted for the first match that is found. If no access groups are specified, all access is granted to all sources. If any access groups are specified, only the specified access is granted. This facility provides minimal security for the time services of the system. However, it can be circumvented by a determined programmer. If tighter security is desired, use the NTP authentication facility.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp access-group** command, the NTP service is activated (if it has not already been activated) and access control to NTP services is configured simultaneously.

In the no form of any **ntp** command, all the keywords are optional. When you enter the **no ntp access-control** command, only access control to NTP services is removed. The NTP service itself remains active, along with any other functions you previously configured.

To terminate NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp access-group** command and you now want to remove not only the access group, but all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

The following example shows how to configure a system to allow itself to be synchronized by a peer from access list 99. However, the system restricts access to allow only time requests from access list 42.

```
Router(config)# ntp access-group peer 99
Router(config)# ntp access-group serve-only 42
```

The following example shows how to remove all the configured NTP options and disable the ntp server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.

ntp authenticate

To enable Network Time Protocol (NTP) authentication, use the **ntp authenticate** command in global configuration mode. To disable the function, use the **no** form of this command.

ntp authenticate

no ntp [**authenticate**]

Syntax Description

This command has no arguments or keywords.

Defaults

No authentication

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command if you want authentication. If this command is specified, the system will not synchronize to a system unless it carries one of the authentication keys specified in the **ntp trusted-key** global configuration command.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp authenticate** command, the NTP service is activated (if it has not already been activated) and NTP authentication is enabled simultaneously.

In the no form of any **ntp** command, all the keywords are optional. When you enter the **no ntp authenticate** command, only the NTP authentication is removed from the NTP service. The NTP service itself remains active, along with any other functions you previously configured.

To terminate NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp authenticate** command and you now want to disable not only the authentication, but all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

The following example shows how to configure the system to synchronize only to systems that provide authentication key 42 in their NTP packets:

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key 42 md5 aNiceKey
Router(config)# ntp trusted-key 42
```

The following example shows how to remove all the configured NTP options and disable the ntp server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp trusted-key	Authenticates the identity of a system to which NTP will synchronize.

ntp authentication-key

To define an authentication key for Network Time Protocol (NTP), use the **ntp authentication-key** command in global configuration mode. To remove the authentication key for NTP, use the **no** form of this command.

ntp authentication-key *number* **md5** *value*

no ntp [**authentication-key**]

Syntax Description

number	Key number from 1 to 4294967295.
md5	Authentication key. Message authentication support is provided using the Message Digest 5 Algorithm (MD5). The key type **md5** is currently the only key type supported.
value	Character string of up to eight characters that is the value of the MD5 key.

Defaults

No authentication key is defined for NTP.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to define authentication keys for use with other NTP commands in order to provide a higher degree of security.

Note When this command is written to NVRAM, the key is encrypted so that it is not displayed when the configuration is viewed.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp authentication-key** command, the NTP service is activated (if it has not already been activated) and the NTP authentication key is defined simultaneously.

In the no form of any **ntp** command, all the keywords are optional. When you enter the **no ntp authentication-key** command, only the NTP authentication key is removed from the NTP service. The NTP service itself remains active, along with any other functions you previously configured.

To terminate NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp authentication-key** command and you now want to remove not only the authentication key, but all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

The following example shows how to configure the system to synchronize only to systems providing authentication key 42 in their NTP packets:

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key 42 md5 aNiceKey
Router(config)# ntp trusted-key 42
```

The following example shows how to remove all the configured NTP options and disable the ntp server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the software clock to be synchronized by a time server.
ntp trusted-key	Authenticates the identity of a system to which NTP will synchronize.

ntp broadcast

To configure the options for broadcasting Network Time Protocol (NTP) traffic, use the **ntp broadcast** command in interface configuration mode. To disable this capability, use the **no** form of this command.

ntp broadcast [**client**] [**destination** {*ip-address* | *hostname*}] [**key** *broadcast-key*] [**version** *number*]

no ntp [**broadcast**]

Syntax Description

client	(Optional) Configures a device to listen to NTP broadcast messages.
destination	(Optional) Configures a device to receive broadcast messages.
ip-address | *hostname*	(Optional) IP address or hostname of the device to send NTP broadcast messages to.
key	(Optional) Configures a broadcast authentication key.
broadcast key	(Optional) Integer from 0 to 4294967295 that is the key number.
version	(Optional) Indicates that an NTP version is configured.
number	(Optional) Integer from 1 to 3 indicating the NTP version.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The NTP service can be activated by entering any **ntp** command. When you use the **ntp broadcast** command, the NTP service is activated (if it has not already been activated) and the options are configured for sending NTP traffic simultaneously.

In the no form of any **ntp** command, all the keywords are optional. When you enter the **no ntp broadcast** command, only the configuration to send NTP broadcast packets on a specified interface is removed from the NTP service. The NTP service itself remains active, along with any other functions you previously configured.

To terminate NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp broadcast** command and you now want to remove not only the broadcast capability, but all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

The following example shows how to configures Ethernet interface 0 to send NTP version 2 broadcasts:

```
Router(config)# interface ethernet 0
Router(config-if)# ntp broadcast version 2
```

The following example shows how to remove all the configured NTP options and disable the ntp server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp broadcast client	Allows the system to receive NTP broadcast packets on an interface.
ntp broadcastdelay	Sets the estimated round-trip delay between the Cisco IOS software and an NTP broadcast server.

ntp broadcast client

To configure a device to receive Network Time Protocol (NTP) broadcast messages on a specified interface, use the **ntp broadcast client** command in interface configuration mode. To disable this capability, use the **no** form of this command.

ntp broadcast client

no ntp broadcast [**client**]

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to allow the system to listen to broadcast packets on an interface-by-interface basis.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp broadcast client** command, the NTP service is activated (if it has not already been activated) and the device is configured to receive NTP broadcast packets on a specified interface simultaneously.

In the no form of any **ntp** command, all the keywords are optional. When you enter the **no ntp broadcast client** command, only the broadcast client configuration is removed from the NTP service. The NTP service itself remains active, along with any other functions you previously configured.

To terminate NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp broadcast client** command and you now want to remove not only the broadcast client capability, but all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

In the following example, the system is configured to receive (listen to) NTP broadcasts on Ethernet interface 1:

```
Router(config)# interface ethernet 1
Router(config-if)# ntp broadcast client
```

The following example shows how to remove all the configured NTP options and disable the ntp server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp broadcast	Configures the specified interface to send NTP broadcast packets.
ntp broadcastdelay	Sets the estimated round-trip delay between the system and an NTP broadcast server.

ntp broadcastdelay

To set the estimated round-trip delay between the Cisco IOS software and a Network Time Protocol (NTP) broadcast server, use the **ntp broadcastdelay** command in global configuration mode. To revert to the default value, use the **no** form of this command.

ntp broadcastdelay *microseconds*

no ntp [**broadcastdelay**]

Syntax Description

microseconds	Estimated round-trip time (in microseconds) for NTP broadcasts. The range is from 1 to 999999.

Defaults

3000 microseconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command when the router is configured as a broadcast client and the round-trip delay on the network is other than 3000 microseconds.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp broadcastdelay** command, the NTP service is activated (if it has not already been activated) and the estimated round-trip delay between the Cisco IOS software and an NTP broadcast server is set simultaneously.

In the no form of any **ntp** command, all the keywords are optional. When you enter the **no ntp broadcastdelay** command, only the estimated round-trip delay between the Cisco IOS software and an NTP broadcast server is removed from the NTP service. The NTP service itself remains active, along with any other functions you previously configured.

To terminate NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp broadcastdelay** command and you now want to remove not only the delay setting, but all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

The following example shows how to set the estimated round-trip delay between a router and the broadcast client to 5000 microseconds:

```
Router(config)# ntp broadcastdelay 5000
```

The following example shows how to remove all the configured NTP options and disable the ntp server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp broadcast	Configures the specified interface to send NTP broadcast packets.
ntp broadcast client	Configures the specified interface to receive NTP broadcast packets.

ntp clock-period

Caution Do not enter this command; it is documented for informational purposes only. The system automatically generates this command as Network Time Protocol (NTP) determines the clock error and compensates.

As NTP compensates for the error in the software clock, it keeps track of the correction factor for this error. When the value for the clock period needs to be adjusted, the system automatically enters the correct value into the running configuration. To remove the automatically generated value for the clock period, use the **no** form of this command.

ntp clock-period *value*

no ntp [**clock-period** *value*]

Syntax Description

value	Amount of time to add to the software clock for each clock hardware tick (this value is multiplied by 2^{-32}).

Defaults

17179869 2^{-32} seconds (4 milliseconds)

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Do not manually set a value for the NTP clock-period.

If the system has automatically entered a value for the clock period into the running configuration, NTP synchronizes faster after the system is restarted when the **copy running-config startup-config** command has been entered to save the configuration to NVRAM.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp clock-period** command, the NTP service is activated (if it has not already been activated) and the system automatically saves the correct value into the running configuration simultaneously.

In the no form of any **ntp** command, all the keywords are optional. When you enter the **no ntp clock-period** command, only the automatically generated value is removed. The NTP service itself remains active, along with any other functions you previously configured.

To terminate NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you want to remove not only the clock period, but all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

The following example shows a typical difference between the values of the NTP clock-period setting in the running configuration and in the startup configuration:

```
Router# show startup-config | include clock-period

ntp clock-period 17180239

Router# show running-config | include clock-period

ntp clock-period 17180255
```

The following example shows how to remove the automatically generated value for the clock period from the running configuration:

```
Router(config)# no ntp clock-period
```

The following example shows how to remove all the configured NTP options and disable the ntp server:

```
Router(config)# no ntp
```

ntp disable

To prevent an interface from receiving Network Time Protocol (NTP) packets, use the **ntp disable** command in interface configuration mode. To enable receipt of NTP packets on an interface, use the **no** form of this command.

ntp disable

no ntp [**disable**]

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command provides a simple method of access control.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp disable** command, the NTP service is activated (if it has not already been activated) and the interface is configured to reject NTP packets simultaneously.

In the no form of any **ntp** command, all the keywords are optional. However, you must remove all NTP commands from the interface before you can enter the **ntp disabl**e command on that interface.

When you enter the **no ntp disable** command, the interface that was configured to reject NTP packets is enabled to receive NTP packets. The NTP service itself remains active, along with any other functions you previously configured.

To terminate NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp disable** command and you now want to remove not only this restriction, but all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

The following example shows how to prevent Ethernet interface 0 from receiving NTP packets:

```
Router(config)# interface ethernet 0
Router(config-if)# ntp disable
```

The following example shows the display after trying to execute **ntp disabl**e on an interface with other NTP commands configured on it:

```
Router(config-if)# ntp disable
%NTP: Unconfigure other NTP commands on this interface before executing ‘ntp disable’
Router(config-if)#
```

The following example shows how to remove all the configured NTP options and disable the ntp server:

```
Router(config)# no ntp
```

ntp logging

To enable Network Time Protocol (NTP) message logging, use the **ntp logging** command in global configuration mode. To disable NTP logging, use the **no** form of this command.

ntp logging

no ntp [**logging**]

Syntax Description

This command has no arguments or keywords.

Defaults

NTP message logging is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use the **ntp logging** command to control the display of NTP logging messages.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp logging** command, the NTP service is activated (if it has not already been activated) and message logging is enabled simultaneously.

In the no form of any **ntp** command, all the keywords are optional. When you enter the **no ntp logging** command, only the message logging is disabled in the NTP service. The NTP service itself remains active, along with any other functions you previously configured.

To terminate NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp logging** command and you now want to disable not only the message logging, but all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

The following example shows how to enable NTP message logging and verify that it is enabled:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# ntp logging
Router(config)# end
Router# show running-config | include ntp
ntp logging
ntp clock-period 17180152
ntp peer 10.0.0.1
ntp server 192.168.166.3
```

In the preceding example, the “ntp logging” entry in the configuration file verifies that NTP message logging is enabled.

The following example shows how to disable NTP message logging and verify that it is disabled:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# no ntp logging
Router# end
Router(config)# show running-config | include ntp

ntp clock-period 17180152
ntp peer 18.0.0.1
ntp server 128.107.166.3
```

The “ntp logging” entry no longer appears in the configuration file, which verifies that NTP message logging is disabled.

The following example shows how to remove all the configured NTP options and disable the ntp server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the software clock to be synchronized by an NTP time server.

ntp master

To configure the Cisco IOS software as a Network Time Protocol (NTP) master clock to which peers synchronize themselves when an external NTP source is not available, use the **ntp master** command in global configuration mode. To disable the master clock function, use the **no** form of this command.

ntp master [*stratum*]

no ntp [**master**]

Caution Use this command with caution. It is very easy to override valid time sources using this command, especially if a low stratum number is configured. Configuring multiple devices in the same network with the **ntp master** command can cause instability in keeping time if the devices do not agree on the time.

Syntax Description

stratum	(Optional) Number from 1 to 15. Indicates the NTP stratum number that the system will claim.

Defaults

By default, the master clock function is disabled. When enabled, the default stratum is 8.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Because the Cisco implementation of NTP does not support directly attached radio or atomic clocks, the router is normally synchronized, directly or indirectly, to an external system that has such a clock. In a network without Internet connectivity, such a time source may not be available. The **ntp master** command is used in such cases.

If the system has **ntp master** configured, and it cannot reach any clock with a lower stratum number, the system will claim to be synchronized at the configured stratum number, and other systems will be willing to synchronize to it via NTP.

Note The software clock must have been set from some source, including manually, before the **ntp master** command will have any effect. This protects against distributing erroneous time after the system is restarted.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp master** command, the NTP service is activated (if it has not already been activated) and the Cisco IOS software is configured as an NTP master clock simultaneously.

In the no form of any **ntp** command, all the keywords are optional. When you enter the **no ntp master** command, only the NTP master clock configuration is removed from the NTP service. The NTP service itself remains active, along with any other functions you previously configured.

To terminate NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp master** command and you now want to remove not only the master clock function, but all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

The following example shows how to configure a router as an NTP master clock to which peers may synchronize:

```
Router(config)# ntp master 10
```

The following example shows how to remove all the configured NTP options and disable the ntp server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
clock calendar-valid	Configures the system hardware clock an authoritative time source for the network.

ntp max-associations

To configure the maximum number of Network Time Protocol (NTP) peers and clients for a routing device, use the **ntp max-associations** command in global configuration mode. To return the maximum associations value to the default, use the **no** form of this command.

ntp max-associations *number*

no ntp [**max-associations**]

Syntax Description

number	Specifies the number of NTP associations. The range is 0 to 4294967295. The default is 100.

Defaults

100 maximum associations.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The router can be configured to define the maximum number of NTP peer and client associations that the router will serve. The **ntp max-associations** command is used to set this limit.

For a router, this command is useful for ensuring that the router is not overwhelmed by NTP synchronization requests. For an NTP master server, this command is useful for allowing numerous devices to synchronize to a router.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp max-associations** command, the NTP service is activated (if it has not already been activated) and the maximum number of NTP peers and clients is configured simultaneously.

In the no form of any **ntp** command, all the keywords are optional. When you enter the **no ntp max-associations** command, only the maximum number value is removed from the NTP service. The NTP service itself remains active, along with any other functions you previously configured.

To terminate NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp max-associations** command and you now want to remove not only that maximum value, but all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

In the following example, the router is configured to act as an NTP server to 200 clients:

```
Router(config)# ntp max-associations 200
```

The following example shows how to remove all the configured NTP options and disable the ntp server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
show ntp associations	Shows all current NTP associations for the device.

ntp multicast

To configure a system to send Network Time Protocol (NTP) multicast packets on a specified interface, use the **ntp multicast** interface configuration command. To disable this capability, use the **no** form of this command.

ntp multicast [*ip-address*] [**key** *key-id*] [**ttl** *value*] [**version** *number*]

no ntp [**multicast**]

Syntax Description

ip-address	(Optional) IP address of the multicast group. Default address is 224.0.1.1.
key	(Optional) Defines a multicast authentication key.
key-id	(Optional) Authentication key number in the range from 1 to 4294967295.
ttl	(Optional) Defines the time-to-live (TTL) value of a multicast NTP packet.
value	(Optional) TTL value in the range from 1 to 255. Default TTL value is 16.
version	(Optional) Defines the NTP version number.
number	(Optional) NTP version number in the range from 1 to 3. Default version number is 3.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The TTL value is used to limit the scope of an audience for multicast routing.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp multicast** command, the NTP service is activated (if it has not already been activated) and the interface on which to send multicast packets is configured simultaneously.

In the no form of any **ntp** command, all the keywords are optional. When you enter the **no ntp multicast** command, only the multicast capability is removed from the NTP service. The NTP service itself remains active, along with any other functions you previously configured.

To terminate NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp multicast** command and you now want to remove not only the multicast capability, but all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

The following example shows how to configure Ethernet interface 0 to send NTP version 2 broadcasts:

```
Router(config)# interface ethernet 0
Router(config-if)# ntp multicast version 2
```

The following example shows how to remove all the configured NTP options and disable the ntp server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp multicast client	Allows the system to receive NTP multicast packets on an interface.

ntp multicast client

To configure the system to receive Network Time Protocol (NTP) multicast packets on a specified interface, use the **ntp multicast client** interface configuration command. To disable this capability, use the **no** form of this command.

ntp multicast client [*ip-address*]

no ntp [**multicast client** [*ip-address*]]

Syntax Description

ip-address	(Optional) IP address of the multicast group. Default address is 224.0.1.1.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to allow the system to listen to multicast packets on an interface-by-interface basis.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp multicast client** command, the NTP service is activated (if it has not already been activated) and the interface on which to receive multicast packets is configured simultaneously.

In the no form of any **ntp** command, all the keywords are optional. When you enter the **no ntp multicast client** command, only the multicast client capability is removed from the NTP service. The NTP service itself remains active, along with any other functions you previously configured.

To terminate NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp multicast client** command and you now want to remove not only the multicast client capability, but all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

In the following example, the system is configured to receive (listen to) NTP multicast packets on Ethernet interface 1:

```
Router(config)# interface ethernet 1
Router(config-if)# ntp multicast client
```

The following example shows how to remove all the configured NTP options and disable the ntp server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp multicast	Configures the specified interface to send NTP multicast packets.

ntp peer

To configure the software clock to synchronize a peer or to be synchronized by a peer, use the **ntp peer** command in global configuration mode. To disable this capability, use the **no** form of this command.

ntp peer {{[**vrf** *vrf-name*] *ip-address* | *hostname*}[**normal-sync**][**version** *number*] [**key** *key-id*] [**source** *interface*] [**prefer**]}

no ntp {[**vrf** *vrf-name*] *ip-address* | *hostname*}

Syntax Description

vrf	(Optional) Specifies that the peer should use a named virtual private network (VPN) routing forwarding instance (VRF) for routing to the destination instead of to the global routing table.
vrf-name	(Optional) Name of the VRF.
ip-address | *hostname*	IP address or hostname of the peer providing or being provided the clock synchronization.
normal-sync	(Optional) Disables the rapid synchronization at startup.
version	(Optional) Defines the Network Time Protocol (NTP) version number.
number	(Optional) NTP version number (1 to 3).
key	(Optional) Defines the authentication key.
keyid	(Optional) Authentication key to use when sending packets to this peer.
source	(Optional) Names the interface.
interface	(Optional) Name of the interface from which to pick the IP source address.
prefer	(Optional) Makes this peer the preferred peer that provides synchronization.

Command Default

No peers are configured.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(14)T	The **normal-sync** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When a peer is configured, the default NTP version number is 3, no authentication key is used, and the source IP address is taken from the outgoing interface.

Use this command to allow a device to synchronize with a peer, or vice versa. Using the **prefer** keyword reduces switching between peers.

Tip If you are using the default version of 3 and NTP synchronization does not occur, try using NTP version 2 (NTPv2).

The NTP service can be activated by entering any **ntp** command. When you use the **ntp peer** command, the NTP service is activated (if it has not already been activated) and the peer is configured simultaneously.

In the no form of any **ntp** command, all the keywords are optional. When you enter the **no ntp peer** command, only the NTP peer configuration is removed from NTP service. The NTP service itself remains active, along with any other functions you previously configured.

To terminate NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp peer** command and you now want to remove not only the peer, but all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

The following example shows how to configure a router to allow its software clock to be synchronized with the clock of the peer (or vice versa) at IP address 192.168.22.33 using NTP version 2. The source IP address is the address of Ethernet 0.

```
Router(config)# ntp peer 192.168.22.33 version 2 source ethernet 0
```

The following example shows how to disable rapid synchronization at startup:

```
Router(config)# ntp peer 192.168.22.33 normal-sync
```

The following example shows how to keep a peer configured but re-enable rapid synchronization at startup after previously disabling it:

```
Router(config)# ntp peer 192.168.22.33
```

The following example shows how to remove all the configured NTP options and disable the ntp server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp server	Allows the software clock to be synchronized by a time server.
ntp source	Uses a particular source address in NTP packets.

ntp refclock

To configure an external clock source for use with Network Time Protocol (NTP) services, use the **ntp refclock** command in line configuration mode. To disable support of the external time source, use the **no** form of this command.

ntp refclock {**trimble** | **telecom-solutions**} **pps** {**cts** | **ri** | **none**} [**inverted**] [**pps-offset** *number*] [**stratum** *number*] [**timestamp-offset** *number*]

no ntp [**refclock**]

Syntax Description

trimble	Enables the reference clock driver for the Trimble Palisade NTP Synchronization Kit (Cisco 7200 series routers only).
telecom-solutions	Enables the reference clock driver for a Telecom Solutions GPS device.
pps	Pulse per second (PPS) signal line. Indicate PPS pulse reference clock support. Choices are **cts**, **ri**, or **none**.
cts	Pulse per second on CTS.
ri	Pulse per second on RI.
none	No PPS signal available.
inverted	(Optional) PPS signal is inverted.
pps-offset *number*	(Optional) Offset of PPS pulse. The number is the offset (in milliseconds).
stratum *number*	(Optional) Number from 0 to 14. Indicates the NTP stratum number that the system will claim.
timestamp-offset *number*	(Optional) Offset of time stamp. The number is the offset (in milliseconds).

Defaults

This command is disabled by default.

Command Modes

Line configuration (for auxilary 0 only)

Command History

Release	Modification
12.1	The **trimble** keyword was added to provide driver activation for a Trimble GPS time source on the Cisco 7200 series router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To configure a PPS signal as the source for NTP synchronization, use the following form of the **ntp refclock** command:

ntp refclock pps {**cts** | **ri**} [**inverted**] [**pps-offset** *number*] [**stratum** *number*] [**timestamp-offset** *number*]

To configure a Trimble Palisade NTP Synchronization Kit as the GPS clock source connected to the auxiliary port of a Cisco 7200 router, use the following form of the **ntp refclock** command:

ntp refclock trimble pps none [**stratum** *number*]

To configure a Telecom Solutions product as the GPS clock source, use the **ntp refclock telecom-solutions** form of the command:

ntp refclock telecom-solutions pps cts [**stratum** *number*]

The NTP service can be activated by entering any **ntp** command. When you use the **ntp refclock** command, the NTP service is activated (if it has not already been activated) and the external clock source is configured simultaneously.

In the no form of any **ntp** command, all the keywords are optional. When you enter the **no ntp refclock** command, only the external clock source is removed from the NTP service. The NTP service itself remains active, along with any other functions you previously configured.

To terminate NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp refclock** command and you now want to remove not only the external clock source, but all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

The following example shows configuration of a Trimble Palisade GPS time source on a Cisco 7200 router:

```
Router(config)# ntp master
Router(config)# ntp update-calendar
Router(config)# line aux 0
Router(config-line)# ntp refclock trimble pps none
```

The following example shows configuration of a Telecom Solutions GPS time source on a Catalyst switch platform:

```
Router(config)# ntp master
Router(config)# ntp update-calendar
Router(config)# line aux 0
Router(config-line)# ntp refclock telecom-solutions pps cts stratum 1
```

The following example shows how to remove all the configured NTP options and disable the ntp server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
show ntp associations	Displays the status of NTP associations configured for your system.

ntp server

To allow the software clock to be synchronized by a Network Time Protocol (NTP) time server, use the **ntp server** command in global configuration mode. To disable this capability, use the **no** form of this command.

ntp server {{[**vrf** *vrf-name*] *ip-address* | *hostname*} [**version** *number*] [**key** *key-id*] [**source** *interface*] [**prefer**]}

no ntp server {[**vrf** *vrf-name*] *ip-address* | *hostname*}

Syntax Description

vrf	(Optional) Specifies that the server should use a named virtual private network (VPN) routing forwarding instance (VRF) for routing to the destination instead of to the global routing table.
vrf-name	(Optional) Name of the VRF.
ip-address | *hostname*	IP address or hostname of the server providing or being provided the clock synchronization.
version	(Optional) Defines the NTP version number.
number	(Optional) NTP version number (1 to 3).
key	(Optional) Defines the authentication key.
key-id	(Optional) Authentication key to use when sending packets to this server.
source	(Optional) Identifies the interface from which to pick the IP source address.
interface	(Optional) Name of the interface from which to pick the IP source address.
prefer	(Optional) Specifies that the server referenced in this command is preferred over other configured NTP servers.

Defaults

No servers are configured by default. If a server is configured, the default NTP version number is 3, no authentication key is used, and the source IP address is taken from the outgoing interface.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command if you want to allow the system to synchronize with the specified server. The server will not synchronize to this machine.

When you use the *hostname* option, the router does a domain name server (DNS) lookup on that name, and stores the IP address in the configuration. For example, if you enter the command **ntp server** *host1* and then check the running configuration, the output shows “ntp server 172.16.0.4,” assuming that the router is correctly configured as a DNS client.

Use the **prefer** keyword if you use this command multiple times, and you want to set a preferred server. Using the **prefer** keyword reduces switching between servers.

If you are using the default version of 3 and NTP synchronization does not occur, try NTP version 2. Some NTP servers on the Internet run version 2.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp server** command, the NTP service is activated (if it has not already been activated) and software clock synchronization is configured simultaneously.

In the no form of any **ntp** command, all the keywords are optional. When you enter the **no ntp server** command, only the server synchronization capability is removed from the NTP service. The NTP service itself remains active, along with any other functions you previously configured.

To terminate NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp server** command and you now want to remove not only the server synchronization capability, but all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

The following example shows how to configure a router to allow its software clock to be synchronized with the clock by the device at IP address 172.16.22.44 using NTP version 2:

```
Router(config)# ntp server 172.16.22.44 version 2
```

The following example shows how to remove all the configured NTP options and disable the ntp server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp source	Uses a particular source address in NTP packets.

ntp source

To use a particular source address in Network Time Protocol (NTP) packets, use the **ntp source** command in global configuration mode. To remove the specified source address, use the **no** form of this command.

ntp source *type number*

no ntp [**source**]

Syntax Description

type	Type of interface.
number	Number of the interface.

Defaults

Source address is determined by the outgoing interface.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command when you want to use a particular source IP address for all NTP packets. The address is taken from the named interface. This command is useful if the address on an interface cannot be used as the destination for reply packets. If the **source** keyword is present on an **ntp server** or **ntp peer** global configuration command, that value overrides the global value set by this command.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp source** command, the NTP service is activated (if it has not already been activated) and the source address is configured simultaneously.

In the no form of any **ntp** command, all the keywords are optional. When you enter the **no ntp source** command, only the source address is removed from the NTP service. The NTP service itself remains active, along with any other functions you previously configured.

To terminate NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp source** command and you now want to remove not only the configured source address, but all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

The following example shows how to configure a router to use the IP address of Ethernet 0 as the source address of all outgoing NTP packets:

```
Router(config)# ntp source ethernet 0
```

The following example shows how to remove all the configured NTP options and disable the ntp server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the software clock to be synchronized by a time server.

ntp trusted-key

To authenticate the identity of a system to which Network Time Protocol (NTP) will synchronize, use the **ntp trusted-key** command in global configuration mode. To disable authentication of the identity of the system, use the **no** form of this command.

ntp trusted-key *key-number*

no ntp [**trusted-key** *key-number*]

Syntax Description

key-number	Key number of authentication key to be trusted.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If authentication is enabled, use this command to define one or more key numbers (corresponding to the keys defined with the **ntp authentication-key** command) that a peer NTP system must provide in its NTP packets, in order for this system to synchronize to it. This function provides protection against accidentally synchronizing the system to a system that is not trusted, because the other system must know the correct authentication key.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp trusted-key** command, the NTP service is activated (if it has not already been activated) and the system to which NTP will synchronize is authenticated simultaneously.

In the no form of any **ntp** command, all the keywords are optional. When you enter the **no ntp trusted-key** command, only the authentication is disabled in the NTP service. The NTP service itself remains active, along with any other functions you previously configured.

To terminate NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp trusted-key** command and you now want to remove not only the authentication, but all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

The following example shows how to configure the system to synchronize only to systems providing authentication key 42 in its NTP packets:

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key 42 md5 aNiceKey
Router(config)# ntp trusted-key 42
```

The following example shows how to remove all the configured NTP options and disable the ntp server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Defines an authentication key for NTP.

ntp update-calendar

To periodically update the hardware clock (calendar) from a Network Time Protocol (NTP) time source, use the **ntp update-calendar** command in global configuration mode. To disable the periodic updates, use the **no** form of this command.

ntp update-calendar

no ntp [**update-calendar**]

Syntax Description

This command has no arguments or keywords.

Defaults

The hardware clock (calendar) is not updated.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Some platforms have a battery-powered hardware clock, referred to in the command-line interface (CLI) as the “calendar,” in addition to the software based system clock. The hardware clock runs continuously, even if the router is powered off or rebooted.

If the software clock is synchronized to an outside time source via NTP, it is a good practice to periodically update the hardware clock with the time learned from NTP. Otherwise, the hardware clock will tend to gradually lose or gain time (drift), and the software clock and hardware clock may become out of synchronization with each other. The **ntp update-calendar** command will enable the hardware clock to be periodically updated with the time specified by the NTP source. The hardware clock will be updated only if NTP has synchronized to an authoritative time server.

Many lower-end routers (for example, the Cisco 2500 series or the Cisco 2600 series) do not have hardware clocks, so this command is not available on those platforms.

To force a single update of the hardware clock from the software clock, use the **clock update-calendar** EXEC command.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp update-calendar** command, the NTP service is activated (if it has not already been activated) and the hardware clock is updated simultaneously.

In the no form of any **ntp** command, all the keywords are optional. When you enter the **no ntp update-calendar** command, only the clock updates are stopped in the NTP service. The NTP service itself remains active, along with any other functions you previously configured.

To terminate NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp update-calendar** command and you now want to disable not only the periodic updates, but all NTP functions running on the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

The following example shows how to configure the system to periodically update the hardware clock from the NTP time source:

```
Router(config)# ntp update-calendar
```

The following example shows how to remove all the configured NTP options and disable the ntp server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
clock read-calendar	Performs a one-time update of the software clock from the hardware clock (calendar).
clock update-calendar	Performs a one-time update of the hardware clock (calendar) from the software clock.

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 (config-bulk-sc)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

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.

Examples

In the following example, the object list named E0InOctets is associated with the schema named E0:

```
Router(config)# snmp mib bulkstat schema E0
Router(config-bulk-sc)# object-list EOInOctets
Router(config-bulk-sc)# instance exact interface Ethernet 3/0
Router(config-bulk-sc)# exit
```

Related Commands

Command	Description
instance	Specifies the instance that, when appended to the object list, gives the OID of the object instance to be monitored in the bulk statistics schema.
snmp mib bulkstat schema	Names a bulk statistics schema and enters Bulk Statistics Schema configuration mode.

policy (ERM)

To configure an Embedded Resource Manager (ERM) resource policy, use the **policy** command in ERM configuration mode. To disable this function, use the **no** form of this command.

policy *policy-name* [**global** | **type** *resource-user-type*]

no policy *policy-name*

Syntax Description

policy-name	Name of the policy you want to configure.
global	(Optional) Configures a global policy.
type	(Optional) Specifies a type for the policy you are configuring.
resource-user-type	(Optional) Name of the resource user type.

Command Default

Disabled

Command Modes

ERM configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

You can configure a resource policy only in ERM configuration mode.

Examples

The following example shows how to configure a resource policy with the policy name cpu_mem_policy and the resource user type iosprocess:

```
Router(config-erm)# policy cpu_mem_policy type iosprocess
```

Related Commands

Command	Description
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.
show resource database	Displays the resource database details.
show resource owner	Displays the resource owner details.
show resource relationship	Displays the resource relationship details.
slot (ERM policy)	Configures line cards.
system (ERM policy)	Configures system level resource owners.

policy (resource group)

To apply an already configured policy to a specified resource group, use the **policy** command in resource group configuration mode. To disable this function, use the **no** form of this command.

policy *policy-name*

no policy *policy-name*

Syntax Description

policy-name	Name of the policy to apply to the resource group.

Command Default

Disabled

Command Modes

Resource group configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Before applying a policy to a resource group, you must configure a resource policy using the **policy** *policy-name* command in Embedded Resource Manager (ERM) configuration mode and create a resource group using the **user group** *resource-group-name* **type** *resource-user-type* command in ERM configuration mode.

When you apply a policy using the **policy** *policy-name* command in resource group configuration mode, you are applying a policy (which contains the thresholds) to the resource group you created using the **user group** *resource-group-name* **type** *resource-user-type* command in ERM configuration mode.

For example, you create a resource group with the name lowPrioUsers and type iosprocess and have low-priority resource users (RUs) or tasks such as HTTP and Simple Network Management Protocol (SNMP) that you want to set a threshold for as a group. You must add the RUs to lowPrioUsers using the **instance** *instance-name* command and then apply a resource policy. If the resource policy you apply sets a minor rising threshold value of 10 percent, a notification is sent to the RUs in lowPrioUsers when the accumulated usage of both HTTP and SNMP RUs crosses the 10 percent threshold (for example, if HTTP usage is 4 percent and SNMP usage is 7 percent).

Examples

The following example shows how to apply a resource policy named group-policy1 to a resource group named lowPrioUsers:

```
Router(config-erm)# user group lowPrioUsers type iosprocess
Router(config-res-group)# policy group-policy1
```

Related Commands

Command	Description
instance (resource group)	Adds the RUs to the resource group.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
user (ERM)	Creates a resource group.

policy-list

To associate a policy list with a Command Scheduler occurrence, use the **policy-list** command in kron-occurrence configuration mode. To delete a policy list from the Command Scheduler occurrence, use the **no** form of this command.

policy-list *list-name*

no policy-list *list-name*

Syntax Description

list-name	Name of the policy list.

Command Default

No policy list is associated.

Command Modes

Kron-occurrence configuration (kron-config-occurrence)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **policy-list** command with the **kron occurrence** command to schedule one or more policy lists to run at the same time or interval. Use the **kron policy-list** command in conjunction with the **cli** command to create a Command Scheduler policy list containing EXEC command line interface (CLI) commands to be scheduled to run on the router at a specified time.

When the *list-name* is new, a policy list structure is created. When the *list-name* is not new, the existing policy list is edited.

The Command Scheduler process is useful to automate the running of EXEC commands at recurring intervals, and can it be used in remote routers to minimize manual intervention.

Examples

The following example shows how to create a Command Scheduler occurrence named may and associate a policy list named sales-may with the occurrence:

```
Router(config)# kron occurrence may at 6:30 may 20 oneshot
Router(config-kron-occurrence)# policy-list sales-may
```

Related Commands

Command	Description
cli	Specifies EXEC CLI commands within a Command Scheduler policy list.

Command	Description
kron occurrence	Specifies schedule parameters for a Command Scheduler occurrence and enters kron-occurrence configuration mode.
kron policy-list	Specifies a name for a Command Scheduler policy and enters kron-policy configuration mode.

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 *minutes*

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 (config-bulk-sc)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

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.

Examples

In the following example, the polling interval for bulk statistics collection is set to once every 3 minutes in the schema called Ethernet2/1-CAR:

```
Router(config)# snmp mib bulkstat schema Ethernet2/1-CAR
Router(config-bulk-sc)# object-list CAR-mib
Router(config-bulk-sc)# poll-interval 3
Router(config-bulk-sc)# instance wildcard oid 3.1
Router(config-bulk-sc)# exit
```

Related Commands

Command	Description
snmp mib bulkstat schema	Names a bulk statistics schema and enters Bulk Statistics Schema configuration mode.

processes cpu autoprofile hog

To enable automatic profiling of CPUHOGs, use the **processes cpu autoprofile hog** command in global configuration mode. To disable this function, use the **no** form of this command.

processes cpu autoprofile hog

no processes cpu autoprofile hog

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command enables automatic profiling of CPUHOGs by monitoring the CPUHOG process and starting the profiling process at the same time.

Examples

The following example shows how to enable automatic profiling of CPUHOGs:

```
Router(config)# processes cpu autoprofile hog
```

Related Commands

Command	Description
show processes cpu autoprofile hog	Displays the profile data for CPUHOG.

processes cpu extended

To enable or disable the collection or to change the history size of an extended CPU load, use the **processes cpu extended** command in global configuration mode. To disable this function, use the **no** form of this command.

processes cpu extended [**history** *history-size*]

no processes cpu extended

Syntax Description

history	(Optional) Specifies the size of the history, in 5-second increments, to be collected for the extended CPU load.
history-size	(Optional) Size of the history. Valid values are from 2 to 720. The default is 12, which is equivalent to a 1-minute history.

Command Default

Enabled. If the command is not configured, the default behavior is to collect one minute of history.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Examples

The following example shows how to enable the collection of an extended CPU load for a history size of 36, which is equivalent to 3 minutes of history:

```
Router(config)# processes cpu extended history 36
```

Related Commands

Command	Description
show processes cpu extended	Displays an extended CPU load report.

resource policy

To enter Embedded Resource Manager (ERM) configuration mode to configure an ERM policy, use the **resource policy** command in global configuration mode. To exit ERM configuration mode, use the **no** form of this command.

resource policy

no resource policy

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Examples

The following example shows how to configure an ERM policy:

```
Router(config)# resource policy
Router(config-erm)# policy memory_policy type iosprocess
Router(config-erm-policy)# system
Router(config-policy-node)# memory processor
Router(config-owner-memory)# critical rising 80
Router(config-owner-memory)# major rising 40 falling 35
```

Related Commands

Command	Description
policy (ERM)	Configures an ERM resource policy.
show resource all	Displays all the resource details.
show resource all	Displays resource details for all RUs.
show resource database	Displays the resource database details.
show resource owner	Displays the resource owner details.
show resource relationship	Displays the resource relationship details.
slot (ERM policy)	Configures line cards.
system (ERM policy)	Configures system level resource owners.

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 (config-bulk-tr)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This 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 will be 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 will be attempted once every 5 minutes. Therefore, if the **retain** command is not configured (retain default is 0), no retries will be attempted.

Examples

In the following example, the bulk statistics transfer retention interval is set to 10 minutes:

```
Router(config)# snmp mib bulkstat transfer bulkstat1
Router(config-bulk-tr)# schema ATM2/0-IFMIB
Router(config-bulk-tr)# url primary ftp://user:pswrd@host/folder/bulkstat1
Router(config-bulk-tr)# retry 2
Router(config-bulk-tr)# retain 10
Router(config-bulk-tr)# exit
```

Related Commands

Command	Description
retry	Configures the number of retries that should be attempted for sending bulk statistics files.
snmp mib bulkstat transfer	Identifies the transfer configuration with a name and enters Bulk Statistics Transfer configuration mode.

retry (bulkstat)

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 (config-bulk-tr)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

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 will be attempted once every 5 minutes. Therefore, if the **retain** command is not configured (or the **retain 0** command is used) no retries will be attempted.

Examples

In the following example, the number of retries for the bulk statistics transfer is set to 2:

```
Router(config)# snmp mib bulkstat transfer bulkstat1
Router(config-bulk-tr)# schema ATM2/0-IFMIB
Router(config-bulk-tr)# url primary ftp://user:pswrd@host/folder/bulkstat1
Router(config-bulk-tr)# retry 2
Router(config-bulk-tr)# retain 10
Router(config-bulk-tr)# exit
```

Related Commands

Command	Description
retain	Configures the retention interval in local system memory (NVRAM) for bulk statistics files.
snmp mib bulkstat transfer	Identifies the transfer configuration with a name and enters Bulk Statistics Transfer configuration mode.

rmon

To enable Remote Monitoring (RMON) on an Ethernet interface, use the **rmon** command in interface configuration mode. To disable RMON on the interface, use the **no** form of this command.

rmon {**native** | **promiscuous**}

no rmon

Syntax Description

native	Enables RMON on the Ethernet interface. In native mode, the router processes only packets destined for this interface.
promiscuous	Enables RMON on the Ethernet interface. In promiscuous mode, the router examines every packet.

Command Default

RMON is disabled on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command enables RMON on Ethernet interfaces. A generic RMON console application is recommended in order to use the RMON network management capabilities. SNMP must also be configured. RMON provides visibility of individual nodal activity and allows you to monitor all nodes and their interaction on a LAN segment. When the **rmon** command is issued, the router automatically installs an Ethernet statistics study for the associated interface.

Note RMON can be very data and processor intensive. Users should measure usage effects to ensure that router performance is not degraded and to minimize excessive management traffic overhead. Native mode is less intensive than promiscuous mode.

All Cisco IOS software feature sets support RMON alarm and event groups. Additional RMON groups are supported in certain feature sets. Refer to the Release Notes for feature set descriptions. As a security precaution, support for the packet capture group allows capture of packet header information only; data payloads are not captured.

The RMON MIB is described in RFC 1757.

Examples

The following example enables RMON on Ethernet interface 0 and allows the router to examine only packets destined for the interface:

```
interface ethernet 0
 rmon native
```

Related Commands

Command	Description
rmon alarm	Sets an alarm on any MIB object.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
rmon queuesize	Changes the size of the queue that holds packets for analysis by the RMON process.
show rmon	Displays the current RMON agent status on the router.

rmon alarm

To set an alarm on any MIB object, use the **rmon alarm** command in global configuration mode. To disable the alarm, use the **no** form of this command.

rmon alarm *number variable interval* {**delta** | **absolute**} **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *string*]

no rmon alarm *number*

Syntax Description

number	Alarm number, which is identical to the *alarmIndex* of the alarmTable in the Remote Monitoring (RMON) MIB.
variable	MIB object to monitor, which translates into the *alarmVariable* used in the alarmTable of the RMON MIB.
interval	Time, in seconds, the alarm monitors the MIB variable, which is identical to the *alarmInterval* used in the alarmTable of the RMON MIB.
delta	Tests the change between MIB variables, which affects the *alarmSampleType* in the alarmTable of the RMON MIB.
absolute	Tests each MIB variable directly, which affects the *alarmSampleType* in the alarmTable of the RMON MIB.
rising-threshold	Sets the value at which the alarm is triggered.
value	When used with the **rising-threshold** keyword, the value at which the alarm is triggered. When used with the **falling-threshold** keyword, the value at which the alarm is reset.
event-number	(Optional) Event number to trigger when the rising or falling threshold exceeds its limit. This value is identical to the alarmRisingEventIndex or the alarmFallingEventIndex in the alarmTable of the RMON MIB.
falling-threshold	Sets the value at which the alarm is reset.
owner	(Optional) Specifies an owner for the alarm, which is identical to the *alarmOwner* in the alarmTable of the RMON MIB.
string	(Optional) Name of the owner for the alarm.

Command Default

No alarms are configured.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must specify the MIB object as a dotted decimal value after the entry sequence (for example, ifEntry.10.1). You cannot specify the variable name and the instance (for example, ifInOctets.1) or the entire dotted decimal notation. The argument must be of the form *entry.integer.instance*.

To disable the RMON alarms, you must use the **no** form of the command on each configured alarm. For example, enter **no rmon alarm 1**, where the 1 identifies which alarm is to be removed.

See RFC 1757 for more information about the RMON alarm group.

Examples

The following example shows how to configure an RMON alarm using the **rmon alarm** command:

```
rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1 falling-threshold 0
owner owner1
```

RMON alarm number 10 is configured in this example. The alarm monitors the MIB variable *ifEntry.20.1* once every 20 seconds until the alarm is disabled, and checks the change in the rise or fall of the variable. If the *ifEntry.20.1* value shows a MIB counter increase of 15 or more, such as from 100000 to 100015, the alarm is triggered. The alarm in turn triggers event number 1, which is configured with the **rmon event** command. Possible events include a log entry or a Simple Network Management Protocol (SNMP) trap. If the *ifEntry.20.1* value changes by 0 (falling threshold is 0), the alarm is reset and can be triggered again.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
show rmon	Displays the current RMON agent status on the router.

rmon capture-userdata

To disable the packet zeroing feature that initializes the user payload portion of each Remote Monitoring (RMON) MIB packet, use the **rmon capture-userdata** command in global configuration mode. To enable packet zeroing, use the **no** form of this command.

rmon capture-userdata

no rmon capture-userdata

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following command shows how to disable the packet zeroing feature:

```
Router(config)# rmon capture-userdata
```

Related Commands

Command	Description
rmon collection matrix	Enables a RMON MIB matrix group of statistics on an interface.
show rmon matrix	Displays RMON statistics.

rmon collection history

To enable Remote Monitoring (RMON) history gathering on an interface, use the **rmon collection history** command in interface configuration mode. To disable the history gathering on an interface, use the **no** form of this command.

rmon collection history controlEntry *integer* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]

no rmon collection history controlEntry *integer* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]

Syntax Description

controlEntry	Specifies the RMON group of statistics using a value.
integer	Value in the range from 1 to 65535 that identifies the RMON group of statistics and matches the index value returned for Simple Network Management Protocol (SNMP) requests.
owner	(Optional) Specifies the name of the owner of the RMON group of statistics.
ownername	(Optional) Name of the owner of the RMON group of statistics.
buckets	(Optional) Specifies that a maximum number of buckets desired is set for the RMON collection history group of statistics.
bucket-number	(Optional) Maximum number of buckets.
interval	(Optional) Specifies the number of seconds for which history should be gathered in a single bucket. When the interval ends, history is collected into a new bucket.
seconds	(Optional) Number of seconds in the interval.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to enables an RMON MIB collection history group of statistics with an ID number of 20 and an owner as john:

```
Router(config-if)# rmon collection history controlEntry 20 owner john
```

Related Commands

Command	Description
show rmon capture	Displays the contents of the RMON history table.
show rmon matrix	Displays the RMON MIB matrix table.

rmon collection host

To enable a Remote Monitoring (RMON) MIB host collection group of statistics on the interface, use the **rmon collection host** command in interface configuration mode. To remove the specified RMON host collection, use the **no** form of this command.

rmon collection host controlEntry *integer* [**owner** *ownername*]

no rmon collection host controlEntry *integer* [**owner** *ownername*]

Syntax Description

controlEntry	Specifies an identification number for the RMON group of statistics.
integer	Integer in the range from 1 to 65535.
owner	(Optional) Indicates that a name is specified for the owner of the RMON group of statistics.
ownername	(Optional) String value identifying the owner.

Command Default

No RMON host collection is specified.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following command shows how to enable an RMON collection host group of statistics with an ID number of 20 and specifies john as the owner:

```
Router(config-if)# rmon collection host controlEntry 20 owner john
```

Related Commands

Command	Description
show rmon hosts	Displays the RMON MIB hosts table.
show rmon matrix	Displays the RMON MIB matrix table.

rmon collection matrix

To enable a Remote Monitoring (RMON) MIB matrix group of statistics on an interface, use the **rmon collection matrix** command in interface configuration mode. To remove a specified RMON matrix group of statistics, use the **no** form of this command.

rmon collection matrix controlEntry *integer* [**owner** *ownername*]

no rmon collection matrix controlEntry *integer* [**owner** *ownername*]

Syntax Description

controlEntry	Specifies an identification number for the RMON matrix group of statistics.
integer	Integer in the range from 1 to 65535.
owner	(Optional) Indicates that a name is specified for the owner of the RMON matrix group of statistics.
ownername	(Optional) String that specifies the name of the owner.

Command Default

No RMON matrix group of statistics is specified.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show rmon matrix** command to display RMON statistics.

Examples

The following command shows how to enable the RMON collection matrix group of statistics with an ID number of 25 and specifies john as the owner:

```
Router(config-if)# rmon collection matrix controlEntry 25 owner john
```

Related Commands

Command	Description
show rmon matrix	Displays the RMON MIB matrix table.

rmon collection rmon1

To enable all possible autoconfigurable Remote Monitoring (RMON) MIB statistic collections on the interface, use the **rmon collection rmon1** command in interface configuration mode. To disable these statistic collections on the interface, use the **no** form of this command.

rmon collection rmon1 controlEntry *integer* [**owner** *ownername*]

no rmon collection rmon1 controlEntry *integer* [**owner** *ownername*]

Syntax Description

controlEntry	Specifies an identification number for the RMON group of statistics.
integer	Integer in the range from 1 to 65535.
owner	(Optional) Indicates that a name is specified for the owner of the RMON group of statistics.
ownername	(Optional) String that identifies the name of the owner.

Command Default

Disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following command shows how to enable the RMON collection rmon1 group of statistics with an ID number of 30 and specifies “john” as the owner:

```
Router(config-if)# rmon collection rmon1 controlEntry 30 owner john
```

Related Commands

Command	Description
show rmon matrix	Displays the RMON MIB matrix table.

rmon event

To add or remove an event (in the Remote Monitoring (RMON) event table) that is associated with an RMON event number, use the **rmon event** command in global configuration mode. To disable RMON on the interface, use the **no** form of this command.

rmon event *number* [**log**] [**trap** *community*] [**description** *string*] [**owner** *string*]

no rmon event *number*

Syntax Description

number	Assigned event number, which is identical to the eventIndex in the eventTable in the RMON MIB.
log	(Optional) Generates an RMON log entry when the event is triggered and sets the *eventType* in the RMON MIB to *log* or *log-and-trap*.
trap	(Optional) Specifies a Simple Network Management Protocol (SNMP) community string used for this trap. Configures the setting of the *eventType* in the RMON MIB for this row as either *snmp-trap* or *log-and-trap*. This value is identical to the *eventCommunityValue* in the eventTable of the RMON MIB.
community	(Optional) SNMP community string used for a trap.
description	(Optional) Specifies a description of the event, which is identical to the event description in the eventTable of the RMON MIB.
string	(Optional) Description of the event.
owner	(Optional) Specifies an owner for this event, which is identical to the *eventOwner* in the eventTable of the RMON MIB.
string	(Optional) Name of the event owner.

Command Default

No events are configured.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2(17d)SXB release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **trap** *community* keyword and argument to configure the setting of the *eventType* in the RMON MIB for this row as either *snmp-trap* or *log-and-trap*. This value is identical to the *eventCommunityValue* in the eventTable in the RMON MIB.

See RFC 1757 for more information about the RMON MIB.

Examples

The following example shows how to enable the **rmon event** command:

```
rmon event 1 log trap eventtrap description "High ifOutErrors" owner owner2
```

This example configuration creates RMON event number 1, which is defined as High ifOutErrors, and generates a log entry when the event is triggered by an alarm. The user owner2 owns the row that is created in the event table by this command. This configuration also generates an SNMP trap when the event is triggered.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon alarm	Sets an alarm on any MIB object.
show rmon	Displays the current RMON agent status on the router.

rmon queuesize

To change the size of the queue that holds packets for analysis by the Remote Monitoring (RMON) process, use the **rmon queuesize** command in global configuration mode. To restore the default value, use the **no** form of this command.

rmon queuesize *size*

no rmon queuesize

Syntax Description

size	Number of packets allowed in the queue awaiting RMON analysis. Default queue size is 64 packets.

Defaults

64 packets

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies to the RMON function, which is available on Ethernet interfaces of Cisco 2500 series and Cisco AS5200 series routers only.

You might want to increase the queue size if the RMON function indicates it is dropping packets. You can determine this from the output of the **show rmon** command or from the etherStatsDropEvents object in the etherStats table. A feasible maximum queue size depends on the amount of memory available in the router and the configuration of the buffer pool.

Examples

The following example configures the RMON queue size to be 128 packets:

```
Router(config)# rmon queuesize 128
```

Related Commands

Command	Description
show rmon	Displays the current RMON agent status on the router.

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 (config-bulk-tr)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Repeat this 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).

Examples

In the following example, the bulk statistics schemas ATM2/0-IFMIB and ATM2/0-CAR are associated with the bulk statistics transfer configuration called bulkstat1:

```
Router(config)# snmp mib bulkstat transfer bulkstat1
Router(config-bulk-tr)# schema ATM2/0-IFMIB
Router(config-bulk-tr)# schema ATM2/0-CAR
Router(config-bulk-tr)# url primary ftp://user:pswrd@host/folder/bulkstat1
Router(config-bulk-tr)# retry 2
Router(config-bulk-tr)# retain 10
Router(config-bulk-tr)# exit
```

Related Commands

Command	Description
snmp mib bulkstat transfer	Names a bulk statistics transfer configuration and enters Bulk Statistics Transfer configuration mode.

scripting tcl encdir

To specify the default location of external encoding files used by the Tool Command Language (Tcl) shell, use the **scripting tcl encdir** command in global configuration mode. To remove the default location, use the **no** form of this command.

scripting tcl encdir *location-url*

no scripting tcl encdir

Syntax Description

location-url	The URL used to access external encoding files used by Tcl.

Defaults

Tcl does not use external encoding files.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Character strings in Tcl are encoded using 16-bit Unicode characters. Different operating system interfaces or applications can generate character strings using other encoding methods. Use the **scripting tcl encdir** command to configure a location URL for the external Tcl character encoding files to support the Tcl **encoding** command.

Tcl contains only a few character sets within the Tcl shell. Additional characters sets are loaded, as needed, from external files.

Examples

The following example shows how to specify a default location for external encoding files to be used by Tcl:

```
Router# configure terminal
Router(config)# scripting tcl encdir tftp://10.18.117.23/file2/
```

Related Commands

Command	Description
scripting tcl init	Specifies an initialization script for the Tcl shell.
tclsh	Enables the Tcl shell and enters Tcl configuration mode.

scripting tcl init

To specify an initialization script for the Tool Command Language (Tcl) shell, use the **scripting tcl init** command in global configuration mode. To remove the initialization script, use the **no** form of this command.

scripting tcl init *init-url*

no scripting tcl init

Syntax Description

init-url	The URL used to access the initialization script to be used by Tcl.

Defaults

Tcl does not run an initialization script.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **scripting tcl init** command when you want to predefine Tcl procedures to run in an initialization script. The initialization script runs when the Tcl shell is entered and saves manual sourcing of the individual scripts.

Examples

The following example shows how to specify an initialization script to run when the Tcl shell is enabled:

```
Router# configure terminal
Router(config)# scripting tcl init ftp://user:password@172.17.40.3/tclscript/initfile3.tcl
```

Related Commands

Command	Description
scripting tcl encdir	Specifies the default location of external encoding files used by the Tcl shell.
tclsh	Enables the Tcl shell and enters Tcl configuration mode.

scripting tcl secure-mode

To enable signature verification of the interactive Tool Command Language (Tcl) scripts, use the **scripting tcl secure-mode** command in global configuration mode. To disable signature verification of the interactive Tcl scripts, use the **no** form of this command.

scripting tcl secure-mode

no scripting tcl secure-mode

Syntax Description

This command has no arguments or keywords.

Command Default

The signature verification of the interactive Tcl scripts is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the **scripting tcl secure-mode** command to enable signature verification of all Tcl scripts run on the router. By default, the signature verification of the interactive Tcl scripts is disabled. You must enable the signature verification in order to verify whether the Tcl scripts match their digital signature. That would indicate they have not been altered since the digital signature was generated. If the script does not contain the digital signature, the script may run in a limited mode for untrusted script (that is, a script that has failed signature verification) or may not run at all. After receiving the results from the signature verification, the scripts are executed.

A Cisco IOS Crypto image software is required to enable this command and configure the Signed Tcl Scripts feature. The Crypto configuration commands enable the Cisco x.509 certificate storage. The **scripting tcl secure-mode** command can be enabled after the Crypto configuration trustpoint commands are enabled.

The **scripting tcl trustpoint name** command must be configured with the **scripting tcl secure-mode** command to verify the integrity of Tcl script signatures run on the router. Both commands must be configured to fully operate the feature; otherwise, a syslog message is generated:

```
*Jun 13 17:35:14.219: %SYS-6-SCRIPTING_TCL_INVALID_OR_MISSING_SIGNATURE: tcl signing
validation failed on script signed with trustpoint name mytrust, cannot run the signed TCL
script.
```

In addition, the **crypto pki trustpoint** *name* command provided should contain a certificate that matches the certificate that was originally used to generate the digital signature on the Tcl script.

Examples

The following example shows how to enable signature verification of the interactive Tcl scripts:

```
Router(config)# crypto pki trustpoint mytrust
Router(ca-trustpoint)# enrolment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate mytrust
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIEuDCCA6CgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBnjELMAkGA1UEBhMCVVMx
EzARBgNVBAgTCkNhbGlmb3JuaWExETAPBgNVBAcTCFNhbiBKb3NlMRwwGgYDVQQK
ExNDaXNjbyBTeXN0ZW1zLCBJbmMuMQ4wDAYDVQQLEwVOU1NURzEWMBQGA1UEAxMN
Sm9obiBMYXV0bWFubjEhMB8GCSqGSIb3DQEJARYSamxhdXRtYW5AY2lzY28uY29t
MB4XDTA2MTExNzE3NTgwMVoXDTA5MTExNjE3NTgwMVowgZ4xCzAJBgNVBAYTAlVT
MRMwEQYDVQQIEwpDYWxpZm9ybmlhMREwDwYDVQQHEwhTYW4gSm9zZTEcMBoGA1UE
ChMTQ2lzY28gU3lzdGVtcywgSW5jLjEOMAwGA1UECxMFTlNTVEcxFjAUBgNVBAMT
DUpvaG4gTGF1dG1hbm4xITAfBgkqhkiG9w0BCQEWEmpsYXV0bWFuQGNpc2NvLmNv
bTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALxtqTMCirMb+CdyWLuH
oWAM8CEJDwQggL7MWBhoi3TSMd/ww2XBB9biBtdlH6jHsjCiOwAR5OorakwfPyf7
mvRJ2PqJALs+Vn93VBKIG6rZUl4+wdOx686BVddIZvEJQPbROiYTzfazWV70aLMV
bd7/B7vF1SG1YK9y1tX9p9nZyZ0x47OAXetwOaGinvlG7VNuTXaASBLUjCRZsIlz
SBrXXedBzZ6+BuoWm1FK45EYSlag5Rt9RGXXMBqzx91iyhrJ3zDDmkExa45yKJET
mAgDVMcpeteJtif47UDZJK30g4MbMyx/c8WGhmJ54qRL9BZEPmDxMQkNP10l8MAl
Q8sCAwEAAaOB/jCB+zAdBgNVHQ4EFgQU9/ToDvbMR3JfJ4xEa4X47oNFq5kwgcsG
A1UdIwSBwzCBwIAU9/ToDvbMR3JfJ4xEa4X47oNFq5mhgaSkgaEwgZ4xCzAJBgNV
BAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMREwDwYDVQQHEwhTYW4gSm9zZTEc
MBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5jLjEOMAwGA1UECxMFTlNTVEcxFjAU
BgNVBAMTDUpvaG4gTGF1dG1hbm4xITAfBgkqhkiG9w0BCQEWEmpsYXV0bWFuQGNp
c2NvLmNvbYIBADAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBBAUAA4IBAQBtEs/4
MQeN9pT+XPCPg2ObQU8y2AadI+I34YK+fDHsFOh68hZhpszTN2VpNEvkFXpADhgr
7DkNGtwTCla481v70iNFViQVL+inNrZwWMxoTnUNCK7Hc5kHkXt6cj0mvsefVUzx
Xl70mauhESRVlmYWrJxSsrEILerZYsuv5HbFdand+/rErmP2HVyfdntLnKdSzmXJ
5lwE/Et2QtYNGor0OBlLesowfslR3LhHi4wn+5is7mALgNw/NuTiUr1zH18OeB4m
wcpBIJsLaJu6ZUJQl7IqdswSa3fHd5qq0/k8P9z0YAYrf3+MFQr4ibvsYvHlO087
o2Js1gW4qz34pqNh

Certificate has the following attributes:
       Fingerprint MD5: 1E327DBB 330936EB 2FB8EACB 4FD1133E
      Fingerprint SHA1: EE7FF9F4 05148842 B9D50FAC D76FDC9C E0703246
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)# scripting tcl secure-mode
Router(config)# scripting tcl trustpoint name mytrust
```

Related Commands

Command	Description
scripting tcl trustpoint name	Associates an existing configured trustpoint name with a certificate to verify Tcl scripts.

scripting tcl trustpoint name

To associate an existing configured trustpoint name with a certificate to verify Tool Command Language (Tcl) scripts, use the **scripting tcl trustpoint name** command in global configuration mode. To remove an existing configured trustpoint name, use the **no** form of this command.

scripting tcl trustpoint name *name*

no scripting tcl trustpoint name *name*

Syntax Description

name	Name of the configured trustpoint name associated with a certificate. Only one name can be associated with one certificate.

Command Default

A trustpoint name is not associated with a certificate to verify the Tcl scripts.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the **scripting tcl trustpoint name** command to associate an existing configured trustpoint name with a certificate to verify Tcl scripts. This way, Tcl identifies which certificate is used for verifying the Tcl scripts. The name must match an existing configured trustpoint name, otherwise, the command is rejected with an error message on the console. You can enter the command multiple times and configure multiple trustpoint names. Once you enter the command, you cannot modify the trustpoint name. However, you can remove the trustpoint name using the **no** form of the command. You must individually remove each name. When the last name is removed, no signature checking is performed, and the untrusted script (that is, a script that has failed signature verification) action configured by the **scripting tcl trustpoint untrusted** command is also removed.

A Cisco IOS Crypto image software is required to enable this command and configure the Signed Tcl Scripts feature. The Crypto configuration commands enable the Cisco x.509 certificate storage. The **scripting tcl trustpoint name** command can be enabled after the Crypto configuration trustpoint commands are enabled.

The **scripting tcl secure-mode** command must be configured with the **scripting tcl trustpoint name** command to verify the integrity of Tcl script signatures run on the router. Both commands must be configured to fully operate this feature; otherwise, a syslog message is generated:

```
*Jun 13 17:53:31.659: %SYS-6-SCRIPTING_TCL_SECURE_TRUSTPOINT: scripting tcl secure-mode is
enabled, however no scripting tcl trustpoint names configured, cannot verify signed TCL
script.
```

In addition, the **crypto pki trustpoint** *name* command provided should contain a certificate that matches the certificate that was originally used to generate the digital signature on the Tcl script.

Examples

The following example shows how the **scripting tcl trustpoint name** command is used to associate existing trustpoint names. Different names can be used for different departments with certificates:

```
Router(config)# crypto pki trustpoint mytrust
Router(ca-trustpoint)# enrolment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate mytrust
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIEuDCCA6CgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBnjELMAkGA1UEBhMCVVMx
EzARBgNVBAgTCkNhbGlmb3JuaWExETAPBgNVBAcTCFNhbiBKb3NlMRwwGgYDVQQK
ExNDaXNjbyBTeXN0ZW1zLCBJbmMuMQ4wDAYDVQQLEwVOU1NURzEWMBQGA1UEAxMN
Sm9obiBMYXV0bWFubjEhMB8GCSqGSIb3DQEJARYSamxhdXRtYW5AY2lzY28uY29t
MB4XDTA2MTExNzE3NTgwMVoXDTA5MTExNjE3NTgwMVowgZ4xCzAJBgNVBAYTAlVT
MRMwEQYDVQQIEwpDYWxpZm9ybmlhMREwDwYDVQQHEwhTYW4gSm9zZTEcMBoGA1UE
ChMTQ2lzY28gU3lzdGVtcywgSW5jLjEOMAwGA1UECxMFTlNTVEcxFjAUBgNVBAMT
DUpvaG4gTGF1dG1hbm4xITAfBgkqhkiG9w0BCQEWEmpsYXV0bWFuQGNpc2NvLmNv
bTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALxtqTMCirMb+CdyWLuH
oWAM8CEJDwQggL7MWBhoi3TSMd/ww2XBB9biBtdlH6jHsjCiOwAR5OorakwfPyf7
mvRJ2PqJALs+Vn93VBKIG6rZUl4+wdOx686BVddIZvEJQPbROiYTzfazWV70aLMV
bd7/B7vF1SG1YK9y1tX9p9nZyZ0x47OAXetwOaGinvlG7VNuTXaASBLUjCRZsIlz
SBrXXedBzZ6+BuoWm1FK45EYSlag5Rt9RGXXMBqzx91iyhrJ3zDDmkExa45yKJET
mAgDVMcpeteJtif47UDZJK30g4MbMyx/c8WGhmJ54qRL9BZEPmDxMQkNP10l8MAl
Q8sCAwEAAaOB/jCB+zAdBgNVHQ4EFgQU9/ToDvbMR3JfJ4xEa4X47oNFq5kwgcsG
A1UdIwSBwzCBwIAU9/ToDvbMR3JfJ4xEa4X47oNFq5mhgaSkgaEwgZ4xCzAJBgNV
BAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMREwDwYDVQQHEwhTYW4gSm9zZTEc
MBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5jLjEOMAwGA1UECxMFTlNTVEcxFjAU
BgNVBAMTDUpvaG4gTGF1dG1hbm4xITAfBgkqhkiG9w0BCQEWEmpsYXV0bWFuQGNp
c2NvLmNvbYIBADAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBBAUAA4IBAQBtEs/4
MQeN9pT+XPCPg2ObQU8y2AadI+I34YK+fDHsFOh68hZhpszTN2VpNEvkFXpADhgr
7DkNGtwTCla481v70iNFViQVL+inNrZwWMxoTnUNCK7Hc5kHkXt6cj0mvsefVUzx
Xl70mauhESRVlmYWrJxSsrEILerZYsuv5HbFdand+/rErmP2HVyfdntLnKdSzmXJ
5lwE/Et2QtYNGor0OBlLesowfslR3LhHi4wn+5is7mALgNw/NuTiUr1zH18OeB4m
wcpBIJsLaJu6ZUJQl7IqdswSa3fHd5qq0/k8P9z0YAYrf3+MFQr4ibvsYvHlO087
o2Js1gW4qz34pqNh

Certificate has the following attributes:
       Fingerprint MD5: 1E327DBB 330936EB 2FB8EACB 4FD1133E
      Fingerprint SHA1: EE7FF9F4 05148842 B9D50FAC D76FDC9C E0703246
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)# scripting tcl secure-mode
Router(config)# scripting tcl trustpoint name mytrust
Router(config)# scripting tcl trustpoint name dept_accounting
Router(config)# scripting tcl trustpoint name dept_hr
```

Related Commands

Command	Description
scripting tcl secure-mode	Enables signature verification of the interactive Tcl scripts.

scripting tcl trustpoint untrusted

To allow the interactive Tool Command Language (Tcl) scripts to run regardless of the scripts failing the signature check, use the **scripting tcl trustpoint untrusted** command in global configuration mode. To disallow the interactive Tcl scripts to run regardless of the scripts failing the signature check, use the **no** form of this command.

scripting tcl trustpoint untrusted {**execute** | **safe-execut**e | **terminate**}

no scripting tcl trustpoint untrusted

Syntax Description

execute	Executes Tcl scripts even if the signature verification fails. If the **execute** keyword is configured, signature verification is not at all performed. **Caution** Use of this keyword is usually not recommended because the signature verification is not at all performed.
safe-execute	Executed the Tcl script in safe mode if the signature verification fails.
terminate	Does not run the Tcl script if the signature verification fails. The default keyword is **terminate**.

Command Default

No script that fails signature verification can run; the script immediately stops.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the **scripting tcl trustpoint untrusted** command to allow the interactive Tcl scripts to run regardless of the scripts failing the signature check or in untrusted mode. The untrusted script (that is, a script that has failed signature verification) is not safe to use.

Caution Use of the **execute** keyword is usually not recommended because the signature verification is not at all performed.

The **execute** keyword is provided for internal testing purposes and to provide flexibility. For example in a situation where a certificate has expired but the other configurations are valid and you want to work with the existing configuration, then you can use the **execute** keyword to work around the expired certificate.

The **safe-execute** keyword allows the script to run in safe mode. You can use the **tclsafe** command and also enter the interactive Tcl shell safe mode to explore the safe mode Tcl commands that are available. In order to get a better understanding of what is available in this limited safe mode, use the **tclsafe** Exec command to explore the options.

The **terminate** keyword stops any script from running and reverts to default behavior. The default policy is to terminate. When the last trustpoint name is removed, the untrusted action is also removed. The untrusted action cannot be entered until at least one trustpoint name is configured for Tcl.

Note This command only applies to the Tcl shell; it does not impact other components that make use of Tcl. For example, Embedded Event Manager (EEM) cannot perform any signature checking.

Examples

The following example shows how to execute the Tcl script in safe mode if the signature verification fails:

```
Router(config)# scripting tcl trustpoint untrusted safe-execute
```

Related Commands

Command	Description
scripting tcl trustpoint name	Associates an existing configured trustpoint name with a certificate to verify Tcl scripts.
tclsafe	Enables the interactive Tcl shell untrusted safe mode.

server (boomerang)

To configure the server address for a specified boomerang domain, use the **server** command in boomerang configuration mode. To remove this 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.

server *server-ip-address*

no server *server-ip-address*

Syntax Description

server-ip-address	IP address of the specified server.

Command Default

No default behavior or values.

Command Modes

Boomerang configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **server** command can be used only on a Director Response Protocol (DRP) agent. The boomerang client is the Director Response Protocol (DRP) agent.

Use the **server** command to specify a server address that is to be associated with a given domain name. This configuration overrides the server-to-DRP agent association that is configured on DistributedDirector.

Examples

The following example configures the server for a domain named www.boom1.com. The server address for www.boom1.com is 172.16.101.101:

```
Router(config)# ip drp domain www.boom1.com
Router(config-boomerang)# server 172.16.101.101

Router# show running-config
.
.
.
ip drp domain www.boom1.com
content-server 172.16.101.101
```

Related Commands

Command	Description
alias (boomerang)	Configures an alias name for a specified domain.
ip drp domain	Adds a new domain to the DistributedDirector client or configures an existing domain and puts the client in boomerang configuration mode.

Command	Description
show ip drp	Displays DRP statistics on DistributedDirector or a DRP server agent.
show ip drp boomerang	Displays boomerang information on the DRP agent.
ttl dns	Configures the number of seconds for which an answer received from the boomerang client will be cached by the DNS client.
ttl ip	Configures the IP TTL value for the boomerang response packets sent from the boomerang client to the DNS client in number of hops.

set (EEM)

To set the value of a local Embedded Event Manager (EEM) applet variable, use the **set** command in applet configuration mode. To remove the value of an EEM applet variable, use the **no** form of this command.

set *label* **_exit_status** *exit-value*

no set *label* **_exit_status** *exit-value*

Syntax Description

label	Unique identifier that can be any string value. Actions are sorted and run in ascending alphanumeric key sequence using the label as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
_exit_status	Specifies the EEM applet variable name. Currently only the **_exit_status** variable is supported. • *exit-value*—Integer value that represents the exit status for the applet. Zero represents an exit status of success, and a nonzero value represents an exit status of failure.

Command Default

No EEM applet variable values are set.

Command Modes

Applet configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

In EEM applet configuration mode, three types of configuration statements are supported. The **event** commands are used to specify the event criteria to trigger the applet to run, the **action** commands are used to specify an action to perform when the EEM applet is triggered, and the **set** command is used to set the value of an EEM applet variable. Currently only the **_exit_status** variable is supported for the **set** command.

Examples

The following example shows how to set the **_exit_status** variable to represent a successful status after an event has occurred three times and an action has been performed:

```
Router(config)# event manager applet cli-match
Router(config-applet)# event cli pattern {.*interface loopback*} sync yes occurs 3
Router(config-applet)# action 1.0 cli command "no shutdown"
Router(config-applet)# set 1.0 _exit_status 0
```

Related Commands

Command	Description
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

set platform software trace

To set the trace level for a specific module within a process, use the **set platform software trace** command privileged EXEC or diagnostic mode command.

set platform software trace *process hardware-module slot module trace-level*

Syntax Description

process	Specifies the process whose tracing level is being set. Options currently include: • **chassis-manager**—The Chassis Manager process. • **cpp-control-process**—The CPP Control process • **cpp-driver**—The CPP driver process • **cpp-ha-server**—The CPP HA server process • **cpp-service-process**—The CPP service process • **forwarding-manager**—The Forwarding Manager process. • **host-manager**—The Host Manager process. • **interface-manager**—The Interface Manager process. • **ios**—The IOS process. • **logger**—The logging manager process • **pluggable-services**—The pluggable services process. • **shell-manager**—The Shell Manager process.
hardware-module	Specifies the hardware module where the process in which the trace level is being set is running. Options include: • **carrier-card**—The process is on a SPA Interface Processor (SIP). • **forwarding-processor**—The process is on an Embedded Services Processor (ESP). • **route-processor**—The process is on an RP.

slot	Specifies the slot of the *hardware-module*. Options include: • *number*—The number of the SIP slot of the hardware module where the trace level is being set. For instance, if you want to specify the SIP in SIP slot 2 of the router, enter 2 as the *number*. • *SIP-slot*/*SPA-bay*—The number of the SIP router slot and the number of the SPA bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in router slot 3, enter 3/2. • **cpp active**—The Cisco Packet Processor (CPP) in the active ESP. • **cpp standby**—The CPP in the standby ESP. • **f0**—The ESP in ESP slot 0. • **f1**—The ESP in ESP slot 1 • **fp active**—The active ESP. • **fp standby**—The standby ESP. • **r0**—The RP in RP slot 0. • **r1**—The RP in RP slot 1. • **rp active**—The active RP. • **rp standby**—The standby RP.

module	Specifies the module within the process where the tracing level is being set. Options include: • **acl**—access control list module. • **all-modules**—all modules within the process • **aom**—Asynchronous Object Manager module. • **apdb**—Access Policies database module. • **bipc**—BIPC process module, which is responsible for inter-process communication. • **btrace**—Btrace tracing module. • **cce**—CCE client process module, which is responsible for common classification. • **cef**—Cisco Express Forwarding module. • **chasfs**—Chassis Filesystem module. • **cman_fp**—Chassis Manager module on the ESP. • **cmand**—Chassis Manager module. • **cmcc**—Chassis Manager module on the SIP. • **cpp_cp**—CPP Client Control process • **cpp-debug**—CPP debugging process module. • **cpp_dr**—CPP Driver process • **cpp_ha**— CPP HA process • **cpp_sp**—CPP Services process • **ec**—Etherchannel module. • **erspan**—Encapsulated Remote Switch Port Analyzer module. • **ess**—Edge Switch Services module. • **evlib**—Event module. • **evutil**—Event Utility module. • **flash**—Flash module. • **fman**—Forwarding Manager module. • **fpm**—Flexible Packet Match module. • **frag**—Fragmentation module. • **fw**—Firewall module. • **hman**—Host Manager module. • **icmp**—ICMP module. • **imand**—Interface Manager module. • **imccd**—Interface Manager module on the SIP. • **interfaces**—interface module. • **IOSCC**—IOS module on the SIP. • **IOSRP**—IOS module on the RP.

- **iosd**—IOS module.
- **ipc**—Inter-Process Communication module.
- **iphc**—IP Header Compression module.
- **ipsec**—IPSEC module.
- **mlp**—Multilink PPP module.
- **mqipc**—Message queue module.
- **nat**—Network Address Translation module.
- **netflow**—Netflow module.
- **om**—Object Manager module.
- **pam_updb**—User database module.
- **peer**—Peer information modules.
- **psdui**—Export module.
- **punt**—Punt information module.
- **qos**—Quality of Service modules.
- **route-map**—Route map modules.
- **services**—Services.
- **stile**—STILE modules.
- **tdllib**—Type management modules.
- **tppiosrp**—The utility library module.
- **ttymon**—The console monitoring module.
- **uihandler**—CLI command handler modules.
- **uiparse**—User interface parsing modules.
- **uipeer**—User interface peer modules.
- **uistatus**—User interface status modules.
- **urpf**—Unicast Reverse Path Forwarding modules.
- **usernames**—User module.

trace-level	Specifies the trace level. Options include: • **emergency**—Emergency level tracing. An emergency-level trace message is a message indicating the system is unusable. • **error**—Error level tracing. An error-level tracing message is a message indicating a system error. • **warning**—Warning level tracing. A warning-level tracing message is a message indicating a warning about the system. • **info**—Information level tracing. An information-level tracing message is a non-urgent message providing information about the system. • **debug**—Debug level tracing. A debug-level trace message is a non-urgent message providing a large amount of detail about the module. • **verbose**—Verbose level tracing. All possible tracing messages are sent when the trace level is set to verbose. • **noise**—Noise level tracing. The noise level is always equal to the highest tracing level possible and always generates every possible tracing message. The noise level is always equal to the highest-level tracing message possible for a module, even if future enhancements to this command introduce options that allow users to set higher tracing levels.

Command Modes

Privileged EXEC (#)
Diagnostic (diag)

Defaults

The default tracing level for all modules on the Cisco ASR 1000 series routers is critical.

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.

Usage Guidelines

The *module* options vary by process and by *hardware-module*. Use the **?** option when entering this command to see which *module* options are available with each keyword sequence.

Use the **show platform software trace message** command to view trace messages.

Trace files are stored in the tracelogs directory in the harddisk: file system. These files can be deleted without doing any harm to your router operation.

Trace file output is used for debugging. The trace level is a setting that determines how much information about a module should be stored in trace files. The levels are documented in Table 18.

Table 18 Tracing Levels and Descriptions

Trace Level	Level Number	Description
Emergency	0	The message is regarding an issue that makes the system unusable.
Alert	1	The message is regarding an action that must be taken immediately.
Critical	2	The message is regarding a critical condition. This is the default setting for every module on the Cisco ASR 1000 Series Routers.
Error	3	The message is regarding a system error.
Warning	4	The message is regarding a system warning
Notice	5	The message is regarding a significant issue, but the router is still working normally.
Informational	6	The message is useful for informational purposes only.
Debug	7	The message provides debug-level output.
Verbose	8	All possible tracing messages are sent.
Noise	-	All possible trace messages for the module. The noise level is always equal to the highest possible tracing level. Even if a future enhancement to tracing introduces a higher tracing level, the noise level will become equal to the level of that new enhancement.

Trace level settings are leveled, meaning that every setting will contain all messages from the lower setting plus the messages from its own setting. For instance, setting the trace level to 3(error) ensures that the trace file will contain all output for the 0 (emergencies), 1 (alerts), 2 (critical), and 3 (error) settings. Setting the trace level to 4 (verbose) will ensure that all trace output for the specific module will be included in that trace file.

All trace levels are not user-configurable. Specifically, the alert, critical, and notice tracing levels cannot be set by users. If you wish to trace these messages, set the trace level to a higher level that will collect these messages.

Caution Setting tracing of a module to the debug level or higher can have a negative performance impact. Setting tracing to this level or higher should be done with discretion.

Caution Setting a large number of modules to a high tracing levels can severely degrade performance. If a high level of tracing is needed in a specific context, it is almost always preferable to set a single module on a higher tracing level rather than setting multiple modules to high tracing levels.

Examples

In the following example, the trace level for the ACL module in the Forwarding Manager of the ESP processor in slot 0 is set to the informational tracing level (info).

```
set platform software trace forwarding-manager F0 acl info
```

Related Commands

Command	Description
show platform software trace level	Displays trace levels for specified modules.
show platform software trace message	Displays trace messages.

show buffers leak

To display the details of all the buffers that are older than one minute in the system, use the **show buffers leak** command in user EXEC or privileged EXEC mode.

show buffers leak [**resource user**]

Syntax Description

resource user	(Optional) Displays the resource user information to which the leaked buffers belong to.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Examples

The following is sample output from the **show buffers leak** command:

```
Router# show buffers leak

Header   DataArea Pool    Size  Link Enc    Flags      Input     Output   User

6488F464  E000084 Small    74    0    0       10       None       None EEM ED Sy
6488FB5C  E000304 Small    74    0    0       10       None       None EEM ED Sy
648905D0  E0006C4 Small    61    0    0        0       None       None EEM ED Sy
648913C0  E000BC4 Small    74    0    0       10       None       None EEM ED Sy
6489173C  E000D04 Small    74    0    0       10       None       None EEM ED Sy
648921B0  E0010C4 Small    60    0    0        0       None       None Init
6489252C  E001204 Small   103    0    0       10       None       None EEM ED Sy
64892C24  E001484 Small    74    0    0       10       None       None EEM ED Sy
64892FA0  E0015C4 Small    74    0    0       10       None       None EEM ED Sy
64893A14  E001984 Small    74    0    0       10       None       None EEM ED Sy
64893D90  E001AC4 Small    61    0    0        0       None       None EEM ED Sy
64894804  E001E84 Small    61    0    0        0       None       None EEM ED Sy
6517CB64  E32F944 Small    74    0    0       10       None       None EEM ED Sy
6517D25C  E176D44 Small    74    0    0       10       None       None EEM ED Sy
6517D5D8  E176E84 Small    74    0    0       10       None       None EEM ED Sy
6517D954  E209A84 Small    74    0    0       10       None       None EEM ED Sy
6517E744  E209D04 Small    61    0    0        0       None       None EEM ED Sy
6517EE3C  E29CBC4 Small    61    0    0        0       None       None EEM ED Sy
65180324  E177844 Small    74    0    0       10       None       None EEM ED Sy
65180D98  E177C04 Small    61    0    0        0       None       None EEM ED Sy
65E1F3A0  E4431A4 Small   102    0    0        0       None       None EEM ED Sy
64895278  E002644 Middl   191    0    0       10       None       None EEM ED Sy
64895CEC  E003004 Middl   173    0    0       10       None       None EEM ED Sy
64896068  E003344 Middl   176    0    0       10       None       None EEM ED Sy
648963E4  E003684 Middl   191    0    0       10       None       None EEM ED Sy
64896E58  E004044 Middl   109    0    0       10       None       None EEM ED Sy
64897C48  E004D44 Middl   194    0    0       10       None       None EEM ED Sy
65181F04  E330844 Middl   173    0    0       10       None       None EEM ED Sy
65183070  E3C3644 Middl   105    0    0       10       None       None EEM ED Sy
```

```
65DF9558  E4746E4 Middl   107    0    0        0       None       None EEM ED Sy
65DFA6C4  E475724 Middl   116    0    0        0       None       None EEM ED Sy
65DFADBC  E475DA4 Middl   115    0    0        0       None       None EEM ED Sy
65DFC620  E477464 Middl   110    0    0        0       None       None EEM ED Sy
64C64AE0        0 FS He     0    0    3        0       None       None Init
64C64E5C        0 FS He     0    0    3        0       None       None Init
64C651D8        0 FS He     0    0    3        0       None       None Init
64C65554        0 FS He     0    0    0        0       None       None Init
64C658D0        0 FS He     0    0    0        0       None       None Init
64C65C4C        0 FS He     0    0    0        0       None       None Init
64C65FC8        0 FS He     0    0    0        0       None       None Init
64C66344        0 FS He     0    0    0        0       None       None Init
64D6164C        0 FS He     0    0    0        0       None       None Init
64EB9D10        0 FS He     0    0    0        0       None       None Init
6523EE14        0 FS He     0    0    0        0       None       None Init
65413648        0 FS He     0    0    0        0       None       None Init
```

The following is sample output from the **show buffers leak resource user** command:

```
Router# show buffers leak resource user

Resource User:  EEM ED Syslog count:       32
Resource User:           Init count:        2
Resource User:         *Dead* count:        2
Resource User: IPC Seat Manag count:       11
Resource User:      XDR mcast count:        2
```

Table 19 describes the significant fields shown in the display.

Table 19 show buffers leak Field Descriptions

Field	Description
Header	Buffer header.
DataArea	The area where the data is available.
Pool	The different buffer pools such as ipc, header, fs header, small, middle, big, very big, large, or huge buffers.
Size	Size of the buffer pool. For example, small buffers are less than or equal to 104 bytes long. Middle buffers are in the range of 105 to 600 bytes long.
Flags	Flags of a packet. The flag indicates whether a particular packet is an incoming packet or is generated by the router.
User	RU name.

Related Commands

Command	Description
buffer public	Enters the buffer owner configuration mode and sets thresholds for buffer usage.
buffer tune automatic	Enables automatic buffer tuning.

show buffers tune

To display the details of automatic tuning of buffers, use the **show buffers tune** command in user EXEC or privileged EXEC mode.

show buffers tune

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Examples

The following is sample output from the **show buffers tune** command:

```
Router# show buffers tune

Tuning happened for the pool Small
Tuning happened at 20:47:25
Oldvalues
permanent:50  minfree:20  maxfree:150
Newvalues
permanent:61  minfree:15  maxfree:76
Tuning happened for the pool Middle
Tuning happened at 20:47:25
Oldvalues
permanent:25  minfree:10  maxfree:150
Newvalues
permanet:36  minfree:9  maxfree:45
```

Table 20 describes the significant fields shown in the display.

Table 20 show buffers tune Field Descriptions

Field	Description
Oldvalues	The minimum and maximum free buffers before automatic tuning was enabled.
Newvalues	The minimum and maximum free buffers after automatic tuning was enabled.

Related Commands

Command	Description
buffer tune automatic	Enables automatic tuning of buffers.

show buffers usage

To display the details of the buffer usage pattern in a specified buffer pool, use the **show buffers usage** command in user EXEC or privileged EXEC mode.

show buffers usage [**pool** *pool-name*]

Syntax Description

pool	(Optional) Displays the details of a specified pool.
pool-name	(Optional) Specified pool. If a pool is not specified, details of all the pools are displayed. Valid values are *ipc*, *header*, *fs header*, *small*, *middle*, *big*, *verybig*, *large*, and *huge*.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Examples

The following is sample output from the **show buffers usage** command:

```
Router# show buffers usage

Statistics for the Small pool
Caller pc    : 0x626BA9E0 count:       20
Resource User: EEM ED Sys count:       20
Caller pc    : 0x60C71F8C count:        1
Resource User:       Init count:        1
Number of Buffers used by packets generated by system:   62
Number of Buffers used by incoming packets:               0

Statistics for the Middle pool
Caller pc    : 0x626BA9E0 count:       12
Resource User: EEM ED Sys count:       12
Number of Buffers used by packets generated by system:   41
Number of Buffers used by incoming packets:               0

Statistics for the Big pool
Number of Buffers used by packets generated by system:   50
Number of Buffers used by incoming packets:               0

Statistics for the VeryBig pool
Number of Buffers used by packets generated by system:   10
Number of Buffers used by incoming packets:               0

Statistics for the Large pool
Number of Buffers used by packets generated by system:    0
Number of Buffers used by incoming packets:               0
```

```
Statistics for the Huge pool
Number of Buffers used by packets generated by system:    0
Number of Buffers used by incoming packets:               0

Statistics for the IPC pool
Number of Buffers used by packets generated by system:    2
Number of Buffers used by incoming packets:               0

Statistics for the Header pool
Number of Buffers used by packets generated by system:  511
Number of Buffers used by incoming packets:               0

Statistics for the FS Header pool
Caller pc    : 0x608F68FC count:        9
Resource User:       Init count:       12
Caller pc    : 0x61A21D3C count:        1
Caller pc    : 0x60643FF8 count:        1
Caller pc    : 0x61C526C4 count:        1
Number of Buffers used by packets generated by system:   28
Number of Buffers used by incoming packets:               0
```

The following is sample output from the **show buffers usage pool** command for the pool named small:

```
Router# show buffers usage pool small

Statistics for the Small pool
Caller pc    : 0x626BA9E0 count:       20
Resource User: EEM ED Sys count:       20
Caller pc    : 0x60C71F8C count:        1
Resource User:       Init count:        1
Number of Buffers used by packets generated by system:   62
Number of Buffers used by incoming packets:               0
```

Related Commands

Command	Description
buffer public	Enters buffer owner configuration mode and sets thresholds for buffer usage.
show buffers leak	Displays details of the buffers that have leaked.

show calendar

To display the current time and date setting for the hardware clock, use the **show calendar** command in EXEC mode:

show calendar

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Some platforms have a hardware clock (calendar) which is separate from the software clock. The hardware clock is battery operated, and runs continuously, even if the router is powered off or rebooted.

You can compare the time and date shown with this command with the time and date listed via the **show clock** EXEC command to verify that the hardware clock and software clock are synchronized with each other. The time displayed is relative to the configured time zone.

Examples

In the following sample display, the hardware clock indicates the time stamp of 12:13:44 p.m. on Friday, July 19, 1996:

```
Router> show calendar

12:13:44 PST Fri Jul 19 1996
```

Related Commands

Command	Description
show clock	Displays the time and date from the system software clock.

show cdp

To display global Cisco Discovery Protocol (CDP) information, including timer and hold-time information, use the **show cdp** command in privileged EXEC mode.

show cdp

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.0(3)T	The output of this command was modified to include CDP Version 2 information.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows that the current router is sending CDP advertisements every 1 minute (the default setting for the **cdp timer** global configuration command). Also shown is that the current router directs its neighbors to hold its CDP advertisements for 3 minutes (the default for the **cdp holdtime** global configuration command), and that the router is enabled to send CDP Version 2 advertisements:

```
router# show cdp

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

Table 21 describes the significant fields shown in the display.

Table 21 show cdp Field Descriptions

Field	Definition
Sending CDP packets every XX seconds	The interval (in seconds) between transmissions of CDP advertisements. This field is controlled by the **cdp timer** command.

Table 21 show cdp Field Descriptions

Field	Definition
Sending a holdtime value of XX seconds	The amount of time (in seconds) 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 XX	The state of whether CDP Version-2 type advertisements are enabled to be sent. Possible states are enabled or disabled. This field is controlled by the **cdp advertise v2** global configuration command.

Related Commands

Command	Description
cdp advertise-v2	Enables CDP Version 2 advertising functionality on a device.
cdp holdtime	Specifies the amount of time the receiving device should hold a CDP packet from your router before discarding it.
cdp timer	Specifies how often the Cisco IOS software sends CDP updates.
show cdp entry	Displays information about a specific neighbor device listed in the CDP table.
show cdp interface	Displays information about the interfaces on which CDP is enabled.
show cdp neighbors	Displays detailed information about neighboring devices discovered using CDP.
show cdp traffic	Displays information about traffic between devices gathered using CDP.

show cdp entry

To display information about a specific neighboring device discovered using Cisco Discovery Protocol (CDP), use the **show cdp entry** command in privileged EXEC mode.

show cdp entry {* | *device-name*[*]} [**version**] [**protocol**]

Syntax Description

*	Displays all of the CDP neighbors.
device-name[*]	Name of the neighbor about which you want information. You can enter an optional asterisk (*) at the end of a *device-name* as a wildcard. For example, entering **show cdp entry dev*** will match all device names that begin with **dev**.
version	(Optional) Limits the display to information about the version of software running on the router.
protocol	(Optional) Limits the display to information about the protocols enabled on a router.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(8)T	Support for IPv6 address and address type information was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following is sample output from the **show cdp entry** command. Information about the neighbor *device.cisco.com* is displayed, including device ID, protocols and addresses, platform, interface, hold time, and version.

```
Router# show cdp entry device.cisco.com

Device ID: device.cisco.com
Entry address(es):
  IP address: 10.1.17.24
  IPv6 address: FE80::203:E3FF:FE6A:BF81  (link-local)
  IPv6 address: 4000::BC:0:0:C0A8:BC06  (global unicast)
  CLNS address: 490001.1111.1111.1111.00
Platform: cisco 3640,  Capabilities: Router
Interface: Ethernet0/1,  Port ID (outgoing port): Ethernet0/1
Holdtime : 160 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-A2IS-M), Experimental Version 12.2
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 08-Aug-01 12:39 by joeuser
```

The following is sample output from the **show cdp entry version** command. Only information about the version of software running on *device.cisco.com* is displayed.

```
Router# show cdp entry device.cisco.com version

Version information for device.cisco.com:
 Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-A2IS-M), Experimental Version 12.2
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 08-Aug-01 12:39 by joeuser
```

The following is sample output from the **show cdp entry protocol** command. Only information about the protocols enabled on *device.cisco.com* is displayed.

```
Router# show cdp entry device.cisco.com protocol

Protocol information for device.cisco.com:
  IP address: 10.1.17.24
  IPv6 address: FE80::203:E3FF:FE6A:BF81  (link-local)
  IPv6 address: 4000::BC:0:0:C0A8:BC06  (global unicast)
  CLNS address: 490001.1111.1111.1111.00
```

Related Commands

Command	Description
show cdp	Displays global CDP information, including timer and hold-time information.
show cdp interface	Displays information about the interfaces on which CDP is enabled.
show cdp neighbors	Displays detailed information about neighboring devices discovered using CDP.
show cdp traffic	Displays traffic information from the CDP table.

show cdp interface

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

show cdp interface [*type number*]

Syntax Description

type	(Optional) Type of interface about which you want information.
number	(Optional) Number of the interface about which you want information.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show cdp interface** command. Status information and information about CDP timer and hold-time settings is displayed for all interfaces on which CDP is enabled.

```
Router# show cdp interface

Serial0 is up, line protocol is up, encapsulation is SMDS
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Ethernet0 is up, line protocol is up, encapsulation is ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

The following is sample output from the **show cdp interface** command with an interface specified. Status information and information about CDP timer and hold-time settings is displayed for Ethernet interface 0 only.

```
Router# show cdp interface ethernet 0

Ethernet0 is up, line protocol is up, encapsulation is ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

Related Commands

Command	Description
show cdp	Displays global CDP information, including timer and hold-time information.
show cdp entry	Displays information about a specific neighbor device or all neighboring devices discovered using CDP.
show cdp neighbors	Displays detailed information about neighboring devices discovered using CDP.
show cdp traffic	Displays traffic information from the CDP table.

show cdp neighbors

To display detailed information about neighboring devices discovered using Cisco Discovery Protocol, use the **show cdp neighbors** command in privileged EXEC mode.

show cdp neighbors [*type number*] [**detail**]

Syntax Description

type	(Optional) Interface type that is connected to the neighbors about which you want information; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel,** and **vlan**.
number	(Optional) Number of the interface connected to the neighbors about which you want information.
detail	(Optional) Displays detailed information about a neighbor (or neighbors) including network address, enabled protocols, hold time, and software version.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.0(3)T	The output of this command using the **detail** keyword was expanded to include Cisco Discovery Protocol Version 2 information.
12.2(8)T	Support for IPv6 address and address type information was added.
12.2(14)S	Support for IPv6 address and address type information was added.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **vlan** keyword is supported in Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The **port-channel** values are from 0 to 282; values from 257 to 282 are supported on the call switching module (CSM) and the FWSM only.

Examples

The following example specifies information related to the **show cdp neighbors** command:

```
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
joe        Eth 0          133      R           4500      Eth 0
sam        Eth 0          152      R           AS5200    Eth 0
```

```
terri      Eth 0          144      R           3640      Eth0/0
maine      Eth 0          141                  RP1       Eth 0/0
sancho     Eth 0          164                  7206      Eth 1/0
```

Table 22 describes the significant fields shown in the example.

Table 22 show cdp neighbors Field Descriptions

Field	Definition
Capability Codes	The type of device that can be discovered.
Device ID	The name of the neighbor device and either the MAC address or the serial number of this device.
Local Intrfce	The local interface through which this neighbor is connected.
Holdtme	The remaining amount of time (in seconds) the current device will hold the Cisco Discovery Protocol advertisement from a sending router before discarding it.
Capability	The type of the device listed in the CDP Neighbors table. Possible values are as follows: R—Router T—Transparent bridge B—Source-routing bridge S—Switch H—Host I—IGMP device r—Repeater
Platform	The product number of the device.
Port ID	The interface and port number of the neighboring device.

The following is sample output for one neighbor from the **show cdp neighbors detail** command. Additional detail is shown about neighbors, including network addresses, enabled protocols, and software version.

```
Router# show cdp neighbors detail

Device ID: device.cisco.com
Entry address(es):
  IPv6 address: FE80::203:E3FF:FE6A:BF81  (link-local)
  IPv6 address: 4000::BC:0:0:C0A8:BC06  (global unicast)
Platform: cisco 3640,  Capabilities: Router
Interface: Ethernet0/1,  Port ID (outgoing port): Ethernet0/1
Holdtime : 160 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-A2IS-M), Experimental Version 12.2
Duplex Mode: half
Native VLAN: 42
VTP Management Domain: 'Accounting Group'
```

Table 23 describes the significant fields shown in the display.

Table 23 show cdp neighbors detail Field Descriptions

Field	Definition
Device ID	The name of the neighbor device and either the MAC address or the serial number of this device.
Entry address(es)	A list of network addresses of neighbor devices.
IPv6 address: FE80::203:E3FF:FE6A:BF81 (link-local)	The network address of the neighbor device. The address can be in IP, IPv6, IPX, AppleTalk, DECnet, or Connectionless Network Service (CLNS) protocol conventions. IPv6 addresses are followed by one of the following IPv6 address types: • global unicast • link-local • multicast • site-local • V4 compatible
Platform	The product name and number of the neighbor device.
Capabilities	The 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	The local interface through which this neighbor is connected.
Port ID	The interface and port number of the neighboring device.
Holdtime	The remaining amount of time (in seconds) the current device will hold the CDP advertisement from a sending router before discarding it.
Version	The software version of the neighbor device.
advertisement version:	Version of CDP that is being used for CDP advertisements.
Duplex Mode	The duplex state of connection between the current device and the neighbor device.
Native VLAN	The ID number of the VLAN on the neighbor device.
VTP Management Domain	A string that is the name of the collective group of VLANs associated with the neighbor device.

Related Commands

Command	Description
show cdp	Displays global CDP information, including timer and hold-time information.
show cdp entry	Displays information about a specific neighbor device listed in the CDP table.
show cdp interface	Displays information about the interfaces on which CDP is enabled.
show cdp traffic	Displays information about traffic between devices gathered using CDP.

show cdp traffic

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

show cdp traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

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

```
Router# show cdp traffic

Total packets output: 543, Input: 333
Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
No memory: 0, Invalid: 0, Fragmented: 0
CDP version 1 advertisements output: 191, Input: 187
CDP version 2 advertisements output: 352, Input: 146
```

Table 24 describes the significant fields shown in the display.

Table 24 show cdp traffic Field Descriptions

Field	Definition
Total packets output	The number of CDP advertisements sent by the local device. Note that this value is the sum of the CDP Version 1 advertisements output and CDP Version 2 advertisements output fields.
Input	The number of CDP advertisements received by the local device. Note that this value is the sum of the CDP Version 1 advertisements input and CDP Version 2 advertisements input fields.
Hdr syntax	The number of CDP advertisements with bad headers, received by the local device.
Chksum error	The number of times the checksum (verifying) operation failed on incoming CDP advertisements.

Table 24 show cdp traffic Field Descriptions (continued)

Field	Definition
Encaps failed	The 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	The number of times 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	The number of invalid CDP advertisements received and sent by the local device.
Fragmented	The number of times fragments or portions of a single CDP advertisement were received by the local device instead of the complete advertisement.
CDP version 1 advertisements output	The number of CDP Version 1 advertisements sent by the local device.
Input	The number of CDP Version 1 advertisements received by the local device.
CDP version 2 advertisements output	The number of CDP Version 2 advertisements sent by the local device.
Input	The number of CDP Version 2 advertisements received by the local device.

Related Commands

Command	Description
show cdp	Displays global CDP information, including timer and hold-time information.
show cdp entry	Displays information about a specific neighbor device listed in the CDP table.
show cdp interface	Displays information about the interfaces on which CDP is enabled.
show cdp neighbors	Displays detailed information about neighboring devices discovered using CDP.

show clock

To display the time and date from the system software clock, use the **show clock** command in EXEC mode.

show clock [**detail**]

Syntax Description

detail	(Optional) Indicates the clock source (NTP, VINES, hardware clock, and so on) and the current summer-time setting (if any).

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The software clock keeps an "authoritative" flag that indicates whether the time is authoritative (believed to be accurate). If the software clock has been set by a timing source (for example, via NTP), the flag is set. If the time is not authoritative, it will be used only for display purposes. Until the clock is authoritative and the "authoritative" flag is set, the flag prevents peers from synchronizing to the software clock.

The symbol that precedes the **show clock** display indicates the following:

Symbol	Description	Example
*	Time is not authoritative: the software clock is not in sync or has never been set.	*15:29:03.158 UTC Tue Feb 25 2003:
(blank)	Time is authoritative: the software clock is in sync or has just been set manually	15:29:03.158 UTC Tue Feb 25 2003:
.	Time is authoritative, but NTP is not synchronized: the software clock was in sync, but has since lost contact with all configured NTP servers	.15:29:03.158 UTC Tue Feb 25 2003:

These symbols are also used in NTP-based timestamping, such as for syslog (SEM) messages.

Note In general, NTP synchronization takes approximately 15 to 20 minutes.

Examples

The following sample output shows that the current clock is authoritative and that the time source is NTP:

```
Router> show clock detail

15:29:03.158 PST Tue Feb 25 2003
Time source is NTP
```

The following example shows the current clock is authoritative, but NTP is not yet synchronized:

```
Router> show clock

.16:42:35.597 UTC Tue Feb 25 2003
```

Related Commands

Command	Description
clock set	Manually sets the software clock.
show calendar	Displays the current time and date setting of the system hardware clock.

show cns config connections

To display the status of the Cisco Networking Services (CNS) event agent connection, use the **show cns config connections** command in privileged EXEC mode.

show cns config connections

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use the **show cns config connections** command to determine whether the CNS event agent is connecting to the gateway, connected, or active, and to display the gateway used by the event agent and its IP address and port number.

Examples

The following is sample output from the **show cns config connections** command:

```
Router# show cns config connections

The partial configuration agent is enabled.

Configuration server:  10.1.1.1
Port number:           80
Encryption:            disabled
Config id:             test1
Connection Status:     Connection not active.
```

Related Commands

Command	Description
show cns config outstanding	Displays information about incremental CNS configurations that have started but not yet completed.
show cns config stats	Displays statistics about the CNS configuration agent.

show cns config outstanding

To display information about incremental (partial) Cisco Networking Services (CNS) configurations that have started but not yet completed, use the **show cns config outstanding** command in privileged EXEC mode.

show cns config outstanding

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	This command was implemented on Cisco 2600 series and Cisco 3600 series routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **show cns config outstanding** command to display information about outstanding incremental (partial) configurations that have started but not yet completed, including the following:

- Queue ID (location of configuration in the config queue)
- Identifier (group ID)
- Config ID (identity of configuration within the group)

Examples

The following is sample output from the **show cns config outstanding** command:

```
Router# show cns config outstanding

The outstanding configuration information:
queue id   identifier       config-id
1          identifierREAD   config_idREAD
```

Related Commands

Command	Description
cns config cancel	Cancels an incremental two-phase synchronization configuration.
config-cli	Displays the status of the CNS event agent connection.
show cns config stats	Displays statistics about the CNS configuration agent.

show cns config stats

To display statistics about the Cisco Networking Services (CNS) configuration agent, use the **show cns config stats** command in privileged EXEC mode.

show cns config stats

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	This command was implemented on Cisco 2600 series and Cisco 3600 series routers.
12.3(1)	Additional output fields were added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command displays the following statistics on the CNS configuration agent:

- The number of configurations requests received
- The number of configurations completed
- The number of configurations failed
- The number of configurations pending
- The number of configurations cancelled
- The time stamp of the last configuration received
- The time stamp of the initial configuration received

Examples

The following is sample output from the **show cns config stats** command:

```
Router# show cns config stats

6 configuration requests received.
4 configurations completed.
1 configurations failed.
1 configurations pending.
0 configurations cancelled.
The time of last received configuration is *May 5 2003 10:42:15 UTC.
Initial Config received *May 5 2003 10:45:15 UTC.
```

Related Commands

Command	Description
clear cns config stats	Clears all the statistics about the CNS configuration agent.
show cns config outstanding	Displays information about incremental CNS configurations that have started but not yet completed.

show cns config status

To display the status of the Cisco Networking Services (CNS) Configuration Agent, use the **show cns config status** command in EXEC mode.

show cns config status

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0 (22)S.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command displays the status of the Configuration Agent. Use this option to display the following information about the Configuration Agent:

- Status of the Configuration Agent, for example, whether it has been configured properly.
- IP address and port number of the trusted server that the Configuration Agent is using.
- Config ID (identity of configuration within the configuration group).

Related Commands

Command	Description
cns config cancel	Cancels a CNS configuration.
cns config initial	Starts the initial CNS Configuration Agent.
cns config partial	Starts the partial CNS Configuration Agent.
cns config retrieve	Gets the configuration of a routing device using CNS.

show cns event connections

To display the status of the Cisco Networking Services (CNS) event agent connection, use the **show cns event connections** command in privileged EXEC mode.

show cns event connections

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **show cns event connections** command to display the status of the event agent connection—such as whether it is connecting to the gateway, connected, or active—and to display the gateway used by the event agent and its IP address and port number.

Examples

The following example displays the IP address and port number of the primary and backup gateways:

```
Router# show cns event connections

The currently configured primary event gateway:
        hostname is 10.1.1.1.
        port number is 11011.
Event-Id is Internal test1
Keepalive setting:
        none.
Connection status:
        Connection Established.
The currently configured backup event gateway:
        none.
The currently connected event gateway:
        hostname is 10.1.1.1.
        port number is 11011.
```

Related Commands

Command	Description
show cns event stats	Displays statistics about the CNS event agent connection.
show cns event subject	Displays a list of subjects about the CNS event agent connection.

show cns event gateway

To display information about the Cisco Networking Services (CNS) Event Agent, use the **show cns event gateway** command in EXEC mode.

show cns event gateway

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0 (18)ST

Usage Guidelines

Use this command to display the following information about CNS gateways:

- Primary gateway:
  - IP address
  - Port number
- Backup gateways:
  - IP address
  - Port number
- Currently connected gateway:
  - IP address
  - Port number

Related Commands

Command	Description
cns event	Configures the CNS Event Gateway.

show cns event stats

To display statistics about the CNS event agent connection, use the **show cns event stats** command in privileged EXEC mode.

show cns event stats

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(8)T	This command was implemented on the Cisco 2600 series and the Cisco 3600 series routers.
12.3(1)	Output was changed to display statistics generated since last cleared.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to display the following statistics for the CNS event agent:

- Number of events received
- Number of events sent
- Number of events not processed successfully
- Number of events in the queue
- Time stamp showing when statistics were last cleared (time stamp is router time)
- Number of events received since the statistics were cleared
- Time stamp of latest event received (time stamp is router time)
- Time stamp of latest event sent
- Number of applications using the Event Agent
- Number of subjects subscribed

Examples

The following example displays statistics for the CNS event agent:

```
Router# show cns event stats

0 events received.
1 events sent.
0 events not processed.
```

```
0 events in the queue.
0 events sent to other IOS applications.
Event agent stats last cleared at Apr 4 2003 00:55:25 UTC
No events received since stats cleared
The time stamp of the last received event is *Mar 30 2003 11:04:08 UTC
The time stamp of the last sent event is *Apr 11 2003 22:21:23 UTC
3 applications are using the event agent.
0 subjects subscribed.
1 subjects produced.
0 subjects replied.
```

Related Commands

Command	Description
clear cns event stats	Clears all the statistics about the CNS event agent.
cns event	Enables and configures CNS event agent services.
show cns event connections	Displays the status of the CNS event agent connection.
show cns event subject	Displays a list of subjects about the CNS event agent connection.

show cns event status

To display information about the Cisco Networking Services (CNS) Event Agent, use the **show cns event status** command in EXEC mode.

show cns event status

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0 (18)ST.

Usage Guidelines

Use this command to display the following information about the CNS Event Agent:

- Status of Event Agent:
  - Connected
  - Active
- Gateway used by the Event Agent:
  - IP address
  - Port number
- Device ID

Related Commands

Command	Description
cns event	Configures the CNS Event Gateway.

show cns event subject

To display a list of subjects about the Cisco Networking Services (CNS) event agent connection, use the **show cns event subject** command in privileged EXEC mode.

show cns event subject [*name*]

Syntax Description

name	(Optional) Displays a list of applications that are subscribing to this specific subject name.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(8)T	This command was implemented on the Cisco 2600 series and the Cisco 3600 series.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **show cns event subject** command to display a list of subjects of the event agent that are subscribed to by applications.

Examples

The following example displays the IP address and port number of the primary and backup gateways:

```
Router# show cns event subject

The list of subjects subscribed by applications.
   cisco.cns.mibaccess:request
   cisco.cns.config.load
   cisco.cns.config.reboot
   cisco.cns.exec.cmd
```

Related Commands

Command	Description
show cns event connections	Displays the status of the CNS event agent connection.
show cns event stats	Displays statistics about the CNS event agent connection.

show cns image connections

To display the status of the Cisco Networking Services (CNS) image management server HTTP connections, use the **show cns image connections** command in privileged EXEC mode.

show cns image connections

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Use the **show cns image connections** command when troubleshooting HTTP connection problems with the CNS image server. The output displays the following information:

- Number of connection attempts
- Number of connections that were never connected and those that were abruptly disconnected
- Date and time of last successful connection

Examples

The following is sample output from the **show cns image connections** command:

```
Router# show cns image connections

CNS Image Agent:  HTTP connections
Connection attempts 1
never connected:0   Abrupt disconnect:0
Last successful connection at 11:45:02.000 UTC Mon May 6 2003
```

Related Commands

Command	Description
show cns image inventory	Displays inventory information about the CNS image agent.
show cns image status	Displays status information about the CNS image agent.

show cns image inventory

To provide a dump of Cisco Networking Services (CNS) image inventory information in XML format, use the **show cns image inventory** command in privileged EXEC mode.

show cns image inventory

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

To view the XML output in a better format, paste the content into a text file and use an XML viewing tool.

Examples

The following is sample output from the **show cns image inventory** command:

```
Router# show cns image inventory

Inventory Report
<imageInventoryReport><deviceName><imageID>Router</imageID><hostName>Router</ho
IOS (tm) C2600 Software (C2600-I-M), Experimental Version 12.3(20030414:081500)]
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Mon 14-Apr-03 02:03 by engineer</versionString><imageFile>tftp://10.25>
```

Related Commands

Command	Description
show cns image connections	Displays connection information for the CNS image agent.
show cns image status	Displays status information about the CNS image agent.

show cns image status

To display status information about the Cisco Networking Services (CNS) image agent, use the **show cns image status** command in privileged EXEC mode.

show cns image status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Use this command to display the following status information about the CNS image agent:

- Start date and time of last upgrade
- End date and time of last upgrade
- End date and time of last successful upgrade
- End date and time of last failed upgrade
- Number of failed upgrades
- Number of successful upgrades with number of received messages and errors
- Transmit status with number of attempts, successes, and failures

Examples

The following is sample output from the **show cns image status** command:

```
Router# show cns image status

Last upgrade started at 11:45:02.000 UTC Mon May 6 2003
Last upgrade ended at 11:56:04.000 UTC Mon May 6 2003 status SUCCESS

Last successful upgrade ended at 00:00:00.000 UTC Mon May 6 2003
Last failed upgrade ended at 00:00:00.000 UTC Wed Apr 16 2003
Number of failed upgrades: 2
Number of successful upgrades: 6
 messages received: 12
 receive errors: 5
Transmit Status
  TX Attempts:4
    Successes:3         Failures 2
```

Related Commands

Command	Description
show cns image connections	Displays connection information for the CNS image agent.
show cns image inventory	Displays image inventory information in XML format.

show event manager directory user

To display the directory to use for storing user library files or user-defined Embedded Event Manager (EEM) policies, use the **show event manager directory user** command in privileged EXEC mode.

show event manager directory user [**library** | **policy**]

Syntax Description

library	(Optional) User library files.
policy	(Optional) User-defined EEM policies.

Command Default

The directories for both user library and user policy files are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

Use the **event manager directory user** command to specify the directory to use for storing user library or user policy files.

Examples

The following example shows the /usr/fm_policies folder on disk 0 as the directory to use for storing EEM user library files:

```
Router# show event manager directory user library

disk0:/usr/fm_policies
```

Related Commands

Command	Description
event manager directory user	Specifies a directory to use for storing user library files or user-defined EEM policies.

show event manager environment

To display the name and value of Embedded Event Manager (EEM) environment variables, use the **show event manager environment** command in privileged EXEC mode.

show event manager environment [**all** | *variable-name*]

Syntax Description

all	(Optional) Displays information for all environment variables. This is the default.
variable-name	(Optional) Displays information about the specified environment variable.

Command Default

If no argument or keyword is specified, information for all environment variables is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Examples

The following is sample output from the **show event manager environment** command:

```
Router# show event manager environment

No.  Name                          Value
1    _cron_entry                   0-59/1 0-23/1 * * 0-7
2    _show_cmd                     show version
3    _syslog_pattern               .*UPDOWN.*Ethernet1/0.*
4    _config_cmd1                  interface Ethernet1/0
5    _config_cmd2                  no shutdown
```

Table 25 describes the significant fields shown in the display.

Table 25 show event manager environment Field Descriptions

Field	Description
No.	The index number assigned to the EEM environment variable.
Name	The name given to the EEM environment variable when it was created.
Value	The text content defined for the EEM environment variable when it was created.

Related Commands

Command	Description
event manager environment	Sets an EEM environment variable.

show event manager history events

To display the Embedded Event Manager (EEM) events that have been triggered, use the **show event manager history events** command in privileged EXEC mode.

show event manager history events [**detailed**] [**maximum** *number*]

Syntax Description

detailed	(Optional) Displays detailed information about each EEM event.
maximum	(Optional) Specifies the maximum number of events to display.
number	(Optional) Number in the range from 1 to 50. The default is 50.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

Use the **show event manager history events** command to track information about the EEM events that have been triggered.

Examples

The following is sample output from the **show event manager history events** command showing that two types of events, Simple Network Management Protocol (SNMP) and application, have been triggered.

```
Router# show event manager history events

No.  Time of Event             Event Type          Name
1    Fri Aug13  21:42:57 2004  snmp                applet: SAAping1
2    Fri Aug13  22:20:29 2004  snmp                applet: SAAping1
3    Wed Aug18  21:54:48 2004  snmp                applet: SAAping1
4    Wed Aug18  22:06:38 2004  snmp                applet: SAAping1
5    Wed Aug18  22:30:58 2004  snmp                applet: SAAping1
6    Wed Aug18  22:34:58 2004  snmp                applet: SAAping1
7    Wed Aug18  22:51:18 2004  snmp                applet: SAAping1
8    Wed Aug18  22:51:18 2004  application         applet: CustApp1
```

Table 26 describes the significant fields shown in the display.

Table 26 show event manager history events Field Descriptions

Field	Description
No.	Event number.
Time of Event	Day, date, and time when the event was triggered.
Event Type	Type of event.
Name	Name of the policy that was triggered.

Related Commands

Command	Description
event manager history size	Modifies the size of the EEM history tables.

show event manager history traps

To display the Embedded Event Manager (EEM) Simple Network Management Protocol (SNMP) traps that have been sent, use the **show event manager history traps** command in privileged EXEC mode.

show event manager history traps [**server** | **policy**]

Syntax Description

server	(Optional) Displays SNMP traps that were triggered from the EEM server.
policy	(Optional) Displays SNMP traps that were triggered from within an EEM policy.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

Use the **show event manager history traps** command to identify whether the SNMP traps were implemented from the EEM server or from an EEM policy.

Examples

The following is sample output from the **show event manager history traps** command:

```
Router# show event manager history traps policy

No.  Time                     Trap Type           Name
1    Wed Aug18  22:30:58 2004 policy              EEM Policy Director
2    Wed Aug18  22:34:58 2004 policy              EEM Policy Director
3    Wed Aug18  22:51:18 2004 policy              EEM Policy Director
```

Table 27 describes the significant fields shown in the display.

Table 27 show event manager history traps Field Descriptions

Field	Description
No.	Trap number.
Time	Date and time when the SNMP trap was implemented.
Trap Type	Type of SNMP trap.
Name	Name of the SNMP trap that was implemented.

Related Commands

Command	Description
event manager history size	Modifies the size of the EEM history tables.

show event manager policy available

To display Embedded Event Manager (EEM) policies that are available to be registered, use the **show event manager policy available** command in privileged EXEC mode.

show event manager policy available [**system** | **user**] [**detailed** *policy-filename*]

Syntax Description

system	(Optional) Displays all available system policies.
user	(Optional) Displays all available user policies.
detailed	(Optional) Displays the actual Cisco sample policy for the specified *policy-filename*.
policy-filename	(Optional) Name of sample policy to be displayed.

Command Default

If no keyword is specified, information for all available system and user policies is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	The **user** keyword was added, and this command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	The **detailed** keyword and the *policy-filename* argument were added, and this command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

This command is useful if you forget the exact name of a policy required for the **event manager policy** command.

The **detailed** keyword displays the actual specified sample policy including details about the environment variables used by the policy and instructions for running the policy.

Examples

The following is sample output from the **show event manager policy available** command:

```
Router# show event manager policy available

No.  Type    Time Created                Name
1    system  Tue Sep 12 09:41:32 2002    sl_intf_down.tcl
2    system  Tue Sep 12 09:41:32 2002    tm_cli_cmd.tcl
```

Table 28 describes the significant fields shown in the display.

Table 28 show event manager policy available Field Descriptions

Field	Description
No.	Index number automatically assigned to the policy.
Type	Indicates whether the policy is a system policy.
Time Created	Time stamp indicating the date and time when the policy file was created.
Name	Name of the EEM policy file.

The following is sample output from the **show event manager policy available** command:

```
Router# show event manager policy available detailed tm_cli_cmd.tcl

::cisco::eem::event_register_timer cron name crontimer2 cron_entry $_cron_entry maxrun 240
#------------------------------------------------------------------
# EEM policy that will periodically execute a cli command and email the
# results to a user.
#
# July 2005, Cisco EEM team
#
# Copyright (c) 2005 by cisco Systems, Inc.
# All rights reserved.
#------------------------------------------------------------------
### The following EEM environment variables are used:
###
### _cron_entry (mandatory)           - A CRON specification that determines
###                                     when the policy will run. See the
###                                     IOS Embedded Event Manager
###                                     documentation for more information
###                                     on how to specify a cron entry.
### Example: _cron_entry                0-59/1 0-23/1 * * 0-7
###
### _email_server (mandatory)         - A Simple Mail Transfer Protocol (SMTP)
###                                     mail server used to send e-mail.
### Example: _email_server              mailserver.customer.com
###
```

Related Commands

Command	Description
event manager policy	Registers an EEM policy with the EEM.

show event manager policy pending

To display Embedded Event Manager (EEM) policies that are pending execution, use the **show event manager policy pending** command in privileged EXEC mode.

show event manager policy pending

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

Pending policies are policies that are pending execution in the EEM server execution queue. When an event is triggered, the policy that is registered to handle the event is queued for execution in the EEM server. Use the **show event manager policy pending** command to display the policies in this queue.

Examples

The following is sample output from the **show event manager policy pending** command:

```
Router# show event manager policy pending

No.  Time of Event             Event Type          Name
1    Sat Oct11  05:02:41 2003  timer watchdog      script:fd_timer_watchdog.tcl
2    Sat Oct11  05:02:41 2003  timer watchdog      script:fd_timer_watchdog2.tcl
```

Table 29 describes the significant fields shown in the display.

Table 29 show event manager policy pending Field Descriptions

Field	Description
No.	Index number automatically assigned to the policy.
Time of Event	Date and time when the policy was queued for execution in the EEM server.
Event Type	Type of event.
Name	Name of the EEM policy file.

Related Commands

Command	Description
event manager policy	Registers an EEM policy with the EEM.

show event manager policy registered

To display Embedded Event Manager (EEM) policies that are already registered, use the **show event manager policy registered** command in privileged EXEC mode.

show event manager policy registered [**event-type** *event-name*] [**system** | **user**] [**time-ordered** | **name-ordered**] [**detailed** *policy-filename*]

Syntax Description

event-type	(Optional) Displays the registered policies for the event type specified in the *event-name* argument. If the event type is not specified, all registered policies are displayed.
event-name	(Optional) Type of event. The following values are valid: • **application**—Application event type. • **cli**—Command-line interface (CLI) event type. • **counter**—Counter event type. • **interface**—Interface event type. • **ioswdsysmon**—Watchdog system monitor event type. • **none**—Manually run policy event type. • **snmp**—Simple Network Management Protocol (SNMP) event type. • **syslog**—Syslog event type. • **timer-absolute**—Absolute timer event type. • **timer-countdown**—Countdown timer event type. • **timer-cron**—Clock daemon (CRON) timer event type. • **timer-watchdog**—Watchdog timer event type.
system	(Optional) Displays the registered system policies.
user	(Optional) Displays the registered user policies.
time-ordered	(Optional) Displays the policies in the order of the time at which they were registered. This is the default.
name-ordered	(Optional) Displays the policies, in alphabetical order, by policy name.
detailed	(Optional) Displays details for the specified *policyname*.
policy-filename	(Optional) Name of policy to be displayed.

Command Default

If this command is invoked with no optional keywords, it displays all registered EEM system and user policies for all event types. The policies are displayed according to the time at which they were registered.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	Additional event types and the **user** keyword were added, and this command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	The **detailed** keyword and the *policy-filename* argument were added, and this command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

The output shows registered policy information in two parts. The first line in each policy description lists the index number assigned to the policy, the policy type (system), the type of event registered, the time when the policy was registered, and the name of the policy file. The remaining lines of each policy description display information about the registered event and how the event is to be handled; the information comes directly from the Tool Command Language (Tcl) command arguments that make up the policy file. Output of the **show event manager policy registered** command is most helpful to persons who are writing and monitoring EEM policies.

The **detailed** keyword displays the actual specified sample policy including details about the environment variables used by the policy and instructions for running the policy.

Examples

The following is sample output from the **show event manager policy registered** command:

```
Router# show event manager policy registered

No.  Class   Type    Event Type          Trap  Time Registered           Name
1    applet  system  snmp                Off   Fri Aug 13 17:42:52 2004  IPSLAping1
 oid {1.3.6.1.4.1.9.9.42.1.2.9.1.6.4} get-type exact entry-op eq entry-val {1}
 exit-op eq exit-val {2} poll-interval 5.000
 action 1.0 syslog priority critical msg Server IPecho Failed: OID=$_snmp_oid_val
 action 1.1 snmp-trap strdata EEM detected server reachability failure to 10.1.88.9
 action 1.2 publish-event sub-system 88000101 type 1 arg1 10.1.88.9 arg2 IPSLAEcho arg3
fail
 action 1.3 counter name _IPSLA1F value 1 op inc
```

Table 30 describes the significant fields shown in the display.

Table 30 show event manager policy registered Field Descriptions

Field	Description
No.	Index number automatically assigned to the policy.
Class	Class of policy, either applet or script.
Type	Identifies whether the policy is a system policy.
Event Type	Type of event.
Trap	Identifies whether an SNMP trap is enabled.

Table 30 show event manager policy registered Field Descriptions (continued)

Field	Description
Time Registered	Time stamp indicating the day, date, and time when the policy file was registered.
Name	Name of the EEM policy file.

The following is sample output from the **show event manager policy registered** command showing the use of the **detailed** keyword for the policy named tm_cli_cmd.tcl:

```
Router# show event manager policy registered detailed tm_cli_cmd.tcl

::cisco::eem::event_register_timer cron name crontimer2 cron_entry $_cron_entry maxrun 240
#------------------------------------------------------------------
# EEM policy that will periodically execute a cli command and email the
# results to a user.
#
# July 2005, Cisco EEM team
#
# Copyright (c) 2005 by cisco Systems, Inc.
# All rights reserved.
#------------------------------------------------------------------
### The following EEM environment variables are used:
###
### _cron_entry (mandatory)            - A CRON specification that determines
###                                        when the policy will run. See the
###                                        IOS Embedded Event Manager
###                                        documentation for more information
###                                        on how to specify a cron entry.
### Example: _cron_entry                 0-59/1 0-23/1 * * 0-7
###
### _email_server (mandatory)          - A Simple Mail Transfer Protocol (SMTP)
###                                        mail server used to send e-mail.
### Example: _email_server               mailserver.example.com
###
```

Related Commands

Command	Description
event manager policy	Registers an EEM policy with the EEM.

show event manager session cli username

To display the username associated with Embedded Event Manager (EEM) policies that use the command-line interface (CLI) library, use the **show event manager session cli username** command in privileged EXEC mode.

show event manager session cli username

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

Use this command to display the username associated with a Tool Command Language (Tcl) EEM policy. If you are using authentication, authorization, and accounting (AAA) security and implement authorization on a command basis, you should use the **event manager session cli username** command to set a username to be associated with a Tcl session. The username is used when a Tcl policy executes a CLI command. TACACS+ verifies each CLI command using the username associated with the Tcl session that is running the policy. Commands from Tcl policies are not usually verified because the router must be in privileged EXEC mode to register the policy.

Examples

The following example shows that the username of eemuser is associated with a Tcl session:

```
Router# show event manager session cli username

eemuser
```

Related Commands

Command	Description
event manager session cli username	Associates a username with EEM policies that use the CLI library.

show facility-alarm

To display the status of a generated alarm, use the **show facility-alarm** command in global configuration mode.

show facility-alarm {**status** [*severity*] | **relay**}

Syntax Description

status	Shows facility alarms by status and displays the settings of all user-configurable alarm thresholds.
severity	(Optional) String that identifies the severity of an alarm. The default severity level is informational, which shows all alarms. Severity levels are defined as the following: • 1—Critical. The condition affects service. • 2—Major. Immediate action is needed. • 3—Minor. Minor warning conditions. • 4—Informational. No action is required. This is the default.
relay	Shows facility alarms by relay.

Command Default

All alarms are shown.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.4(4)T	The *severity* argument was added in Cisco IOS Release 12.4(4)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was implemented on the PRE3 for the Cisco 10000 series router.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

When a severity level is configured, statuses of alarms at that level and higher are shown. For example, when you set a severity of major, all major and critical alarms are shown.

Examples

The following is a sample output from the **show facility-alarm status** command:

```
Router# show facility-alarm status
```

```
System Totals  Critical:1  Major:0  Minor:0
Source              Severity     Description [Index]
------              --------     -------------------
Fa0/0               CRITICAL     Physical Port Link Down [0]
Fa1/0               INFO         Physical Port Administrative State Down [1]
```

The following is a sample output from the **show facility-alarm status** command with a severity level set at major:

```
Router# show facility-alarm status major

System Totals  Critical:1  Major:0  Minor:0

Source              Severity     Description [Index]
------              --------     -------------------
Fa0/0               CRITICAL     Physical Port Link Down [0]
```

Table 31 describes the significant fields shown in the displays.

Table 31 show facility-alarm status Field Descriptions

Field	Description
System Totals	Total number of alarms generated, identified by severity.
Source	Interface from which the alarm was generated.
Severity	Severity level of the alarm generated.
Description [Index]	Type of the alarm and the index of the alarm type. The index can be any number based on the number of alarm types that the device supports.

Related Commands

Command	Description
clear facility-alarm	Clears alarm conditions and resets the alarm contacts.
facility-alarm	Configures threshold temperatures for minor, major, and critical alarms.

show ip director default

To verify default metric configuration information for DistributedDirector metrics, use the **show ip director default** command in privileged EXEC mode.

show ip director default [**priority** | **weight**]

Syntax Description

priority	(Optional) Default priorities for metrics.
weight	(Optional) Displays the weights for metrics.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

Use this command to verify default metric configurations.

Examples

The following is sample output from the **show ip director default priority** command:

```
Router# show ip director default priority

Director default metric priorities:
random priority = 2
DRP route lookup external to AS priority = 1
administrative preference priority = 0
DRP route lookup internal to AS priority = 0
DRP distance to associated server priority = 0
portion priority = 0
Round-trip time from DRP to client priority = 0
DFP originated weight priority = 0
Route-map evaluation priority = 0
```

Related Commands

Command	Description
ip director default priorities	Sets default priorities for DistributedDirector metrics.

show ip director dfp

To display information about the current status of the DistributedDirector connections with a particular Dynamic Feedback Protocol (DFP) agent, use the **show ip director dfp** command in EXEC mode.

show ip director dfp [*host-name* | *ip-address*]

Syntax Description

host-name	(Optional) Host name.
ip-address	(Optional) IP address.

Command Modes

EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show ip director dfp** command:

```
Router# show ip director dfp

172.24.9.9:
    Max retries: 5
    Timeout between connect attempts: 60
    Timeout between updates: 90
    Last update received: 00:00:12 ago
    Server  Port BindID Address Mask
    172.28.9.9 80 0  0.0.0.0 0.0.0.0
192.168.25.25
    Max retries: 5
    Timeout between connect attempts: 60
    Timeout between updates: 90
    Last update received: 00:00:44 ago
    Server Port BindIDAddress Mask
    192.168.30.30 800 0.0.0.0 0.0.0.0
```

show ip director drp

To display information that the DistributedDirector has about specific Director Response Protocol (DRP) agents, use the **show ip director drp** command in privileged EXEC mode.

show ip director drp [*host-name* | *ip-address*]

Syntax Description

host-name	(Optional) DRP hostname.
ip-address	(Optional) DRP IP address.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **show ip director drp** command displays host-specific statistics, such as the number of queries received and the number of replies sent for a host.

Examples

The following is sample output from the **show ip director drp** command:

```
Router# show ip director drp

DRP agent 172.21.34.2:
    14 requests, 6 replies, 4 requeries, 0 bad replies
    Supported Servers:
    172.21.34.10
    172.21.34.11
DRP agent 192.168.34.2:
    14 requests, 6 replies, 4 requeries, 0 bad replies
    Supported servers:
    192.168.34.10
```

show ip drp

To display information about the Director Response Protocol (DRP) Server Agent for DistributedDirector, use the **show ip drp** command in user EXEC or privileged EXEC mode.

show ip drp

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show ip drp** command:

```
Router# show ip drp

Director Responder Protocol Agent is enabled
717 director requests, 712 successful lookups, 5 failures, 0 no route
Authentication is enabled, using “test” key-chain
```

Table 32 describes the significant fields shown in the display.

Table 32 show ip drp Field Descriptions

Field	Description
director requests	Number of DRP requests that have been received (including any using authentication key-chain encryption that failed).
successful lookups	Number of successful DRP lookups that produced responses.
failures	Number of DRP failures (for various reasons including authentication key-chain encryption failures).

Related Commands

Command	Description
ip drp access-group	Controls the sources of DRP queries to the DRP server agent.
ip drp authentication key-chain	Configures authentication on the DRP server agent for DistributedDirector.

show ip drp boomerang

To display the status of various boomerang domains, use the **show ip drp boomerang** command in privileged EXEC mode.

show ip drp boomerang [*domain-name*]

Syntax Description

domain-name	(Optional) Specified domain name.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **show ip drp boomerang** command can be used on the boomerang client to display the status of the various boomerang domains. The following information can be shown for each domain:

- Alias information—The number of DNS requests for each alias.
- Content server address information:
  - Number of DNS requests.
  - Number of requests dropped because server is down.
  - Number of requests dropped because there is no original server.
  - Number of requests dropped because of security failures.

Examples

The following is sample output from the **show ip drp boomerang** command:

```
Router# show ip drp boomerang www.boom1.com

DNS packets with unknown domain 0

  Domain www.boom1.com
    Content server            172.16.101.101 up
    Origin server                    0.0.0.0
    DNS A record requests                  0
    Dropped (server down)                  0
    Dropped (no origen server)             0
    Security failures                      0

  Alias www.boom2.com
    DNS A record requests                  0
```

Related Commands

Command	Description
alias (boomerang configuration)	Configures an alias name for a specified domain.
ip drp domain	Adds a new domain to the DistributedDirector client or configures an existing domain and puts the client in boomerang configuration mode.
server (boomerang configuration)	Configures the server address for a specified boomerang domain.
show ip drp	Displays DRP statistics on DistributedDirector or a DRP server agent.
ttl dns	Configures the number of seconds for which an answer received from the boomerang client will be cached by the DNS client.
ttl ip	Configures the IP TTL value for the boomerang response packets sent from the boomerang client to the DNS client in number of hops.

show ip http client

To display a report about the HTTP client, use the **show ip http client** command in user EXEC or privileged EXEC mode.

show ip http client {**all** | **cache** | **connection** | **history** | **secure status** | **session-module** | **statistics**}

Syntax Description

all	Displays a report that contains all of the information available about the HTTP client: status (enabled or disabled), registered application or session modules, active connections, cache, history, and statistics.
cache	Displays a list of information about the HTTP client cache.
connection	Displays HTTP client active connections and configured values for connections.
history	Displays a list of up to 20 URLs most recently accessed by the HTTP client.
secure status	Displays the status of the secure HTTP client configuration. **Note** This keyword is not supported with Cisco IOS Release 12.2(31)SB2.
session-module	Displays a report about sessions or applications that have registered with the HTTP client.
statistics	No statistics are collected for the HTTP client. This feature will be implemented at a later date.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. The **all**, **cache**, and **statistics** keywords were added.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to display information about the HTTP client.

Note The secure HTTP (HTTPS) server is not supported in Cisco IOS Release 12.2(31)SB.

Examples

The following is sample output from the **show ip http client cache** command:

```
Router# show ip http client cache

HTTP client cache:
Maximum Memory size for cache    : 100000 bytes (default)
Maximum memory per cache entry   : 2000 bytes (default)
```

```
Memory used                      : 1381 bytes
Memory Available                 : 98619 bytes
Cache Ager interval              : 5 minutes (default)
Total entries created            : 2
Id    Type    Url              Memory-size(Bytes)     Refcnt     Valid(Sec)
__________________________________________________________________________
  536  Hdr   172.25.125.69/              673            0       -1
  32   Hdr   172.25.125.7:8888/          708            0       -1
```

The report is self-explanatory and lists information about the cache.

The following is sample output from the **show ip http client connection** command:

```
Router# show ip http client connection

HTTP client current connections:
    Persistent connection = enabled (default)
    Connection establishment timeout = 10s (default)
    Connection idle timeout = 30s (default)
    Maximum number of connection establishment retries = 1 (default)
    Maximum http client connections per host : 2
    HTTP secure client capability: Not present

    local-ipaddress:port  remote-ipaddress:port in-bytes   out-bytes
                          :80    172.20.67.174:11012 12584      176

    Total client connections : 1
```

The report is self-explanatory and lists the active connections and user-configured or default values for the connections.

The following is sample output from the **show ip http client history** command:

```
Router# show ip http client history

HTTP client history:
        GET 03:25:36 UTC Thu Feb 26 2004
mailer.cisco.com/mailer.html
        GET 03:25:56 UTC Thu Feb 26 2004
mailer.cisco.com/mailer.html
        GET 03:26:10 UTC Thu Feb 26 2004
mailer.cisco.com/mailer.html
```

The report is self-explanatory and lists the most recent URLs accessed by the HTTP client.

The following is sample output from the **show ip http client secure status** command:

```
Router# show ip http client secure status

HTTP secure client ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure client trustpoint: TP-1
```

Table 33 describes the significant fields shown in the display.

Table 33 show ip http client secure status Field Descriptions

Field	Description
HTTP secure client ciphersuite:	Displays the configuration of the **ip http client secure-ciphersuite** command.
HTTP secure client trustpoint:	Displays the configuration of the **ip http client secure-trustpoint** command.

The following is sample output from the **show ip http client session-module** command:

```
Router# show ip http client session-module

HTTP client application session modules:
Id                 :1
Application Name :HTTP CFS
Version            :HTTP/1.1
Persistent         :non-persistent
Response-timeout :0
Retries            :0
Proxy              :

Id                 :6
Application Name :httpc_ifs_0
Version            :HTTP/1.1
Persistent         :non-persistent
Response-timeout :16
Retries            :0
Proxy              :
```

Table 34 describes the fields shown in the display.

Related Commands

Table 34 show ip http client session-module Field Descriptions

Field	Description
Id	A number that identifies the registering application. Every application or session that registers with the HTTP client is provided an identification number.
Application Name	Name of the application in use. Every application or session that registers with the HTTP client provides a name that is displayed by this field. In the sample output, HTTP CFS is the name for the HTTP Client File Session (CFS) application, and the name httpc_ifs_0 is the HTTP client (HTTPC) Cisco IOS File System (IFS) Copy application.
Version	HTTP protocol version supported by the application. Every application or session that registers with the HTTP client indicates the HTTP protocol version it supports in this field. HTTP 1.0 does not support persistent connections; HTTP 1.1 supports both persistent and nonpersistent connections.
Persistent	Value of the persistent connection. Persistent indicates that the application needs the HTTP client to maintain connection after data transfer from itself to the remote server. Nonpersistent indicates that the application does not need the HTTP client to maintain connections after the data transfer.
Response-timeout	Configured response timeout period, in seconds. The application specifies the amount of time the HTTP client has to wait for a response from the remote server before returning a failure notice, for those data transfers initiated by this application.

Table 34 show ip http client session-module Field Descriptions (continued)

Field	Description
Retries	Configured connection retries. The application specifies the number of retries for establishing connection that the HTTP client must attempt before returning a failure notice to the application.
Proxy	Specifies a proxy name that the HTTP client uses to route all HTTP data transfer requests to or from the application.

Related Commands

Command	Description
copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
debug ip http client	Enables debugging output for the HTTP client.
ip http client connection	Configures the HTTP client connection.
ip http client password	Configures a password for all HTTP client connections.
ip http client proxy-server	Configures an HTTP proxy server.
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.

show ip http client connection

To display a report about HTTP client active connections, use the **show ip http client connection** command in privileged EXEC mode.

show ip http client connection

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to display active connections and configured values for connections.

Examples

The following is sample output from the **show ip http client connection** command:

```
Router# show ip http client connection

HTTP client current connections:
    Persistent connection = enabled (default)
    Connection establishment timeout = 10s (default)
    Connection idle timeout = 30s (default)
    Maximum number of connection establishment retries = 1 (default)
    Maximum http client connections per host : 2
    HTTP secure client capability: Not present

    local-ipaddress:port  remote-ipaddress:port in-bytes   out-bytes
                          :80    172.20.67.174:11012 12584      176

    Total client connections : 1
```

The report is self-explanatory and lists the active connections and user-configured or default values for the connections.

Related Commands

Command	Description
copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
debug ip http client	Enables debugging output for the HTTP client.
ip http client connection	Configures the HTTP client connection.
ip http client password	Configures a password for all HTTP client connections.
ip http client proxy-server	Configures an HTTP proxy server.
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.
show ip http client history	Displays the URLs accessed by the HTTP client.
show ip http client session-module	Displays a report about sessions that have registered with the HTTP client.

show ip http client history

To display up to 20 URLs accessed by the HTTP client, use the **show ip http client history** command in privileged EXEC mode.

show ip http client history

Syntax Description

This command has no arguments or keywords

Defaults

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command displays a list of up to 20 URLs most recently accessed by the HTTP client.

Examples

The following is sample output from the **show ip http client history** command:

```
Router# show ip http client history

HTTP client history:
        GET 03:25:36 UTC Thu Feb 26 2004
mailer.cisco.com/mailer.html
        GET 03:25:56 UTC Thu Feb 26 2004
mailer.cisco.com/mailer.html
        GET 03:26:10 UTC Thu Feb 26 2004
mailer.cisco.com/mailer.html
```

The report is self-explanatory and lists the most recent URLs accessed by the HTTP client.

Related Commands

Command	Description
copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
debug ip http client	Enables debugging output for the HTTP client.
ip http client connection	Configures the HTTP client connection.
ip http client password	Configures a password for all HTTP client connections.

Command	Description
ip http client proxy-server	Configures an HTTP proxy server.
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.
show ip http client connection	Displays a report about HTTP client active connections.
show ip http client session-module	Displays a report about sessions that have registered with the HTTP client.

show ip http client secure status

To display the status of the secure HTTP client configuration, use the **show ip http client secure status** command in privileged EXEC mode.

show ip http client secure status

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Examples

The following is sample output from the **show ip http client secure status** command:

```
Router# show ip http client secure status

HTTP secure client ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure client trustpoint: TP-1
```

Table 35 describes the significant fields shown in the display.

Table 35 show ip http client secure status Field Descriptions

Field	Description
HTTP secure client ciphersuite:	Displays the configuration of the **ip http client secure-ciphersuite** command.
HTTP secure client trustpoint:	Displays the configuration of the **ip http client secure-trustpoint** command.

Related Commands

Command	Description
ip http client secure-ciphersuite	Specifies the CipherSuites that should be used for encryption over the secure HTTP connection from the client to a remote server.
ip http client secure-trustpoint	Specifies the CA trustpoint that should be used if the remote HTTP server requests client authentication.

show ip http client session-module

To display a report about sessions or applications that have registered with the HTTP client, use the **show ip http client session-module** command in privileged EXEC mode.

show ip http client session-module

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to display information about applications that have registered with the HTTP client.

Examples

The following is sample output from the **show ip http client session-module** command:

```
Router# show ip http client session-module

HTTP client application session modules:
Id               :1
Application Name :HTTP CFS
Version          :HTTP/1.0
Persistent       :non-persistent
Response-timeout :0
Retries          :0
Proxy            :

Id               :6
Application Name :httpc_ifs_0
Version          :HTTP/1.1
Persistent       :non-persistent
Response-timeout :16
Retries          :0
Proxy            :
```

Table 36 describes the fields shown in the display.

Table 36 show ip http client session-module Field Descriptions

Field	Description
Id	A number that identifies the registering application. Every application or session that registers with the HTTP client is provided an identification number.
Application Name	Name of the application in use. Every application or session that registers with the HTTP client provides a name that is displayed by this field. In the sample output, HTTP CFS is the name for the HTTP Client File Session application, and the name httpc_ifs_0 is the HTTPC IFS Copy application.
Version	HTTP protocol version supported by the application. Every application or session that registers with the HTTP client indicates the HTTP protocol version it supports in this field. HTTP1.0 does not support persistent connections; HTTP1.1 supports both persistent and nonpersistent connections.
Persistent	Value of the persistent connection. Persistent indicates that the application needs the HTTP client to maintain connection after data transfer from itself to the remote server. Nonpersistent indicates that the application does not need the HTTP client to maintain connections after the data transfer.
Response-timeout	Configured response timeout period, in seconds. The application specifies the amount of time the HTTP Client has to wait for a response from the remote server before returning a failure notice, for those data transfers initiated by this application.
Retries	Configured connection retries. The application specifies the number of retries for establishing connection that the HTTP client must attempt before returning a failure notice to the application.
Proxy	Specifies a proxy name that the HTTP client uses to route all HTTP data transfer requests to or from the application.

Related Commands

Command	Description
copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
debug ip http client	Enables debugging output for the HTTP client.
ip http client connection	Configures the HTTP client connection.
ip http client password	Configures a password for all HTTP client connections.
ip http client proxy-server	Configures an HTTP proxy server.
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.
show ip http client connection	Displays a report about HTTP client active connections.
show ip http client history	Displays the URLs accessed by the HTTP client.

show ip http help-path

To display the current complete configured path of help files for use by the user's current GUI screen, use the **show ip http help-path** command in user EXEC or privileged EXEC mode.

show ip http help-path

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

Use this command to display the current complete help path configured in the HTTP server. This path is expected to hold help files relating to the user's current GUI screen.

Examples

The following is sample output from the **show ip http help-path** command:

```
Router# show ip http help-path

http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/ivory/1100
```

Related Commands

Command	Description
ip http help-path	Configures the HTTP help-root URL.

show ip http server

To display details about the current configuration of the HTTP server, use the **show ip http server** command in user EXEC or privileged EXEC mode.

show ip http server {**all** | **status** | **session-module** | **connection** | **statistics** | **history**}

Syntax Description

all	Displays all HTTP server information.
status	Displays only HTTP server status configuration.
session-module	Displays only supported HTTP services (Cisco IOS modules).
connection	Displays only the current connections to the HTTP server, including the local and remote IP addresses being accessed.
statistics	Displays only HTTP server connection statistics.
history	Displays only the previous 20 connections to the HTTP server, including the IP address accessed, and the time when the connection was closed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to show detailed status information about the HTTP server.

If the HTTP secure server capability is present, the output of the **show ip http server all** command will also include the information found in the output of the **show ip http server secure status** command.

Note The secure HTTP (HTTPS) server is not supported in Cisco IOS Release 12.2(31)SB.

Examples

The following is sample output from the **show ip http server all** command:

```
Router# show ip http server all

HTTP server status: Enabled
HTTP server port: 80
HTTP server authentication method: enable
HTTP server access class: 0
HTTP server base path:
Maximum number of concurrent server connections allowed: 5
Server idle time-out: 30 seconds
Server life time-out: 120 seconds
```

```
Maximum number of requests allowed on a connection: 2
HTTP secure server capability: Not Present
HTTP server application session modules:
 Session module Name  Handle  Description
Homepage_Server       5       IOS Homepage Server
QDM                   2       QOS Device Manager Server
HTTP IFS Server       1       HTTP based IOS File Server
QDM SA                3       QOS Device Manager Signed Applet Server
WEB_EXEC              4       HTTP based IOS EXEC Server
XSM                   6       XML Session Manager
VDM                   7       VPN Device Manager Server
ITS                   8       IOS Telephony Service
ITS_LOCDIR            9       ITS Local Directory Search

HTTP server current connections:
local-ipaddress:port   remote-ipaddress:port in-bytes  out-bytes
  172.19.254.37:80     192.168.254.45:33737  70        2294

HTTP server statistics:
Accepted connections total: 1360

HTTP server history:
local-ipaddress:port  remote-ipaddress:port  in-bytes  out-bytes  end-time
  172.19.254.37:80     192.168.254.45:63530  60        1596       10:50:00 12/19
```

Table 37 describes the significant fields shown in the display.

Table 37 show ip http server Field Descriptions

Field	Description
HTTP server status:	Enabled or disabled. Corresponds to the [**no**] **ip http server** command.
HTTP server port:	Port used by the HTTP server. Corresponds to the **ip http port** command.
HTTP server authentication method:	Authentication method used for HTTP server logins. Corresponds to the **ip http authentication** command.
HTTP server access class:	Access list number assigned to the HTTP server. A value of zero (0) indicates no access list is assigned. Corresponds to the **ip http access-class** command.
HTTP server base path:	Base HTTP path specifying the location of the HTTP server files (HTML files). Corresponds to the **ip http path** command.
Maximum number of concurrent server connections allowed:	Corresponds to the **ip http max-connections** command.
Server idle time-out:	The maximum number of seconds the connection will be kept open if no data is received or if response data can not be sent out. Corresponds to the **ip http timeout-policy** command.
Server life time-out:	The maximum number of seconds the connection will be kept open. Corresponds to the **ip http timeout-policy** command.
Maximum number of requests allowed on a connection:	The maximum number of requests that will be processed on a connection before the connection is closed. Corresponds to the **ip http timeout-policy** command.

Table 37 show ip http server Field Descriptions (continued)

Field	Description
HTTP secure server capability:	Indicates if the running software image supports the secure HTTP server (“Present” or “Not Present”). If the capability is present, the output from the **show ip http server secure status** command will appear after this line.
HTTP server application session modules:	Cisco IOS services that use the HTTP server. Services are provided for application interfaces, including: • The Cisco Web browser user interface, which uses the Cisco IOS Homepage Server, HTTP-based EXEC Server, and HTTP IOS File System (IFS) Server • The VPN Device Manager (VDM) application, which uses the VDM Server and the XML Session Manager (XSM) • The QoS Device Manager (QDM) application, which uses the QDM Server • The IP Phone and Cisco IOS Telephony Service applications, which use the ITS Local Directory Search and IOS Telephony Server (ITS) **Note** The IP Phone and Telephony Service applications use the ITS Local Directory Search and IOS Telephony Server (ITS). Therefore, these two applications are not supported with Cisco IOS Release 12.2(31)SB2.
HTTP server current connections:	Currently active HTTP connections.
HTTP server statistics:	How many connections have been accepted.
HTTP server history:	Details about the last 20 connections, including the time the connection was closed (endtime). Endtime is given in Universal Coordinated Time (UTC or GMT), using a 24-hour clock and the following format: *hh*:*mm*:*ss month*/*day*

The following example shows sample output for the **show ip http server status** command:

```
Router# show ip http server status

HTTP server status: Disabled
HTTP server port: 80
HTTP server authentication method: enable
HTTP server access class: 0
HTTP server base path:
Maximum number of concurrent server connections allowed: 5
Server idle time-out: 600 seconds
Server life time-out: 600 seconds
Maximum number of requests allowed on a connection: 1
HTTP secure server capability: Present
HTTP secure server status: Disabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:
```

The lines indicating the status of the HTTP secure (HTTPS) server will only be visible if your software image supports the HTTPS server. If your software image does not support SSL, only the following line will be visible:

HTTP secure server capability: Not present

Related Commands

Command	Description
debug ip http server all	Enables debugging output for all HTTP processes on the system.
ip http secure-server	Enables the HTTPS server.
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.
show ip http server secure status	Displays the status of the HTTPS server.

show ip http server secure status

To display the status of the HTTP secure server configuration, use the **show ip http server secure status** command in privileged EXEC mode.

show ip http server secure status

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Examples

The following is sample output from the **show ip http server secure status** command:

```
Router# show ip http server secure status

HTTP secure server status: Enabled
HTTP secure server port: 1025
HTTP secure server ciphersuite: rc4-128-sha rc4-128-md5
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint: CA-trust-local
```

Table 38 describes the significant fields shown in the display.

Table 38 show ip http server secure status Field Descriptions

Field	Description
HTTP secure server status:	Displays the state of secure HTTP server (“Enabled” or “Disabled”). Corresponds to the configuration of the **ip http secure-server** command.
HTTP secure server port:	Displays the configuration of the **ip http secure-port** command.
HTTP secure server ciphersuite:	Displays the configuration of the **ip http secure-ciphersuite** command.

Table 38 show ip http server secure status Field Descriptions (continued)

Field	Description
HTTP secure server client authentication:	Displays the configuration of the **ip http secure-client-auth** command.
HTTP secure server trustpoint:	Displays the configuration of the **ip http secure-trustpoint** command. If no trustpoint is configured, the line will appear blank after the colon.

Related Commands

Command	Description
ip http secure-ciphersuite	Specifies the CipherSuites that should be used for encryption over the secure HTTP connection from the server to a remote client.
ip http secure-client-auth	Configures the HTTP server to authenticate the remote client during the connection process.
ip http secure-port	Specifies the port (socket) to be used for HTTPS connections.
ip http secure-server	Enables the HTTPS server.
ip http secure-trustpoint	Specifies the CA trustpoint that should be used for obtaining signed certificates for the secure HTTP server.

show kron schedule

To display the status and schedule information of Command Scheduler occurrences, use the **show kron schedule** command in user EXEC or privileged EXEC mode.

show kron schedule

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **show kron schedule** command to view all currently configured occurrences and when they are next scheduled to run.

Examples

The following sample output displays each configured policy name and the time interval before the policy is scheduled to run:

```
Router# show kron schedule

Kron Occurrence Schedule
week inactive, will run again in 7 days 01:02:33
may inactive, will run once in 32 days 20:43:31 at 6:30 on Jun 20
```

Table 39 describes the significant fields shown in the display.

Table 39 show kron schedule Field Descriptions

Field	Description
week inactive	The policy list named week is currently inactive.
run again in 7 days 01:02:33	Time in days, hours, minutes and seconds before the policy will run. This policy is scheduled to run on a recurring basis.
run once in 32 days 20:43:31	Time in days, hours, minutes and seconds before the policy will run. This policy is scheduled to run just once.

Related Commands

Command	Description
kron occurrence	Specifies schedule parameters for a Command Scheduler occurrence and enters kron-occurrence configuration mode.
policy-list	Specifies the policy list associated with a Command Scheduler occurrence.

show logging

To display the state of system logging (syslog) and the contents of the standard system logging buffer, use the **show logging** command in privileged EXEC mode.

show logging [**slot** *slot-number* | **summary**]

Syntax Description

slot *slot-number*	(Optional) Displays information in the syslog history table for a specific line card. Slot numbers range from 0 to 11 for the Cisco 12012 Internet router and 0 to 7 for the Cisco 12008 Internet router.
summary	(Optional) Displays counts of messages by type for each line card.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.2 GS	The **slot** and **summary** keywords were added for the Cisco 12000.
12.2(8)T	Command output was expanded to show the status of the logging count facility (“Count and time-stamp logging messages”).
12.2(15)T	Command output was expanded to show the status of XML syslog formatting.
12.3(2)T	Command output was expanded (on supported software images) to show details about the status of system logging processed through the Embedded Syslog Manager (ESM). These lines appear as references to “filtering” or “filter modules”.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	Command-line interface (CLI) output was modified to show message discriminators defined at the router and syslog sessions associated with those message discriminators.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command displays the state of syslog error and event logging, including host addresses, and which logging destinations (console, monitor, buffer, or host) logging is enabled. This command also displays Simple Network Management Protocol (SNMP) logging configuration parameters and protocol activity.

This command will also display the contents of the standard system logging buffer, if logging to the buffer is enabled. Logging to the buffer is enabled or disabled using the [**no**] **logging buffered** command. The number of system error and debugging messages in the system logging buffer is determined by the configured size of the syslog buffer. This size of the syslog buffer is also set using the **logging buffered** command.

To enable and set the format for syslog message time stamping, use the **service timestamps log** command.

If debugging is enabled (using any **debug** command), and the logging buffer is configured to include level 7 (debugging) messages, debug output will be included in the system log. Debugging output is not formatted like system error messages and will not be preceded by the percent symbol (%).

Examples

The following is sample output from the **show logging** command on a software image that supports the Embedded Syslog Manager (ESM) feature:

```
Router# show logging

Syslog logging: enabled (10 messages dropped, 5 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)
    Console logging: level debugging, 31 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: disabled
    Buffer logging: level errors, 36 messages logged, xml disabled,
                    filtering disabled
    Logging Exception size (8192 bytes)
    Count and timestamp logging messages: disabled

No active filter modules.


    Trap logging: level informational, 45 message lines logged

Log Buffer (8192 bytes):
```

The following example shows output from the **show logging** command after a message discriminator has been configured. Included in this example is the command to configure the message discriminator.

```
c7200-3(config)# logging discriminator ATTFLTR1 severity includes 1,2,5 rate-limit 100

Specified MD by the name ATTFLTR1 is not found.
Adding new MD instance with specified MD attribute values.

Router(config)# end
Router#

000036: *Oct 20 16:26:04.570: %SYS-5-CONFIG_I: Configured from console by console

Router# show logging

Syslog logging: enabled (11 messages dropped, 0 messages rate-limited,
    0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

Inactive Message Discriminator:
ATTFLTR1  severity group includes 1,2,5
    rate-limit not to exceed 100 messages per second

Console logging: level debugging, 25 messages logged, xml disabled, filtering disabled
Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled
Buffer logging:  level debugging, 25 messages logged, xml disabled, filtering disabled
Logging Exception size (8192 bytes)
Count and timestamp logging messages: disabled

No active filter modules.
```

```
Trap logging: level debugging, 28 message lines logged
Logging to 172.25.126.15  (udp port 1300,  audit disabled, authentication disabled,
    encryption disabled, link up),
    28 message lines logged,
    0 message lines rate-limited,
    0 message lines dropped-by-MD,
    xml disabled, sequence number disabled
    filtering disabled
Logging to 172.25.126.15  (tcp port 1307,  audit disabled, authentication disabled,
    encryption disabled, link up),
    28 message lines logged,
    0 message lines rate-limited,
    0 message lines dropped-by-MD,
    xml disabled, sequence number disabled, filtering disabled
Logging to 172.20.1.1  (udp port 514,  audit disabled,
    authentication disabled, encryption disabled, link up),
    28 message lines logged,
    0 message lines rate-limited,
    0 message lines dropped-by-MD,
    xml disabled, sequence number disabled
    filtering disabled

Log Buffer (1000000 bytes):
```

Table 40 describes the significant fields shown in the output for the two preceding examples.

Table 40 show logging Field Descriptions

Field	Description
Syslog logging:	Shows general state of system logging (enabled or disabled), the status of logged messages (number of messages dropped, rate-limited, or flushed), and whether XML formatting or ESM filtering is enabled.
No Active Message Discriminator	Indicates that a message discriminator is not being used.
Inactive Message Discriminator:	Identifies a configured message discriminator that has not been invoked.
Console logging:	Logging to the console port. Shows "disabled" or, if enabled, the severity level limit, number of messages logged, and whether XML formatting or ESM filtering is enabled. Corresponds to the configuration of the **logging console**, **logging console xml**, or **logging console filtered** command.
Monitor logging:	Logging to the monitor (all TTY lines). Shows "disabled" or, if enabled, the severity level limit, number of messages logged, and whether XML formatting or ESM filtering is enabled. Corresponds to the configuration of the **logging monitor**, **logging monitor xml**, or **logging monitor filtered** command.
Buffer logging:	Logging to the standard syslog buffer. Shows "disabled" or, if enabled, the severity level limit, number of messages logged, and whether XML formatting or ESM filtering is enabled. Corresponds to the configuration of the **logging buffered**, **logging buffered xml**, or **logging buffered filtered** command.

Table 40 show logging Field Descriptions (continued)

Field	Description
Trap logging:	Logging to a remote host (syslog collector). Shows "disabled" or, if enabled, the severity level limit, number of messages logged, and whether XML formatting or ESM filtering is enabled. (The word "trap" means a trigger in the system software for sending error messages to a remote host.) Corresponds to the configuration of the **logging host** command. The severity level limit is set using the **logging trap** command.
SNMP logging	Displays whether SNMP logging is enabled, the number of messages logged, and the retransmission interval. If not shown on your platform, use the **show logging history** command.
Logging Exception size (8192 bytes)	Corresponds to the configuration of the **logging exception** command.
Count and timestamp logging messages:	Corresponds to the configuration of the **logging count** command.
No active filter modules.	Appears if no syslog filter modules are configured with the **logging filter** command. Syslog filter modules are Tcl script files used when the Embedded Syslog Manager (ESM) is enabled. ESM is enabled when any of the **filtered** keywords are used in the logging commands. If configured, the URL and filename of configured syslog filter modules will appear at this position in the output. Syslog filter modules are executed in the order in which they appear here.
Log Buffer (8192 bytes):	The value in parentheses corresponds to the configuration of the **logging buffered** *buffer-size* command. If no messages are currently in the buffer, the output ends with this line. If messages are stored in the syslog buffer, they appear after this line.

The following example shows that syslog messages from the system buffer are included, with time stamps. In this example, the software image does not support XML formatting or ESM filtering of syslog messages.

```
Router# show logging

Syslog logging:enabled (2 messages dropped, 0 flushes, 0 overruns)
    Console logging:disabled
    Monitor logging:level debugging, 0 messages logged
    Buffer logging:level debugging, 4104 messages logged
    Trap logging:level debugging, 4119 message lines logged
        Logging to 192.168.111.14, 4119 message lines logged
Log Buffer (262144 bytes):

Jul 11 12:17:49 EDT:%BGP-4-MAXPFX:No. of prefix received from 209.165.200.225
(afi 0) reaches 24, max 24
! THE FOLLOWING LINE IS A DEBUG MESSAGE FROM NTP.
! NOTE THAT IT IS NOT PRECEEDED BY THE % SYMBOL.
Jul 11 12:17:48 EDT: NTP: Maxslew = 213866
Jul 11 15:15:41 EDT:%SYS-5-CONFIG:Configured from
tftp://host.com/addc5505-rsm.nyiix
.Jul 11 15:30:28 EDT:%BGP-5-ADJCHANGE:neighbor 209.165.200.226 Up
```

```
.Jul 11 15:31:34 EDT:%BGP-3-MAXPFXEXCEED:No. of prefix received from
209.165.200.226 (afi 0):16444 exceed limit 375
.Jul 11 15:31:34 EDT:%BGP-5-ADJCHANGE:neighbor 209.165.200.226 Down BGP
Notification sent
.Jul 11 15:31:34 EDT:%BGP-3-NOTIFICATION:sent to neighbor 209.165.200.226 3/1
(update malformed) 0 bytes
 .
 .
 .
```

The software clock keeps an “authoritative” flag that indicates whether the time is authoritative (believed to be accurate). If the software clock has been set by a timing source (for example, via NTP), the flag is set. If the time is not authoritative, it will be used only for display purposes. Until the clock is authoritative and the “authoritative” flag is set, the flag prevents peers from synchronizing to the software clock.

Table 41 describes the symbols that precede the time stamp.

Table 41 Time Stamping Symbols for syslog Messages

Symbol	Description	Example
*	Time is not authoritative: the software clock is not in sync or has never been set.	*15:29:03.158 UTC Tue Feb 25 2003:
(blank)	Time is authoritative: the software clock is in sync or has just been set manually.	15:29:03.158 UTC Tue Feb 25 2003:
.	Time is authoritative, but NTP is not synchronized: the software clock was in sync, but has since lost contact with all configured NTP servers.	.15:29:03.158 UTC Tue Feb 25 2003:

The following is sample output from the **show logging summary** command for a Cisco 12012 router. A number in the column indicates that the syslog contains that many messages for the line card. For example, the line card in slot 9 has 1 error message, 4 warning messages, and 47 notification messages.

Note For similar log counting on other platforms, use the **show logging count** command.

```
Router# show logging summary

+-----+-------+-------+-------+-------+-------+-------+-------+-------+
 SLOT | EMERG | ALERT | CRIT  | ERROR |WARNING| NOTICE| INFO  | DEBUG |
+-----+-------+-------+-------+-------+-------+-------+-------+-------+
|* 0* |     . |     . |     . |     . |     . |     . |     . |     . |
|  1  |       |       |       |       |       |       |       |       |
|  2  |       |       |       |     1 |     4 |    45 |       |       |
|  3  |       |       |       |       |       |       |       |       |
|  4  |       |       |       |     5 |     4 |    54 |       |       |
|  5  |       |       |       |       |       |       |       |       |
|  6  |       |       |       |       |       |       |       |       |
|  7  |       |       |       |    17 |     4 |    48 |       |       |
|  8  |       |       |       |       |       |       |       |       |
|  9  |       |       |       |     1 |     4 |    47 |       |       |
| 10  |       |       |       |       |       |       |       |       |
| 11  |       |       |       |    12 |     4 |    65 |       |       |
+-----+-------+-------+-------+-------+-------+-------+-------+-------+
Router#
```

Table 42 describes the logging level fields shown in the display.

Table 42 show logging summary Field Descriptions

Field	Description
SLOT	Indicates the slot number of the line card. An asterisk next to the slot number indicates the GRP card whose error message counts are not displayed. For information on the GRP card, use the **show logging** command.
EMERG	Indicates that the system is unusable.
ALERT	Indicates that immediate action is needed.
CRIT	Indicates a critical condition.
ERROR	Indicates an error condition.
WARNING	Indicates a warning condition.
NOTICE	Indicates a normal but significant condition.
INFO	Indicates an informational message only.
DEBUG	Indicates a debugging message.

Related Commands

Command	Description
clear logging	Clears messages from the logging buffer.
logging count	Enables the error log count capability.
logging history size	Changes the number of syslog messages stored in the history table of the router.
logging linecard	Logs messages to an internal buffer on a line card and limits the logging messages displayed on terminal lines other than the console line to messages with a level at or above level.
service timestamps	Configures the system to time-stamp debugging or logging messages.
show logging count	Displays a summary of system error messages (syslog messages) by facility and severity.
show logging xml	Displays the state of system logging and the contents of the XML-specific logging buffer.

show logging onboard (Cat 6K)

To display onboard failure logs (OBFL) on Cisco Catalyst 6000 series switches, use the **show logging onboard** command in privileged EXEC mode.

show logging onboard [**module** *module-number*] [**status** | [[**temperature** | **uptime** | **message**] [[**continuous** [**start** *start-time-and-date*] [**end** *end-time-and-date*]] | [**detail** [**start** *start-time-and-date*] [**end** *end-time-and-date*]] | [**summary**]]]]

Syntax Description

module *module-number*	(Optional) Specifies the module number.
status	(Optional) Displays the platform and CLI enable status for each of the test applications (system message, interrupt, temperature, and uptime).
temperature	(Optional) Displays temperature data.
uptime	(Optional) Displays system uptime data.
message	(Optional) Displays system messages collected at the level set by the **hw-module logging onboard** global configuration command.
continuous	(Optional) Can be used with the **message**, **temperature**, and **uptime** keywords to display continuously collected data.
start *start-time-and-date* **end** *end-time-and-date*	(Optional) Specifies a start and end time for **message**, **temperature**, and **uptime** reports. The **start** and **end** keywords can optionally be entered with the **continuous** and **detail** keywords. The **start** and **end** keywords prompt for the time in 24-hour format (hh:mm:ss) followed by the date, the month in three-letter format (Jun for June, as an example), and the year in the range 1993 to 2035. Examples: start 15:01:57 7 Mar 2007 end 15:04:57 14 Mar 2007
detail	(Optional) Can be used with the **message**, **temperature**, and **uptime** keywords to display both summary and continuous data.
summary	(Optional) Displays summary data (default).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

The **show logging onboard** command can be entered without any arguments, which is the same as entering the **show logging onboard summary** command to display summarized information about OBFL for the device residing on the same module where the command is entered.

Use this command to view OBFL data from system hardware. The OBFL feature is enabled by default and records operating temperatures, hardware uptime, interrupts, and other important events and messages that can assist with diagnosing problems with hardware cards (or *modules*) installed in a Cisco router or switch. Data is logged to files stored in nonvolatile memory. When the onboard hardware is started up, a first record is made for each area monitored and becomes a base value for subsequent records.

The OBFL feature provides a circular updating scheme for collecting continuous records and archiving older (historical) records, ensuring accurate data about the system. Data is recorded in one of two formats: continuous information that displays a snapshot of measurements and samples in a continuous file, and summary information that provides details about the data being collected. The message “No historical data to display” is seen when historical data is not available.

See the examples for more information about the type of data collected.

Examples

Temperature

Temperatures surrounding hardware modules can exceed recommended safe operating ranges and cause system problems such as packet drops. Higher than recommended operating temperatures can also accelerate component degradation and affect device reliability. Monitoring temperatures is important for maintaining environmental control and system reliability. Once a temperature sample is logged, the sample becomes the base value for the next record. From that point on, temperatures are recorded either when there are changes from the previous record or if the maximum storage time is exceeded. Temperatures are measured and recorded in degrees Celsius.

The following example shows how you might enter this command:

```
Router# show logging onboard module 2 temperature detail

--------------------------------------------------------------------------------
TEMPERATURE SUMMARY INFORMATION
--------------------------------------------------------------------------------
Number of sensors          : 12
Sampling frequency         : 5 minutes
Maximum time of storage    : 120 minutes
--------------------------------------------------------------------------------
Sensor                            |   ID  | Maximum Temperature 0C
--------------------------------------------------------------------------------
MB-Out                              980201     43
MB-In                               980202     28
MB                                  980203     29
MB                                  980204     38
EARL-Out                            910201     0
EARL-In                             910202     0
SSA 1                               980301     38
SSA 2                               980302     36
JANUS 1                             980303     36
JANUS 2                             980304     35
GEMINI 1                            980305     0
GEMINI 2                            980306     0
---------------------------------------------------------------
Temp                         Sensor ID
0C     1    2    3    4    5    6    7    8    9   10   11   12
---------------------------------------------------------------
No historical data to display
---------------------------------------------------------------
--------------------------------------------------------------------------------
TEMPERATURE CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
Sensor                            |   ID  |
--------------------------------------------------------------------------------
MB-Out                              980201
MB-In                               980202
MB                                  980203
MB                                  980204
EARL-Out                            910201
EARL-In                             910202
SSA 1                               980301
SSA 2                               980302
JANUS 1                             980303
JANUS 2                             980304
GEMINI 1                            980305
GEMINI 2                            980306

-------------------------------------------------------------------------------
       Time Stamp   |Sensor Temperature 0C
MM/DD/YYYY HH:MM:SS |  1    2    3    4    5    6    7    8    9   10   11   12
-------------------------------------------------------------------------------
03/06/2007 22:32:51   31   26   27   27   NA   NA   33   32   30   29   NA   NA
03/06/2007 22:37:51   43   28   29   38   NA   NA   38   36   36   35   NA   NA
-------------------------------------------------------------------------------
```

Table 43 describes the significant fields shown in the display.

Table 43 Temperature Summary Descriptions

Field	Description
Number of sensors	The total number of temperature sensors that will be recorded. A column for each sensor is displayed with temperatures listed under the number of each sensor, as available.
Sampling frequency	The time between measurements.
Maximum time of storage	Determines the maximum amount of time, in minutes, that can pass when the temperature remains unchanged and the data is not saved to storage media. After this time, a temperature record will be saved even if the temperature has not changed.
Sensor column	Lists the name of the sensor.
ID column	Lists an assigned identifier for the sensor.
Maximum Temperature 0C	Shows the highest recorded temperature per sensor.
Temp	Indicates a recorded temperature in degrees Celsius in the historical record. Columns following show the total time each sensor has recorded that temperature.
Sensor ID	An assigned number, so that temperatures for the same sensor can be stored together.
offset	Relative time of peer clock to local clock (in milliseconds).
disp	Dispersion

Operational Uptime

The operational uptime tracking begins when the module is powered on, and information is retained for the life of the module.

The following example shows how you might enter this command:

```
Router# show logging onboard module 2 uptime detail

--------------------------------------------------------------------------------
UPTIME SUMMARY INFORMATION
--------------------------------------------------------------------------------
```

```
First customer power on : 03/06/2007 22:32:51
Total uptime            :   0 years   0 weeks   2 days  18 hours  10 minutes
Total downtime          :   0 years   0 weeks   0 days   8 hours   7 minutes
Number of resets        : 130
Number of slot changes  : 16
Current reset reason    : 0xA1
Current reset timestamp : 03/07/2007 13:29:07
Current slot            : 2
Current uptime          :   0 years   0 weeks   1 days   7 hours   0 minutes
--------------------------------------------------------------------------------
Reset  |        |
Reason | Count  |
--------------------------------------------------------------------------------
0x5         64
0x6         62
0xA1         4
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
UPTIME CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
Time Stamp          | Reset  | Uptime
MM/DD/YYYY HH:MM:SS | Reason | years weeks days hours  minutes
--------------------------------------------------------------------------------
03/06/2007 22:32:51   0xA1      0     0     0     0     0
--------------------------------------------------------------------------------
```

The operational uptime application tracks the following events:

- Date and time the customer first powered on a component.
- Total uptime and downtime for the component in years, weeks, days, hours, and minutes.
- Total number of component resets.
- Total number of slot (module) changes.
- Current reset timestamp to include the date and time.
- Current slot (module) number of the component.
- Current uptime in years, weeks, days, hours, and minutes.
- Reset reason; see Table 44 to translate the numbers displayed.
- Count is the number of resets that have occurred for each reset reason.

Table 44 Reset Reason Codes and Explanations

Reset Reason Code (in hex)	Component/Explanation
0x01	Chassis on
0x02	Line card hot plug in
0x03	Supervisor requests line card off or on
0x04	Supervisor requests hard reset on line card
0x05	Line card requests Supervisor off or on
0x06	Line card requests hard reset on Supervisor
0x07	Line card self reset using the internal system register
0x08	—
0x09	—

Table 44 Reset Reason Codes and Explanations (continued)

Reset Reason Code (in hex)	Component/Explanation
0x0A	Momentary power interruption on the line card
0x0B	—
0x0C	—
0x0D	—
0x0E	—
0x0F	—
0x10	—
0x11	Off or on after Supervisor non-maskable interrupts (NMI)
0x12	Hard reset after Supervisor NMI
0x13	Soft reset after Supervisor NMI
0x14	—
0x15	Off or on after line card asks Supervisor NMI
0x16	Hard reset after line card asks Supervisor NMI
0x17	Soft reset after line card asks Supervisor NMI
0x18	—
0x19	Off or on after line card self NMI
0x1A	Hard reset after line card self NMI
0x1B	Soft reset after line card self NMI
0x21	Off or on after spurious NMI
0x22	Hard reset after spurious NMI
0x23	Soft reset after spurious NMI
0x24	—
0x25	Off or on after watchdog NMI
0x26	Hard reset after watchdog NMI
0x27	Soft reset after watchdog NMI
0x28	—
0x29	Off or on after parity NMI
0x2A	Hard reset after parity NMI
0x2B	Soft reset after parity NMI
0x31	Off or on after system fatal interrupt
0x32	Hard reset after system fatal interrupt
0x33	Soft reset after system fatal interrupt
0x34	—
0x35	Off or on after application-specific integrated circuit (ASIC) interrupt
0x36	Hard reset after ASIC interrupt

Table 44 Reset Reason Codes and Explanations (continued)

Reset Reason Code (in hex)	Component/Explanation
0x37	Soft reset after ASIC interrupt
0x38	—
0x39	Off or on after unknown interrupt
0x3A	Hard reset after unknown interrupt
0x3B	Soft reset after unknown interrupt
0x41	Off or on after CPU exception
0x42	Hard reset after CPU exception
0x43	Soft reset after CPU exception
0xA1	Reset data converted to generic data

Interrupts

Interrupts are generated by system components that require attention from the CPU, such as ASICs and NMIs. Interrupts are generally related to hardware limit conditions or errors that need to be corrected.

The continuous format records each time a component is interrupted, and this record is stored and used as base information for subsequent records. Each time the list is saved, a timestamp is added. Time differences from the previous interrupt are counted, so that technical personnel can gain a complete record of the component's operational history when an error occurs.

The following example shows how you might enter this command:

```
Router# show logging onboard module 2 interrupt detail

--------------------------------------------------------------------------------
INTERRUPT SUMMARY INFORMATION
--------------------------------------------------------------------------------
Name                                              |  ID | Offset | Bit |  Count
--------------------------------------------------------------------------------
No historical data to display
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
CONTINUOUS INTERRUPT INFORMATION
--------------------------------------------------------------------------------
MM/DD/YYYY HH:MM:SS mmm | Name                              |  ID | Offset | Bit
--------------------------------------------------------------------------------
03/06/2007 22:33:06 450   Port-ASIC #2                         9   0x00E7      6
--------------------------------------------------------------------------------
```

Table 45 describes the significant fields shown in the display.

Table 45 Interrupt Summary Information

Field	Description
Name	A description of the component including its position in the device.
ID	An assigned field for data storage.
Offset	The location of the next block in bytes.

Table 45 Interrupt Summary Information (continued)

Field	Description
Bit	The interrupt bit number recorded from the component’s internal register.
The timestamp	Shows the date and time that an interrupt occurred to the millisecond.

Message Logging

The OBFL feature logs standard system messages. Instead of displaying the message to a terminal, the message is written to and stored in a file, so the message can be accessed and read at a later time. System messages range from level 1 alerts to level 7 debug messages, and these levels can be specified in the **hw module logging onboard** command.

The following example shows how you might enter this command:

```
Router# show logging onboard module 2 message detail

--------------------------------------------------------------------------------
ERROR MESSAGE SUMMARY INFORMATION
--------------------------------------------------------------------------------
Facility-Sev-Name      | Count | Persistence Flag
MM/DD/YYYY HH:MM:SS
--------------------------------------------------------------------------------
No historical data to display
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
ERROR MESSAGE CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
MM/DD/YYYY HH:MM:SS Facility-Sev-Name
--------------------------------------------------------------------------------
03/06/2007 22:33:35  %GOLD_OBFL-3-GOLD : Diagnostic OBFL: Diagnostic OBFL testing
```

Table 46 describes the significant fields shown in the display.

Table 46 Error Message Summary Information

Field	Description
A timestamp	Shows the date and time the message was logged.
Facility-Sev-Name	A coded naming scheme for a system message, as follows: • The Facility code consists of two or more uppercase letters that indicate the hardware device (facility) to which the message refers. • Sev is a single-digit code from 1 to 7 that reflects the severity of the message. • Name is one or two code names separated by a hyphen that describe the part of the system from where the message is coming.
Error message	Follows the Facility-Sev-Name codes. For more information about system messages, see the *Cisco IOS System and Error Messages* guide.

Table 46 Error Message Summary Information (continued)

Field	Description
Count	Indicates the number of instances of this message that is allowed in the history file. Once that number of instances has been recorded, the oldest instance will be removed from the history file to make room for new ones.
Persistence Flag	Gives a message priority over others that do not have the flag set.

Related Commands

Command	Description
attach	Connects to a specific line card for the purpose of executing commands on that card.
clear logging onboard (Cat 6K)	Clears onboard failure logs.
copy logging onboard (Cat 6K)	Copies OBFL data from the target OBFL-enabled module to a local or remote file system.
hw-module logging onboard (Cat 6K)	Disables and enables OBFL.

show management event

To display the Simple Network Management Protocol (SNMP) Event values that have been configured on your routing device through the use of the Event MIB, use the **show management event** command in privileged EXEC mode.

show management event

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Event MIB allows you to configure your own traps, informs, or set operations through the use of an external network management application. The **show management event** command is used to display the values for the Events configured on your system. There are no Cisco IOS CLI commands for configuring Event MIB values. For information on Event MIB functionality, see RFC 2981, available at http://www.ietf.org.

Examples

The following example shows sample output of the **show management event** command:

```
Router# show management event

Mgmt Triggers:
 (1): Owner: joe_user
  (1): 01, Comment: TestEvent, Sample: Abs, Freq: 120
      Test: Existence Threshold Boolean
         ObjectOwner: aseem, Object: sethi
         OID: ifEntry.10.3, Enabled 1, Row Status 1
      Existence Entry: , Absent, Changed
      StartUp:  Present, Absent
         ObjOwn: , Obj: , EveOwn: aseem, Eve: 09
      Boolean Entry:
         Value: 10, Cmp: 1, Start: 1
         ObjOwn: , Obj: , EveOwn: aseem, Eve: 09
      Threshold Entry:
         Rising: 50000, Falling: 20000
         ObjOwn: ase, Obj: 01 RisEveOwn: ase, RisEve: 09 , FallEveOwn: ase, FallEve: 09

      Delta Value Table:
  (0): Thresh: Rising, Exis: 1, Read: 0, OID: ifEntry.10.3 , val: 69356097
```

```
Mgmt Events:
(1): Owner: aseem
  (1)Name: 09 , Comment: , Action: Set, Notify, Enabled: 1 Status: 1
     Notification Entry:
        ObjOwn: , Obj: , OID: ifEntry.10.1
     Set:
        OID: ciscoSyslogMIB.1.2.1.0, SetValue: 199, Wildcard: 2 TAG: , ContextName:

Object Table:
(1): Owner: aseem
  (1)Name: sethi, Index: 1, OID: ifEntry.10.1, Wild: 1, Status: 1
```

Related Commands

Command	Description
debug management event	Allows real-time monitoring of Event MIB activities for the purposes of debugging.

show monitor event-trace

To display event trace messages for Cisco IOS software subsystem components, use the **show monitor event-trace** command in privileged EXEC mode.

show monitor event-trace [**all-traces**] [*component* {**all** | **back** *hour:minute* | **clock** *hour:minute* | **from-boot** *seconds* | **latest** | **parameters**}]

Syntax Description

all-traces	(Optional) Displays all event trace messages in memory to the console.
component	(Optional) Name of the Cisco IOS software subsystem component that is the object of the event trace. To get a list of components that support event tracing in this release, use the **monitor event-trace ?** command.
all	Displays all event trace messages currently in memory for the specified component.
back *hour:minute*	Specifies how far back from the current time you want to view messages. For example, you can gather messages from the last 30 minutes. The time argument is specified in hours and minutes format (hh:mm).
clock *hour:minute*	Displays event trace messages starting from a specific clock time in hours and minutes format (hh:mm).
from-boot *seconds*	Displays event trace messages starting from a specified number of seconds after booting (uptime). To display the uptime, in seconds, enter the **show monitor event-trace** *component* **from-boot ?** command.
latest	Displays only the event trace messages since the last **show monitor event-trace** command was entered.
parameters	Displays the trace parameters. The only parameter displayed is the size (number of trace messages) of the trace file.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(18)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE. The **spa** component keyword was added to support online insertion and removal (OIR) event messages for shared port adapters (SPAs). The **bfd** keyword was added for the *component* argument to display trace messages relating to the Bidirectional Forwarding Detection (BFD) feature.
12.4(4)T	Support for the **bfd** keyword was added for Cisco IOS Release 12.4(4)T.
12.0(31)S	Support for the **bfd** keyword was added for Cisco IOS Release 12.0(31)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.

Release	Modification
12.4(9)T	The **cfd** keyword was added as an entry for the *component* argument to display trace messages relating to crypto fault detection.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **show monitor event-trace** command to display trace message information.

The trace function is not locked while information is being displayed to the console, which means that new trace messages can accumulate in memory. If entries accumulate faster than they can be displayed, some messages can be lost. If this happens, the **show monitor event-trace** command will generate a message indicating that some messages might be lost; however, messages will continue to display on the console. If the number of lost messages is excessive, the **show monitor event-trace** command will stop displaying messages.

Use the **bfd** keyword for the *component* argument to display trace messages relating to the BFD feature.

Use the **cfd** keyword for the *component* argument to display trace messages relating to the crypto fault detection feature. This keyword displays the contents of the error trace buffers in an encryption data path.

Examples

IPC Component Example

The following is sample output from the **show monitor event-trace** *component* command for the interprocess communication (IPC) component. Notice that each trace message is numbered and is followed by a time stamp (derived from the device uptime). Following the time stamp is the component-specific message data.

```
Router# show monitor event-trace ipc

3667:  6840.016:Message type:3 Data=0123456789
3668:  6840.016:Message type:4 Data=0123456789
3669:  6841.016:Message type:5 Data=0123456789
3670:  6841.016:Message type:6 Data=0123456
```

BFD Component for Cisco IOS Release 12.2(18)SXE, 12.0(31)S, and 12.4(4)T

Use the **show monitor event-trace bfd all** command to display logged messages for important BFD events in the recent past. The following trace messages show BFD session state changes:

```
 Router# show monitor event-trace bfd all

     3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], event Session
            create, state Unknown -> Fail
     3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], state Fail -> Down
             (from LC)
     3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], state Down -> Init
             (from LC)
     3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], state Init -> Up
            (from LC)
     3d07h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,2], event Session
            create, state Unknown -> Fail
     3d07h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,2], state Fail -> Down
             (from LC)
     3d07h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,2], state Down -> Up
            (from LC)
```

To display trace information for all components configured for event tracing on the networking device, enter the **show monitor event-trace all-traces** command. In this example, separate output is provided for each event, and message numbers are interleaved between the events.

```
Router# show monitor event-trace all-traces

Test1 event trace:
3667: 6840.016:Message type:3 Data=0123456789
3669: 6841.016:Message type:4 Data=0123456789
3671: 6842.016:Message type:5 Data=0123456789
3673: 6843.016:Message type:6 Data=0123456789

Test2 event trace:
3668: 6840.016:Message type:3 Data=0123456789
3670: 6841.016:Message type:4 Data=0123456789
3672: 6842.016:Message type:5 Data=0123456789
3674: 6843.016:Message type:6 Data=0123456789
```

SPA Component Example

The following is sample output from the **show monitor event-trace** *component* **latest** command for the **spa** component:

```
Router# show monitor event-trace spa latest

00:01:15.364: subslot 2/3: 4xOC3 POS SPA, TSM Event:inserted  New state:wait_psm
_ready
     spa type 0x440
00:02:02.308: subslot 2/0: not present, TSM Event:empty  New state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/0: not present, TSM Event:remove_complete  New state:idle
00:02:02.308: subslot 2/1: not present, TSM Event:empty  New state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/1: not present, TSM Event:remove_complete  New state:idle
00:02:02.308: subslot 2/2: not present, TSM Event:empty  New state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/2: not present, TSM Event:remove_complete  New state:idle
00:02:02.312: subslot 2/3: not present(plugin 4xOC3 POS SPA), TSM Event:empty  New
state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.312: subslot 2/3: not present, TSM Event:remove_complete  New state:idle
```

Cisco Express Forwarding Component Examples

If you select Cisco Express Forwarding as the component for which to display event messages, you can use the following additional arguments and keywords: **show monitor event-trace cef** [**events** | **interface** | **ipv6** | **ipv4**][**all**].

The following example shows the IPv6 or IPv4 events related to the Cisco Express Forwarding component. Each trace message is numbered and is followed by a time stamp (derived from the device uptime). Following the time stamp is the component-specific message data.

```
Router# show monitor event-trace cef ipv6 all

00:00:24.612:  [Default] *::*/*'00             New FIB table          [OK]

Router# show monitor event-trace cef ipv4 all

00:00:24.244:  [Default] 127.0.0.81/32'01       FIB insert             [OK]
```

In the following example, all event trace messages for the Cisco Express Forwarding component are displayed:

```
Router# show monitor event-trace cef events all

00:00:18.884: SubSys  fib_ios_chain init
00:00:18.884: Inst    unknown -> RP
00:00:24.584: SubSys  fib init
00:00:24.592: SubSys  fib_ios init
00:00:24.592: SubSys  fib_ios_if init
00:00:24.596: SubSys  ipv4fib init
00:00:24.608: SubSys  ipv4fib_ios init
00:00:24.612: SubSys  ipv6fib_ios init
00:00:24.620: Flag    IPv4 CEF enabled set to yes
00:00:24.620: Flag    0x7BF6B62C set to yes
00:00:24.620: Flag    IPv4 CEF switching enabled set to yes
00:00:24.624: GState  CEF enabled
00:00:24.628: SubSys  ipv4fib_les init
00:00:24.628: SubSys  ipv4fib_pas init
00:00:24.632: SubSys  ipv4fib_util init
00:00:25.304: Process Background created
00:00:25.304: Flag    IPv4 CEF running set to yes
00:00:25.304: Process Background event loop enter
00:00:25.308: Flag    IPv4 CEF switching running set to yes
```

The following example shows Cisco Express Forwarding interface events:

```
Router# show monitor event-trace cef interface all

00:00:24.624: <empty>      (sw  4) Create   new
00:00:24.624: <empty>      (sw  4) SWIDBLnk FastEthernet0/0(4)
00:00:24.624: Fa0/0        (sw  4) NameSet
00:00:24.624: <empty>      (hw  1) Create   new
00:00:24.624: <empty>      (hw  1) HWIDBLnk FastEthernet0/0(1)
00:00:24.624: Fa0/0        (hw  1) NameSet
00:00:24.624: <empty>      (sw  3) Create   new
00:00:24.624: <empty>      (sw  3) SWIDBLnk FastEthernet0/1(3)
00:00:24.624: Fa0/1        (sw  3) NameSet
00:00:24.624: <empty>      (hw  2) Create   new
```

Cisco Express Forwarding Component Examples for Cisco 10000 Series Routers Only

The following example shows the IPv4 events related to the Cisco Express Forwarding component. Each trace message is numbered and is followed by a time stamp (derived from the device uptime). Following the time stamp is the component-specific message data.

```
Router# show monitor event-trace cef ipv4 all

00:00:48.244:  [Default] 127.0.0.81/32'01      FIB insert               [OK]
```

In the following example, all event trace message for the Cisco Express Forwarding component are displayed:

```
Router# show monitor event-trace cef events all

00:00:18.884: SubSys  fib_ios_chain init
00:00:18.884: Inst    unknown -> RP
00:00:24.584: SubSys  fib init
00:00:24.592: SubSys  fib_ios init
00:00:24.592: SubSys  fib_ios_if init
00:00:24.596: SubSys  ipv4fib init
00:00:24.608: SubSys  ipv4fib_ios init
00:00:24.620: Flag    IPv4 CEF enabled set to yes
00:00:24.620: Flag    0x7BF6B62C set to yes
```

```
00:00:24.620: Flag    IPv4 CEF switching enabled set to yes
00:00:24.624: GState  CEF enabled
00:00:24.628: SubSys  ipv4fib_les init
00:00:24.628: SubSys  ipv4fib_pas init
00:00:24.632: SubSys  ipv4fib_util init
00:00:25.304: Process Background created
00:00:25.304: Flag    IPv4 CEF running set to yes
00:00:25.304: Process Background event loop enter
00:00:25.308: Flag    IPv4 CEF switching running set to yes
```

The following examples show Cisco Express Forwarding interface events:

```
Router# show monitor event-trace cef interface all

00:00:24.624: <empty>      (sw  4) Create   new
00:00:24.624: <empty>      (sw  4) SWIDBLnk FastEthernet1/0/0(4)
00:00:24.624: Fa0/0        (sw  4) NameSet
00:00:24.624: <empty>      (hw  1) Create   new
00:00:24.624: <empty>      (hw  1) HWIDBLnk FastEthernet1/0/0(1)
00:00:24.624: Fa0/0        (hw  1) NameSet
00:00:24.624: <empty>      (sw  3) Create   new
00:00:24.624: <empty>      (sw  3) SWIDBLnk FastEthernet1/1/0(3)
00:00:24.624: Fa0/1        (sw  3) NameSet
00:00:24.624: <empty>      (hw  2) Create   new
```

CFD Component for Cisco IOS Release 12.4(9)T

To troubleshoot errors in an encryption datapath, enter the **show monitor event-trace cfd all** command. In this example, events are shown separately, each beginning with a time stamp, followed by data from the error trace buffer. Cisco Technical Assistence Center (TAC) engineers can use this information to diagnose the cause of the errors.

Note If no packets have been dropped, this command does not display any output.

```
Router# show monitor event-trace cfd all

00:00:42.452: 450000B4 00060000 FF33B306 02020203 02020204 32040000 F672999C
        00000001 7A7690C2 A0A4F8BC E732985C D6FFDCC8 00000001 C0902BD0
        A99127AE 8EAA22D4

00:00:44.452: 450000B4 00070000 FF33B305 02020203 02020204 32040000 F672999C
        00000002 93C01218 2325B697 3C384CF1 D6FFDCC8 00000002 BFA13E8A
        D21053ED 0F62AB0E

00:00:46.452: 450000B4 00080000 FF33B304 02020203 02020204 32040000 F672999C
        00000003 7D2E11B7 A0BA4110 CC62F91E D6FFDCC8 00000003 7236B930
        3240CA8C 9EBB44FF

00:00:48.452: 450000B4 00090000 FF33B303 02020203 02020204 32040000 F672999C
        00000004 FB6C80D9 1AADF938 CDE57ABA D6FFDCC8 00000004 E10D8028
        6BBD748F 87F5E253

00:00:50.452: 450000B4 000A0000 FF33B302 02020203 02020204 32040000 F672999C
        00000005 697C8D9D 35A8799A 2A67E97B D6FFDCC8 00000005 BC21669D
        98B29FFF F32670F6

00:00:52.452: 450000B4 000B0000 FF33B301 02020203 02020204 32040000 F672999C
        00000006 CA18CBC4 0F387FE0 9095C27C D6FFDCC8 00000006 87A54811
        AE3A0517 F8AC4E64
```

Related Commands

Command	Description
monitor event-trace (EXEC)	Controls event trace functions for a specified Cisco IOS software subsystem component.
monitor event-trace (global)	Configures event tracing for a specified Cisco IOS software subsystem component.
monitor event-trace dump-traces	Saves trace messages for all event traces currently enabled on the networking device.

show monitor event-trace cpu-report

To display event trace messages for the CPU, use the **show monitor event-trace cpu-report** command in user EXEC or privileged EXEC mode.

show monitor event-trace cpu-report {**brief** {**all** [**detail**] | **back** *time* | **clock** *time* | **from-boot** *seconds* | [**detail**] | **latest** [**detail**]} | **handle** *handle-number*}

Syntax Description

brief	Displays a brief CPU report.
all	Displays all event trace messages currently in memory for the CPU.
detail	(Optional) Displays detailed event trace information.
back	Specifies how far back from the current time you want to view messages. For example, you can gather messages from the last 30 minutes.
time	Integer value that is the length of time, in hours and minutes. The format is hh:mm.
clock	Displays event trace messages starting from a specific clock time.
from-boot	Displays event trace messages starting from a specified number of seconds after booting.
seconds	Number of seconds since the networking device was last booted (uptime).
latest	Displays only the event trace messages since the last **show monitor event-trace** command was entered.
handle	Displays a detailed CPU report for a specified handle number.
handle-number	Handle number. Valid values are from 1 to 255.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **show monitor event-trace cpu-report** command with the **brief** keyword to display the CPU report details. To see individual snapshots, use the **show monitor event-trace cpu-report handle** *handle-number* command.

To view the uptime, in seconds, enter the **show monitor event-trace cpu-report from-boot ?** command.

Examples

To view CPU report details for event tracing on a networking device, enter the **show monitor event-trace cpu-report brief all** command:

```
Router# show monitor event-trace cpu-report brief all

Timestamp   : Handle Name               Description
00:01:07.320:  1     CPU                None
```

To view CPU report details for event tracing on a networking device for the handle number 1, enter the **show monitor event-trace cpu-report handle 1** command:

```
Router# show monitor event-trace cpu-report handle 1

00:01:07.320:  1     CPU                None
################################################################################
Global Statistics
-----------------
5 sec CPU util 0%/0% Timestamp 21:03:56
Queue Statistics
----------------
             Exec Count  Total CPU    Response Time        Queue Length
                                       (avg/max)             (avg/max)
Critical           1          0          0/0                   1/1
High               5          0          0/0                   1/1
Normal           178          0          0/0                   2/9
Low               15          0          0/0                   2/3
Common Process Information
-------------------------------
 PID Name            Prio Style
-------------------------------
  10 AAA high-capacit M  New
 133 RADIUS TEST CMD  M  New
  47 VNM DSPRM MAIN   H  New
  58 TurboACL         M  New
  97 IP Background    M  New
  99 CEF: IPv4 proces L  New
 112 X.25 Background  M  New
 117 LFDp Input Proc  M  New
   3 Init             M  Old
CPU Intensive processes
-------------------------------------------------------------------------------
 PID Total       Exec    Quant         Burst  Burst size  Schedcall  Schedcall
     CPUms      Count   avg/max        Count avg/max(ms)      Count Per avg/max
-------------------------------------------------------------------------------
   3   820          6   136/236         1     24/24             18  887/15172
Priority Suspends
------------------------------------
 PID Exec Count Prio-Susps
------------------------------------
   3          6          1
Latencies
-------------------------
 PID Exec Count   Latency
                  avg/max
-------------------------
  10          1 15192/15192
 133          1 15192/15192
  58          1 15192/15192
 112          1 15192/15192
 117          1 15192/15192
  99          1 15172/15172
  47          1 15172/15172
  97          1 15172/15172
```

```
################################################################################
Global Statistics
-----------------
5 sec CPU util 0%/0% Timestamp 00:00:00
Queue Statistics
----------------
        Exec Count  Total CPU     Response Time           Queue Length
                                    (avg/max)                (avg/max)
Critical      0          0              0/0                    0/0
High          0          0              0/0                    0/0
Normal        0          0              0/0                    0/0
Low           0          0              0/0                    0/0

Common Process Information
-------------------------------
 PID Name            Prio Style
-------------------------------

CPU Intensive processes
-------------------------------------------------------------------------------
 PID Total       Exec    Quant         Burst  Burst size  Schedcall  Schedcall
     CPUms      Count   avg/max        Count avg/max(ms)      Count Per avg/max
-------------------------------------------------------------------------------
Priority Suspends
------------------------------------
 PID Exec Count Prio-Susps
------------------------------------
Latencies
-------------------------
 PID Exec Count   Latency
                  avg/max
-------------------------
################################################################################
```

Related Commands

Command	Description
monitor event-trace cpu-report (EXEC)	Monitors event tracing of the CPU reports.
monitor event-trace cpu-report (global)	Monitors the collection of CPU report traces.
monitor event-trace dump-traces	Saves trace messages for all event traces currently enabled on the networking device.

show netconf

To display network configuration protocol (NETCONF) statistics counters and session information, use the **show netconf** command in privileged EXEC mode.

show netconf {**counters** | **session**}

Syntax Description

counters	Displays NETCONF statistics and informational counters.
session	Displays the current state of all connected NETCONF sessions across all transports and any resources and locks in use by the session.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Examples

The following is sample output from the **show netconf counters** command:

```
Router# show netconf counters

NETCONF Counters
Connection Attempts:0: rejected:0 no-hello:0 success:0
Transactions
        total:0, success:0, errors:0
detailed errors:
        in-use 0        invalid-value 0         too-big 0
        missing-attribute 0     bad-attribute 0         unknown-attribute 0
        missing-element 0       bad-element 0   unknown-element 0
        unknown-namespace 0     access-denied 0         lock-denied 0
        resource-denied 0       rollback-failed 0       data-exists 0
        data-missing 0  operation-not-supported 0       operation-failed 0
        partial-operation 0
```

The following is sample output from the **show netconf session** command:

```
Router# show netconf session

(Current | max) sessions:   3 | 4
Operations received: 100               Operation errors: 99
Connection Requests: 5                 Authentication errors: 2   Connection Failures: 0
ACL dropped : 30
Notifications  Sent: 20
```

Table 47 describes the significant fields shown in the displays.

Table 47 show netconf Field Descriptions

Field	Description
Connection Attempts	Number of NETCONF Connection attempts.
rejected	Number of rejected NETCONF sessions.
no-hello	Number of NETCONF sessions that were dropped because Hello messages were not received.
success	Number of successful NETCONF sessions.
in-use 0	The request requires a resource that is already in use.
invalid-value 0	The request specifies an invalid value for one or more parameters.
too-big 0	The request or response that would be generated would be too large for the implementation to handle.
missing-attribute 0	An expected attribute is missing.
bad-attribute 0	An attribute value is incorrect. An attribute that is the incorrect type, out of range, or contains a pattern mismatch will be displayed as a bad attribute.
unknown-attribute 0	An unexpected attribute is present.
missing-element 0	An expected element is missing.
bad-element 0	An element value is not correct. An element that is the incorrect type, out of range, or contains a pattern mismatch will be displayed as a bad element.
unknown-element 0	An unexpected element is present.
unknown-namespace 0	An unexpected name space is present.
access-denied 0	Access to a requested NETCONF session is denied because authorization failed.
lock-denied 0	Access to a requested lock is denied because the lock is currently in use.
resource-denied 0	A request could not be completed because of insufficient resources.
rollback-failed 0	A request to roll back a configuration change was not completed.
data-exists 0	A request could not be completed because the relevant content already exists.
data-missing 0	A request could not be completed because the relevant content does not exist.
operation-not-supported 0	A request could not be completed because the requested operation is not supported.
operation-failed 0	A request could not be completed because the requested operation failed for a reason not specified by another error notice.
partial-operation 0	Part of a requested operation failed or was not attempted.

Table 47 show netconf Field Descriptions (continued)

Field	Description
(Current | max) sessions: 3 | 4	Number of current NETCONF sessions and the maximum number of concurrent NETCONF sessions allowed.
Operations received: 100	Number of NETCONF operations received.
Operation errors: 99	Number of NETCONF operation errors.
Connection Requests: 5	Number of NETCONF connection requests.
Authentication errors: 2	Number of NETCONF authentication errors.
Connection Failures: 0	Number of unsuccessful NETCONF session connections.
ACL dropped: 30	Number of NETCONF sessions dropped due to an access list.
Notifications Sent: 20	Number of NETCONF notifications sent.

show ntp associations

Command	Description
clear netconf	Clears NETCONF statistics counters, NETCONF sessions, and frees associated resources and locks.
debug netconf	Enables debugging of NETCONF sessions.
netconf lock-time	Specifies the maximum time a NETCONF configuration lock is in place without an intermediate operation.
netconf max-sessions	Specifies the maximum number of concurrent NETCONF sessions allowed.
netconf ssh	Enables NETCONF over SSHv2.

To show the status of Network Time Protocol (NTP) associations, use the **show ntp associations** command in EXEC mode.

show ntp associations [**detail**]

Syntax Description

detail	(Optional) Displays detailed information about each NTP association.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

Detailed descriptions of the information displayed by this command can be found in the NTP specification (RFC 1305).

The following is sample output from the **show ntp associations** command:

```
Router> show ntp associations

     address         ref clock     st  when  poll  reach  delay  offset    disp
 ~172.31.32.2      172.31.32.1       5    29  1024  377     4.2   -8.59     1.6
+~192.168.13.33    192.168.1.111     3    69   128  377     4.1    3.48     2.3
*~192.168.13.57    192.168.1.111     3    32   128  377     7.9   11.18     3.6
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

Table 48 describes the significant fields shown in the display.

Table 48 show ntp associations Field Descriptions

Field	Description
(leading characters in display lines)	The first characters in a display line can be one or more of the following characters: * —Synchronized to this peer # —Almost synchronized to this peer + —Peer selected for possible synchronization - —Peer is a candidate for selection ~ —Peer is statically configured
address	Address of peer.
ref clock	Address of reference clock of peer.
st	Stratum of peer.
when	Time since last NTP packet was received from peer.
poll	Polling interval (in seconds).
reach	Peer reachability (bit string, in octal).
delay	Round-trip delay to peer (in milliseconds).
offset	Relative time of peer clock to local clock (in milliseconds).
disp	Dispersion

The following is sample output of the **show ntp associations detail** command:

```
Router> show ntp associations detail

172.31.32.2 configured, insane, invalid, stratum 5
ref ID 172.31.32.1, time AFE252C1.6DBDDFF2 (00:12:01.428 PDT Mon Jul 5 1993)
our mode active, peer mode active, our poll intvl 1024, peer poll intvl 64
root delay 137.77 msec, root disp 142.75, reach 376, sync dist 215.363
delay 4.23 msec, offset -8.587 msec, dispersion 1.62
precision 2**19, version 3
org time AFE252E2.3AC0E887 (00:12:34.229 PDT Mon Jul 5 1993)
rcv time AFE252E2.3D7E464D (00:12:34.240 PDT Mon Jul 5 1993)
xmt time AFE25301.6F83E753 (00:13:05.435 PDT Mon Jul 5 1993)
filtdelay =     4.23    4.14    2.41    5.95    2.37    2.33    4.26    4.33
filtoffset =   -8.59   -8.82   -9.91   -8.42  -10.51  -10.77  -10.13  -10.11
filterror =     0.50    1.48    2.46    3.43    4.41    5.39    6.36    7.34

192.168.13.33 configured, selected, sane, valid, stratum 3
ref ID 192.168.1.111, time AFE24F0E.14283000 (23:56:14.078 PDT Sun Jul 4 1993)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 83.72 msec, root disp 217.77, reach 377, sync dist 264.633
delay 4.07 msec, offset 3.483 msec, dispersion 2.33
precision 2**6, version 3
org time AFE252B9.713E9000 (00:11:53.442 PDT Mon Jul 5 1993)
rcv time AFE252B9.7124E14A (00:11:53.441 PDT Mon Jul 5 1993)
xmt time AFE252B9.6F625195 (00:11:53.435 PDT Mon Jul 5 1993)
filtdelay =     6.47    4.07    3.94    3.86    7.31    7.20    9.52    8.71
filtoffset =    3.63    3.48    3.06    2.82    4.51    4.57    4.28    4.59
filterror =     0.00    1.95    3.91    4.88    5.84    6.82    7.80    8.77

192.168.13.57 configured, our_master, sane, valid, stratum 3
ref ID 192.168.1.111, time AFE252DC.1F2B3000 (00:12:28.121 PDT Mon Jul 5 1993)
```

```
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 125.50 msec, root disp 115.80, reach 377, sync dist 186.157
delay 7.86 msec, offset 11.176 msec, dispersion 3.62
precision 2**6, version 2
org time AFE252DE.77C29000 (00:12:30.467 PDT Mon Jul 5 1993)
rcv time AFE252DE.7B2AE40B (00:12:30.481 PDT Mon Jul 5 1993)
xmt time AFE252DE.6E6D12E4 (00:12:30.431 PDT Mon Jul 5 1993)
filtdelay =    49.21    7.86    8.18    8.80    4.30    4.24    7.58    6.42
filtoffset =   11.30   11.18   11.13   11.28    8.91    9.09    9.27    9.57
filterror =     0.00    1.95    3.91    4.88    5.78    6.76    7.74    8.71
```

Table 49 describes the significant fields shown in the display.

Table 49 show ntp associations detail Field Descriptions

Field	Descriptions
configured	Peer was statically configured.
dynamic	Peer was dynamically discovered.
our_master	Local machine is synchronized to this peer.
selected	Peer is selected for possible synchronization.
candidate	Peer is a candidate for selection.
sane	Peer passes basic sanity checks.
insane	Peer fails basic sanity checks.
valid	Peer time is believed to be valid.
invalid	Peer time is believed to be invalid.
leap_add	Peer is signalling that a leap second will be added.
leap-sub	Peer is signalling that a leap second will be subtracted.
unsynced	Peer is not synchronized to any other machine.
ref ID	Address of machine peer is synchronized to.
time	Last time stamp peer received from its master.
our mode	Our mode relative to peer (active/passive/client/server/bdcast/bdcast client).
peer mode	Peer's mode relative to us.
our poll intvl	Our poll interval to peer.
peer poll intvl	Peer's poll interval to us.
root delay	Delay along path to root (ultimate stratum 1 time source).
root disp	Dispersion of path to root.
reach	Peer reachability (bit string in octal).
sync dist	Peer synchronization distance.
delay	Round-trip delay to peer.
offset	Offset of peer clock relative to our clock.
dispersion	Dispersion of peer clock.
precision	Precision of peer clock in Hertz.
version	NTP version number that peer is using.

Table 49 show ntp associations detail Field Descriptions (continued)

Field	Descriptions
org time	Originate time stamp.
rcv time	Receive time stamp.
xmt time	Transmit time stamp.
filtdelay	Round-trip delay (in milliseconds) of each sample.
filtoffset	Clock offset (in milliseconds) of each sample.
filterror	Approximate error of each sample.

Related Commands

Command	Description
show ntp status	Displays the status of the NTP.

show ntp status

To show the status of the Network Time Protocol (NTP), use the **show ntp status** command in EXEC mode.

show ntp status

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show ntp status** command:

```
Router> show ntp status

Clock is synchronized, stratum 4, reference is 192.168.13.57
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**19
reference time is AFE2525E.70597B34 (00:10:22.438 PDT Mon Jul 5 1993)
clock offset is 7.33 msec, root delay is 133.36 msec
root dispersion is 126.28 msec, peer dispersion is 5.98 msec
```

Table 50 describes the significant fields shown in the display.

Table 50 show ntp status Field Descriptions

Field	Description
synchronized	System is synchronized to an NTP peer.
unsynchronized	System is not synchronized to any NTP peer.
stratum	NTP stratum of this system.
reference	Address of peer the system is synchronized to.
nominal freq	Nominal frequency of system hardware clock.
actual freq	Measured frequency of system hardware clock.
precision	Precision of the clock of this system (in Hertz).
reference time	Reference time stamp.
clock offset	Offset of the system clock to synchronized peer.
root delay	Total delay along path to root clock.

Table 50 show ntp status Field Descriptions (continued)

Field	Description
root dispersion	Dispersion of root path.
peer dispersion	Dispersion of synchronized peer.

Related Commands

Command	Description
show ntp associations	Displays the status of the NTP associations.

show platform software trace level

To view the trace levels for a specific module, enter the **show platform software trace level** priviliged EXEC and diagnostic mode command.

show platform software trace level *process hardware-module slot*

Syntax Description

process

Specifies the process in which the tracing level is being set. Options currently include:

- **chassis-manager**—The Chassis Manager process.
- **cpp-control-process**—The CPP Control process
- **cpp-driver**—The CPP driver process
- **cpp-ha-server**—The CPP HA server process
- **cpp-service-process**—The CPP service process
- **forwarding-manager**—The Forwarding Manager process.
- **host-manager**—The Host Manager process.
- **interface-manager**—The Interface Manager process.
- **ios**—The IOS process.
- **logger**—The logging manager process
- **pluggable-services**—The pluggable services process.
- **shell-manager**—The Shell Manager process.

hardware-module	Specifies the hardware module where the process in which the trace level is being set is running. Options include: • **carrier-card**—The process is on a SPA Interface Processor (SIP). • **forwarding-processor**—The process is on an Embedded Services Processor (ESP). • **route-processor**—The process is on a Route Processor (RP).
slot	Specifies the slot of the *hardware-module*. Options include: • *number*—The number of the SIP slot of the hardware module where the trace level is being set. For instance, if you want to specify the SIP in SIP slot 2 of the router, enter 2 as the *number.* • *SIP-slot*/*SPA-bay*—The number of the SIP router slot and the number of the SPA bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in router slot 3, enter 3/2. • **cpp active**—The Cisco Packet Processor (CPP) in the active ESP. • **cpp standby**—The CPP in the standby ESP. • **f0**—The ESP in ESP slot 0. • **f1**—The ESP in ESP slot 1 • **fp active**—The active ESP. • **fp standby**—The standby ESP. • **r0**—The RP in RP slot 0. • **r1**—The RP in RP slot 1. • **rp active**—The active RP. • **rp standby**—The standby RP.

Command Modes

Privileged EXEC (#)
Diagnostic (diag)

Command Default

No default behavior or values.

The default tracing level on a Cisco ASR 1000 Series Router is critical. The tracing level can be changed using the **set platform software trace** command.

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.

Usage Guidelines

This command is used to view trace levels. Trace levels, which determine which trace messages are generated, can be defined using the **set platform software trace** command.

Table 51 shows all of the trace levels that are available and provides descriptions of what types of messages are displayed with each set tracing level. This command is used to review these trace levels for various modules on the Aggregation Services routers.

Table 51 Tracing Levels and Descriptions

Trace Level	Level Number	Description
Emergency	0	The message is regarding an issue that makes the system unusable.
Alert	1	The message is regarding an action that must be taken immediately.
Critical	2	The message is regarding a critical condition. This is the default setting for every module on the Cisco ASR 1000 Series Routers.
Error	3	The message is regarding a system error.
Warning	4	The message is regarding a system warning
Notice	5	The message is regarding a significant issue, but the router is still working normally.
Informational	6	The message is useful for informational purposes only.
Debug	7	The message provides debug-level output.
Verbose	8	All possible tracing messages are sent when the trace level is set to verbose.
Noise	-	The noise tracing level will always send all possible trace messages for the module. The noise level is always equal to the highest possible tracing level. Even if a future enhancement to this command introduces a higher tracing level, the noise level will become equal to the level of that new enhancement.

Examples

In the following example, the **show platform software trace level** command is used to view the tracing levels of the Forwarding Manager processes on the active RP:

```
Router# show platform software trace level forwarding-manager rp active
Module Name                     Trace Level
-----------------------------------------------
acl                             Error
binos                           Error
binos/brand                     Error
bipc                            Error
btrace                          Error
cce                             Error
cdllib                          Error
cef                             Error
chasfs                          Error
chasutil                        Error
erspan                          Error
ess                             Error
ether-channel                   Error
evlib                           Error
evutil                          Error
```

```
file_alloc                      Error
fman_rp                         Error
fpm                             Error
fw                              Error
icmp                            Error
interfaces                      Error
iosd                            Error
ipc                             Error
ipclog                          Error
iphc                            Error
ipsec                           Error
mgmte-acl                       Error
mlp                             Error
mqipc                           Error
nat                             Error
nbar                            Error
netflow                         Error
om                              Error
peer                            Error
qos                             Error
route-map                       Error
sbc                             Error
services                        Error
sw_wdog                         Error
tdl_acl_config_type             Error
tdl_acl_db_type                 Error
tdl_cdl_message                 Error
tdl_cef_config_common_type      Error
tdl_cef_config_type             Error
tdl_dpidb_config_type           Error
tdl_fman_rp_comm_type           Error
tdl_fman_rp_message             Error
tdl_fw_config_type              Error
tdl_hapi_tdl_type               Error
tdl_icmp_type                   Error
tdl_ip_options_type             Error
tdl_ipc_ack_type                Error
tdl_ipsec_db_type               Error
tdl_mcp_comm_type               Error
tdl_om_type                     Error
tdl_ui_type                     Error
tdl_urpf_config_type            Error
tdllib                          Error
trans_avl                       Error
uihandler                       Error
uipeer                          Error
uistatus                        Error
urpf                            Error
vista                           Error
```

Related Commands

Command	Description
set platform software trace	Sets the trace level for a specific module.
show platform software trace message	Displays the trace message for a specified module.

show platform software trace message

To view trace messages for a module, enter the **show platform software trace message** command.

show platform software trace message *process hardware-module slot module*

Syntax Description

process	Specifies the process in which the tracing level is being set. Options include: • **chassis-manager**—The Chassis Manager process. • **cpp-control-process**—The CPP Control process • **cpp-driver**—The CPP driver process • **cpp-ha-server**—The CPP HA server process • **cpp-service-process**—The CPP service process • **forwarding-manager**—The Forwarding Manager process. • **host-manager**—The Host Manager process. • **interface-manager**—The Interface Manager process. • **ios**—The IOS process. • **logger**—The logging manager process • **pluggable-services**—The pluggable services process. • **shell-manager**—The Shell Manager process.

hardware-module	Specifies the hardware module where the process whose trace level is being set is running. Options include: • **carrier-card**—The process is on a SPA Interface Processor (SIP). • **forwarding-processor**—The process is on an ESP. • **route-processor**—The process is on an RP.
slot	Specifies the slot of the *hardware-module*. Options include: • *number*—The number of the SIP slot of the hardware module where the trace level is being set. For instance, if you want to specify the SIP in SIP slot 2 of the router, enter 2 as the *number*. • *SIP-slot*/*SPA-bay*—The number of the SIP router slot and the number of the SPA bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in router slot 3, enter 3/2. • **cpp active**—The Cisco Packet Processor (CPP) in the active ESP. • **cpp standby**—The CPP in the standby ESP. • **f0**—The ESP in ESP slot 0. • **f1**—The ESP in ESP slot 1 • **fp active**—The active ESP. • **fp standby**—The standby ESP. • **r0**—The RP in RP slot 0. • **r1**—The RP in RP slot 1. • **rp active**—The active RP. • **rp standby**—The standby RP.

Command Modes

Privileged EXEC (#)
Diagnostic (diag)

Command Default

No default behavior or values.

The default tracing level on a Cisco ASR 1000 Series Router is critical. The tracing level can be changed using the **set platform software trace** command.

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.

Usage Guidelines

This command is used to view trace messages. Trace levels, which determine which trace messages are generated, can be defined using the **set platform software trace** command.

Examples

In the following example, the trace messages for the Host Manager process in Route Processor slot 0 are viewed using the **show platform software trace message** command.

```
Router# show platform software trace message host-manager R0
08/23 12:09:14.408 [uipeer]: (info): Looking for a ui_req msg
08/23 12:09:14.408 [uipeer]: (info): Start of request handling for con 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Accepted connection for 14 as 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Received new connection 0x100a61c8 on descriptor 14
08/23 12:09:14.398 [uipeer]: (info): Accepting command connection on listen fd 7
08/23 11:53:57.440 [uipeer]: (info): Going to send a status update to the shell manager in
slot 0
08/23 11:53:47.417 [uipeer]: (info): Going to send a status update to the shell manager in
slot 0
```

Related Commands

Command	Description
set platform software trace	Sets the trace level for a specific module.
show platform software trace levels	Displays trace levels for a module.

show processes cpu

To display detailed CPU utilization statistics (CPU use per process) when Cisco IOS or Cisco IOS Software Modularity images are running, use the **show processes cpu** command in privileged EXEC mode.

Cisco IOS Software

show processes cpu [**history** | **sorted**]

Cisco IOS Software Modularity

show processes cpu [**detailed** [*process-id* | *process-name*] | **history**]

Syntax Description

history	(Optional) Displays CPU history in a graph format.
sorted	(Optional) For cisco IOS images only. Displays CPU utilization sorted by percentage.
detailed	(Optional) For Cisco IOS Software Modularity images only. Displays more detailed information about Cisco IOS processes (not for POSIX processes).
process-id	(Optional) For Cisco IOS Software Modularity images only. Process identifier.
process-name	(Optional) For Cisco IOS Software Modularity images only. Process name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0	This command was introduced.
12.2(2)T	The **history** keyword was added.
12.3(8)	This command was enhanced to display ARP output.
12.3(14)T	This command was enhanced to display ARP output.
12.2(18)SXF4	This command was enhanced to support Cisco IOS Software Modularity images.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Cisco IOS Software

If you use the optional **history** keyword, three graphs are displayed for Cisco IOS images:

- CPU utilization for the last 60 seconds
- CPU utilization for the last 60 minutes
- CPU utilization for the last 72 hours

Maximum usage is measured and recorded every second; average usage is calculated on periods of more than one second. Consistently high CPU utilization over an extended period of time indicates a problem and using the **show processes cpu** command is useful for troubleshooting. Also, you can use the output of this command in the Cisco Output Interpreter tool to display potential issues and fixes. Output Interpreter is available to registered users of Cisco.com who are logged in and have Java Script enabled.

For a list of system processes, go to http://www.cisco.com/warp/public/63/showproc_cpu.html.

Cisco IOS Software Modularity

Cisco IOS Software Modularity images display only one graph that shows the CPU utilization for the last 60 minutes. The horizontal axis shows times (for example, 0, 5, 10, 15 minutes), and the vertical axis shows total percentage of CPU utilization (0 to 100 percent).

Examples

Example output varies between Cisco IOS software images and Cisco IOS Software Modularity software images. To view the appropriate output, choose one of the following sections:

- Cisco IOS Software
- Cisco IOS Software Modularity

Cisco IOS Software

The following is sample output from the **show processes cpu** command without keywords:

```
Router# show processes cpu

CPU utilization for five seconds: 5%/2%; one minute: 3%; five minutes: 2%
  PID  Runtime (ms)    Invoked   uSecs   5Sec  1Min  5Min  TTY  Process
    1          1736         58   29931     0%    0%    0%  0    Check heaps
    2            68        585     116  1.00% 1.00%    0%  0    IP Input
    3             0        744       0     0%    0%    0%  0    TCP Timer
    4             0          2       0     0%    0%    0%  0    TCP Protocols
    5             0          1       0     0%    0%    0%  0    BOOTP Server
    6            16        130     123     0%    0%    0%  0    ARP Input
    7             0          1       0     0%    0%    0%  0    Probe Input
    8             0          7       0     0%    0%    0%  0    MOP Protocols
    9             0          2       0     0%    0%    0%  0    Timers
   10           692         64   10812     0%    0%    0%  0    Net Background
   11             0          5       0     0%    0%    0%  0    Logger
   12             0         38       0     0%    0%    0%  0    BGP Open
   13             0          1       0     0%    0%    0%  0    Net Input
   14           540       3466     155     0%    0%    0%  0    TTY Background
   15             0          1       0     0%    0%    0%  0    BGP I/O
   16          5100       1367    3730     0%    0%    0%  0    IGRP Router
   17            88       4232      20  0.20% 1.00%    0%  0    BGP Router
   18           152      14650      10     0%    0%    0%  0    BGP Scanner
   19           224         99    2262     0%    0% 1.00%  0    Exec
```

The following is sample output of the one-hour portion of the output. The Y-axis of the graph is the CPU utilization. The X-axis of the graph is the increment within the time period displayed in the graph. This example shows the individual minutes during the previous hour. The most recent measurement is on the left of the X-axis.

```
Router# show processes cpu history

!--- One minute output omitted

6665776865756676676666667667677676766666766767767666566667
6378016198993513709771991443732358689932740858269643922613
100
```

```
90
80         *  *                     * *     *  * *  *
70  * * ***** *  ** ***** ***  **** ******  *  *******     * *
60  #***##*##*#***#####*#*###*****#*###*#*#*##*#*##*#*##*****#
50  ##########################################################
40  ##########################################################
30  ##########################################################
20  ##########################################################
10  ##########################################################
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
              CPU% per minute (last 60 minutes)
             * = maximum CPU% # = average CPU%

!--- 72-hour output omitted
```

The top two rows, read vertically, display the highest percentage of CPU utilization recorded during the time increment. In this example, the CPU utilization for the last minute recorded is 66 percent. The device may have reached 66 percent only once during that minute, or it may have reached 66 percent multiple times. The device records only the peak reached during the time increment and the average over the course of that increment.

The following is sample output from the **show processes cpu** command that shows an ARP probe process:

```
Router# show processes cpu | include ARP

17       38140    389690         97  0.00%  0.00%  0.00%   0 ARP Input
36           0         1          0  0.00%  0.00%  0.00%   0 IP ARP Probe
40           0         1          0  0.00%  0.00%  0.00%   0 ATM ARP INPUT
80           0         1          0  0.00%  0.00%  0.00%   0 RARP Input
114          0         1          0  0.00%  0.00%  0.00%   0 FR ARP
```

Table 52 describes the fields shown in the output.

Table 52 show processes cpu Field Descriptions

Field	Description
CPU utilization for five seconds	CPU utilization for the last 5 seconds. The second number indicates the percent of CPU time spent at the interrupt level.
one minute	CPU utilization for the last minute.
five minutes	CPU utilization for the last 5 minutes.
PID	Process ID.
Runtime (ms)	CPU time that the process has used (in milliseconds).
Invoked	Number of times that the process has been invoked.
uSecs	Microseconds of CPU time for each process invocation.
5Sec	CPU utilization by task in the last 5 seconds.
1Min	CPU utilization by task in the last minute.
5Min	CPU utilization by task in the last 5 minutes.
TTY	Terminal that controls the process.
Process	Name of the process.

Note Because platforms have a 4- to 8-millisecond clock resolution, run times are considered reliable only after several invocations or a reasonable, measured run time.

Cisco IOS Software Modularity

The following is sample output from the **show processes cpu** command when a Software Modularity image is running:

```
Router# show processes cpu

Total CPU utilization for 5 seconds: 99.6%; 1 minute: 98.5%; 5 minutes: 85.3%
PID       5Sec    1Min     5Min Process
1         0.0%    0.1%     0.8% kernel
3         0.0%    0.0%     0.0% qdelogger
4         0.0%    0.0%     0.0% devc-pty
6         0.7%    0.2%     0.1% devc-ser2681
7         0.0%    0.0%     0.0% dumper.proc
4104      0.0%    0.0%     0.0% pipe
8201      0.0%    0.0%     0.0% mqueue
8202      0.0%    0.0%     0.0% fsdev.proc
8203      0.0%    0.0%     0.0% flashfs_hes_slot1.proc
8204      0.0%    0.0%     0.0% flashfs_hes_slot0.proc
8205      0.0%    0.0%     0.0% flashfs_hes_bootflash.proc
8206      0.0%    0.0%     0.0% dfs_disk2.proc
8207      0.0%    0.0%     0.0% dfs_disk1.proc
8208      0.0%    0.0%     0.0% dfs_disk0.proc
8209      0.0%    0.0%     0.0% ldcache.proc
8210      0.0%    0.0%     0.0% watchdog.proc
8211      0.0%    0.0%     0.0% syslogd.proc
8212      0.0%    0.0%     0.0% name_svr.proc
8213      0.0%    0.1%     0.0% wdsysmon.proc
8214      0.0%    0.0%     0.0% sysmgr.proc
8215      0.0%    0.0%     0.0% kosh.proc
12290     0.0%    0.0%     0.0% chkptd.proc
12312     0.0%    0.0%     0.0% sysmgr.proc
12313     0.0%    0.0%     0.0% syslog_dev.proc
12314     0.0%    0.0%     0.0% itrace_exec.proc
12315     0.0%    0.0%     0.0% packet.proc
12316     0.0%    0.0%     0.0% installer.proc
12317    29.1%   28.5%    19.6% ios-base
12318     0.0%    0.0%     0.0% fh_fd_oir.proc
12319     0.0%    0.0%     0.1% fh_fd_cli.proc
12320     0.0%    0.0%     0.0% fh_metric_dir.proc
12321     0.0%    0.0%     0.0% fh_fd_snmp.proc
12322     0.0%    0.0%     0.0% fh_fd_none.proc
12323     0.0%    0.0%     0.0% fh_fd_intf.proc
12324    48.5%   48.5%    35.8% iprouting.iosproc
12325     0.0%    0.0%     0.0% fh_fd_timer.proc
12326     0.0%    0.0%     0.0% fh_fd_ioswd.proc
12327     0.0%    0.0%     0.0% fh_fd_counter.proc
12328     0.0%    0.0%     0.0% fh_fd_rf.proc
12329     0.0%    0.0%     0.0% fh_server.proc
12330     0.0%    0.0%     0.0% cdp2.iosproc
12331     0.0%    0.0%     0.0% fh_policy_dir.proc
12332     0.0%    0.0%     0.0% ipfs_daemon.proc
12333     0.0%    0.0%     0.0% raw_ip.proc
12334     0.0%    0.0%     0.0% inetd.proc
12335    19.1%   20.4%    12.6% tcp.proc
12336     0.0%    0.0%     0.0% udp.proc
```

Table 53 describes the significant fields shown in the display.

Table 53 show processes cpu (Software Modularity) Field Descriptions

Field	Description
Total CPU utilization for five seconds	Total CPU utilization for the last 5 seconds. The second number indicates the percent of CPU time spent at the interrupt level.
one minute	Total CPU utilization for the last minute.
five minutes	Total CPU utilization for the last 5 minutes.
PID	Process ID.
5Sec	Percentage of CPU time spent at the interrupt level for this process during the last five seconds.
1Min	Percentage of CPU time spent at the interrupt level for this process during the last minute.
5Min	Percentage of CPU time spent at the interrupt level for this process during the last five minutes.
Process	Process name.

The following is partial sample output from the **show processes cpu** command with the **detailed** keyword when a Software Modularity image is running:

```
Router# show processes cpu detailed

Total CPU utilization for 5 seconds: 99.6%; 1 minute: 99.3%; 5 minutes: 88.6%
PID/TID   5Sec    1Min     5Min Process             Prio  STATE        CPU
1         0.0%    0.7%     0.7% kernel                                 8.900
      1   0.4%    0.7%    11.4% [idle thread]          0  Ready        2m28s
      2   0.0%    0.0%     0.0%                       63  Receive      0.000
      3   0.0%    0.0%     0.0%                       10  Receive      0.000
      4   0.0%    0.0%     0.1%                       11  Receive      1.848
      5   0.0%    0.0%     0.0%                       63  Receive      0.000
.
.
.
PID/TID   5Sec    1Min     5Min Process             Prio  STATE        CPU
8214      0.0%    0.0%     0.0% sysmgr.proc                            0.216
      1   0.0%    0.0%     0.0%                       10  Receive      0.132
      2   0.0%    0.0%     0.0%                       10  Sigwaitin    0.000
      3   0.0%    0.0%     0.0%                       10  Receive      0.004
      4   0.0%    0.0%     0.0%                       10  Receive      0.000
      5   0.0%    0.0%     0.0%                       10  Receive      0.000
      6   0.0%    0.0%     0.0%                       10  Receive      0.004
      7   0.0%    0.0%     0.0%                       10  Receive      0.000
      8   0.0%    0.0%     0.0%                       10  Receive      0.000
      9   0.0%    0.0%     0.0%                       10  Receive      0.000
     10   0.0%    0.0%     0.0%                       10  Receive      0.000
     11   0.0%    0.0%     0.0%                       10  Receive      0.000
     12   0.0%    0.0%     0.0%                       10  Receive      0.000
     13   0.0%    0.0%     0.0%                       10  Receive      0.028
     14   0.0%    0.0%     0.0%                       10  Receive      0.040
     15   0.0%    0.0%     0.0%                       10  Receive      0.000
     16   0.0%    0.0%     0.0%                       10  Receive      0.000
     17   0.0%    0.0%     0.0%                       10  Receive      0.004
     18   0.0%    0.0%     0.0%                       10  Receive      0.000
     19   0.0%    0.0%     0.0%                       10  Receive      0.000
     20   0.0%    0.0%     0.0%                        10  Receive      0.000
     21   0.0%    0.0%     0.0%                        10  Receive      0.004
     22   0.0%    0.0%     0.0%                        10  Receive      0.000
PID/TID   5Sec    1Min     5Min Process              Prio  STATE        CPU
8215      0.0%    0.0%     0.0% kosh.proc                               0.044
      1   0.0%    0.0%     0.0%                        10  Reply        0.044
PID/TID   5Sec    1Min     5Min Process              Prio  STATE        CPU
12290     0.0%    0.0%     0.0% chkptd.proc                             0.080
      1   0.0%    0.0%     0.0%                        10  Receive      0.080
      2   0.0%    0.0%     0.0%                        10  Receive      0.000
PID/TID   5Sec    1Min     5Min Process              Prio  STATE        CPU
12312     0.0%    0.0%     0.0% sysmgr.proc                             0.112
      1   0.0%    0.0%     0.0%                        10  Receive      0.112
      2   0.0%    0.0%     0.0%                        10  Sigwaitin    0.000
PID/TID   5Sec    1Min     5Min Process              Prio  STATE        CPU
12316     0.0%    0.0%     0.0% installer.proc                          0.072
      1   0.0%    0.0%     0.0%                        10  Receive      0.000
      3   0.0%    0.0%     0.0%                        10  Nanosleep    0.000
      4   0.0%    0.0%     0.0%                        10  Sigwaitin    0.000
      6   0.0%    0.0%     0.0%                        10  Receive      0.000
Process sbin/ios-base, type IOS, PID = 12317
CPU utilization for five seconds: 12%/9%; one minute: 13%; five minutes: 10%
Task  Runtime(ms)  Invoked  uSecs     5Sec   1Min   5Min TTY Task Name
   1          219     1503    145    0.00%  0.00%  0.00%   0 Hot Service Task
   2        23680    42384    558    2.39%  6.72%  4.81%   0 Service Task
   3         6104    11902    512    3.51%  1.99%  1.23%   0 Service Task
   4         1720     5761    298    1.91%  0.90%  0.39%   0 Service Task
   5            0        5      0    0.00%  0.00%  0.00%   0 Chunk Manager
   6            0        1      0    0.00%  0.00%  0.00%   0 Connection Mgr
   7            4      106     37    0.00%  0.00%  0.00%   0 Load Meter
   8         6240     7376    845    0.23%  0.15%  0.55%   0 Exec
   9          379       62   6112    0.00%  0.07%  0.04%   0 Check heaps
  10            0        1      0    0.00%  0.00%  0.00%   0 Pool Manager
  11            3        2   1500    0.00%  0.00%  0.00%   0 Timers
  12            0        1      0    0.00%  0.00%  0.00%   0 AAA_SERVER_DEADT
  13            0        2      0    0.00%  0.00%  0.00%   0 AAA high-capacit
  14          307      517    593    0.00%  0.05%  0.03%   0 EnvMon
  15            0        1      0    0.00%  0.00%  0.00%   0 OIR Handler
  16          283       58   4879    0.00%  0.04%  0.02%   0 ARP Input
  17            0        2      0    0.00%  0.00%  0.00%   0 Serial Backgroun
  18            0       81      0    0.00%  0.00%  0.00%   0 ALARM_TRIGGER_SC
  19            0        2      0    0.00%  0.00%  0.00%   0 DDR Timers
  20            0        2      0    0.00%  0.00%  0.00%   0 Dialer event
  21            4        2   2000    0.00%  0.00%  0.00%   0 Entity MIB API
  22            0       54      0    0.00%  0.00%  0.00%   0 Compute SRP rate
  23            0        9      0    0.00%  0.00%  0.00%   0 IPC Dynamic Cach
  24            0        1      0    0.00%  0.00%  0.00%   0 IPC Zone Manager
  25            0        1      0    0.00%  0.00%  0.00%   0 IPC Punt Process
  26            4      513      7    0.00%  0.00%  0.00%   0 IPC Periodic Tim
  27           11      513     21    0.00%  0.00%  0.00%   0 IPC Deferred Por
  28            0        1      0    0.00%  0.00%  0.00%   0 IPC Seat Manager
  29           83     1464     56    0.00%  0.00%  0.00%   0 EEM ED Syslog
.
.
.
```

Table 54 describes the significant fields shown in the display.

Table 54 show processes cpu detailed (Software Modularity) Field Descriptions

Field	Description
Total CPU utilization for five seconds	Total CPU utilization for the last 5 seconds. The second number indicates the percent of CPU time spent at the interrupt level.
one minute	Total CPU utilization for the last minute.
five minutes	Total CPU utilization for the last 5 minutes.
PID/TID	Process ID or task ID.
5Sec	Percentage of CPU time spent at the interrupt level for this process during the last five seconds.
1Min	Percentage of CPU time spent at the interrupt level for this process during the last minute.
5Min	Percentage of CPU time spent at the interrupt level for this process during the last five minutes.
Process	Process name.
Prio	Priority level of the process.
STATE	Current state of the process.
CPU	CPU utilization of the process in minutes and seconds.
type	Type of process; can be either IOS or POSIX.
Task	Task sequence number.
Runtime(ms)	CPU time that the process has used (in milliseconds).
Invoked	Number of times that the process has been invoked.
uSecs	Microseconds of CPU time for each process invocation.
5Sec	CPU utilization by task in the last 5 seconds.
1Min	CPU utilization by task in the last minute.
5Min	CPU utilization by task in the last 5 minutes.
TTY	Terminal that controls the process.
Task Name	Task name.

Related Commands

Command	Description
show processes	Displays information about active processes.
show processes memory	Displays the amount of system memory used per system process.

show processes cpu autoprofile hog

To see the CPUHOG profile data, use the **show processes cpu autoprofile hog** command in user EXEC or privileged EXEC mode.

show processes cpu autoprofile hog

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Examples

The following is sample output from the **show processes cpu autoprofile hog** command:

```
Router# show processes cpu autoprofile hog

0x6075DD40 0x60755638
0x6075DD24 0x60755638
0x6075563C 0x60755638
0x60755638 0x60755638
0x60755638 0x60755638
0x6075DD10 0x60755638
0x6075DD40 0x60755638
0x6075DD40 0x60755638
0x6075563C 0x60755638
0x6075DCE0 0x60755638
0x6075DD44 0x60755638
.
.
.
0x6075DCCC 0x60755638
0x6075DCDC 0x60755638
0x6075563C 0x60755638
0x6075DD3C 0x60755638
0x6075DD20 0x60755638
0x6075DD58 0x60755638
0x6075DD1C 0x60755638
0x6075DD10 0x60755638
0x6075DCDC 0x60755638
0x6075DCF8 0x60755638
```

Related Commands

Command	Description
processes cpu autoprofile hog	Enables automatic CPU profiling.

show processes cpu extended

To see an extended CPU load report, use the **show processes cpu extended** command in user EXEC or privileged EXEC mode.

show processes cpu extended [**history**]

Syntax Description

history	(Optional) Displays the extended CPU load statistics for the entire history available, as configured by the **process cpu extended** [**history** *history-size*] command. The absence of the **history** keyword displays only the last report.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Examples

The following is sample output from the **show processes cpu extended** command:

```
Router# show processes cpu extended

################################################################################
Global Statistics
-----------------
5 sec CPU util 0%/0% Timestamp 21:03:56
Queue Statistics
----------------
          Exec Count    Total CPU     Response Time        Queue Length
                                      (avg/max)             (avg/max)
Critical           1          0          0/0                  1/1
High               5          0          0/0                  1/1
Normal           178          0          0/0                  2/9
Low               15          0          0/0                  2/3
Common Process Information
-------------------------------
 PID Name            Prio Style
-------------------------------
CPU Intensive processes
--------------------------------------------------------------------------------
 PID Total       Exec    Quant         Burst  Burst size  Schedcall  Schedcall
     CPUms      Count   avg/max        Count avg/max(ms)      Count Per avg/max
--------------------------------------------------------------------------------
Priority Suspends
------------------------------------
 PID Exec Count Prio-Susps
------------------------------------
Latencies
-------------------------
 PID Exec Count   Latency
```

```
                  avg/max
################################################################################
```

The following is sample output from the **show processes cpu extended history** command:

```
Router# show processes cpu extended history

################################################################################
Global Statistics
-----------------
5 sec CPU util 0%/0% Timestamp 21:04:26
Queue Statistics
----------------
          Exec Count    Total CPU    Response Time         Queue Length
                                      (avg/max)             (avg/max)
Critical           1          0          0/0                   1/1
High               5          0          0/0                   1/1
Normal           179         12          0/12                  2/9
Low               18          0          0/12                  1/3
Common Process Information
-------------------------------
 PID Name            Prio Style
-------------------------------
CPU Intensive processes
-------------------------------------------------------------------------------
 PID Total       Exec    Quant         Burst  Burst size  Schedcall  Schedcall
     CPUms      Count   avg/max        Count avg/max(ms)      Count Per avg/max
-------------------------------------------------------------------------------
Priority Suspends
------------------------------------
 PID Exec Count Prio-Susps
------------------------------------
Latencies
-------------------------
 PID Exec Count   Latency
                  avg/max
-------------------------
################################################################################
Global Statistics
-----------------
5 sec CPU util 0%/0% Timestamp 21:04:21
Queue Statistics
----------------
          Exec Count      Total CPU   Response Time        Queue Length
                                       (avg/max)            (avg/max)
Critical           1          0          0/0                   1/1
High               5          0          0/0                   1/1
Normal           174          0          0/0                   2/9
Low               15          0          0/0                   2/3
Common Process Information
-------------------------------
 PID Name            Prio Style
-------------------------------
CPU Intensive processes
-------------------------------------------------------------------------------
 PID Total       Exec    Quant         Burst  Burst size  Schedcall  Schedcall
     CPUms      Count   avg/max        Count avg/max(ms)      Count Per avg/max
-------------------------------------------------------------------------------
Priority Suspends
------------------------------------
 PID Exec Count Prio-Susps
------------------------------------
```

```
Latencies
-------------------------
 PID Exec Count   Latency
                  avg/max
-------------------------
################################################################################
Global Statistics
-----------------
5 sec CPU util 0%/0% Timestamp 21:03:31
Queue Statistics
----------------
          Exec Count  Total CPU    Response Time           Queue Length
                                    (avg/max)                (avg/max)
Critical           1          0          0/0                   1/1
High               5          0          0/0                   1/1
Normal           176          0          0/0                   2/9
Low               15          0          0/0                   2/3
Common Process Information
-------------------------------
 PID Name            Prio Style
-------------------------------
CPU Intensive processes
-------------------------------------------------------------------------------
 PID Total       Exec    Quant         Burst  Burst size  Schedcall  Schedcall
     CPUms      Count   avg/max        Count avg/max(ms)      Count Per avg/max
-------------------------------------------------------------------------------
Priority Suspends
------------------------------------
 PID Exec Count Prio-Susps
------------------------------------
Latencies
-------------------------
 PID Exec Count   Latency
                  avg/max
-------------------------
```

Related Commands

Command	Description
process cpu extended	Collects the extended CPU load for the specified history size.

show resource all

To display the details of a Resource Owner (RO), use the **show resource all** command in user EXEC or privileged EXEC mode.

show resource all [**brief** | **detailed**]

Syntax Description

brief	(Optional) Displays the brief details of the ROs.
detail	(Optional) Displays all the details of the ROs.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Examples

The following is sample output from the **show resource all** command:

```
Router# show resource all

Resource Owner: cpu
Resource User Type: iosprocess
Resource User: Init(ID: 0x1000001)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777217           0         0          0  0.00%  0.00%  0.00% Init
  Resource User: Scheduler(ID: 0x1000002)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777218           0         0          0  0.00%  0.00%  0.00% Scheduler
  Resource User: Dead(ID: 0x1000003)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777219           0         0          0  0.00%  0.00%  0.00% Dead
  Resource User: Interrupt(ID: 0x1000004)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777220           0         0          0  0.00%  0.00%  0.00% Interrupt
  Resource User: Memory RO RU(ID: 0x1000005)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777221           0         0          0  0.00%  0.00%  0.00% Memory RO RU
  Resource User: Chunk Manager(ID: 0x1000006)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777222           0        13          0  0.00%  0.00%  0.00% Chunk Manager
  Resource User: Load Meter(ID: 0x1000007)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777223        2872     36029         79  0.00%  0.00%  0.00% Load Meter
  Resource User: Check heaps(ID: 0x1000009)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777225      352744     33446      10546  0.00%  0.20%  0.17% Check heaps
  Resource User: Pool Manager(ID: 0x100000A)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777226           0         1          0  0.00%  0.00%  0.00% Pool Manager
```

```
  Resource User: Buffer RO RU(ID: 0x100000B)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777227           0         0          0  0.00%  0.00%  0.00% Buffer RO RU
  Resource User: Timers(ID: 0x100000C)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777228           0         2          0  0.00%  0.00%  0.00% Timers
  Resource User: Serial Background(ID: 0x100000D)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777229           0         2          0  0.00%  0.00%  0.00% Serial Backgroun
  Resource User: AAA_SERVER_DEADTIME(ID: 0x100000E)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777230           0         1          0  0.00%  0.00%  0.00% AAA_SERVER_DEADT
  Resource User: AAA high-capacity counters(ID: 0x100000F)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777231           0         2          0  0.00%  0.00%  0.00% AAA high-capacit
  Resource User: Policy Manager(ID: 0x1000010)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777232           0         1          0  0.00%  0.00%  0.00% Policy Manager
  Resource User: Crash writer(ID: 0x1000011)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777233           0         1          0  0.00%  0.00%  0.00% Crash writer
  Resource User: RO Notify Timers(ID: 0x1000012)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777234           0         1          0  0.00%  0.00%  0.00% RO Notify Timers
  Resource User: RMI RM Notify Watched Policy(ID: 0x1000013)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777235           0         1          0  0.00%  0.00%  0.00% RMI RM Notify Wa
  Resource User: EnvMon(ID: 0x1000014)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777236       11164     92859        120  0.00%  0.00%  0.00% EnvMon
  Resource User: IPC Dynamic Cache(ID: 0x1000015)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777237           0      3004          0  0.00%  0.00%  0.00% IPC Dynamic Cach
  Resource User: IPC Periodic Timer(ID: 0x1000017)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777239           0    180082          0  0.00%  0.00%  0.00% IPC Periodic Tim
  Resource User: IPC Managed Timer(ID: 0x1000018)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777240         572     79749          7  0.00%  0.00%  0.00% IPC Managed Time
  Resource User: IPC Deferred Port Closure(ID: 0x1000019)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777241           4    180088          0  0.00%  0.00%  0.00% IPC Deferred Por
  Resource User: IPC Seat Manager(ID: 0x100001A)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777242       97560   1408799         69  0.23%  0.02%  0.00% IPC Seat Manager
  Resource User: IPC Session Service(ID: 0x100001B)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777243           0         1          0  0.00%  0.00%  0.00% IPC Session Serv
  Resource User: ARP Input(ID: 0x100001C)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777244          20      3082          6  0.00%  0.00%  0.00% ARP Input
  Resource User: EEM ED Syslog(ID: 0x100001D)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
.
.
.
Resource Owner: memory
 Resource User Type: iosprocess
  Resource User: Init(ID: 0x1000001)
Chunk Elements :
Allocated Size(b): 35152564 Count: 91901 Freed Size(b): 31793276 Count: 39159

Processor memory
Total Memory held : 46596832 bytes
```

```
pc = 0x403089D8, size =  10499724, count =    1
pc = 0x402996C8, size =   6737976, count = 8298
pc = 0x402F0C9C, size =   5821352, count =   10
pc = 0x40A25134, size =   4194324, count =    1
pc = 0x41D6D414, size =   1704144, count =   52
pc = 0x40451BE0, size =   1114180, count =   17
pc = 0x402D0DAC, size =    917600, count =    1
pc = 0x4043E5F4, size =    836076, count = 12291
pc = 0x404A276C, size =    617476, count =    1
pc = 0x41CDED1C, size =    569844, count =  125
pc = 0x4194C2D0, size =    524292, count =    1
pc = 0x405FD93C, size =    516100, count =    1
pc = 0x414D67AC, size =    473224, count =  199
pc = 0x41016294, size =    458756, count =    1
pc = 0x4046E618, size =    432096, count =    1
pc = 0x400A1134, size =    412420, count =    1
pc = 0x402ABB50, size =    317316, count =   93
pc = 0x41D53668, size =    262148, count =    1
pc = 0x4049BA04, size =    206640, count =   84
pc = 0x41E3FE30, size =    196620, count =    3
pc = 0x40B05214, size =    196612, count =    1
pc = 0x40494D94, size =    180180, count = 4095
pc = 0x402ABB6C, size =    144708, count =   93
pc = 0x41586A38, size =    144004, count =    1
pc = 0x4030B408, size =    140028, count =    7
pc = 0x415090EC, size =    131768, count =    4
pc = 0x41E37B94, size =    131088, count =    4
pc = 0x4195C348, size =    131076, count =    1
pc = 0x400A1194, size =    124420, count =    1
pc = 0x41503BC4, size =    122768, count =    1
pc = 0x404E888C, size =    114660, count = 4095
pc = 0x40494D50, size =    114660, count = 4095
pc = 0x404D99B0, size =    114660, count = 4095
pc = 0x4023F5B4, size =     98312, count =    2
pc = 0x41E45894, size =     97456, count =  626
pc = 0x41E2D4C4, size =     91584, count =   12
pc = 0x416D9768, size =     84004, count =    1
pc = 0x40452790, size =     84000, count = 3000
pc = 0x40322A74, size =     81948, count =    7
pc = 0x41D0FF4C, size =     81924, count =    1
pc = 0x40E9F7B0, size =     81364, count =    1
pc = 0x414FB1BC, size =     78740, count =    2
pc = 0x414D4A64, size =     72916, count =    2
pc = 0x40328770, size =     72144, count =   36
pc = 0x414FA938, size =     71592, count =    2
pc = 0x414EF938, size =     71096, count =    2
pc = 0x41947EEC, size =     65540, count =    1
pc = 0x41935B5C, size =     65540, count =    1
pc = 0x4193A348, size =     65540, count =    1
pc = 0x4193FF5C, size =     65540, count =    1
pc = 0x41D6E32C, size =     65540, count =    1
pc = 0x41DD534C, size =     65540, count =    1
pc = 0x414B5870, size =     65540, count =    1
pc = 0x4078521C, size =     65540, count =    1
.
.
.
I/O memory
Total Memory held : 9816224 bytes
pc = 0x4029983C, size =   9791584, count = 8290
pc = 0x403EC2A4, size =      8208, count =    1
pc = 0x403F8CD0, size =      8208, count =    1
pc = 0x403EC2E0, size =      4112, count =    1
pc = 0x403F8D0C, size =      4112, count =    1
```

```
Resource User: Scheduler(ID: 0x1000002)
Chunk Elements :
Allocated Size(b): 0 Count: 0 Freed Size(b): 0 Count: 0

Processor memory
Total Memory held : 13052 bytes
pc = 0x4037BCC8, size =     12004, count =    1
pc = 0x40327110, size =      1048, count =   24

Resource User: Dead(ID: 0x1000003)
Chunk Elements :
Allocated Size(b): 0 Count: 0 Freed Size(b): 0 Count: 0

Processor memory
Total Memory held : 447448 bytes
pc = 0x404A276C, size =    395636, count =    5
pc = 0x4043E5F4, size =     18676, count =  271
pc = 0x40494D94, size =      6888, count =   82
pc = 0x4044B9E4, size =      6672, count =    6
pc = 0x40C8BAB4, size =      5780, count =   34
pc = 0x404943DC, size =      2836, count =   82
pc = 0x40494D50, size =      2796, count =   82
pc = 0x4044DAF0, size =      2224, count =    2
pc = 0x40393168, size =      1772, count =    1
pc = 0x40FF2688, size =       728, count =    6
pc = 0x40CBC5A4, size =       400, count =    4
pc = 0x40455144, size =       320, count =   10
pc = 0x40C9A8D8, size =       288, count =    8
pc = 0x40CADE10, size =       260, count =    5
pc = 0x40B19484, size =       256, count =    2
pc = 0x4052BD2C, size =       208, count =    4
pc = 0x40CADE50, size =       188, count =    5
pc = 0x4044FBD8, size =       184, count =    1
pc = 0x40A9B2F0, size =       184, count =    1
pc = 0x40CBC45C, size =       160, count =    2
pc = 0x4038BF34, size =       144, count =    2
pc = 0x40529610, size =       136, count =    2
pc = 0x405CF034, size =       104, count =    1
pc = 0x414D67AC, size =       104, count =    1
pc = 0x4038BF68, size =        88, count =    2
pc = 0x4044F078, size =        84, count =    3
pc = 0x41555624, size =        84, count =    1
pc = 0x40685250, size =        76, count =    1
pc = 0x40481AD4, size =        68, count =    1
pc = 0x4044DB18, size =        56, count =    2
pc = 0x401B6960, size =        48, count =    1

Resource User: Interrupt(ID: 0x1000004)
Chunk Elements :
Allocated Size(b): 0 Count: 0 Freed Size(b): 39652 Count: 1070

Processor memory
Total Memory held : 0 bytes

Resource User: Memory RO RU(ID: 0x1000005)
Chunk Elements :
Allocated Size(b): 12320 Count: 120 Freed Size(b): 10164 Count: 99

Processor memory
Total Memory held : 131080 bytes
pc = 0x40357C54, size =     65540, count =    1
pc = 0x40357D98, size =     65540, count =    1
```

```
Resource User: Chunk Manager(ID: 0x1000006)
Chunk Elements :
Allocated Size(b): 124 Count: 6 Freed Size(b): 48 Count: 3

Processor memory
Total Memory held : 9788 bytes
pc = 0x4037BCC8, size =      6004, count =    1
pc = 0x40332490, size =      3008, count =    2
pc = 0x4035E160, size =       636, count =    1
pc = 0x403604BC, size =       140, count =    1

Resource User: Load Meter(ID: 0x1000007)
Chunk Elements :
Allocated Size(b): 44 Count: 1 Freed Size(b): 44 Count: 1

Processor memory
Total Memory held : 3780 bytes
pc = 0x4037BCC8, size =      3004, count =    1
pc = 0x4035E160, size =       636, count =    1
pc = 0x403604BC, size =       140, count =    1

Resource User: Check heaps(ID: 0x1000009)
Chunk Elements :
Allocated Size(b): 44 Count: 1 Freed Size(b): 44 Count: 1

Processor memory
Total Memory held : 7236 bytes
pc = 0x4037BCC8, size =      6004, count =    1
pc = 0x4035E160, size =       636, count =    1
pc = 0x41E2B0D0, size =       324, count =    1
pc = 0x403604BC, size =       140, count =    1
pc = 0x40351D2C, size =        76, count =    1
pc = 0x40351CF8, size =        56, count =    1

Resource User: Pool Manager(ID: 0x100000A)
Chunk Elements :
Allocated Size(b): 44 Count: 1 Freed Size(b): 0 Count: 0

Processor memory
Total Memory held : 6780 bytes
pc = 0x4037BCC8, size =      6004, count =    1
pc = 0x4035E160, size =       636, count =    1
pc = 0x403604BC, size =       140, count =    1

Resource User: Buffer RO RU(ID: 0x100000B)
Chunk Elements :
Allocated Size(b): 4960 Count: 40 Freed Size(b): 4092 Count: 33

Processor memory
Total Memory held : 0 bytes

Resource User: Timers(ID: 0x100000C)
Chunk Elements :
Allocated Size(b): 44 Count: 1 Freed Size(b): 44 Count: 1
.
.
.
Resource User: PF_Init Process(ID: 0x100004F)
Chunk Elements :
Allocated Size(b): 8104 Count: 126 Freed Size(b): 1400 Count: 29

Processor memory
Total Memory held : 31204 bytes
pc = 0x4027EF10, size =     21540, count =    5
pc = 0x4037BCC8, size =      6004, count =    1
pc = 0x4044DAF0, size =      1112, count =    1
pc = 0x4035E160, size =       636, count =    1
pc = 0x4038BF68, size =       308, count =    7
pc = 0x4038BF34, size =       280, count =    7
pc = 0x403604BC, size =       280, count =    2
pc = 0x41E45ED0, size =       240, count =    5
pc = 0x401FB400, size =       236, count =    5
pc = 0x40529610, size =       136, count =    2
pc = 0x4047D560, size =       108, count =    2
pc = 0x4038C114, size =        88, count =    2
pc = 0x4044DB18, size =        72, count =    1
pc = 0x40211DCC, size =        56, count =    2
pc = 0x4038E038, size =        44, count =    1
pc = 0x40402C98, size =        32, count =    1
pc = 0x40455144, size =        32, count =    1

Resource User: PF_Split Sync Process(ID: 0x1000052)
Chunk Elements :
Allocated Size(b): 6092 Count: 87 Freed Size(b): 5644 Count: 81

Processor memory
Total Memory held : 10356 bytes
pc = 0x4037BCC8, size =      6004, count =    1
pc = 0x4060364C, size =      1760, count =   10
pc = 0x41E45894, size =       960, count =    2
pc = 0x4060AE18, size =       856, count =   10
pc = 0x4035E160, size =       636, count =    1
pc = 0x403604BC, size =       140, count =    1

Resource User: RPC pf-split-rp(ID: 0x1000053)
Chunk Elements :
Allocated Size(b): 1348 Count: 20 Freed Size(b): 1304 Count: 19

Processor memory
Total Memory held : 6780 bytes
pc = 0x4037BCC8, size =      6004, count =    1
pc = 0x4035E160, size =       636, count =    1
pc = 0x403604BC, size =       140, count =    1

Resource User: RPC idprom-MP(ID: 0x1000054)
Chunk Elements :
Allocated Size(b): 4708 Count: 68 Freed Size(b): 4664 Count: 67

Processor memory
Total Memory held : 16648 bytes
pc = 0x405023D4, size =      9732, count =   18
pc = 0x4037BCC8, size =      6004, count =    1
pc = 0x4035E160, size =       636, count =    1
pc = 0x403604BC, size =       140, count =    1
pc = 0x405D000C, size =       136, count =    1

Resource User: Net Input(ID: 0x1000055)
Chunk Elements :
Allocated Size(b): 88 Count: 2 Freed Size(b): 0 Count: 0

Processor memory
Total Memory held : 6780 bytes
pc = 0x4037BCC8, size =      6004, count =    1
pc = 0x4035E160, size =       636, count =    1
pc = 0x403604BC, size =       140, count =    1
```

```
Resource User: Compute load avgs(ID: 0x1000056)
Chunk Elements :
Allocated Size(b): 11948724 Count: 215941 Freed Size(b): 11948724 Count: 215941

Processor memory
Total Memory held : 10720 bytes
pc = 0x4037BCC8, size =      6004, count =    1
pc = 0x404FC9C0, size =      3940, count =    1
pc = 0x4035E160, size =       636, count =    1
pc = 0x403604BC, size =       140, count =    1

Resource User: RTTYS Process(ID: 0x1000057)
Chunk Elements :
Allocated Size(b): 44 Count: 1 Freed Size(b): 0 Count: 0

Processor memory
Total Memory held : 6780 bytes
pc = 0x4037BCC8, size =      6004, count =    1
pc = 0x4035E160, size =       636, count =    1
pc = 0x403604BC, size =       140, count =    1

Resource User: BACK CHECK(ID: 0x1000059)
Chunk Elements :
Allocated Size(b): 0 Count: 0 Freed Size(b): 0 Count: 0

Processor memory
Total Memory held : 6780 bytes
pc = 0x4037BCC8, size =      6004, count =    1
pc = 0x4035E160, size =       636, count =    1
pc = 0x403604BC, size =       140, count =    1

Resource User: chkpt message handler(ID: 0x100005A)
Chunk Elements :
Allocated Size(b): 156 Count: 2 Freed Size(b): 0 Count: 0

Processor memory
Total Memory held : 6780 bytes
pc = 0x4037BCC8, size =      6004, count =    1
pc = 0x4035E160, size =       636, count =    1
pc = 0x403604BC, size =       140, count =    1

Resource User: cpf_process_msg_holdq(ID: 0x100005B)
Chunk Elements :
Allocated Size(b): 152 Count: 3 Freed Size(b): 0 Count: 0
.
.
.
Resource Owner: Buffer
 Resource User Type: iosprocess
  Resource User: Init(ID: 0x1000001)
Getbufs  Retbufs  Holding  RU Name
1367     31237    4294937426 Init

Resource User: Scheduler(ID: 0x1000002)
Getbufs  Retbufs  Holding  RU Name
0        0        0        Scheduler

Resource User: Dead(ID: 0x1000003)
Getbufs  Retbufs  Holding  RU Name
6        3        3        Dead

Resource User: Interrupt(ID: 0x1000004)
Getbufs  Retbufs  Holding  RU Name
221580   221580   0        Interrupt
```

```
Resource User: Memory RO RU(ID: 0x1000005)
Getbufs  Retbufs  Holding  RU Name
0        0        0        Memory RO RU

Resource User: Chunk Manager(ID: 0x1000006)
Getbufs  Retbufs  Holding  RU Name
0        0        0        Chunk Manager

Resource User: Load Meter(ID: 0x1000007)
Getbufs  Retbufs  Holding  RU Name
0        0        0        Load Meter

Resource User: Check heaps(ID: 0x1000009)
Getbufs  Retbufs  Holding  RU Name
0        0        0        Check heaps

Resource User: Pool Manager(ID: 0x100000A)
Getbufs  Retbufs  Holding  RU Name
5554     0        5554     Pool Manager

Resource User: Buffer RO RU(ID: 0x100000B)
Getbufs  Retbufs  Holding  RU Name
0        0        0        Buffer RO RU

Resource User: Timers(ID: 0x100000C)
Getbufs  Retbufs  Holding  RU Name
0        0        0        Timers

Resource User: Serial Background(ID: 0x100000D)
Getbufs  Retbufs  Holding  RU Name
0        0        0        Serial Backgroun

Resource User: AAA_SERVER_DEADTIME(ID: 0x100000E)
Getbufs  Retbufs  Holding  RU Name
0        0        0        AAA_SERVER_DEADT

Resource User: AAA high-capacity counters(ID: 0x100000F)
Getbufs  Retbufs  Holding  RU Name
0        0        0        AAA high-capacit

Resource User: Policy Manager(ID: 0x1000010)
Getbufs  Retbufs  Holding  RU Name
0        0        0        Policy Manager

Resource User: Crash writer(ID: 0x1000011)
Getbufs  Retbufs  Holding  RU Name
0        0        0        Crash writer

Resource User: RO Notify Timers(ID: 0x1000012)
Getbufs  Retbufs  Holding  RU Name
0        0        0        RO Notify Timers

Resource User: RMI RM Notify Watched Policy(ID: 0x1000013)
Getbufs  Retbufs  Holding  RU Name
0        0        0        RMI RM Notify Wa

.
.
.
Resource User: DHCPD Timer(ID: 0x100011B)
Getbufs  Retbufs  Holding  RU Name
0        0        0        DHCPD Timer

Resource User: DHCPD Database(ID: 0x100011C)
```

```
Getbufs  Retbufs  Holding  RU Name
0        0        0        DHCPD Database

Resource User: draco-oir-process:slot 2(ID: 0x100011E)
Getbufs  Retbufs  Holding  RU Name
0        0        0        draco-oir-proces

Resource User: SCP async: Draco-LC4(ID: 0x1000125)
Getbufs  Retbufs  Holding  RU Name
35849    243101   4294760044 SCP async: Draco

Resource User: IFCOM Msg Hdlr(ID: 0x1000127)
Getbufs  Retbufs  Holding  RU Name
2        2        0        IFCOM Msg Hdlr

Resource User: IFCOM Msg Hdlr(ID: 0x1000128)
Getbufs  Retbufs  Holding  RU Name
28       28       0        IFCOM Msg Hdlr

Resource User: Exec(ID: 0x100012C)
Getbufs  Retbufs  Holding  RU Name
912      912      0        Exec

Resource Owner: test_mem
Resource User Type: test_process
Resource User Type: mem_rut
Resource Owner: test_cpu
Resource User Type: test_process
Resource User Type: cpu_rut
```

The following is a sample output from the **show resource all brief** command:

```
Router# show resource all brief

Resource Owner: cpu
 Resource User Type: iosprocess
  Resource User: Init(ID: 0x1000001)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777217           0         0           0  0.00%  0.00%  0.00% Init
  Resource User: Scheduler(ID: 0x1000002)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777218           0         0           0  0.00%  0.00%  0.00% Scheduler
  Resource User: Dead(ID: 0x1000003)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777219           0         0           0  0.00%  0.00%  0.00% Dead
  Resource User: Interrupt(ID: 0x1000004)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777220           0         0           0  0.00%  0.00%  0.00% Interrupt
  Resource User: Memory RO RU(ID: 0x1000005)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777221           0         0           0  0.00%  0.00%  0.00% Memory RO RU
  Resource User: Chunk Manager(ID: 0x1000006)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777222           0        13           0  0.00%  0.00%  0.00% Chunk Manager
  Resource User: Load Meter(ID: 0x1000007)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777223        2872     36069          79  0.00%  0.00%  0.00% Load Meter
  Resource User: Check heaps(ID: 0x1000009)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777225      353092     33481       10546  0.00%  0.17%  0.17% Check heaps
  Resource User: Pool Manager(ID: 0x100000A)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777226           0         1           0  0.00%  0.00%  0.00% Pool Manager
  Resource User: Buffer RO RU(ID: 0x100000B)
```

```
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777227           0         0          0  0.00%  0.00%  0.00% Buffer RO RU
  Resource User: Timers(ID: 0x100000C)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777228           0         2          0  0.00%  0.00%  0.00% Timers
  Resource User: Serial Background(ID: 0x100000D)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777229           0         2          0  0.00%  0.00%  0.00% Serial Backgroun
  Resource User: AAA_SERVER_DEADTIME(ID: 0x100000E)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777230           0         1          0  0.00%  0.00%  0.00% AAA_SERVER_DEADT
  Resource User: AAA high-capacity counters(ID: 0x100000F)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777231           0         2          0  0.00%  0.00%  0.00% AAA high-capacit
  Resource User: Policy Manager(ID: 0x1000010)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777232           0         1          0  0.00%  0.00%  0.00% Policy Manager
  Resource User: Crash writer(ID: 0x1000011)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777233           0         1          0  0.00%  0.00%  0.00% Crash writer
  Resource User: RO Notify Timers(ID: 0x1000012)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777234           0         1          0  0.00%  0.00%  0.00% RO Notify Timers
  Resource User: RMI RM Notify Watched Policy(ID: 0x1000013)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777235           0         1          0  0.00%  0.00%  0.00% RMI RM Notify Wa
  Resource User: EnvMon(ID: 0x1000014)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777236       11176     92958        120  0.00%  0.00%  0.00% EnvMon
  Resource User: IPC Dynamic Cache(ID: 0x1000015)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777237           0      3007          0  0.00%  0.00%  0.00% IPC Dynamic Cach
  Resource User: IPC Periodic Timer(ID: 0x1000017)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777239           0    180279          0  0.00%  0.00%  0.00% IPC Periodic Tim
  Resource User: IPC Managed Timer(ID: 0x1000018)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777240         572     79833          7  0.00%  0.00%  0.00% IPC Managed Time
  Resource User: IPC Deferred Port Closure(ID: 0x1000019)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777241           4    180285          0  0.00%  0.00%  0.00% IPC Deferred Por
  Resource User: IPC Seat Manager(ID: 0x100001A)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777242       97684   1410183         69  0.00%  0.03%  0.00% IPC Seat Manager
  Resource User: IPC Session Service(ID: 0x100001B)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777243           0         1          0  0.00%  0.00%  0.00% IPC Session Serv
  Resource User: ARP Input(ID: 0x100001C)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777244          20      3085          6  0.00%  0.00%  0.00% ARP Input
  Resource User: EEM ED Syslog(ID: 0x100001D)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777245           0        49          0  0.00%  0.00%  0.00% EEM ED Syslog
  Resource User: DDR Timers(ID: 0x100001E)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777246           0         2          0  0.00%  0.00%  0.00% DDR Timers
  Resource User: Dialer event(ID: 0x100001F)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777247           0         2          0  0.00%  0.00%  0.00% Dialer event
  Resource User: Entity MIB API(ID: 0x1000020)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777248          28        16       1750  0.00%  0.00%  0.00% Entity MIB API
  Resource User: Compute SRP rates(ID: 0x1000021)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
```

```
16777249           0     18037          0  0.00%  0.00%  0.00% Compute SRP rate
  Resource User: SERIAL A'detect(ID: 0x1000022)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777250           0         1          0  0.00%  0.00%  0.00% SERIAL A'detect
  Resource User: GraphIt(ID: 0x1000023)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777251           0    180267          0  0.00%  0.00%  0.00% GraphIt
  Resource User: rf proxy rp agent(ID: 0x1000024)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777252          40       416         96  0.00%  0.00%  0.00% rf proxy rp agen
  Resource User: HC Counter Timers(ID: 0x1000025)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777253          60     41360          1  0.00%  0.00%  0.00% HC Counter Timer
  Resource User: Snmp ICC Process(ID: 0x1000026)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777254           0         1          0  0.00%  0.00%  0.00% Snmp ICC Process
  Resource User: Cat6k SNMP(ID: 0x1000027)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777255          20        29        689  0.00%  0.00%  0.00% Cat6k SNMP
  Resource User: Cat6k SNMP Trap handler(ID: 0x1000028)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777256           0         7          0  0.00%  0.00%  0.00% Cat6k SNMP Trap
  Resource User: Critical Bkgnd(ID: 0x1000029)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777257           0         1          0  0.00%  0.00%  0.00% Critical Bkgnd
  Resource User: Net Background(ID: 0x100002A)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777258         112     44787          2  0.00%  0.00%  0.00% Net Background
  Resource User: Logger(ID: 0x100002B)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777259           0        50          0  0.00%  0.00%  0.00% Logger
  Resource User: TTY Background(ID: 0x100002C)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777260           0    180263          0  0.00%  0.00%  0.00% TTY Background
  Resource User: Per-Second Jobs(ID: 0x100002D)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777261          52    180549          0  0.00%  0.00%  0.00% Per-Second Jobs
  Resource User: Per-minute Jobs(ID: 0x100002E)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
.
.
.
Resource User: Exec(ID: 0x100012C)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777516        8964       965       9289  0.39%  0.66%  1.55% Exec
Resource Owner: memory
 Resource User Type: iosprocess
  Resource User: Init(ID: 0x1000001)
Processor memory
Allocated   Freed  Holding   Blocks
55233064  8636232 46596832    48832

I/O memory
Allocated   Freed  Holding   Blocks
 9816224        0  9816224     8294

  Resource User: Scheduler(ID: 0x1000002)
Processor memory
Allocated   Freed  Holding   Blocks
   13052        0    13052       25

  Resource User: Dead(ID: 0x1000003)
Processor memory
Allocated   Freed  Holding   Blocks
```

```
  687916   240468   447448      630

  Resource User: Interrupt(ID: 0x1000004)
Processor memory
Allocated   Freed  Holding   Blocks
       0        0        0        0

  Resource User: Memory RO RU(ID: 0x1000005)
Processor memory
Allocated   Freed  Holding   Blocks
  131080        0   131080        2

  Resource User: Chunk Manager(ID: 0x1000006)
Processor memory
Allocated   Freed  Holding   Blocks
   14300     4512     9788        5

  Resource User: Load Meter(ID: 0x1000007)
Processor memory
Allocated   Freed  Holding   Blocks
    3920      140     3780        3

  Resource User: Check heaps(ID: 0x1000009)
Processor memory
Allocated   Freed  Holding   Blocks
    7376      140     7236        6

  Resource User: Pool Manager(ID: 0x100000A)
Processor memory
Allocated   Freed  Holding   Blocks
    6780        0     6780        3

  Resource User: Buffer RO RU(ID: 0x100000B)
Processor memory
Allocated   Freed  Holding   Blocks
       0        0        0        0

  Resource User: Timers(ID: 0x100000C)
Processor memory
Allocated   Freed  Holding   Blocks
    6920      140     6780        3

  Resource User: Serial Background(ID: 0x100000D)
Processor memory
Allocated   Freed  Holding   Blocks
    6920      140     6780        3
.
.
.
Resource User: IFCOM Msg Hdlr(ID: 0x1000128)
Getbufs  Retbufs  Holding  RU Name
28       28       0        IFCOM Msg Hdlr

  Resource User: Exec(ID: 0x100012C)
Getbufs  Retbufs  Holding  RU Name
1404     1404     0        Exec

Resource Owner: test_mem
 Resource User Type: test_process
 Resource User Type: mem_rut
Resource Owner: test_cpu
 Resource User Type: test_process
 Resource User Type: cpu_rut
```

The following is sample output from the **show resource all detailed** command:

```
Router# show resource all detailed

Resource Owner: cpu
 Resource User Type: iosprocess
  Resource User: Init(ID: 0x1000001)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777217           0         0          0  0.00%  0.00%  0.00% Init
  Resource User: Scheduler(ID: 0x1000002)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777218           0         0          0  0.00%  0.00%  0.00% Scheduler
  Resource User: Dead(ID: 0x1000003)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777219           0         0          0  0.00%  0.00%  0.00% Dead
  Resource User: Interrupt(ID: 0x1000004)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777220           0         0          0  0.00%  0.00%  0.00% Interrupt
  Resource User: Memory RO RU(ID: 0x1000005)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777221           0         0          0  0.00%  0.00%  0.00% Memory RO RU
  Resource User: Chunk Manager(ID: 0x1000006)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777222           0        13          0  0.00%  0.00%  0.00% Chunk Manager
  Resource User: Load Meter(ID: 0x1000007)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777223        2872     36075         79  0.00%  0.00%  0.00% Load Meter
  Resource User: Check heaps(ID: 0x1000009)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777225      353168     33486      10546  0.00%  0.10%  0.15% Check heaps
  Resource User: Pool Manager(ID: 0x100000A)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777226           0         1          0  0.00%  0.00%  0.00% Pool Manager
  Resource User: Buffer RO RU(ID: 0x100000B)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777227           0         0          0  0.00%  0.00%  0.00% Buffer RO RU
  Resource User: Timers(ID: 0x100000C)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777228           0         2          0  0.00%  0.00%  0.00% Timers
  Resource User: Serial Background(ID: 0x100000D)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777229           0         2          0  0.00%  0.00%  0.00% Serial Backgroun
  Resource User: AAA_SERVER_DEADTIME(ID: 0x100000E)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777230           0         1          0  0.00%  0.00%  0.00% AAA_SERVER_DEADT
  Resource User: AAA high-capacity counters(ID: 0x100000F)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777231           0         2          0  0.00%  0.00%  0.00% AAA high-capacit
  Resource User: Policy Manager(ID: 0x1000010)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777232           0         1          0  0.00%  0.00%  0.00% Policy Manager
  Resource User: Crash writer(ID: 0x1000011)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777233           0         1          0  0.00%  0.00%  0.00% Crash writer
  Resource User: RO Notify Timers(ID: 0x1000012)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777234           0         1          0  0.00%  0.00%  0.00% RO Notify Timers
  Resource User: RMI RM Notify Watched Policy(ID: 0x1000013)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777235           0         1          0  0.00%  0.00%  0.00% RMI RM Notify Wa
  Resource User: EnvMon(ID: 0x1000014)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777236       11176     92958        120  0.00%  0.00%  0.00% EnvMon
  Resource User: IPC Dynamic Cache(ID: 0x1000015)
```

```
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777237           0      3008          0  0.00%  0.00%  0.00% IPC Dynamic Cach
  Resource User: IPC Periodic Timer(ID: 0x1000017)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
.
.
.
Resource Owner: memory
 Resource User Type: iosprocess
  Resource User: Init(ID: 0x1000001)
Chunk Elements :
Allocated Size(b): 35152564 Count: 91901 Freed Size(b): 31793276 Count: 39159

Processor memory
 Address      Bytes     Prev     Next Ref   Alloc PC  What
4393BAA0 0010499772 00000000 4433F15C 001 513DD000  *Init*
4433F15C 0000012852 4393BAA0 44342390 001 513DD000  *Init*
44342390 0000005052 4433F15C 4434374C 001 513DD000  List Headers
4434374C 0000000096 44342390 443437AC 001 513DD000  *Init*
443437AC 0000000096 4434374C 4434380C 001 513DD000  *Init*
4434380C 0000000096 443437AC 4434386C 001 513DD000  *Init*
4434386C 0000000096 4434380C 443438CC 001 513DD000  *Init*
443438CC 0000000096 4434386C 4434392C 001 513DD000  *Init*
4434392C 0000004356 443438CC 44344A30 001 513DD000  TTY data
44344A30 0000000564 4434392C 44344C64 001 513DD000  TTY Output Buf
44344C64 0000000096 44344A30 44344CC4 001 513DD000  *Init*
44344CC4 0000001552 44344C64 443452D4 001 513DD000  Watched messages
443452D4 0000010052 44344CC4 44347A18 001 513DD000  Watched Boolean
44347A18 0000001552 443452D4 44348028 001 513DD000  Watched Semaphore
44348028 0000000380 44347A18 443481A4 001 513DD000  Watched Message Queue
443481A4 0000003052 44348028 44348D90 001 513DD000  Read/Write Locks
44348D90 0000020052 443481A4 4434DBE4 001 513DD000  RMI-RO_RU Chunks
4434DBE4 0000000116 44348D90 4434DC58 001 513DD000  Resource Owner IDs
4434DC58 0000001552 4434DBE4 4434E268 001 513DD000  String-DB entries
4434E268 0000000532 4434DC58 4434E47C 001 513DD000  String-DB handles
4434E47C 0000000076 4434E268 4434E4C8 001 513DD000  NameDB String
4434E4C8 0000000116 4434E47C 4434E53C 001 513DD000  Resource User Type IDs
4434E53C 0000000184 4434E4C8 4434E5F4 001 513DD000  *Init*
4434E5F4 0000002100 4434E53C 4434EE28 001 513DD000  Resource Owner IDs
4434EE28 0000000076 4434E5F4 4434EE74 001 513DD000  NameDB String
4434EE74 0000000076 4434EE28 4434EEC0 001 513DD000  NameDB String
4434EEC0 0000065588 4434EE74 4435EEF4 001 513DD000  Buffer RU Notify Chunks
44360754 0000000076 44360698 443607A0 001 513DD000  *Init*
443607A0 0000002100 44360754 44360FD4 001 513DD000  Resource User Type IDs
44360FD4 0000004148 443607A0 44362008 001 513DD000  Resource User IDs
44362008 0000000076 44360FD4 44362054 001 513DD000  NameDB String
44362054 0000000076 44362008 443620A0 001 513DD000  NameDB String
443620A0 0000000096 44362054 44362100 001 513DD000  *Init*
443623AC 0000000076 44362100 443623F8 001 513DD000  NameDB String
443623F8 0000010052 443623AC 44364B3C 001 513DD000  List Elements
44364B3C 0000010052 443623F8 44367280 001 513DD000  List Elements
4436758C 0000001552 4436752C 44367B9C 001 513DD000  Reg Function iList
44367B9C 0000000164 4436758C 44367C40 001 513DD000  *Init*
44367C40 0000000076 44367B9C 44367C8C 001 513DD000  Parser Linkage
44367C8C 0000000076 44367C40 44367CD8 001 513DD000  Parser Linkage
44367CD8 0000000076 44367C8C 44367D24 001 513DD000  Parser Linkage
44367D70 0000000076 44367D24 44367DBC 001 513DD000  Parser Linkage
44367DBC 0000000076 44367D70 44367E08 001 513DD000  Cond Debug definition
44367E08 0000000076 44367DBC 44367E54 001 513DD000  Parser Linkage
44367E54 0000000076 44367E08 44367EA0 001 513DD000  Cond Debug definition
44367EA0 0000000076 44367E54 44367EEC 001 513DD000  Cond Debug definition
44367EEC 0000000076 44367EA0 44367F38 001 513DD000  Cond Debug definition
44367F38 0000000076 44367EEC 44367F84 001 513DD000  Cond Debug definition
44367F84 0000000384 44367F38 44368104 001 513DD000  *Init*
```

```
4436B5C8 0000000076 4436B57C 4436B614 001 513DD000  Init
4436B614 0000000076 4436B5C8 4436B660 001 513DD000  Init
4436B660 0000000076 4436B614 4436B6AC 001 513DD000  Init
4436BC04 0000000076 4436BBB8 4436BC50 001 513DD000  Init
4436BC50 0000003460 4436BC04 4436C9D4 001 513DD000  *Hardware IDB*
4436C9D4 0000000076 4436BC50 4436CA20 001 513DD000  Init
4436CA20 0000001080 4436C9D4 4436CE58 001 513DD000  Index Table Block
4436CE58 0000000076 4436CA20 4436CEA4 001 513DD000  Init
4436CEA4 0000000076 4436CE58 4436CEF0 001 513DD000  Init
4436CEF0 0000000308 4436CEA4 4436D024 001 513DD000  Init
4436D024 0000000076 4436CEF0 4436D070 001 513DD000  NameDB String
4436D070 0000000104 4436D024 4436D0D8 001 513DD000  NameDB String
4436D434 0000000096 4436D188 4436D494 001 513DD000  Init
4436D740 0000000096 4436D494 4436D7A0 001 513DD000  Init
4436D7A0 0000010052 4436D740 4436FEE4 001 513DD000  Packet Elements
4436FEE4 0000000372 4436D7A0 44370058 001 513DD000  Pool Info
44370058 0000000372 4436FEE4 443701CC 001 513DD000  Pool Info
443701CC 0000000372 44370058 44370340 001 513DD000  Pool Info
44370340 0000000860 443701CC 4437069C 001 513DD000  *Packet Header*
4437069C 0000000372 44370340 44370810 001 513DD000  Pool Info
44370810 0000000860 4437069C 44370B6C 001 513DD000  *Packet Header*
44370B6C 0000000860 44370810 44370EC8 001 513DD000  *Packet Header*
44370EC8 0000000860 44370B6C 44371224 001 513DD000  *Packet Header*
44371224 0000000860 44370EC8 44371580 001 513DD000  *Packet Header*
44371580 0000000860 44371224 443718DC 001 513DD000  *Packet Header*
443718DC 0000000860 44371580 44371C38 001 513DD000  *Packet Header*
44371C38 0000000860 443718DC 44371F94 001 513DD000  *Packet Header*
44371F94 0000000860 44371C38 443722F0 001 513DD000  *Packet Header*
443722F0 0000000860 44371F94 4437264C 001 513DD000  *Packet Header*
4437264C 0000000860 443722F0 443729A8 001 513DD000  *Packet Header*
443729A8 0000000860 4437264C 44372D04 001 513DD000  *Packet Header*
.
.
.
Resource User: Compute SRP rates(ID: 0x1000021)
Chunk Elements :
Allocated Size(b): 0 Count: 0 Freed Size(b): 0 Count: 0

Processor memory
 Address      Bytes     Prev     Next Ref   Alloc PC  What
446D502C 0000006052 446D4D5C 446D67D0 001 513DD000  Init
446D67D0 0000000188 446D502C 446D688C 001 513DD000  Process Events
5055163C 0000000684 505512CC 505518E8 001 513DD000  Init
  Resource User: SERIAL A'detect(ID: 0x1000022)
Chunk Elements :
Allocated Size(b): 44 Count: 1 Freed Size(b): 0 Count: 0

Processor memory
 Address      Bytes     Prev     Next Ref   Alloc PC  What
44722FCC 0000000684 4471DE58 44723278 001 513DD000  Init
50598A4C 0000006052 505989E8 5059A1F0 001 513DD000  Init
5059A1F0 0000000188 50598A4C 5059A2AC 001 513DD000  Process Events
  Resource User: GraphIt(ID: 0x1000023)
Chunk Elements :
Allocated Size(b): 44 Count: 1 Freed Size(b): 44 Count: 1

Processor memory
 Address      Bytes     Prev     Next Ref   Alloc PC  What
447235B8 0000000684 4472356C 44723864 001 513DD000  Init
5059A8A8 0000006052 5059A350 5059C04C 001 513DD000  Init
5059C04C 0000000188 5059A8A8 5059C108 001 513DD000  Process Events
  Resource User: rf proxy rp agent(ID: 0x1000024)
Chunk Elements :
Allocated Size(b): 39056 Count: 504 Freed Size(b): 33756 Count: 452
```

```
Processor memory
 Address      Bytes     Prev     Next Ref   Alloc PC  What
446B752C 0000000144 446B74D4 446B75BC 001 513DD000  NameDB String
44728FC0 0000000684 44728F74 4472926C 001 513DD000  Init
44B19780 0000001160 44B1867C 44B19C08 001 513DD000  IPC Port
44B204A0 0000000148 44B2042C 44B20534 001 513DD000  IPC Name String
44B220E8 0000000096 44B2202C 44B22148 001 513DD000  rf proxy rp agent
44B22148 0000001160 44B220E8 44B225D0 001 513DD000  IPC Port
44B22938 0000000076 44B2287C 44B22984 001 513DD000  NameDB String
44B22984 0000000096 44B22938 44B229E4 001 513DD000  rf proxy rp agent
44B22D4C 0000000076 44B22C90 44B22D98 001 513DD000  NameDB String
44B22D98 0000000096 44B22D4C 44B22DF8 001 513DD000  rf proxy rp agent
44B23160 0000000076 44B230A4 44B231AC 001 513DD000  NameDB String
44B231AC 0000000096 44B23160 44B2320C 001 513DD000  rf proxy rp agent
44B2320C 0000000076 44B231AC 44B23258 001 513DD000  IPC Name String
50543ABC 0000000104 50543A00 50543B24 001 513DD000  IPC Name
5061CC34 0000000188 5059EC00 5061CCF0 001 513DD000  Process Events
5061CDB4 0000006052 5061CD68 5061E558 001 513DD000  Init
50A8780C 0000000132 50A877C0 50A87890 001 513DD000  IPC Name String
50AC8094 0000065588 50AC7C0C 50AD80C8 001 513DD000  EvtMgr active chunk
50AD986C 0000001160 50AD80C8 50AD9CF4 001 513DD000  IPC Port
  Resource User: HC Counter Timers(ID: 0x1000025)
Chunk Elements :
Allocated Size(b): 0 Count: 0 Freed Size(b): 0 Count: 0
.
.
.
Resource User: NetFlow Agg Task(ID: 0x1000114)
Getbufs  Retbufs  Holding  RU Name
0        0        0        NetFlow Agg Task

  Resource User: CWAN OIR IPC Ready Process(ID: 0x1000115)
Getbufs  Retbufs  Holding  RU Name
0        0        0        CWAN OIR IPC Rea

  Resource User: PF Clock Process(ID: 0x1000116)
Getbufs  Retbufs  Holding  RU Name
0        0        0        PF Clock Process

  Resource User: CEF IPC Background(ID: 0x1000117)
Getbufs  Retbufs  Holding  RU Name
0        0        0        CEF IPC Backgrou

  Resource User: RTTYS Process(ID: 0x1000118)
Getbufs  Retbufs  Holding  RU Name
0        0        0        RTTYS Process

  Resource User: DHCPD Timer(ID: 0x100011B)
Getbufs  Retbufs  Holding  RU Name
0        0        0        DHCPD Timer

  Resource User: DHCPD Database(ID: 0x100011C)
Getbufs  Retbufs  Holding  RU Name
0        0        0        DHCPD Database

  Resource User: draco-oir-process:slot 2(ID: 0x100011E)
Getbufs  Retbufs  Holding  RU Name
0        0        0        draco-oir-proces

  Resource User: SCP async: Draco-LC4(ID: 0x1000125)
Getbufs  Retbufs  Holding  RU Name
35908    243517   4294759687 SCP async: Draco
```

```
  Resource User: IFCOM Msg Hdlr(ID: 0x1000127)
Getbufs  Retbufs  Holding  RU Name
2        2        0        IFCOM Msg Hdlr

  Resource User: IFCOM Msg Hdlr(ID: 0x1000128)
Getbufs  Retbufs  Holding  RU Name
28       28       0        IFCOM Msg Hdlr

  Resource User: Exec(ID: 0x100012C)
Getbufs  Retbufs  Holding  RU Name
17552    17552    0        Exec

Resource Owner: test_mem
 Resource User Type: test_process
 Resource User Type: mem_rut
Resource Owner: test_cpu
 Resource User Type: test_process
 Resource User Type: cpu_rut
```

Table 55 describes the significant fields shown in the display.

Table 55 show resource all Field Descriptions

Field	Description
Runtime(ms)	The runtime of the process in milliseconds.
Invoked	The number of times a Resource User (RU) has been allowed to run.
uSecs	The amount of runtime per invocation in microseconds.
Allocated Size(b)	The number of bytes of memory that is allocated.
Freed Size(b)	The number of bytes of memory that is freed.
Count	The number of elements that are allocated or freed. For example, if two elements of 50 bytes each are allocated, then the allocated count is 2 and allocated size is 100.
pc	Displays the details of the memory that is held by a process. Each line of the output displays one or more blocks of memory. The pc is the allocator pc of a particular block of memory.
size	The total size of memory allocated to each block. The sum of the size of all blocks is equivalent to the total memory held by the process.
count	The count is the number of blocks of memory.
Getbufs	The number of buffers allocated by the RU.
Retbufs	The number of buffers freed by the RU.
Holding	The number of buffers the RU is holding currently.

Related Commands

Command	Description
buffer public	Enters the buffer owner configuration mode and sets thresholds for buffer usage.
cpu interrupt	Enters the CPU owner configuration mode and sets thresholds for interrupt level CPU utilization.

Command	Description
cpu process	Enters the CPU owner configuration mode and sets thresholds for processor level CPU utilization.
cpu total	Enters the CPU owner configuration mode and sets thresholds for total CPU utilization.
critical rising	Sets the critical level threshold values for the buffer, CPU, and memory ROs.
major rising	Sets the major level threshold values for the buffer, CPU, and memory ROs.
memory io	Enters the memory owner configuration mode and sets threshold values for I/O memory.
memory processor	Enters the memory owner configuration mode and sets threshold values for processor memory.
minor rising	Sets the minor level threshold values for the buffer, CPU, and memory ROs.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource database	Displays the database details of ROs.
show resource owner	Displays the RO details.
show resource relationship	Displays the relationship between the RUs and the ROs.

show resource database

To display the details of a resource owner, use the **show resource database** command in user EXEC or privileged EXEC mode.

show resource database

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Examples

The following is sample output from the **show resource database** command:

```
Router# show resource database

List of all Resource Owners :
Owner: cpu                       Id:0x1
Owner's list of monitors is empty.
Owner: memory                    Id:0x2
Owner's list of monitors is empty.
Owner: Buffer                    Id:0x3
Owner's list of monitors is empty.
Owner: test_mem                  Id:0x4
Owner's list of monitors is empty.
Owner: test_cpu                  Id:0x5
Owner's list of monitors is empty.
Owner: test_RO0                  Id:0x7
Owner's list of monitors is empty.
Owner: test_RO1                  Id:0x8
Owner's list of monitors is empty.
Owner: test_RO2                  Id:0x9
Owner's list of monitors is empty.
Owner: test_RO3                  Id:0xA
Owner's list of monitors is empty.
Owner: test_RO4                  Id:0xB
Owner's list of monitors is empty.
Owner: test_RO5                  Id:0xC
Owner's list of monitors is empty.
.
.
.
List of all Resource Usertypes :
RUT: iosprocess                Id:0x1
RUT: test_process              Id:0x2
RUT: mem_rut                   Id:0x3
RUT: cpu_rut                   Id:0x4
```

```
RUT: test_RUT0                 Id:0x5
RUT: test_RUT1                 Id:0x6
RUT: test_RUT2                 Id:0x7
RUT: test_RUT3                 Id:0x8
RUT: test_RUT4                 Id:0x9
RUT: test_RUT5                 Id:0xA
.
.
.
List of all Resource User Groups :

List of all Resource Users :
usertype: iosprocess                Id:0x1
 user: Init                      Id:0x1000001, priority:0
 user: Scheduler                 Id:0x1000002, priority:0
 user: Dead                      Id:0x1000003, priority:0
 user: Interrupt                 Id:0x1000004, priority:0
 user: Memory RO RU              Id:0x1000005, priority:0
 user: Chunk Manager             Id:0x1000006, priority:1
 user: Load Meter                Id:0x1000007, priority:1
 user: Check heaps               Id:0x1000009, priority:4
 user: Pool Manager              Id:0x100000A, priority:1
 user: Buffer RO RU              Id:0x100000B, priority:0
 user: Timers                    Id:0x100000C, priority:3
 user: Serial Background         Id:0x100000D, priority:3
 user: ALARM_TRIGGER_SCAN        Id:0x100000E, priority:4
 user: AAA_SERVER_DEADTIME       Id:0x100000F, priority:4
 user: AAA high-capacity counter Id:0x1000010, priority:3
 user: Policy Manager            Id:0x1000011, priority:3
 user: Crash writer              Id:0x1000012, priority:3
 user: RO Notify Timers          Id:0x1000013, priority:3
 user: RMI RM Notify Watched Pol Id:0x1000014, priority:3
 user: EnvMon                    Id:0x1000015, priority:3
 user: OIR Handler               Id:0x1000016, priority:3
 user: IPC Dynamic Cache         Id:0x1000017, priority:3
 user: IPC Zone Manager          Id:0x1000018, priority:3
 user: IPC Periodic Timer        Id:0x1000019, priority:3
 user: IPC Managed Timer         Id:0x100001A, priority:3
 user: IPC Deferred Port Closure Id:0x100001B, priority:3
.
.
.
Resource Monitor: test_ROM0, ID: 0x1B
 Not Watching any Relations.
 Not Watching any Policies.
Resource Monitor: test_ROM1, ID: 0x1C
 Not Watching any Relations.
 Not Watching any Policies.
Resource Monitor: test_ROM2, ID: 0x1D
 Not Watching any Relations.
 Not Watching any Policies.
```

Related Commands

Command	Description
buffer public	Enters the buffer owner configuration mode and sets thresholds for buffer usage.
cpu interrupt	Enters the CPU owner configuration mode and sets thresholds for interrupt level CPU utilization.
cpu process	Enters the CPU owner configuration mode and sets thresholds for processor level CPU utilization.

Command	Description
cpu total	Enters the CPU owner configuration mode and sets thresholds for total CPU utilization.
critical rising	Sets the critical level threshold values for the buffer, CPU, and memory ROs.
major rising	Sets the major level threshold values for the buffer, CPU, and memory ROs.
memory io	Enters the memory owner configuration mode and sets threshold values for I/O memory.
memory processor	Enters the memory owner configuration mode and sets threshold values for processor memory.
minor rising	Sets the minor level threshold values for the buffer, CPU, and memory ROs.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.
show resource owner	Displays the RO details.
show resource relationship	Displays the relationship between the RUs and the ROs.

show resource owner

To display the details of a resource owner (RO), use the **show resource owner** command in user EXEC or privileged EXEC mode.

show resource owner {*resource-owner-name* | **all**} **user** {*resource-user-type-name* | **all**} [**brief** [**triggers**] | **detailed** [**triggers**] | **triggers**]

Syntax Description

resource-owner-name	Name of the specified RO whose details are displayed.
all	Displays details of all the ROs.
user	Displays details of the specified resource user (RU) type.
resource-user-type-name	Single resource user type.
all	Displays details of all the resource user types.
brief	(Optional) Displays brief details.
detailed	(Optional) Displays complete details.
triggers	(Optional) Displays the triggers.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Examples

The following is sample output from the **show resource owner** command:

```
Router# show resource owner all user all

Resource Owner: cpu
 Resource User Type: iosprocess
  Resource User: Init(ID: 0x1000001)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777217           0         0          0  0.00%  0.00%  0.00% Init
Resource User: Scheduler(ID: 0x1000002)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777218           0         0          0  0.00%  0.00%  0.00% Scheduler
Resource User: Dead(ID: 0x1000003)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777219           0         0          0  0.00%  0.00%  0.00% Dead
Resource User: Interrupt(ID: 0x1000004)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777220           0         0          0  0.00%  0.00%  0.00% Interrupt
Resource User: Memory RO RU(ID: 0x1000005)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777221           0         0          0  0.00%  0.00%  0.00% Memory RO RU
Resource User: Chunk Manager(ID: 0x1000006)
```

```
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777222           4         3       1333  0.00%  0.00%  0.00% Chunk Manager
Resource User: Load Meter(ID: 0x1000007)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777223           4       292         13  0.00%  0.00%  0.00% Load Meter
Resource User: Check heaps(ID: 0x1000009)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777225         376       192       1958  0.00%  0.02%  0.00% Check heaps
Resource User: Pool Manager(ID: 0x100000A)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777226           0         1          0  0.00%  0.00%  0.00% Pool Manager
Resource User: Buffer RO RU(ID: 0x100000B)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777227           0         0          0  0.00%  0.00%  0.00% Buffer RO RU
Resource User: Timers(ID: 0x100000C)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777228           0         2          0  0.00%  0.00%  0.00% Timers
Resource User: Serial Background(ID: 0x100000D)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
.
.
.
Resource Owner: memory
 Resource User Type: iosprocess
  Resource User: Init(ID: 0x1000001)
Chunk Elements :
Allocated Size(b): 25967632 Count: 46612 Freed Size(b): 21487684 Count: 26053

Processor memory
Total Memory held : 15250376 bytes
pc = 0x6072D840, size =   4040536, count =    6
pc = 0x6034E040, size =   1937508, count =    2
pc = 0x6070DAF0, size =    560096, count =    1
pc = 0x606D7530, size =    556220, count =  685
pc = 0x613AFA74, size =    350972, count =   25
pc = 0x60ECA4F0, size =    280004, count =    1
pc = 0x606DEC1C, size =    270600, count =  100
pc = 0x616EF268, size =    262148, count =    1
pc = 0x6085C318, size =    196620, count =    3
pc = 0x61479630, size =    144004, count =    1
pc = 0x613E1DB0, size =    131768, count =    4
.
.
.
I/O memory
Total Memory held : 4059856 bytes
pc = 0x606DEC30, size =   3408704, count =   52
pc = 0x606DEB94, size =    442464, count =    6
pc = 0x606D76A4, size =    179872, count =  146
pc = 0x600ED530, size =     16448, count =    4
pc = 0x600ED498, size =      8256, count =    4
pc = 0x6080D3F0, size =      4112, count =    1

  Resource User: Scheduler(ID: 0x1000002)
Chunk Elements :
Allocated Size(b): 0 Count: 0 Freed Size(b): 0 Count: 0

Processor memory
Total Memory held : 12172 bytes
pc = 0x607B44F0, size =     12004, count =    1
pc = 0x607643B8, size =       168, count =    4

.
.
```

```
.
Resource User: Critical Bkgnd(ID: 0x1000026)
Chunk Elements :
Allocated Size(b): 44 Count: 1 Freed Size(b): 0 Count: 0

Processor memory
Total Memory held : 6780 bytes
pc = 0x607B44F0, size =      6004, count =    1
pc = 0x6079CB28, size =       636, count =    1
pc = 0x6079EE84, size =       140, count =    1
.
.
.
Resource Owner: Buffer
 Resource User Type: iosprocess
  Resource User: Init(ID: 0x1000001)
Getbufs  Retbufs  Holding  RU Name
319      51       268      Init

Resource User: Scheduler(ID: 0x1000002)
Getbufs  Retbufs  Holding  RU Name
0        0        0        Scheduler

Resource User: Dead(ID: 0x1000003)
Getbufs  Retbufs  Holding  RU Name
0        0        0        Dead

Resource User: Interrupt(ID: 0x1000004)
Getbufs  Retbufs  Holding  RU Name
1356     1356     0        Interrupt

Resource User: Memory RO RU(ID: 0x1000005)
Getbufs  Retbufs  Holding  RU Name
0        0        0        Memory RO RU

Resource User: Chunk Manager(ID: 0x1000006)
Getbufs  Retbufs  Holding  RU Name
0        0        0        Chunk Manager

.
.
.
Resource Owner: test_mem
 Resource User Type: test_process
 Resource User Type: mem_rut
Resource Owner: test_cpu
 Resource User Type: test_process
 Resource User Type: cpu_rut
Resource User: test_RU0(ID: 0x4000001)
>>>RU: Blank
Resource User: test_RU1(ID: 0x4000002)
>>>RU: Blank
Resource User: test_RU2(ID: 0x4000003)
>>>RU: Blank
Resource User: test_RU3(ID: 0x4000004)
>>>RU: Blank
.
.
.
Resource User Type: test_RUT143
 Resource User Type: test_RUT144
 Resource User Type: test_RUT145
 Resource User Type: test_RUT146
 Resource User Type: test_RUT147
```

The following is sample output from the **show resource owner all user all brief** command:

```
Router# show resource owner all user all brief

Resource Owner: cpu
 Resource User Type: iosprocess
  Resource User: Init(ID: 0x1000001)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777217           0         0           0  0.00%  0.00%  0.00% Init
Resource User: Scheduler(ID: 0x1000002)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777218           0         0           0  0.00%  0.00%  0.00% Scheduler
Resource User: Dead(ID: 0x1000003)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777219           0         0           0  0.00%  0.00%  0.00% Dead
Resource User: Interrupt(ID: 0x1000004)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777220           0         0           0  0.00%  0.00%  0.00% Interrupt
Resource User: Memory RO RU(ID: 0x1000005)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777221           0         0           0  0.00%  0.00%  0.00% Memory RO RU
Resource User: Chunk Manager(ID: 0x1000006)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777222           4         3        1333  0.00%  0.00%  0.00% Chunk Manager
Resource User: Load Meter(ID: 0x1000007)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777223           4       322          12  0.00%  0.01%  0.00% Load Meter
Resource User: Check heaps(ID: 0x1000009)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777225         424       214        1981  0.00%  0.04%  0.00% Check heaps
.
.
.
Resource Owner: memory
 Resource User Type: iosprocess
  Resource User: Init(ID: 0x1000001)
Processor memory
Allocated   Freed  Holding   Blocks
21916780  6666404 15250376     8688

I/O memory
Allocated   Freed  Holding   Blocks
 4059856        0  4059856      213

Resource User: Scheduler(ID: 0x1000002)
Processor memory
Allocated   Freed  Holding   Blocks
   12172        0    12172        5
.
.
.
Resource Owner: test_mem
 Resource User Type: test_process
 Resource User Type: mem_rut
Resource Owner: test_cpu
 Resource User Type: test_process
 Resource User Type: cpu_rut
Resource User: test_RU0(ID: 0x4000001)
>>>RU: Blank
Resource User: test_RU1(ID: 0x4000002)
>>>RU: Blank
Resource User: test_RU2(ID: 0x4000003)
>>>RU: Blank
```

```
Resource User: test_RU3(ID: 0x4000004)
>>>RU: Blank
Resource User: test_RU4(ID: 0x4000005)
>>>RU: Blank
.
.
.
Resource Owner: test_RO0
Resource User Type: test_RUT0
Resource User Type: test_RUT1
Resource User Type: test_RUT2
Resource User Type: test_RUT3
Resource User Type: test_RUT4
Resource User Type: test_RUT5
Resource User Type: test_RUT6
Resource User Type: test_RUT7
Resource User Type: test_RUT8
Resource User Type: test_RUT9
Resource User Type: test_RUT10
Resource User Type: test_RUT11
Resource User Type: test_RUT12
Resource User Type: test_RUT13
Resource User Type: test_RUT14
Resource User Type: test_RUT15
Resource User Type: test_RUT16
```

The following is sample output from the **show resource owner all user all brief triggers** command:

```
Router# show resource owner all user all brief triggers

Resource Owner: cpu
 Resource User Type: iosprocess
  Resource User: Init(ID: 0x1000001)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777217           0         0          0  0.00%  0.00%  0.00% Init
Resource User: Scheduler(ID: 0x1000002)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777218           0         0          0  0.00%  0.00%  0.00% Scheduler
Resource User: Dead(ID: 0x1000003)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777219           0         0          0  0.00%  0.00%  0.00% Dead
Resource User: Interrupt(ID: 0x1000004)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777220           0         0          0  0.00%  0.00%  0.00% Interrupt
Resource User: Memory RO RU(ID: 0x1000005)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777221           0         0          0  0.00%  0.00%  0.00% Memory RO RU
Resource User: Chunk Manager(ID: 0x1000006)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777222           4         3       1333  0.00%  0.00%  0.00% Chunk Manager
.
.
.
Resource Owner: test_mem
Resource User Type: test_process
Resource User Type: mem_rut
Resource Owner: test_cpu
Resource User Type: test_process
Resource User Type: cpu_rut
Resource User: test_RU0(ID: 0x4000001)
>>>RU: Blank
Resource User: test_RU1(ID: 0x4000002)
>>>RU: Blank
Resource User: test_RU2(ID: 0x4000003)
```

```
>>>RU: Blank
Resource User: test_RU3(ID: 0x4000004)
>>>RU: Blank
Resource User: test_RU4(ID: 0x4000005)
>>>RU: Blank
Resource User: test_RU5(ID: 0x4000006)
>>>RU: Blank
```

The following is sample output from the **show resource owner all user all detailed** command:

```
Router# show resource owner all user all detailed

Resource Owner: cpu
 Resource User Type: iosprocess
  Resource User: Init(ID: 0x1000001)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777217           0         0           0  0.00%  0.00%  0.00% Init
Resource User: Scheduler(ID: 0x1000002)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777218           0         0           0  0.00%  0.00%  0.00% Scheduler
Resource User: Dead(ID: 0x1000003)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777219           0         0           0  0.00%  0.00%  0.00% Dead
Resource User: Interrupt(ID: 0x1000004)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777220           0         0           0  0.00%  0.00%  0.00% Interrupt
Resource User: Memory RO RU(ID: 0x1000005)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777221           0         0           0  0.00%  0.00%  0.00% Memory RO RU
Resource User: Chunk Manager(ID: 0x1000006)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777222           4         3       1333  0.00%  0.00%  0.00% Chunk Manager
Resource User: Load Meter(ID: 0x1000007)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777223           4       353          11  0.00%  0.01%  0.00% Load Meter
Resource User: Check heaps(ID: 0x1000009)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777225         456       232       1965  0.00%  0.01%  0.00% Check heaps
Resource User: Pool Manager(ID: 0x100000A)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777226           0         1           0  0.00%  0.00%  0.00% Pool Manager
Resource User: Buffer RO RU(ID: 0x100000B)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777227           0         0           0  0.00%  0.00%  0.00% Buffer RO RU
Resource User: Timers(ID: 0x100000C)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777228           0         2           0  0.00%  0.00%  0.00% Timers
.
.
.
Resource Owner: memory
 Resource User Type: iosprocess
  Resource User: Init(ID: 0x1000001)
Chunk Elements :
Allocated Size(b): 25967632 Count: 46612 Freed Size(b): 21487684 Count: 26053

Processor memory
 Address      Bytes     Prev     Next Ref   Alloc PC  What
63700E18 0000020052 636FDCD4 63705C6C 001 6412D2C0  Managed Chunk Queue Elements
63705C6C 0000012852 63700E18 63708EA0 001 6412D2C0  *Init*
63708EA0 0000010052 63705C6C 6370B5E4 001 6412D2C0  List Elements
6370B5E4 0000005052 63708EA0 6370C9A0 001 6412D2C0  List Headers
6370C9A0 0000009052 6370B5E4 6370ECFC 001 6412D2C0  Interrupt Stack
6370ECFC 0000000096 6370C9A0 6370ED5C 001 6412D2C0  *Init*
```

```
6370ED5C 0000000084 6370ECFC 6370EDB0 001 6412D2C0  *Init*
6370EDB0 0000000132 6370ED5C 6370EE34 001 6412D2C0  *Init*
6370EE34 0000000092 6370EDB0 6370EE90 001 6412D2C0  *Init*
6370EE90 0000000436 6370EE34 6370F044 001 6412D2C0  *Init*
6370F044 0000000076 6370EE90 6370F090 001 6412D2C0  *Init*
6370F090 0000000132 6370F044 6370F114 001 6412D2C0  *Init*
6370F114 0000000092 6370F090 6370F170 001 6412D2C0  *Init*
.
.
.
Resource User: Scheduler(ID: 0x1000002)
Chunk Elements :
Allocated Size(b): 0 Count: 0 Freed Size(b): 0 Count: 0

Processor memory
 Address      Bytes     Prev     Next Ref   Alloc PC  What
63799F04 0000012052 63799EB8 6379CE18 001 6412D2C0  Scheduler Stack
643E9A38 0000000076 643D9A04 643E9A84 001 6412D2C0  *Sched*
644C47F0 0000000076 644C4790 644C483C 001 6412D2C0  *Sched*
645FF744 0000000096 645FF6E8 645FF7A4 001 6412D2C0  *Sched*
64904354 0000000112 649040D0 649043C4 001 6412D2C0  *Sched*
  Resource User: Dead(ID: 0x1000003)
Chunk Elements :
Allocated Size(b): 0 Count: 0 Freed Size(b): 0 Count: 0

Processor memory
 Address      Bytes     Prev     Next Ref   Alloc PC  What
63F9D328 0000000096 63F984D4 63F9D388 001 6412D2C0  AAA MI SG NAME
  Resource User: Interrupt(ID: 0x1000004)
Chunk Elements :
Allocated Size(b): 0 Count: 0 Freed Size(b): 0 Count: 0
```

The following is sample output from the **show resource owner all user all detailed triggers** command:

```
Router# show resource owner all user all detailed triggers

Resource Owner: cpu
 Resource User Type: iosprocess
  Resource User: Init(ID: 0x1000001)
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777217           0         0          0  0.00%  0.00%  0.00% Init
Resource User: Scheduler(ID: 0x1000002)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777218           0         0          0  0.00%  0.00%  0.00% Scheduler
Resource User: Dead(ID: 0x1000003)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777219           0         0          0  0.00%  0.00%  0.00% Dead
Resource User: Interrupt(ID: 0x1000004)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777220           0         0          0  0.00%  0.00%  0.00% Interrupt
Resource User: Memory RO RU(ID: 0x1000005)
RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777221           0         0          0  0.00%  0.00%  0.00% Memory RO RU
Resource User: Chunk Manager(ID: 0x1000006)
.
.
.
Resource User: Scheduler(ID: 0x1000002)
Chunk Elements :
Allocated Size(b): 0 Count: 0 Freed Size(b): 0 Count: 0

Processor memory
 Address      Bytes     Prev     Next Ref   Alloc PC  What
63799F04 0000012052 63799EB8 6379CE18 001 6412D2C0  Scheduler Stack
```

```
643E9A38 0000000076 643D9A04 643E9A84 001 6412D2C0  *Sched*
644C47F0 0000000076 644C4790 644C483C 001 6412D2C0  *Sched*
645FF744 0000000096 645FF6E8 645FF7A4 001 6412D2C0  *Sched*
64904354 0000000112 649040D0 649043C4 001 6412D2C0  *Sched*
  Resource User: Dead(ID: 0x1000003)
Chunk Elements :
Allocated Size(b): 0 Count: 0 Freed Size(b): 0 Count: 0
.
.
.
Resource User Type: test_RUT142
Resource User Type: test_RUT143
Resource User Type: test_RUT144
Resource User Type: test_RUT145
Resource User Type: test_RUT146
Resource User Type: test_RUT147
Resource User Type: test_RUT148
Resource User Type: test_RUT149
```

Table 55 describes the significant fields shown in the display.

Table 56 show resource owner Field Descriptions

Field	Description
Runtime(ms)	The runtime of the process in milliseconds.
Invoked	The number of times an RU has been allowed to run.
uSecs	The amount of runtime per invocation in microseconds.
Allocated Size(b)	The number of bytes of memory that are allocated.
Freed Size(b)	The number of bytes of memory that are freed.
Count	The number of elements that are allocated or freed. For example, if two elements of 50 bytes each are allocated, the allocated count is 2 and allocated size is 100.
pc	Displays the details of the memory that is held by a process. Each line of the output displays one or more blocks of memory. The pc is the allocator pc of a particular block of memory.
size	The total size of memory allocated to each block. The sum of the size of all blocks is equivalent to the total memory held by the process.
count	The count is the number of blocks of memory.
Getbufs	The number of buffers allocated by the RU.
Retbufs	The number of buffers freed by the RU.
Holding	The number of buffers the RU is holding currently.

Related Commands

Command	Description
buffer public	Enters buffer owner configuration mode and sets thresholds for buffer usage.
cpu interrupt	Enters CPU owner configuration mode and sets thresholds for interrupt level CPU utilization.
cpu process	Enters CPU owner configuration mode and sets thresholds for processor level CPU utilization.

Command	Description
cpu total	Enters CPU owner configuration mode and sets thresholds for total CPU utilization.
critical rising	Sets the critical level threshold values for the buffer, CPU, and memory ROs.
major rising	Sets the major level threshold values for the buffer, CPU, and memory ROs.
memory io	Enters memory owner configuration mode and sets threshold values for I/O memory.
memory processor	Enters memory owner configuration mode and sets threshold values for processor memory.
minor rising	Sets the minor level threshold values for the buffer, CPU, and memory ROs.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.
show resource database	Displays the entire database of all resource entry relationships.
show resource relationship	Displays the relationship between the RUs and the ROs.

show resource relationship

To display the details of relationships between different resource owners, use the **show resource relationship** command in user EXEC or privileged EXEC mode.

show resource relationship user *resource-user-type*

Syntax Description

user	Identifies a resource user (RU).
resource-user-type	Type of RU.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Examples

The following is sample output from the **show resource relationship** command:

```
Router# show resource relationship

Resource User Type: iosprocess (ID: 0x1)
 -> Resource Owner: cpu (ID: 0x1)
 -> Resource Owner: memory (ID: 0x2)
 -> Resource Owner: Buffer (ID: 0x3)
 -> Resource User: Init (ID: 0x1000001)
 -> Resource User: Scheduler (ID: 0x1000002)
 -> Resource User: Dead (ID: 0x1000003)
 -> Resource User: Interrupt (ID: 0x1000004)
 -> Resource User: Memory RO RU (ID: 0x1000005)
 -> Resource User: Chunk Manager (ID: 0x1000006)
 -> Resource User: Load Meter (ID: 0x1000007)
 -> Resource User: Check heaps (ID: 0x1000009)
 -> Resource User: Pool Manager (ID: 0x100000A)
 -> Resource User: Buffer RO RU (ID: 0x100000B)
 -> Resource User: Timers (ID: 0x100000C)
 -> Resource User: Serial Background (ID: 0x100000D)
 -> Resource User: ALARM_TRIGGER_SCAN (ID: 0x100000E)
 -> Resource User: AAA_SERVER_DEADTIME (ID: 0x100000F)
 -> Resource User: AAA high-capacity counters (ID: 0x1000010)
 -> Resource User: Policy Manager (ID: 0x1000011)
 -> Resource User: Crash writer (ID: 0x1000012)
 -> Resource User: RO Notify Timers (ID: 0x1000013)
 -> Resource User: RMI RM Notify Watched Policy (ID: 0x1000014)
 -> Resource User: EnvMon (ID: 0x1000015)
 -> Resource User: OIR Handler (ID: 0x1000016)
 -> Resource User: IPC Dynamic Cache (ID: 0x1000017)
 -> Resource User: IPC Zone Manager (ID: 0x1000018)
 -> Resource User: IPC Periodic Timer (ID: 0x1000019)
 -> Resource User: IPC Managed Timer (ID: 0x100001A)
 -> Resource User: IPC Deferred Port Closure (ID: 0x100001B)
 -> Resource User: IPC Seat Manager (ID: 0x100001C)
 -> Resource User: IPC Session Service (ID: 0x100001D)
 -> Resource User: Compute SRP rates (ID: 0x100001E)
 -> Resource User: ARP Input (ID: 0x100001F)
 -> Resource User: DDR Timers (ID: 0x1000020)
 -> Resource User: Dialer event (ID: 0x1000021)
 -> Resource User: Entity MIB API (ID: 0x1000022)
 -> Resource User: SERIAL A'detect (ID: 0x1000023)
 -> Resource User: GraphIt (ID: 0x1000024)
 -> Resource User: HC Counter Timers (ID: 0x1000025)
.
.
.
Resource User Type: test_RUT141 (ID: 0x92)
 -> Resource Owner: test_RO0 (ID: 0x7)
 Resource User Type: test_RUT142 (ID: 0x93)
 -> Resource Owner: test_RO0 (ID: 0x7)
 Resource User Type: test_RUT143 (ID: 0x94)
 -> Resource Owner: test_RO0 (ID: 0x7)
 Resource User Type: test_RUT144 (ID: 0x95)
 -> Resource Owner: test_RO0 (ID: 0x7)
 Resource User Type: test_RUT145 (ID: 0x96)
 -> Resource Owner: test_RO0 (ID: 0x7)
 Resource User Type: test_RUT146 (ID: 0x97)
 -> Resource Owner: test_RO0 (ID: 0x7)
 Resource User Type: test_RUT147 (ID: 0x98)
 -> Resource Owner: test_RO0 (ID: 0x7)
 Resource User Type: test_RUT148 (ID: 0x99)
 -> Resource Owner: test_RO0 (ID: 0x7)
 Resource User Type: test_RUT149 (ID: 0x9A)
 -> Resource Owner: test_RO0 (ID: 0x7)
```

Related Commands

Command	Description
buffer public	Enters buffer owner configuration mode and sets thresholds for buffer usage.
cpu interrupt	Enters CPU owner configuration mode and sets thresholds for interrupt level CPU utilization.
cpu process	Enters CPU owner configuration mode and sets thresholds for processor level CPU utilization.
cpu total	Enters CPU owner configuration mode and sets thresholds for total CPU utilization.
critical rising	Sets the critical level threshold values for the buffer, CPU, and memory ROs.
major rising	Sets the major level threshold values for the buffer, CPU, and memory ROs.
memory io	Enters memory owner configuration mode and sets threshold values for the I/O memory.
memory processor	Enters memory owner configuration mode and sets threshold values for the processor memory.
minor rising	Sets the minor level threshold values for the buffer, CPU, and memory ROs.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.

Command	Description
show resource database	Displays the entire database of all resource entry relationships.
show resource owner	Displays the RO details.

show resource user

To display the policy details or Resource User (RU) template details of a resource user, use the **show resource user** command in user EXEC or privileged EXEC mode.

show resource user {**all** | *resource-user-type*} [**brief** | **detailed**]

Syntax Description

all	Displays the policy details of all the RUs.
resource-user-type	Type of RU. For example, iosprocess.
brief	(Optional) Displays a short description of the policy details.
detailed	(Optional) Displays all details of a policy.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Examples

The following is sample output from the **show resource user** command:

```
Router# show resource user all

Resource User Type: iosprocess
Resource Grp: Init
Resource Owner: memory
Processor memory
Allocated   Freed  Holding   Blocks
27197780  8950144 18247636     6552

I/O memory
Allocated   Freed  Holding   Blocks
 7296000     9504  7286496      196

Resource Owner: cpu
    RUID Runtime(ms)   Invoked      uSecs    5Sec   1Min   5Min Res Usr
16777224       14408       116      124206 100.40%  8.20%  1.70% Init
Resource Owner: Buffer
Getbufs  Retbufs  Holding  RU Name
332      60       272      Init

Resource User: Init
Resource User: Scheduler
Resource Owner: memory
Processor memory
Allocated   Freed  Holding   Blocks
   77544        0    77544        2

Resource Owner: cpu
```

```
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777218           0         0          0  0.00%  0.00%  0.00% Scheduler
Resource Owner: Buffer
Getbufs  Retbufs  Holding  RU Name
0        0        0        Scheduler

Resource User: Dead
Resource Owner: memory
Processor memory
Allocated   Freed  Holding   Blocks
 1780540      260  1780280      125

Resource Owner: cpu
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777219           0         0          0  0.00%  0.00%  0.00% Dead
Resource Owner: Buffer
Getbufs  Retbufs  Holding  RU Name
9        8        1        Dead

Resource User: Interrupt
Resource Owner: memory
Processor memory
Allocated   Freed  Holding   Blocks
       0        0        0        0

Resource Owner: cpu
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777220           0         0          0  0.00%  0.00%  0.00% Interrupt
Resource Owner: Buffer
Getbufs  Retbufs  Holding  RU Name
14128    14128    0        Interrupt

Resource User: Memory RO RU
Resource Owner: memory
Processor memory
Allocated   Freed  Holding   Blocks
  132560     1480   131080        2

Resource Owner: cpu
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777221           0         0          0  0.00%  0.00%  0.00% Memory RO RU
Resource Owner: Buffer
Getbufs  Retbufs  Holding  RU Name
64       64       0        Memory RO RU
.
.
.
Resource Owner: cpu
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777401        7124      4250       1676  0.00%  0.03%  0.01% Exec
  Resource Owner: Buffer
Getbufs  Retbufs  Holding  RU Name
38       38       0        Exec

 Resource User: BGP Router
  Resource Owner: memory
Processor memory
Allocated   Freed  Holding   Blocks
   43380    26556    16824        8

  Resource Owner: cpu
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777404          12     19705          0  0.00%  0.00%  0.00% BGP Router
  Resource Owner: Buffer
```

```
Getbufs  Retbufs  Holding  RU Name
0        0        0        BGP Router

 Resource User: BGP I/O
  Resource Owner: memory
Processor memory
Allocated   Freed  Holding   Blocks
    6892     6892        0        0

  Resource Owner: cpu
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777405           0         1           0  0.00%  0.00%  0.00% BGP I/O
  Resource Owner: Buffer
Getbufs  Retbufs  Holding  RU Name
0        0        0        BGP I/O

 Resource User: BGP Scanner
  Resource Owner: memory
Processor memory
Allocated   Freed  Holding   Blocks
    9828     9828        0        0

  Resource Owner: cpu
    RUID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min Res Usr
16777406         660       659        1001  0.00%  0.00%  0.00% BGP Scanner
  Resource Owner: Buffer
Getbufs  Retbufs  Holding  RU Name
0        0        0        BGP Scanner

Resource User Type: test_process
Resource User Type: mem_rut
Resource User Type: cpu_rut
```

Table 55 describes the significant fields shown in the display.

Table 57 show resource user Field Descriptions

Field	Description
Allocated	The number of bytes of memory that is allocated.
Freed	The number of bytes of memory that is freed.
Count	The number of elements that are allocated or freed. For example, if two elements of 50 bytes each are allocated, the allocated count is 2 and allocated size is 100.
Runtime(ms)	The runtime of the process in milliseconds.
Invoked	The number of times an RU has been allowed to run.
uSecs	The amount of runtime per invocation in microseconds.
Getbufs	The number of buffers allocated by the RU.
Retbufs	The number of buffers freed by the RU.
Holding	The number of buffers the RU is holding currently.

Related Commands

Command	Description
buffer public	Enters buffer owner configuration mode and sets thresholds for buffer usage.
cpu interrupt	Enters CPU owner configuration mode and sets thresholds for interrupt-level CPU utilization.
cpu process	Enters CPU owner configuration mode and sets thresholds for processor-level CPU utilization.
cpu total	Enters CPU owner configuration mode and sets thresholds for total CPU utilization.
critical rising	Sets the critical level threshold values for the buffer, CPU, and memory ROs.
major rising	Sets the major level threshold values for the buffer, CPU, and memory ROs.
memory io	Enters memory owner configuration mode and sets threshold values for I/O memory.
memory processor	Enters memory owner configuration mode and sets threshold values for processor memory.
minor rising	Sets the minor level threshold values for the buffer, CPU, and memory ROs.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.
show resource database	Displays entire database of all resource entry relationships.
show resource owner	Displays the RO details.

show rmon

To display the current RMON agent status on the router, use the **show rmon** command in EXEC mode.

show rmon [**alarms** | **capture** | **events** | **filter** | **history** | **hosts** | **matrix** | **statistics** | **task** | **topn**]

Syntax Description

alarms	(Optional) Displays the RMON alarm table.
capture	(Optional) Displays the RMON buffer capture table. Available on Cisco 2500 series and Cisco AS5200 series only.
events	(Optional) Displays the RMON event table.
filter	(Optional) Displays the RMON filter table. Available on Cisco 2500 series and Cisco AS5200 series only.
history	(Optional) Displays the RMON history table. Available on Cisco 2500 series and Cisco AS5200 series only.
hosts	(Optional) Displays the RMON hosts table. Available on Cisco 2500 series and Cisco AS5200 series only.
matrix	(Optional) Displays the RMON matrix table. Available on Cisco 2500 series and Cisco AS5200 series only.
statistics	(Optional) Displays the RMON statistics table. Available on Cisco 2500 series and Cisco AS5200 series only.
task	(Optional) Displays general RMON statistics. This is the default.
topn	(Optional) Displays the RMON top-n hosts table. Available on Cisco 2500 series and Cisco AS5200 series only.

Command Default

If no option is specified, the **task** option is displayed.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Refer to the specific **show rmon** command for an example and description of the fields.

For additional information, refer to the RMON MIB described in RFC 1757.

Examples

The following is sample output from the **show rmon** command. All counters are from the time the router was initialized.

```
Router# show rmon

145678 packets input (34562 promiscuous), 0 drops
145678 packets processed, 0 on queue, queue utilization 15/64
```

Table 58 describes the significant fields shown in the ouput.

Table 58 show rmon Field Descriptions

Field	Description
x packets input	Number of packets received on RMON-enabled interfaces.
x promiscuous	Number of input packets that were seen by the router only because RMON placed the interface in promiscuous mode.
x drops	Number of input packets that could not be processed because the RMON queue overflowed.
x packets processed	Number of input packets actually processed by the RMON task.
x on queue	Number of input packets that are sitting on the RMON queue, waiting to be processed.
queue utilization *x*/*y*	*y* is the maximum size of the RMON queue; *x* is the largest number of packets that were ever on the queue at a particular time.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon alarm	Sets an alarm on any MIB object.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
rmon queuesize	Changes the size of the queue that holds packets for analysis by the RMON process.
show rmon alarms	Displays the contents of the router's RMON alarm table.
show rmon capture	Displays the contents of the router's RMON capture table.
show rmon events	Displays the contents of the router's RMON event table.
show rmon filter	Displays the contents of the router's RMON filter table.
show rmon history	Displays the contents of the router's RMON history table.
show rmon hosts	Displays the contents of the router's RMON hosts table.
show rmon matrix	Displays the contents of the router's RMON matrix table.
show rmon statistics	Displays the contents of the router's RMON statistics table.
show rmon topn	Displays the contents of the router's RMON p-N host table.

show rmon alarms

To display the contents of the RMON alarm table of the router, use the **show rmon alarms** command in EXEC mode.

show rmon alarms

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For additional information, refer to the RMON MIB described in RFC 1757.

You must have first enabled RMON on the interface, and configured RMON alarms to display alarm information with the **show rmon alarms** command.

Examples

The following is sample output from the **show rmon alarms** command:

```
Router# show rmon alarms

Alarm 2 is active, owned by manager1
 Monitors ifEntry.1.1 every 30 seconds
 Taking delta samples, last value was 0
 Rising threshold is 15, assigned to event 12
 Falling threshold is 0, assigned to event 0
 On startup enable rising or falling alarm
```

Table 59 describes the significant fields shown in the display.

Table 59 show rmon alarms Field Descriptions

Field	Description
Alarm 2 is active, owned by manager1	Unique index into the alarmTable, showing the alarm status is active, and the owner of this row, as defined in the alarmTable of RMON.
Monitors ifEntry.1.1	Object identifier of the particular variable to be sampled. Equivalent to alarmVariable in RMON.

Table 59 show rmon alarms Field Descriptions (continued)

Field	Description
every 30 seconds	Interval in seconds over which the data is sampled and compared with the rising and falling thresholds. Equivalent to alarmInterval in RMON.
Taking delta samples	Method of sampling the selected variable and calculating the value to be compared against the thresholds. Equivalent to alarmSampleType in RMON.
last value was	Value of the statistic during the last sampling period. Equivalent to alarmValue in RMON.
Rising threshold is	Threshold for the sampled statistic. Equivalent to alarmRisingThreshold in RMON.
assigned to event	Index of the eventEntry that is used when a rising threshold is crossed. Equivalent to alarmRisingEventIndex in RMON.
Falling threshold is	Threshold for the sampled statistic. Equivalent to alarmFallingThreshold in RMON.
assigned to event	Index of the eventEntry that is used when a falling threshold is crossed. Equivalent to alarmFallingEventIndex in RMON.
On startup enable rising or falling alarm	Alarm that may be sent when this entry is first set to valid. Equivalent to alarmStartupAlarm in RMON.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon alarm	Sets an alarm on any MIB object.
show rmon	Displays the current RMON agent status on the router.

show rmon capture

To display the contents of the router's RMON capture table, use the **show rmon capture** command in EXEC mode.

show rmon capture

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For additional information, refer to the RMON MIB described in RFC 1757.

You must have first enabled RMON on the interface, and configured RMON alarms and events to display alarm information with the **show rmon capture** command.

This command is available on the Cisco 2500 series and Cisco AS5200 series only.

Examples

The following is sample output from the **show rmon capture** command:

```
Router# show rmon capture

Buffer 4096 is active, owned by manager1
 Captured data is from channel 4096
 Slice size is 128, download size is 128
 Download offset is 0
 Full Status is spaceAvailable, full action is lockWhenFull
 Granted 65536 octets out of 65536 requested
 Buffer has been on since 00:01:16, and has captured 1 packets
  Current capture buffer entries:
   Packet 1 was captured 416 ms since buffer was turned on
   Its length is 326 octets and has a status type of 0
   Packet ID is 634, and contains the following data:
00 00 0c 03 12 ce 00 00 0c 08 9d 4e 08 00 45 00
01 34 01 42 00 00 1d 11 e3 01 ab 45 30 15 ac 15
31 06 05 98 00 a1 01 20 9f a8 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00
```

Table 60 describes the significant fields shown in the ouput.

Table 60 show rmon capture Field Descriptions

Field	Description
Buffer 4096 is active	Equates to bufferControlIndex in the bufferControlTable of RMON. Uniquely identifies a valid (active) row in this table.
owned by manager1	Denotes the owner of this row. Equates to bufferControlOwner in the bufferControlTable of RMON.
Captured data is from channel	Equates to the bufferControlChannelIndex and identifies which RMON channel is the source of these packets.
Slice size is	Identifies the maximum number of octets of each packet that will be saved in this capture buffer. Equates to bufferControlCaptureSliceSize of RMON.
download size is	Identifies the maximum number of octets of each packet in this capture buffer that will be returned in an SNMP retrieval of that packet. Equates to bufferControlDownloadSliceSize in RMON.
Download offset is	Offset of the first octet of each packet in this capture buffer that will be returned in an SNMP retrieval of that packet. Equates to bufferControlDownloadOffset in RMON.
Full Status is spaceAvailable	Shows whether the buffer is full or has room to accept new packets. Equates to bufferControlFullStatus in RMON.
full action is lockWhenFull	Controls the action of the buffer when it reaches full status. Equates to bufferControlFullAction in RMON.
Granted 65536 octets	Actual maximum number of octets that can be saved in this capture buffer. Equates to bufferControlMaxOctetsGranted in RMON.
out of 65536 requested	Requested maximum number of octets to be saved in this capture buffer. Equates to bufferControlMaxOctetsRequested in RMON.
Buffer has been on since	Indicates how long the buffer has been available.
and has captured 1 packets	Number of packets captured since buffer was turned on. Equates to bufferControlCapturedPackets in RMON.
Current capture buffer entries:	Lists each packet captured.
Packet 1 was captured 416 ms since buffer was turned on Its length is 326 octets and has a status type of 0	Zero indicates the error status of this packet. Equates to captureBufferPacketStatus in RMON, where its value options are documented.
Packet ID is	Index that describes the order of packets received on a particular interface. Equates to captureBufferPacketID in RMON.
and contains the following data:	Data inside the packet, starting at the beginning of the packet.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon alarm	Sets an alarm on any MIB object.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
show rmon	Displays the current RMON agent status on the router.

show rmon events

To display the contents of the router’s RMON event table, use the **show rmon events** command in EXEC mode.

show rmon events

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For additional information, refer to the RMON MIB described in RFC 1757.

You must have first enabled RMON on the interface, and configured RMON events to display alarm information with the **show rmon events** command.

Examples

The following is sample output from the **show rmon events** command:

```
Router# show rmon events

Event 12 is active, owned by manager1
 Description is interface-errors
 Event firing causes log and trap to community rmonTrap, last fired 00:00:00
```

Table 61 describes the significant fields shown in the display.

Table 61 show rmon events Field Descriptions

Field	Description
Event 12 is active, owned by manager1	Unique index into the eventTable, showing the event status is active, and the owner of this row, as defined in the eventTable of RMON.
Description is interface-errors	Type of event, in this case an interface error.
Event firing causes log and trap	Type of notification that the router will make about this event. Equivalent to eventType in RMON.

Table 61 show rmon events Field Descriptions (continued)

Field	Description
community rmonTrap	If an SNMP trap is to be sent, it will be sent to the SNMP community specified by this octet string. Equivalent to eventCommunity in RMON.
last fired	Last time the event was generated.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
show rmon	Displays the current RMON agent status on the router.

show rmon filter

To display the contents of a router’s Remote Monitoring (RMON) filter table, use the **show rmon filter** command in privileged EXEC mode.

show rmon filter

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For additional information, see the RMON MIB described in RFC 1757.

You must have first enabled RMON on the interface and configured RMON alarms and events to display alarm information with the **show rmon filter** command.

This command is available on the Cisco 2500 series and Cisco AS5200 series only.

Examples

The following is sample output from the **show rmon filter** command:

```
Router# show rmon filter

Filter 4096 is active, and owned by manager1
 Data offset is 12, with
 Data of  08 00 00 00 00 00 00 00 00 00 00 00 00 ab 45 30 15 ac 15 31 06
 Data Mask is ff ff 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff
 Data Not Mask is 0
 Pkt status is 0, status mask is 0, not mask is 0
 Associated channel 4096 is active, and owned by manager1
 Type of channel is acceptFailed, data control is off
 Generate event index 0
 Event status is eventFired, # of matches is 1482
 Turn on event index is 0, turn off event index is 0
 Description:
```

Table 62 describes the significant fields shown in the display.

Table 62 show rmon filter Field Descriptions

Field	Description
Filter *x* is active, and owned by *y*	Unique index of the filter, its current state, and the owner, as defined in the filterTable of RMON.
Data offset is	Offset from the beginning of each packet where a match of packet data will be attempted. Equivalent to filterPktDataOffset in RMON.
Data of	Data that is to be matched with the input packet. Equivalent to filterPktData in RMON.
Data Mask is	Mask that is applied to the match process. Equivalent to filterPktDataMask in RMON.
Data Not Mask is	Inversion mask that is applied to the match process. Equivalent to filterPktDataNotMask in RMON.
Pkt status is	Status that is to be matched with the input packet. Equivalent to filterPktStatus in RMON.
status mask is	Mask that is applied to the status match process. Equivalent to filterPktStatusMask in RMON.
not mask is	Inversion mask that is applied to the status match process. Equivalent to filterPktStatusNotMask in RMON.
Associated channel *x* is active, and owned by *y*	Unique index of the channel, its current state, and the owner, as defined in the channelTable of RMON.
Type of channel is {acceptMatched | acceptFailed}	This object controls the action of the filters associated with this channel. Equivalent to channelAcceptType of RMON.
data control is {off | on }	This object controls the flow of data through this channel. Equivalent to channelDataControl in RMON.
Generate event index 0	Value of this object identifies the event that is to be generated when the associated channelDataControl is on and a packet is matched. Equivalent to channelEventIndex in RMON.
Event status is eventFired	When the channel is configured to generate events and when packets are matched, this message indicates the means of controlling the flow of those events. Equivalent to channelEventStatus in RMON.
# of matches is	Number of times this channel has matched a packet. Equivalent to channelMatches in RMON.
Turn on event index is	Value of this object identifies the event that is configured to turn the associated channelDataControl from off to on when the event is generated. Equivalent to channelTurnOnEventIndex in RMON.

Table 62 show rmon filter Field Descriptions (continued)

Field	Description
Turn off event index is	Value of this object identifies the event that is configured to turn the associated channelDataControl from on to off when the event is generated. Equivalent to channelTurnOffEventIndex in RMON.
Description:	Comment describing this channel.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon alarm	Sets an alarm on any MIB object.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
show rmon	Displays the current RMON agent status on the router.

show rmon history

To display the contents of the router's RMON history table, use the **show rmon history** command in EXEC mode.

show rmon history

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For additional information, refer to the RMON MIB described in RFC 1757.

You must have first enabled RMON on the interface, and configured RMON alarms and events to display alarm information with the **show rmon history** command.

This command is available on the Cisco 2500 series and Cisco AS5200 series only.

Examples

The following is sample output from the **show rmon history** command:

```
Router# show rmon history

Entry 1 is active, and owned by manager1
 Monitors ifEntry.1.1 every 30 seconds
 Requested # of time intervals, ie buckets, is 5
 Granted # of time intervals, ie buckets, is 5
  Sample # 14 began measuring at 00:11:00
   Received 38346 octets, 216 packets,
   0 broadcast and 80 multicast packets,
   0 undersized and 0 oversized packets,
   0 fragments and 0 jabbers,
   0 CRC alignment errors and 0 collisions.
   # of dropped packet events is 0
   Network utilization is estimated at 10
```

Table 63 describes the significant fields shown in the display.

Table 63 show rmon history Field Descriptions

Field	Description
Entry 1 is active, and owned by manager1	Unique index of the history entry, its current state, and the owner as defined in the historyControlTable of RMON.
Monitors ifEntry.1.1	This object identifies the source of the data for which historical data was collected and placed in a media-specific table. Equivalent to historyControlDataSource in RMON.
every 30 seconds	Interval in seconds over which the data is sampled for each bucket in the part of the media-specific table associated with this historyControlEntry. Equivalent to historyControlInterval in RMON.
Requested # of time intervals, ie buckets, is	Requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this historyControlEntry. Equivalent to historyControlBucketsRequested in RMON.
Granted # of time intervals, ie buckets, is	Actual number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this historyControlEntry. Equivalent to historyControlBucketsGranted in RMON.
Sample # 14 began measuring at	Time at the start of the interval over which this sample was measured.
Received 38346 octets	Total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). Equivalent to etherHistoryOctets in RMON.
x packets	Number of packets (including bad packets) received during this sampling interval. Equivalent to etherHistoryPkts in RMON.
x broadcast	Number of good packets received during this sampling interval that were directed to the broadcast address. Equivalent to etherHistoryBroadcastPkts in RMON.
x multicast packets	Number of good packets received during this sampling interval that were directed to a multicast address. Equivalent to etherHistoryMulticastPkts in RMON.
x undersized	Number of packets received during this sampling interval that were fewer than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed. Equivalent to etherHistoryUndersizedPkts in RMON.
x oversized packets	Number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed. Equivalent to etherHistoryOversizePkts in RMON.

Table 63 show rmon history Field Descriptions (continued)

Field	Description
x fragments	Total number of packets received during this sampling interval that were fewer than 64 octets in length (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). Equivalent to etherHistoryFragments in RMON.
x jabbers	Number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). Equivalent to etherHistoryJabbers in RMON.
x CRC alignment errors	Number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) from 64 to 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). Equivalent to etherHistoryCRCAlignErrors in RMON.
x collisions	Best estimate of the total number of collisions on this Ethernet segment during this sampling interval. Equivalent to etherHistoryCollisions in RMON.
# of dropped packet events is	Total number of events in which packets were dropped by the operation because of resources during this sampling interval. Note that this number is not necessarily the number of packets dropped, it is just the number of times this condition has been detected. Equivalent to etherHistoryDropEvents in RMON.
Network utilization is estimated at	Best estimate of the mean physical-layer network usage on this interface during this sampling interval, in hundredths of a percent. Equivalent to etherHistoryUtilization in RMON.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon alarm	Sets an alarm on any MIB object.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
show rmon	Displays the current RMON agent status on the router.

show rmon hosts

To display the contents of the router's RMON hosts table, use the **show rmon hosts** command in EXEC mode.

show rmon hosts

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must have first enabled RMON on the interface, and configured RMON alarms and events to display alarm information with the **show rmon hosts** command.

This command is available on the Cisco 2500 series and Cisco AS5200 series only.

For additional information, refer to the RMON MIB described in RFC 1757.

Examples

The following is sample output from the **show rmon hosts** command:

```
Router# show rmon hosts

Host Control Entry 1 is active, and owned by manager1
 Monitors host ifEntry.1.1
 Table size is 51, last time an entry was deleted was 00:00:00
  Creation Order number is 1
   Physical address is 0000.0c02.5808
   Packets: rcvd 6963, transmitted 7041
   Octets: rcvd 784062, transmitted 858530
   # of packets transmitted: broadcast 28, multicast 48
   # of bad packets transmitted is 0
```

Table 64 describes the significant fields shown in the display.

Table 64 show rmon hosts Field Descriptions

Field	Description
Host Control Entry 1 is active, and owned by manager1	Unique index of the host entry, its current state, and the owner as defined in the hostControlTable of RMON.
Monitors host ifEntry.1.1	This object identifies the source of the data for this instance of the host function. Equivalent to hostControlDataSource in RMON.
Table size is	Number of hostEntries in the hostTable and the hostTimeTable associated with this hostControlEntry. Equivalent to hostControlTableSize in RMON.
last time an entry was deleted was	Time when the last entry was deleted from the hostTable.
Creation Order number is	Index that defines the relative ordering of the creation time of hosts captured for a particular hostControlEntry. Equivalent to hostCreationOrder in RMON.
Physical address is	Physical address of this host. Equivalent to hostAddress in RMON.
Packets: rcvd	Number of good packets transmitted to this address. Equivalent to hostInPkts in RMON.
transmitted	Number of packets, including bad packets transmitted by this address. Equivalent to hostOutPkts in RMON.
Octets: rcvd	Number of octets transmitted to this address since it was added to the hostTable (excluding framing bits but including FCS octets), except for those octets in bad packets. Equivalent to hostInOctets in RMON.
transmitted	Number of octets transmitted by this address since it was added to the hostTable (excluding framing bits but including FCS octets), including those octets in bad packets. Equivalent to hostOutOctets in RMON.
# of packets transmitted:	Number of good packets transmitted by this address that were broadcast or multicast.
# of bad packets transmitted is	Number of bad packets transmitted by this address.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon alarm	Sets an alarm on any MIB object.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
show rmon	Displays the current RMON agent status on the router.

show rmon matrix

To display the contents of the router's RMON matrix table, use the **show rmon matrix** command in EXEC mode.

show rmon matrix

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must have first enabled RMON on the interface, and configured RMON alarms and events to display alarm information with the **show rmon matrix** command.

This command is available on the Cisco 2500 series and Cisco AS5200 series only.

For additional information, refer to the RMON MIB described in RFC 1757.

Examples

The following is sample output from the **show rmon matrix** command:

```
Router# show rmon matrix

Matrix 1 is active, and owned by manager1
 Monitors ifEntry.1.1
 Table size is 451, last time an entry was deleted was at 00:00:00
```

Table 65 describes the significant fields shown in the display.

Table 65 show rmon matrix Field Descriptions

Field	Description
Matrix 1 is active, and owned by manager1	Unique index of the matrix entry, its current state, and the owner as defined in the matrixControlTable of RMON.
Monitors ifEntry.1.1	This object identifies the source of the data for this instance of the matrix function. Equivalent to matrixControlDataSource in RMON.
Table size is 451, last time an entry was deleted was at	Size of the matrix table and the time that the last entry was deleted.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon alarm	Sets an alarm on any MIB object.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
show rmon	Displays the current RMON agent status on the router.

show rmon statistics

To display the contents of the router's RMON statistics table, use the **show rmon statistics** command in EXEC mode.

show rmon statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For additional information, refer to the RMON MIB described in RFC 1757.

You must have first enabled RMON on the interface, and configured RMON alarms and events to display alarm information with the **show rmon statistics** command.

This command is available on the Cisco 2500 series and Cisco AS5200 series only.

Examples

The following is sample output from the **show rmon statistics** command:

```
Router# show rmon statistics

Interface 1 is active, and owned by config
 Monitors ifEntry.1.1 which has
 Received 60739740 octets, 201157 packets,
 1721 broadcast and 9185 multicast packets,
 0 undersized and 0 oversized packets,
 0 fragments and 0 jabbers,
 0 CRC alignment errors and 32 collisions.
 # of dropped packet events (due to lack of resources): 511
 # of packets received of length (in octets):
  64: 92955, 65-127: 14204, 128-255: 1116,
  256-511: 4479, 512-1023: 85856, 1024-1518:2547
```

Table 66 describes the significant fields shown in the display.

Table 66 show rmon statistics Field Descriptions

Field	Description
Interface 1 is active, and owned by config	Unique index of the statistics entry, its current state, and the owner as defined in the etherStatsTable of RMON.
Monitors ifEntry.1.1	This object identifies the source of the data that this etherStats entry is configured to analyze. Equivalent to etherStatsDataSource in RMON.
Received 60739740 octets	Total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). Equivalent to etherStatsOctets in RMON.
x packets	Number of packets (including bad packets) received. Equivalent to etherStatsPkts in RMON.
x broadcast	Number of good packets received that were directed to the broadcast address. Equivalent to etherStatsBroadcastPkts in RMON.
x multicast packets	Number of good packets received that were directed to a multicast address. Equivalent to etherStatsMulticastPkts in RMON.
x undersized	Number of packets received that were fewer than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed. Equivalent to etherStatsUndersizedPkts in RMON.
x oversized packets	Number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed. Equivalent to etherStatsOversizePkts in RMON.
x fragments	Total number of packets received that were fewer than 64 octets in length (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). Equivalent to etherStatsFragments in RMON.
x jabbers	Number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). Equivalent to etherStatsJabbers in RMON.

Table 66 show rmon statistics Field Descriptions (continued)

Field	Description
x CRC alignment errors	Number of packets received that had a length (excluding framing bits but including FCS octets) from 64 to 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). Equivalent to etherStatsCRCAlignErrors in RMON.
x collisions	Best estimate of the total number of collisions on this Ethernet segment. Equivalent to etherHistoryCollisions in RMON.
# of dropped packet events (due to lack of resources):	Total number of events in which packets were dropped by the operation because of a lack of resources. Note that this number is not necessarily the number of packets dropped, it is just the number of times this condition has been detected. Equivalent to etherStatsDropEvents in RMON.
# of packets received of length (in octets):	Separates the received packets (good and bad) by packet size in the given ranges (64, 65 to 127,128 to 255, 256 to 511, 512 to 1023, 1024 to 1516).

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon alarm	Sets an alarm on any MIB object.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
show rmon	Displays the current RMON agent status on the router.

show rmon topn

To display the contents of the router's RMON Top-N host table, use the **show rmon topn** command in EXEC mode.

show rmon topn

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For additional information, refer to the RMON MIB described in RFC 1757.

You must have first enabled RMON on the interface, and configured RMON events to display alarm information with the **show rmon events** command.

This command is available on the Cisco 2500 series and Cisco AS5200 series only.

Examples

The following is sample output from the **show rmon topn** command:

```
Router# show rmon topn

Host Entry 1 of report 1 is active, owned by manager1
 The rate of change is based on hostTopNInPkts
 This report was last started at 00:00:00
 Time remaining in this report is 0 out of 0
 Hosts physical address is 00ad.beef.002b
 Requested # of hosts: 10, # of hosts granted: 10
Report # 1 of Top N hosts entry 1 is recording
Host 0000.0c02.5808 at a rate of 12
```

Table 67 describes the significant fields shown in the display.

Table 67 show rmon topn Field Descriptions

Field	Description
Host Entry 1 of report 1 is active, owned by manager1	Unique index of the hostTopN entry, its current state, and the owner as defined in the hostTopNControlTable of RMON.
The rate of change is based on hostTopNInPkts	Variable for each host that the hostTopNRate variable is based on.
This report was last started at	Time the report was started.
Time remaining in this report is	Number of seconds left in the report currently being collected. Equivalent to hostTopNTimeRemaining in RMON.
out of	Number of seconds that this report has collected during the last sampling interval, or if this report is currently being collected, the number of seconds that this report is being collected during this sampling interval. Equivalent to hostTopNDuration in RMON.
Hosts physical address is	Host address.
Requested # of hosts:	Maximum number of hosts requested for the Top-N table. Equivalent to hostTopNRequestedSize in RMON.
# of hosts granted:	Maximum number of hosts granted for the Top-N table.Eqivalent to hostTopNGrantedSiz in RMON.
Report # 1 of Top N hosts entry 1 is recording	Report number and entry.
Host 0000.0c02.5808 at a rate of	Physical address of the host, and the amount of change in the selected variable during this sampling interval. Equivalent to hostTopNAddress and hostTopNRate in RMON.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon alarm	Sets an alarm on any MIB object.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
show rmon	Displays the current RMON agent status on the router.

show snmp

To check 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 arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command provides counter information for SNMP operations. It also displays the chassis ID string defined with the **snmp-server chassis-id** global configuration command.

Examples

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

```
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 171.69.58.33.162, 0/10, 13 sent, 0 dropped.
```

```
SNMP Manager-role output packets
    4 Get-request PDUs
    4 Get-next PDUs
    6 Get-bulk PDUs
    4 Set-request PDUs
    23 Inform-request PDUs
    30 Timeouts
    0 Drops
SNMP Manager-role input packets
    0 Inform response PDUs
    2 Trap PDUs
    7 Response PDUs
    1 Responses with errors

SNMP informs: enabled
    Informs in flight 0/25 (current/max)
    Logging to 171.69.217.141.162
        4 sent, 0 in-flight, 1 retries, 0 failed, 0 dropped
    Logging to 171.69.58.33.162
        0 sent, 0 in-flight, 0 retries, 0 failed, 0 dropped
```

Table 68 describes the significant fields shown in the display.

Table 68 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 router.
Too big errors	Number of SNMP packets which 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 was not a noSuchName error, badValue error, or any of the other specific errors.)

Table 68 show snmp Field Descriptions (continued)

Field	Description
Response PDUs	Number of responses sent in reply to requests.
Trap PDUs	Number of SNMP traps sent.
SNMP logging	Indicates whether logging is enabled or disabled.
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** global configuration command.
SNMP Manager-role output packets	Information related to packets sent by the router as an SNMP manager.
Get-request PDUs	Number of get requests sent.
Get-next PDUs	Number of get-next requests sent.
Get-bulk PDUs	Number of get-bulk requests sent.
Set-request PDUs	Number of set requests sent.
Inform-request PDUs	Number of inform requests sent.
Timeouts	Number of request timeouts.
Drops	Number of requests dropped. Reasons for drops include no memory, a bad destination address, or an unreasonable destination address.
SNMP Manager-role input packets	Information related to packets received by the router as an SNMP manager.
Inform response PDUs	Number of inform request responses received.
Trap PDUs	Number of SNMP traps received.
Response PDUs	Number of responses received.
Responses with errors	Number of responses containing errors.
SNMP informs	Indicates whether SNMP informs are enabled.
Informs in flight	Current and maximum possible number of informs waiting to be acknowledged.
Logging to	Destination of the following informs.
sent	Number of informs sent to this host.
in-flight	Number of informs currently waiting to be acknowledged.
retries	Number of inform retries sent.
failed	Number of informs that were never acknowledged.
dropped	Number of unacknowledged informs that were discarded to make room for new informs.

Related Commands

Command	Description
show snmp pending	Displays the current set of pending SNMP requests.
show snmp sessions	Displays the current SNMP sessions.

Command	Description
snmp-server chassis-id	Provides a message line identifying the SNMP server serial number.
snmp-server manager	Starts the SNMP manager process.
snmp-server manager session-timeout	Sets the amount of time before a nonactive session is destroyed.
snmp-server queue-length	Establishes the message queue length for each trap host.

show snmp engineID

To display the identification of the local Simple Network Management Protocol (SNMP) engine and all remote engines that have been configured on the router, use the **show snmp engineID** command in EXEC mode.

show snmp engineID

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An SNMP engine is a copy of SNMP that can reside on a local or remote device.

Examples

The following example specifies 00000009020000000C025808 as the local engineID and 123456789ABCDEF000000000 as the remote engine ID, 172.16.37.61 as the IP address of the remote engine (copy of SNMP) and 162 as the port from which the remote device is connected to the local device:

```
Router# show snmp engineID

Local SNMP engineID: 00000009020000000C025808
Remote Engine ID           IP-addr          Port
123456789ABCDEF000000000   172.16.37.61     162
```

Table 69 describes the fields shown in the display.

Table 69 show snmp engineID Field Descriptions

Field	Definition
Local SNMP engine ID	A string that identifies the copy of SNMP on the local device.
Remote Engine ID	A string that identifies the copy of SNMP on the remote device.
IP-addr	The IP address of the remote device.
Port	The port number on the local device to which the remote device is connected.

Related Commands

Command	Description
snmp-server engineID local	Configures a name for either the local or remote SNMP engine on the router.

show snmp group

To display the names of configured SNMP groups, the security model being used, the status of the different views, and the storage type of each group, use the **show snmp group** command in privileged EXEC mode.

show snmp group

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP groups are configured using the snmp-server group command.

SNMP groups and users are used in the context of the View-based Access Control Model (VACM) for SNMP (for further information, see the “VACM for SNMP” IETF internet draft document).

Examples

The following example specifies the group name as public, the security model as v1, the read view name as v1default, the notify view name as *tv.FFFFFFFF, and the storage type as volatile:

```
Router# show snmp group
groupname: ILMI                             security model:v1
readview : *ilmi                            writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: ILMI                             security model:v2c
readview : *ilmi                            writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: public                           security model:v1
readview : <no readview specified>          writeview: <no writeview specified>
notifyview: *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
row status: active

groupname: public                           security model:v2c
readview : <no readview specified>          writeview: <no writeview specified>
notifyview: *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
row status: active
```

Table 70 describes the fields shown in the example.

Table 70 show snmp group Field Descriptions

Field	Definition
groupname	The name of the SNMP group, or collection of users that have a common access policy.
security model	The security model used by the group, either v1, v2c, or v3.
readview	A string identifying the read view of the group. • For further information on the SNMP views, use the **show snmp view** command.
writeview	A string identifying the write view of the group.
notifyview	A string identifying the notify view of the group. The notify view indicates the group for SNMP notifications, and corresponds to the setting of the **snmp-server group** *group-name version* **notify** *notify-view* command.

Related Commands

Command	Description
snmp-server group	Configures a new SNMP group or a table that maps SNMP users to SNMP views.
show snmp user	Displays the configured characteristics for SNMP users.
show snmp view	Displays a list of configured SNMP views.

show snmp mib

To display a list of the MIB module instance identifiers (OIDs) registered on your system, use the **show snmp mib** command in EXEC mode.

show snmp mib

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP management information is viewed as a collection of managed objects, residing in a virtual information store, termed the Management Information Base (MIB). Collections of related objects are defined in MIB modules. These modules are written using a subset of OSIs Abstract Syntax Notation One (ASN.1), termed the Structure of Management Information (SMI).

This command is intended for network administrators who are familiar with the SMI and ASN.1 syntax.

While this command can be used to display a list of MIB object identifiers (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 will display the instance identifiers for all the MIB objects on the system. The instance identifier is the final part of the OID. An object can have one or more instance identifiers. Before displaying the instance identifier, the system attempts to find the best match with the list of table names. The MIB module table names are registered when the system initializes.

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.

Tip This command produces a high volume of output if SNMP is enabled on your system. To exit from a --More-- prompt, press Ctrl-Z.

Examples

The following is sample output from the **show snmp mib** command:

```
Router# show snmp mib

system.1
system.2
sysUpTime
system.4
system.5
system.6
system.7
system.8
sysOREntry.2
sysOREntry.3
sysOREntry.4
interfaces.1
ifEntry.1
ifEntry.2
ifEntry.3
ifEntry.4
ifEntry.5
ifEntry.6
ifEntry.7
ifEntry.8
ifEntry.9
ifEntry.10
ifEntry.11
 --More--
  .
  .
  .
captureBufferEntry.2
captureBufferEntry.3
captureBufferEntry.4
captureBufferEntry.5
captureBufferEntry.6
captureBufferEntry.7
capture.3.1.1
eventEntry.1
eventEntry.2
eventEntry.3
eventEntry.4
eventEntry.5
eventEntry.6
eventEntry.7
logEntry.1
logEntry.2
logEntry.3
logEntry.4
rmon.10.1.1.2
rmon.10.1.1.3
rmon.10.1.1.4
rmon.10.1.1.5
rmon.10.1.1.6
rmon.10.1.1.7
rmon.10.2.1.2
rmon.10.2.1.3
rmon.10.3.1.2
--More--
  .
  .
  .
rmon.192.168.1.1
rmon.192.168.1.2
rmon.192.168.1.3
rmon.192.168.1.2
rmon.192.168.1.3
rmon.192.168.1.4
rmon.192.168.1.5
rmon.192.168.1.6
rmon.192.168.1.2
rmon.192.168.1.3
rmon.192.168.1.4
rmon.192.168.1.5
rmon.192.168.1.6
rmon.192.168.1.7
rmon.192.168.1.8
rmon.192.168.1.9
dot1dBase.1
dot1dBase.2
dot1dBase.3
dot1dBasePortEntry.1
dot1dBasePortEntry.2
dot1dBasePortEntry.3
dot1dBasePortEntry.4
--More--
 .
 .
 .
ifXEntry.1
ifXEntry.2
ifXEntry.3
ifXEntry.4
ifXEntry.5
ifXEntry.6
ifXEntry.7
ifXEntry.8
ifXEntry.9
ifXEntry.10
ifXEntry.11
ifXEntry.12
ifXEntry.13
ifXEntry.14
ifXEntry.15
ifXEntry.16
ifXEntry.17
ifXEntry.18
ifXEntry.19
ifStackEntry.3
ifTestEntry.1
ifTestEntry.2
--More--
 .
 .
 .
```

Related Commands

Command	Description
show snmp mib ifmib ifindex	Displays SNMP Interface Index identification numbers (ifIndex values) for all the system interfaces or the specified system interface

show snmp mib bulkstat transfer

To display the transfer status of files generated by the Periodic MIB Data Collection and Transfer Mechanism (Bulk Statistics feature), use the **show snmp mib bulkstat transfer** command in privileged EXEC mode.

show snmp mib bulkstat transfer [*transfer-id*]

Syntax Description

transfer-id	(Optional) Name of a specific bulk statistics transfer configuration. Use the *transfer-id* argument to display the status of a specific bulk statistics transfer configuration.

Command Default

If the optional *transfer-id* argument is not used, the status of all configured bulk statistics transfers is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

In the following example, the initial transfer attempt and the first retry for the file IfMIB_objects_Router_030307_102519739 to the primary and secondary URL have failed, and four additional retry attempts will be made. The time stamp for this file indicates the file was created on March 7, 2003, at 10:25:19 a.m.

```
Router# show snmp mib bulkstat transfer

Transfer Name : IfMIB_objects

Primary URL ftp://user:XXXXXXXX@192.168.1.229/
Secondary ftp://user:XXXXXXXX@192.168.1.230/

   Retained files

   File Name                           :Time Left (in seconds)     : STATE
   ----------------------------------------------------------------------
   IfMIB_objects_Router_030307_102519739 :  1196   :Retry(5 Retry attempt(s) Left)
   IfMIB_objects_Router_030307_102219739 :  1016   :Retained
   IfMIB_objects_Router_030307_101919739 :   836   :Retained
   IfMIB_objects_Router_030307_101619739 :   656   :Retained
   IfMIB_objects_Router_030307_101319739 :   475   :Retained
   IfMIB_objects_Router_030307_101119739 :   295   :Retained
```

Table 71 describes the significant fields shown in the output.

Table 71 show snmp mib bulkstat transfer Field Descriptions

Field	Description
Transfer Name	The name of the transfer configuration, specified in the **snmp mib bulkstat transfer** global configuration command.
Retained files	Indicates that the following output shows the status of files that are in system memory (retained), as opposed to files that have already been set.
File Name	The name of the bulk statistics file as it will appear after transfer. The filename of the file is generated using the following components: *transfer-name_device-name_date_time-stamp* The *transfer-name* is the name *s*pecified by the corresponding **snmp mib bulkstat transfer** command. The *device-name* is the name used in the command-line interface (CLI) router prompt. The format of the *date* and *time-stamp* depends on your system configuration, but is typically YYMMDD and HHMMSSmmm, where HH is hour, MM is minutes, SS is seconds and mmm is milliseconds.
Time Left (in seconds)	Indicates how much time is left before the specified file will be deleted (retention period), as specified with the **retain** Bulk Statistics Transfer configuration command. **Note** Regardless of the configured retention period, all retry attempts will be made before the file is deleted.
STATE	The state of the local bulk statistics file will be one of the following: • Queued—Collection time for this file is completed and the file is waiting for transfer to configured primary and secondary URL. • Retained—The file has been either successfully transferred to its destination or, if all transfer attempts have failed, all retry attempts have been completed. • Retry—The local bulk statistics file will be in this state if an attempt to transfer it to its configured destination fails and one or more retries are pending. The number of retries left will also be displayed in parenthesis.

Related Commands

Command	Description
snmp mib bulkstat transfer	Names a bulk statistics transfer configuration and enters Bulk Statistics Transfer configuration mode.

show snmp mib ifmib ifindex

To display Simple Network Management Protocol (SNMP) Interface Index (ifIndex) identification numbers for all system interfaces or a specified system interface, use the **show snmp mib ifmib ifindex** command in privileged EXEC mode.

show snmp mib ifmib ifindex [*type number*]

Syntax Description

type number

(Optional) Type and number of the interface. Valid types are in the following list. The *number* argument is an integer. Valid *type* and *number* values are the following:

- **atm**—Asynchronous transfer mode interface.
- **async**—Asynchronous interface; *number* will vary by platform.
- **ctunnel**—CTunnel interface; *number* is 0 to 2147483647.
- **dialer**—Dialer interface; *number* is 0 to 255.
- **ethernet**—IEEE 802.3 interface; *number* is 0 to 15.
- **group-async**—Asynchronous Group interface; *number* is 0 to 64.
- **lex**—Lex interface; *number* is 0 to 2147483647.
- **loopback**—Loopback interface; *number* is 0 to 2147483647.
- **mfr**—Multilink Frame Relay bundle interface; *number* is 0 to 2147483647.
- **multilink**—Multilink-group interface; *number* is 1 to 2147483647.
- **null**—Null interface; *number* is 0 to 0.
- **serial**—Serial interface; *number* is 0 to 15.
- **tunnel**—Tunnel interface; *number* is 0 to 2147483647.
- **vif**—Pragmatic General Multicast (PGM) Host interface; *number* is 0 to 1.
- **virtual-ppp**—Virtual Point-to-Point interface; *number* is 1 to 2147483647.
- **virtual-template**—Virtual Template interface; *number* is 1 to 200.
- **virtual-tokenring**—Virtual Token Ring interface; *number* is 0 to 2147483647.

Command Default

The ifIndex values for all interfaces are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **show snmp mib ifmib ifindex** command allows you to use the command-line interface (CLI) to display SNMP ifIndex values assigned to interfaces and subinterfaces. By using the CLI, a network management station is not needed.

If an interface is not specified using the optional *type number* arguments, the interface description (ifDescr) and ifIndex pairs of all interfaces and subinterfaces present on the system are shown.

Examples

The following example shows sample output for Ethernet interface 2/0:

```
Router# show snmp mib ifmib ifindex Ethernet2/0

Ethernet2/0: Ifindex = 2
```

The following example shows sample output for all interfaces (no optional arguments are specified):

```
Router# show snmp mib ifmib ifindex

ATM1/0: Ifindex = 1
ATM1/0-aal5 layer: Ifindex = 12
ATM1/0-atm layer: Ifindex = 10
ATM1/0.0-aal5 layer: Ifindex = 13
ATM1/0.0-atm subif: Ifindex = 11
ATM1/0.9-aal5 layer: Ifindex = 32
ATM1/0.9-atm subif: Ifindex = 31
ATM1/0.99-aal5 layer: Ifindex = 36
ATM1/0.99-atm subif: Ifindex = 35
Ethernet2/0: Ifindex = 2
Ethernet2/1: Ifindex = 3
Ethernet2/2: Ifindex = 4
Ethernet2/3: Ifindex = 5
Null0: Ifindex = 14
Serial3/0: Ifindex = 6
Serial3/1: Ifindex = 7
Serial3/2: Ifindex = 8
Serial3/3: Ifindex = 9
```

Each line of output indicates the system interface followed by the ifindex identification number.

Related Commands

Command	Description
show snmp mib	Displays a list of the MIB OIDs registered on the system.
snmp ifindex persist	Enables ifIndex values in the IF-MIB that persist across reboots only on a specific interface.
snmp ifmib ifalias long	Configures the system to handle IfAlias descriptions of up to 256 characters in length.
snmp-server ifindex persist	Enables ifIndex values in the IF-MIB that persist across reboots for all interfaces (globally).

show snmp mib notification-log

To display information about the state of local SNMP notification logging, use the **show snmp mib notification-log** command in EXEC mode.

show snmp mib notification-log [**all** | **default**]

Syntax Description

all	(Optional) Displays all notification log entries stored in the local Notification Log MIB database.
default	(Optional) Displays summary information for the default (unnamed) SNMP Notification Log.

Command Modes

EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Release 12.2(13)T.

Usage Guidelines

The SNMP Notification Log works in conjunction with the NOTIFICATION-LOG-MIB.my MIB module (available at ftp://ftp.cisco.com/pub/mibs/v2/). This MIB module is based on RFC 3014. The local logs can be polled by external network management applications to verify that they have not missed important SNMP notifications (traps and informs).

The **show snmp mib notification-log all** command displays all logged notification entries currently in the local MIB database. Entries are displayed from the oldest to the newest. The time of entry creation is determined using the system-up-time (sysUpTime) value; this means that the age of the entry is set using the amount of time that has passed since the router was last restarted. Other information for the entries includes the notificationID, and the filters (varbinds) associated with the log, if any.

Examples

The following is sample output from the **show snmp mib notification-log** command:

```
Router# show snmp mib notification-log

GlobalAgeout 15, GlobalEntryLimit 500
Total Notifications logged in all logs 0
Log Name"", Log entry Limit 500, Notifications logged 0
Logging status enabled
Created by cli
```

Note that in this example, the Log Name of "" indicates the default "null-named" Notification Log.

Related Commands

Command	Description
snmp mib notification-log default	Creates and activates an SNMP Notification Log.

Command	Description
snmp mib notification-log globalageout	Sets the maximum age for a notification.
snmp mib notification-log globalsize	Sets the maximum number of notifications allowed in all logs.

show snmp pending

To display the current set of pending Simple Network Management Protocol (SNMP) requests, use the **show snmp pending** command in EXEC mode.

show snmp pending

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

After the SNMP manager sends a request, the request is “pending” until the manager receives a response or the request timeout expires.

Examples

The following is sample output from the **show snmp pending** command:

```
Router# show snmp pending

req id: 47, dest: 171.69.58.33.161, V2C community: public, Expires in 5 secs
req id: 49, dest: 171.69.58.33.161, V2C community: public, Expires in 6 secs
req id: 51, dest: 171.69.58.33.161, V2C community: public, Expires in 6 secs
req id: 53, dest: 171.69.58.33.161, V2C community: public, Expires in 8 secs
```

Table 72 describes the significant fields shown in the display.

Table 72 show snmp pending Field Descriptions

Field	Description
req id	ID number of the pending request.
dest	IP address of the intended receiver of the request.
V2C community	SNMP version 2C community string sent with the request.
Expires in	Remaining time before request timeout expires.

Related Commands

Command	Description
show snmp	Checks the status of SNMP communications.
show snmp sessions	Displays the current SNMP sessions.

Command	Description
snmp-server manager	Starts the SNMP manager process.
snmp-server manager session-timeout	Sets the amount of time before a nonactive session is destroyed.

show snmp sessions

To display the current Simple Network Management Protocol (SNMP) sessions, use the **show snmp sessions** command in EXEC mode.

show snmp sessions [**brief**]

Syntax Description

brief	(Optional) Displays a list of sessions only. Does not display session statistics.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Sessions are created when the SNMP manager in the router sends SNMP requests, such as inform requests, to a host or receives SNMP notifications from a host. One session is created for each destination host. If there is no further communication between the router and host within the session timeout period, the corresponding session will be deleted.

Examples

The following is sample output from the **show snmp sessions** command:

```
Router# show snmp sessions

Destination: 171.69.58.33.162, V2C community: public
  Round-trip-times: 0/0/0 (min/max/last)
  packets output
    0 Gets, 0 GetNexts, 0 GetBulks, 0 Sets, 4 Informs
    0 Timeouts, 0 Drops
  packets input
    0 Traps, 0 Informs, 0 Responses (0 errors)
Destination: 171.69.217.141.162, V2C community: public, Expires in 575 secs
  Round-trip-times: 1/1/1 (min/max/last)
  packets output
    0 Gets, 0 GetNexts, 0 GetBulks, 0 Sets, 4 Informs
    0 Timeouts, 0 Drops
  packets input
    0 Traps, 0 Informs, 4 Responses (0 errors)
```

Table 73 describes the significant fields shown in the output.

The following is sample output from the **show snmp sessions brief** command:

```
Router# show snmp sessions brief

Destination: 171.69.58.33.161, V2C community: public, Expires in 55 secs
```

Table 73 show snmp sessions Field Descriptions

Field	Description
Destination	IP address of the remote agent.
V2C community	SNMP version 2C community string used to communicate with the remote agent.
Expires in	Remaining time before the session timeout expires.
Round-trip-times	Minimum, maximum, and the last round-trip time to the agent.
packets output	Packets sent by the router.
Gets	Number of get requests sent.
GetNexts	Number of get-next requests sent.
GetBulks	Number of get-bulk requests sent.
Sets	Number of set requests sent.
Informs	Number of inform requests sent.
Timeouts	Number of request timeouts.
Drops	Number of packets that could not be sent.
packets input	Packets received by the router.
Traps	Number of traps received.
Informs	Number of inform responses received.
Responses	Number of request responses received.
errors	Number of responses that contained an SNMP error code.

Related Commands

Command	Description
show snmp	Checks the status of SNMP communications.
show snmp pending	Displays the current set of pending SNMP requests.
snmp-server manager	Starts the SNMP manager process.
snmp-server manager session-timeout	Sets the amount of time before a nonactive session is destroyed.

show snmp sysobjectid

To identify a Simple Network Management Protocol (SNMP) device, use the **show snmp sysobjectid** command in privileged EXEC mode.

show snmp sysobjectid

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(10)	This command was introduced.

Usage Guidelines

Using the **show snmp sysobjectid** command is a quick way to identify a device. The same information can be obtained by issuing an SNMP query on the MIB object sysObjectID. Output from the command shows the system object ID in dotted decimal format. The system object ID is the identifier of the network management subsystem, which is SNMP, and is typically the starting point at which network management applications try to discover a device.

Examples

The following example shows the **show snmp sysobjectid** command and sample output. In this example, the object ID translates to iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.ciscoGatewayServer.

```
Router# show snmp sysobjectid

1.3.6.1.4.1.9.1.1
```

Related Commands

Command	Description
show snmp	Displays the status of SNMP communications.
show snmp engineID	Displays the identification of the local SNMP engine and all remote engines that have been configured on the router.
show snmp group	Displays the names of configured SNMP groups, the security model being used, the status of the different views, and the storage type of each group.
show snmp mib	Displays a list of the MIB module instance identifiers (OIDs) registered on your system.
show snmp pending	Displays the current set of pending SNMP requests.

Command	Description
show snmp sessions	Displays the current SNMP sessions.
show snmp user	Displays information about the configured characteristics of SNMP users.
show snmp view	Displays the family name, storage type, and status of a SNMP configuration and associated MIB.

show snmp user

To display information about the configured characteristics of Simple Network Management Protocol (SNMP) users, use the **show snmp user** command in privileged EXEC mode.

show snmp user [*username*]

Syntax Description

username	(Optional) Name of a specific user or users about which to display SNMP information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.3(2)T	The *username* argument was added. The output for this command was enhanced to show the authentication protocol (MD5 or SHA) and group name.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

An SNMP user must be part of an SNMP group, as configured using the **snmp-server user** *username group-name* command.

When the *username* argument is not entered, the **show snmp user** command displays information about all configured users. If you specify the *username* argument, if one or more users of that name exists, the information pertaining to those users is displayed. Because this command displays users configured with the SNMP engine ID of the local agent and other engine IDs, there can be multiple users with the same username.

When configuring SNMP, you may see the logging message “Configuring snmpv3 USM user.” USM stands for the User-based Security Model for version 3 of the Simple Network Management Protocol (SNMPv3). For further information on the USM, see RFC 2574.

Examples

The following is sample output from the **show snmp user** command. The output indicates the username as authuser, the engine ID string as 00000009020000000C025808, and the storage type as nonvolatile:

```
Router# show snmp user authuser

User name: authuser
Engine ID: 00000009020000000C025808
storage-type: nonvolatile       active access-list: 10
Rowstatus: active
```

```
Authentication Protocol: MD5
Privacy protocol: DES
Group name: VacmGroupName
```

Table 74 describes the significant fields shown in the display.

Table 74 show snmp user Field Descriptions

Field	Description
User name	A string identifying the name of the SNMP user.
Engine ID	A string identifying the name of the copy of SNMP on the device.
storage-type	Indicates whether the settings have been set in volatile or temporary memory on the device, or in nonvolatile or persistent memory where settings will remain after the device has been turned off and on again.
active access-list	Standard IP access list associated with the SNMP user.
Rowstatus	Indicates whether Rowstatus is active or inactive.
Authentication Protocol	Identifies which authentication protocol is used. Options are message digest algorithm 5 (MD5), Secure Hash Algorithm (SHA) packet authentication, or None. • If authentication is not supported in your software image, this field will not be displayed.
Privacy protocol	Indicates whether Data Encryption Standard (DES) packet encryption is enabled. • If DES is not supported in your software image, this field will not be displayed.
Group name	Indicates the SNMP group the user is a part of. • SNMP groups are defined in the context of a View-based Access Control Model (VACM).

show snmp view

To display the family name, storage type, and status of a Simple Network Management Protocol (SNMP) configuration and associated MIB, use the **show snmp view** command in privileged EXEC mode.

show snmp view

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.

Usage Guidelines

Use this command to display the SNMP view configuration.

Examples

The following is sample output from the **show snmp view** command.

```
Router# show snmp view

View Family Name/View Family Subtree/View Family Mask/View Family Type/storage/status

myview              mib-2               -          included         nonvolatile active
myview              cisco               -          included         nonvolatile active
myview              atEntry             -          excluded         nonvolatile active
v1default           iso                 -          included         permanent   active
v1default           internet            -          included         volatile    active
v1default           internet.6.3.15     -          excluded         volatile    active
v1default           internet.6.3.16     -          excluded         volatile    active
v1default           internet.6.3.18     -          excluded         volatile    active
```

Table 75 describes the significant fields shown in the display.

Table 75 show snmp view Field Descriptions

Field	Description
View Family Name	Family name.
View Family Subtree	MIB name.
View Family Mask	Family mask. A hyphen (-) appears in this column when no mask is associated.
View Family Type	Type of family, either included or excluded.
storage	Type of memory storage, for example, volatile.
status	Status of the configuration, either active or nonactive.

show sntp

To show information about the Simple Network Time Protocol (SNTP), use the **show sntp** command in EXEC mode on a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router.

show sntp

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

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

```
Router> show sntp

SNTP server     Stratum   Version    Last Receive
171.69.118.9       5         3        00:01:02
172.21.28.34       4         3        00:00:36    Synced  Bcast

Broadcast client mode is enabled.
```

Table 76 describes the significant fields shown in the display.

Table 76 show sntp Field Descriptions

Field	Description
SNTP server	Address of the configured or broadcast NTP server.
Stratum	NTP stratum of the server. The stratum indicates how far away from an authoritative time source the server is.
Version	NTP version of the server.
Last Receive	Time since the last NTP packet was received from the server.
Synced	Indicates the server chosen for synchronization.
Bcast	Indicates a broadcast server.

Related Commands

Command	Description
sntp broadcast client	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to accept NTP traffic from any broadcast server.
sntp server	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to request and accept NTP traffic from a time server.

show time-range

To display information about configured time ranges, use the **show time-range** command in user EXEC or privileged EXEC mode.

show time-range

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior.

Command Modes

User EXEC and Privileged EXEC

Command History

Release	Modification
12.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.33(SRA).
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to display configured time ranges.

Examples

The following is sample output for the **show time-range** command. The word (active) indicates that the time range is in effect at that moment; otherwise, the output will indicate (inactive).

```
Router# show time-range
time-range entry: test (active)
    absolute start 00:00 01 January 2006 end 23:59 31 December 2006
    periodic weekdays 8:00 to 20:00
```

Related Commands

Command	Description
time-range	Specifies a time range by name and allows you configure a range during which an access list, for example, is active.

show track

To display information about objects that are tracked by the tracking process, use the **show track** command in privileged EXEC mode.

show track [*object-number* [**brief**] | **interface** [**brief**] | **ip route** [**brief**] | **resolution** | **timers**]

Syntax Description

object-number	(Optional) Object number that represents the object to be tracked. The range is from 1 to 500.
brief	(Optional) Displays a single line of information related to the preceding argument or keyword.
interface	(Optional) Displays tracked interface objects.
ip route	(Optional) Displays tracked IP-route objects.
resolution	(Optional) Displays resolution of tracked parameters.
timers	(Optional) Displays polling interval timers.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(8)T	The output was enhanced to include the track-list objects.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.4(2)T	The output was enhanced to display stub objects.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(9)T	This command was enhanced to display information about the status of an interface when carrier-delay detection has been enabled.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use this command to display information about objects that are tracked by the tracking process. When no arguments or keywords are specified, information for all objects is displayed.

Examples

The following example shows information about the state of IP routing on the interface that is being tracked:

```
Router# show track 1

Track 1
 Interface Ethernet0/2 ip routing
 IP routing is Down (no IP addr)
  1 change, last change 00:01:08
 Tracked by:
  HSRP Ethernet0/3 1
```

The following example shows information about the line-protocol state on the interface that is being tracked:

```
Router# show track 1

Track 1
 Interface Ethernet0/1 line-protocol
 Line protocol is Up
  1 change, last change 00:00:05
 Tracked by:
  HSRP Ethernet0/3 1
```

The following example shows information about the reachability of a route that is being tracked:

```
Router# show track 1

Track 1
 IP route 10.16.0.0 255.255.0.0 reachability
 Reachability is Up (RIP)
  1 change, last change 00:02:04
 First-hop interface is Ethernet0/1
 Tracked by:
  HSRP Ethernet0/3 1
```

The following example shows information about the threshold metric of a route that is being tracked:

```
Router# show track 1

Track 1
 IP route 10.16.0.0 255.255.0.0 metric threshold
 Metric threshold is Up (RIP/6/102)
  1 change, last change 00:00:08
 Metric threshold down 255 up 254
 First-hop interface is Ethernet0/1
 Tracked by:
  HSRP Ethernet0/3 1
```

The following example shows the object type, the interval in which it is polled, and the time until the next poll:

```
Router# show track timers

 Object type   Poll Interval  Time to next poll
 interface     1              expired
 ip route      30             29.364
```

Table 77 describes the significant fields shown in the displays.

Table 77 show track Field Descriptions

Field	Description
Track	Object number that is being tracked.
Interface Ethernet0/2 ip routing	Interface type, number, and object that is being tracked.
IP routing is	State value of the object, displayed as Up or Down. If the object is down, the reason is displayed.
1 change, last change	Number of times that the state of a tracked object has changed and the time (in *hh:mm:ss*) since the last change.
Tracked by	Client process that is tracking the object.

Table 77 show track Field Descriptions (continued)

Field	Description
First-hop interface is	Displays the first-hop interface.
Object type	Object type that is being tracked.
Poll Interval	Interval (in seconds) in which the tracking process polls the object.
Time to next poll	Period of time, in seconds, until the next polling of the object.

The following output shows that there are two objects. Object 1 has been configured with a weight of 10 "down," and object 2 has been configured with a weight of 20 "up." Object 1 is down (expressed as 0/10) and object 2 is up. The total weight of the tracked list is 20 with a maximum of 30 (expressed as 20/30). The "up" threshold is 20, so the list is "up."

```
Router# show track

 Track 6
 List threshold weight
  Threshold weight is Up (20/30)
   1 change, last change 00:00:08
   object 1 Down (0/10)
   object 2 weight 20 Up (20/30)
  Threshold weight down 10 up 20
   Tracked by:
    HSRP Ethernet0/3 1
```

The following example shows information about the Boolean configuration:

```
Router# show track

 Track 3
 List boolean and
 Boolean AND is Down
  1 change, last change 00:00:08
   object 1 not Up
   object 2 Down
 Tracked by:
  HSRP Ethernet0/3 1
```

Table 78 describes the significant fields shown in the displays.

Table 78 show track Field Descriptions

Field	Description
Track	Object number that is being tracked.
Boolean AND is Down	Each object defined in the list must be in a down state.
1 change, last change	Number of times that the state of a tracked object has changed and the time (in *hh:mm:ss*) since the last change.
Tracked by	Client process that is tracking the object; in this case, HSRP.

The following example shows information about a stub object that has been created to be tracked using Embedded Event Manager (EEM):

```
Router# show track

Track 1
  Stub-object
  State is Up
    1 change, last change 00:00:04, by Undefined
```

The following example shows information about a stub object when the **brief** keyword is used:

```
Router# show track brief

Track   Object                           Parameter        Value Last Change
1       Stub-object Undefined                             Up    00:00:12
```

The following example shows information about the line-protocol state on an interface that is being tracked and which has carrier-delay detection enabled:

```
Router# show track

Track 101
Interface Ethernet1/0 line-protocol
Line protocol is Down (carrier-delay)
1 change, last change 00:00:03
```

Table 79 describes the significant fields shown in the displays.

Table 79 show track brief Field Descriptions

Field	Description
Track	Object number that is being tracked.
Interface Ethernet1/0 line-protocol	Interface type, number, and object that is being tracked.
Line protocol is Down (carrier-delay)	State of the interface with the carrier-delay parameter taken into consideration.
last change	Time (in *hh:mm:ss*) since the state of a tracked object last changed.

Table 80 describes the significant fields shown in the displays.

Table 80 show track brief Field Descriptions

Field	Description
Track	Object number that is being tracked.
Object	Definition of stub object.
Parameter	Tracking parameters.
Value	State value of the object, displayed as Up or Down.
last change	Time (in *hh:mm:ss*) since the state of a tracked object last changed.

Related Commands

Command	Description
track interface	Configures an interface to be tracked and enters tracking configuration mode.
track ip route	Tracks the state of an IP route and enters tracking configuration mode.

show xsm status

To display information and subscription status of the XML Subscription Manager (XSM) server and clients (such as VPN Device Manager [VDM]), and to display a list of XML data from the XSM server, use the **show xsm status** command in privileged EXEC mode.

show xsm status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to display the following information: which subsystems and histories are enabled or disabled (XSM, Embedded Device Manager [EDM], VDM), XSM client version, number of XSM sessions, duration of XSM session, session IDs, client version and IP address, configuration and monitor privilege levels, and list of subscribed XML Request Descriptors (XRDs).

Examples

The following example shows one XSM session (Session ID = 2) active on the Cisco device for the XSM client at IP address 172.17.129.134, and how long this session has been connected to the XSM server (Session 2: Connected since 22:47:07 UTC Mon Jan 8 2001). The output shows that the XSM, VDM, and EDM subsystems, and EDM and VDM history collecting are enabled. XSM configuration privilege level is set at 15, with XSM monitor privilege level set at 1.

This output also shows the active XRDs (and their version) for Session 2:

```
Router# show xsm status

XSM subsystem is Enabled.
VDM subsystem is Enabled.
EDM subsystem is Enabled.
EDM History is Enabled.
VDM History is Enabled.
XSM privilege configuration level 15.
XSM privilege monitor level 1.
```

```
Number of XSM Sessions : 1.

  Session ID = 2.
    XSM Client v0.0(0.0)- @ 172.17.129.134
    Connected since 22:47:07 UTC Mon Jan 8 2001

    List of subscribed xrds:
    0 ) device-about                             v1.0
    1 ) ios-image                                v1.0
    2 ) if-list                                  v1.0
    3 ) device-health                            v1.0
    4 ) ike-stats                                v1.0
    5 ) ike                                      v1.0
    6 ) ipsec-topn-tunnels-by-traffic            v1.0
    7 ) ipsec-topn-tunnels-by-duration           v1.0
    8 ) ipsec-stats                              v1.0
    9 ) crypto-maps                              v1.0
    10) ipsec                                    v1.0
```

Table 81 describes the significant fields shown in the display. (See documention of the **show xsm xrd-list** command for a full description of subscribed XRDs).

Table 81 show xsm status Field Descriptions

Field	Description
XSM privilege configuration level	XSM configuration privilege level.
XSM privilege monitor level	XSM monitor privilege level.
Number of XSM Sessions	Total number of concurrent XSM sessions.
Session ID	Specific XSM session number.
XSM Client	Version and IP address of the XSM client.
Connected since	Start time for each session connection to the XSM server.
List of subscribed xrds	Details XRDs available from the XSM server (see **show xsm xrd-list** command for complete list of XRDs).

Related Commands

Command	Description
clear xsm	Clears XSM client sessions.
show xsm xrd-list	Displays all XRDs for clients subscribed to the XSM server.
xsm	Enables XSM client access to the router.
xsm privilege configuration level	Enables configuration privilege level to subscribe to XRDs.
xsm privilege monitor level	Enables monitor privilege level to subscribe to XRDs.

show xsm xrd-list

To display all XML Request Descriptors (XRDs) for XML Subscription Manager (XSM) clients (such as the VPN Device Manager [VDM]) made available by subscription to the XSM server and to identify the required privilege levels, use the **show xsm xrd-list** command in privileged EXEC mode.

show xsm xrd-list

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to display the XRD version and minimum privilege level and type (configuration or monitor) required to view each XRD.

Examples

The following example shows some active XRDs on the XSM server. The end of each line displays the following:

- XRD version number.
- XRD privilege type (configuration or monitor), indicating the privilege level required.

This example displays all available XRDs because both relevant commands (**xsm edm** and **xsm vdm**) have been configured. However, if one command is not configured, only an abbreviated XRD list will appear.

```
Router# show xsm xrd-list
List of all available xrds:
0 ) vlan-db                                   v1.0  privilege=configuration
1 ) entity                                    v1.0  privilege=configuration
2 ) ip                                        v1.0  privilege=configuration
3 ) ios-users                                 v1.0  privilege=configuration
4 ) device-about                              v1.0  privilege=monitor
5 ) ios-image                                 v1.0  privilege=configuration
6 ) if-stats                                  v1.0  privilege=monitor
7 ) if-list                                   v1.0  privilege=configuration
```

```
8 ) device-health                           v1.0  privilege=monitor
9 ) time                                    v1.0  privilege=monitor
10) access-lists                            v1.0  privilege=configuration
11) ike-topn-tunnels-by-traffic             v1.0  privilege=monitor
12) ike-topn-tunnels-by-errors              v1.0  privilege=monitor
13) ike-topn-tunnels-by-duration            v1.0  privilege=monitor
14) ike-stats                               v1.0  privilege=monitor
15) ike                                     v1.0  privilege=configuration
16) certificate-authorities                 v1.0  privilege=configuration
17) ipsec-topn-tunnels-by-traffic           v1.0  privilege=monitor
18) ipsec-topn-tunnels-by-errors            v1.0  privilege=monitor
19) ipsec-topn-tunnels-by-duration          v1.0  privilege=monitor
20) ipsec-stats                             v1.0  privilege=monitor
21) crypto-maps                             v1.0  privilege=configuration
22) ipsec                                   v1.0  privilege=configuration
23) vdm-history                             v1.0  privilege=configuration
24) gre-tunnels                             v1.0  privilege=monitor
end list.
```

Table 82 describes (in alphabetical order) typical XRDs shown in the display.

Table 82 show xsm xrd-list Field Descriptions

Field	Descriptions
access-lists	IOS access control list (ACL) configuration.
certificate-authorities	IOS certificate authority (CA) configuration.
crypto-maps	IOS Crypto Map configuration.
device-about	General network device information.
device-health	General network device health statistics.
edm-history	Selected, historical statistics related to general embedded device management. (This field is not shown in the example above.)
entity	Summary of all physical and logical entities within a device.
gre-tunnels	All current GRE tunnels and respective statistics.
if-list	List of all interfaces and their respective IOS configurations.
if-stats	Statistics for all interfaces and their respective IOS configurations.
ike	IOS Internet Key Exchange (IKE) configuration.
ike-stats	Statistics related to IKE.
ike-topn-tunnels-by-duration	Top 10 IKE tunnels by duration (time).
ike-topn-tunnels-by-errors	Top 10 IKE tunnels by errors.
ike-topn-tunnels-by-traffic	Top 10 IKE tunnels by traffic volume.
ios-image	Information about the current running IOS image.
ios-users	Local IOS user configuration.
ip	IOS IP configuration statistics.
ipsec	IOS IPSec configuration.
ipsec-stats	Interface name and IPSec input and output statistics including: number of packets, dropped packets, octets and errors.
ipsec-topn-tunnels-by-duration	Top 10 IPSec tunnels by duration.
ipsec-topn-tunnels-by-errors	Top 10 IPSec tunnels by errors.

Table 82 show xsm xrd-list Field Descriptions (continued)

Field	Descriptions
ipsec-topn-tunnels-by-traffic	Top 10 IPSec tunnels by traffic.
time	Device’s clock reading in UTC.
vdm-history	Selected, historical VPN-related statistics.
vlan-db	VLAN database configuration (switches only).
xsm-session	Status of the current XSM session and related subscriptions. (This field is not shown in the example above.)

Related Commands

Command	Description
clear xsm	Clears XSM client sessions.
show xsm status	Displays information and status about clients subscribed to the XSM server.
xsm	Enables XSM client access to the router.
xsm privilege configuration level	Enables configuration privilege level to subscribe to XRDs.
xsm privilege monitor level	Enables monitor privilege level to subscribe to XRDs.

slot (ERM policy)

To configure line cards, use the **slot** command in ERM policy configuration mode.

slot *slot-number*

Syntax Description

slot-number	Integer that identifies a slot number or the start of a range of slots.

Command Default

Disabled.

Command Modes

ERM policy configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

You can configure line cards using the **slot** *slot-number* command in ERM policy configuration mode. This command is available only in distributed platforms such as the Route Switch Processor (RSP). You must use a Cisco 7500 router with a line card for executing this command.

Examples

The following example shows how to configure the line card 0:

```
Router(config-erm-policy)# slot 0
```

Related Commands

Command	Description
buffer public	Enters the buffer owner configuration mode and sets thresholds for buffer usage.
cpu interrupt	Enters the CPU owner configuration mode and sets thresholds for interrupt level CPU utilization.
cpu process	Enters the CPU owner configuration mode and sets thresholds for processor level CPU utilization.
cpu total	Enters the CPU owner configuration mode and sets thresholds for total CPU utilization.
critical rising	Sets the critical level threshold values for the buffer, CPU, and memory ROs.
major rising	Sets the major level threshold values for the buffer, CPU, and memory ROs.
memory io	Enters the memory owner configuration mode and sets threshold values for I/O memory.
memory processor	Enters the memory owner configuration mode and sets threshold values for processor memory.

Command	Description
minor rising	Sets the minor level threshold values for the buffer, CPU, and memory ROs.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.

snmp ifmib ifalias long

To configure the system to handle IfAlias descriptions of up to 256 characters, use the **snmp ifmib ifalias long** command in global configuration mode. To limit the IfAlias description to 64 characters, use the **no** form of this command.

snmp ifmib ifalias long

no snmp ifmib ifalias long

Syntax Description

This command has no arguments or keywords.

Command Default

The ifAlias description is limited to 64 characters.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The ifAlias object (ifXEntry 18) of the Interfaces MIB (IF-MIB) is called the Interface Alias. The Interface Alias (ifAlias) is a user-specified description of an interface used for Simple Network Management Protocol (SNMP) network management. The ifAlias is an object in the Interfaces Group MIB (IF-MIB) which can be set by a network manager to “name” an interface.

The ifAlias value for an interface or subinterface can be set using the **description** command in interface configuration mode or subinterface configuration mode, or by using a Set operation from an NMS. Prior to the introduction of this command, ifAlias descriptions for subinterfaces were limited to 64 characters. (The OLD-CISCO-INTERFACES-MIB allows up to 255 characters for the locIfDescr MIB variable, but this MIB does not support subinterfaces.) IfAlias descriptions appear in the output of the **show interfaces** command in EXEC mode, and in the output of the **more system: running-config** or **show running-config** commands in EXEC mode.

Examples

In the following example, the system is configured to retain and return ifAlias values of up to 256 characters in length:

```
Router(config)# snmp ifmib ifalias long
```

Related Commands

Command	Description
description	Allows you to specify a description for the specified interface in human-readable form.
show snmp mib	Displays a list of the MIB module instance identifiers (OIDs) registered on your system.
show snmp mib ifmib ifindex	Displays SNMP Interface Index identification numbers (ifIndex values) for all the system interfaces or the specified system interface

snmp mib bulkstat object-list

To configure a Simple Network Management Protocol (SNMP) bulk statistics object list, use the **snmp mib bulkstat object-list** command in global configuration mode. To remove an SNMP bulk statistics object list, use the **no** form of this command.

snmp mib bulkstat object-list *name*

no snmp mib bulkstat object-list *name*

Syntax Description

name	Name of the object list to be configured.

Command Default

No SNMP bulk statistics object list is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **snmp 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.

After you enter this command, the router enters Bulk Statistics Object List configuration mode, in which you can use the **add** command to add specific MIB objects to the list.

Bulk statistics object lists can be reused in multiple schemas.

Examples

In the following example, a bulk statistics object list called ifMib is configured to include the ifInoctets, ifOutoctets, ifInUcastPkts, and ifInDiscards objects from the Interfaces Group MIB (IF-MIB):

```
Router(config)# snmp mib bulkstat object-list ifmib
Router(config-bulk-objects)# add ifInoctets
Router(config-bulk-objects)# add ifOutoctets
Router(config-bulk-objects)# add ifInUcastPkts
Router(config-bulk-objects)# add ifInDiscards
Router(config-bulk-objects)# end
```

Related Commands

Command	Description
add	Adds specific MIB objects to a defined SNMP bulk statistics object list.
snmp mib bulkstat schema	Names an SNMP bulk statistics schema and enters Bulk Statistics Schema configuration mode.

snmp mib bulkstat schema

To define a bulk statistics schema, use the **snmp mib bulkstat schema** command in global configuration mode. To delete a previously configured bulk statistics schema, use the **no** form of this command.

snmp mib bulkstat schema *schema-name*

no snmp mib bulkstat schema *schema-name*

Syntax Description

schema-name	Name of the bulk statistics schema to be configured.

Command Default

No schemas are defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **snmp 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.

Examples

The following example shows the configuration of a bulk statistics schema called ATM2/0-IFMIB:

```
Router(config)# snmp mib bulkstat schema ATM2/0-IFMIB
Router(config-bulk-sc)# object-list ifmib
Router(config-bulk-sc)# poll-interval 5
Router(config-bulk-sc)# instance exact interface ATM2/0 subif
Router(config-bulk-sc)# exit
```

Related Commands

Command	Description
instance	Specifies the instance that, when appended to the object list, gives the OID of the object instance to be monitored in a bulk statistics schema.
object-list	Adds specific MIB objects to a defined SNMP bulk statistics object list.
poll-interval	Configures the polling interval for a bulk statistics schema.
snmp mib bulkstat transfer	Names a bulk statistics transfer configuration and enters Bulk Statistics Transfer configuration mode.

ssnmp mib bulkstat transfer

To identify the bulk statistics transfer configuration and enter Bulk Statistics Transfer configuration mode, use the **snmp mib bulkstat transfer** command in global configuration mode. To remove a previously configured transfer, use the **no** form of this command.

snmp mib bulkstat transfer *transfer-id*

no snmp mib bulkstat transfer *transfer-id*

Syntax Description

transfer-id	Name of the transfer configuration.

Command Default

No bulk statistics transfer configuration exists.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

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.

This command enters Bulk Statistics Transfer configuration mode, as indicated by the prompt (config-bulk-tr).

Examples

In the following example, the transfer configuration is given the name bulkstat1 and is configured to include the schemas ATM2/0-IFMIB and ATM2/0-CAR:

```
Router(config)# snmp mib bulkstat transfer bulkstat1
Router(config-bulk-tr)# schema ATM2/0-IFMIB
Router(config-bulk-tr)# schema ATM2/0-CAR
Router(config-bulk-tr)# url primary ftp://user1:pswrd@cbin2-host/users/user1/bulkstat1
Router(config-bulk-tr)# url secondary tftp://user1@10.1.0.1/tftpboot/user1/bulkstat1
Router(config-bulk-tr)# format schemaASCII
Router(config-bulk-tr)# transfer-interval 30
Router(config-bulk-tr)# retry 5
Router(config-bulk-tr)# buffer-size 1024
Router(config-bulk-tr)# retain 30
Router(config-bulk-tr)# end
Router# copy running-config startup-config
```

Related Commands

Command	Description
show snmp mib bulkstat transfer	Displays the transfer status of files generated by the Periodic MIB Data Collection and Transfer Mechanism.

snmp mib community-map

To associate a Simple Network Management Protocol (SNMP) community with an SNMP context, engine ID, or security name, use the **snmp mib 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 mib community-map *community-name* [**context** *context-name*] [**engineid** *engine-id*] [**security-name** *security-name*] [**target-list** *vpn-list-name*]

no snmp mib community-map *community-name* [**context** *context-name*] [**engineid** *engine-id*] [**security-name** *security-name*] [**target-list** *vpn-list-name*]

Syntax Description

community-name	String that identifies the SNMP community.
context	(Optional) Specifies that an SNMP context name is mapped to the SNMP community.
context-name	(Optional) String that identifies the name of the SNMP context.
engineid	(Optional) Specifies that an SNMP engine ID is mapped to the SNMP community.
engine-id	(Optional) String that identifies the SNMP engine ID. Default is the local engine ID
security-name	(Optional) Specifies that a security name is mapped to the SNMP community.
security-name	(Optional) String that identifies the SNMP security name. Default is the community name
target-list	(Optional) Specifies that a VPN routing and forwarding (VRF) list is mapped to the SNMP community.
vpn-list-name	(Optional) String value that should correspond to the list name used in the **snmp mib target list** command.

Command Default

No SNMP communities and contexts are associated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to create a mapping between an SNMP community and an SNMP context, engine ID, or security name that is different from the default settings.

Use the **snmp-server community** command to configure an SNMP community. When an SNMP community is associated with an SNMP context and a request is made from this community, the request is applied to the context. You also can use the **snmp mib community-map** command to specify the source address validation for an SNMP community by associating a list of target VRFs. The target VRF list specifies the valid host or hosts for this SNMP community.

Examples

The following example shows how to create an SNMP community named community1 and associate it with an SNMP context named context1:

```
Router(config)# snmp-server community community1
Router(config)# snmp mib community-map community1 context context1
```

The following example shows a mapping of community A (commA) to VPN list commAvpn and community B (commB) to VPN list commBvpn:

```
Router(config)# snmp mib community-map commA context A target-list commAvpn
Router(config)# snmp mib community-map commB context B target-list commBvpn
Router(config)# snmp mib target list commAvpn vrf CustomerA
Router(config)# snmp mib target list commBvpn vrf CustomerB
```

Related Commands

Command	Description
context	Associates an SNMP context with a particular VPN.
snmp-server community	Sets up the community access string to permit access to the SNMP.

snmp mib notification-log default

To create an unnamed Simple Network Management Protocol (SNMP) notification log, use the **snmp mib notification-log default** command in global configuration mode. To delete the log, use the **no** form of this command.

snmp mib notification-log default [**size** *number*]

no snmp mib notification-log default [**size** *number*]

Syntax Description

size	(Optional) Sets the maximum number of entries that the log can contain.
number	(Optional) Maximum number of entries. The default is 500.

Command Default

500 entries

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

This command creates an unnamed default SNMP notification log. The default log has a zero length string as its name (appears in the output of the **show snmp mib notification-log** command as `Log Name"")`.

Creation and removal of the default log can be performed using only the command-line interface (CLI). Creation of named logs using the CLI or SNMP tools (SET operations) is not currently supported. No filters (varbinds) can be associated with the default log.

SNMP notification logging is enabled by default, but logging does not start until either a specific log is created and defined using this command or a named log is created using a SNMP Set operation from a network management station (NMS).

The **no** form of this command deletes the default notification log and removes the notifications that were a part of this log from the Notification Log MIB database (recursively deletes the log and all its entries).

Examples

The following example shows how to create and activate a default SNMP notification log with a size of 600:

```
Router(config)# snmp mib notification-log default size 600
```

Related Commands

Command	Description
show snmp mib notification-log	Displays information about the state of local SNMP notification logging.
snmp mib notification-log globalageout	Sets the maximum age for a notification.
snmp mib notification-log globalsize	Sets the maximum number of notifications allowed in all logs.

snmp mib notification-log default disable

To disable Simple Network Management Protocol (SNMP) notification logging to the "default" log without deleting existing notification log entries, use the **snmp mib notification-log default disable** command in global configuration mode. To reenable logging, use the **no** form of this command.

snmp mib notification-log default disable

no snmp mib notification-log default disable

Syntax Description

This command has no arguments or keywords

Command Default

Logging is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The "default" notification log is the null-named notification log.

This command disables SNMP notification logging. However, this command does not delete existing logs. To clear the existing "default" log, use the **no snmp mib notification-log default** command.

SNMP notification logging is enabled by default, but logging does not start until a specific log is created and defined using the **snmp mib notification-log default** command, or a named log is created using an SNMP Set operation from a network management station (NMS).

Examples

In the following example, SNMP notification logging is disabled, but existing logs are not deleted:

```
Router(config)# snmp mib notification-log default ?
  disable  disable logging
  size     size of the default log
  <cr>
Router(config)# snmp mib notification-log default disable
Router(config)#
```

Related Commands

Command	Description
show snmp mib notification-log	Displays information about the state of local SNMP notification logging.
snmp mib notification-log default	Creates an SNMP notification log.

Command	Description
snmp mib notification-log globalageout	Sets the maximum age for a notification.
snmp mib notification-log globalsize	Sets the maximum number of notifications allowed in all logs.

snmp mib notification-log globalageout

To set the maximum amount of time Simple Network Management Protocol (SNMP) notification log entries remain in the system memory, use the **snmp mib notification-log globalageout** command in global configuration mode. To restore the default value, use the **no** form of this command.

snmp mib notification-log globalageout *minutes*

no snmp mib notification-log globalageout *minutes*

Syntax Description

minutes	Maximum age (in minutes) that a notification entry is retained in the system memory. The default is 15.

Command Default

The default global ageout value is 15 minutes.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The ageout value specifies the maximum time a notification log can remain in the Notification Log MIB database. This value applies to all logs (default log and named logs) in the Notification Log MIB database.

The **no** form of the command restores the default value.

Examples

In the following example, the system is configured to delete entries in the SNMP Notification Log that were logged more than 20 minutes ago:

```
Router(config)# snmp mib notification-log globalageout 20
```

Related Commands

Command	Description
show snmp mib notification-log	Provides a summary of logs.
snmp mib notification-log default	Creates the default log in the MIB.
snmp mib notification-log globalsize	Sets the maximum number of notifications allowed in all logs.

snmp mib notification-log globalsize

To set the maximum number of entries that can be stored in all Simple Network Management Protocol (SNMP) notification Logs, use the **snmp mib notification-log globalsize** command in global configuration mode. To restore the default value, use the **no** form of this command.

snmp mib notification-log globalsize *number*

no snmp mib notification-log globalsize *number*

Syntax Description

number	Maximum number of log entries. The range is from 1 to 15000. This value cannot be set to 0 (limitless). The default is 500.

Command Default

The default global log size is 500 entries.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The size of the SNMP notification log database can be set globally (for all SNMP notification logs combined) or for each named log. The **snmp mib notification-log globalsize** command sets the maximum number of entries for all notification logs on the local system; in other words, this setting affects the whole Notification Log MIB database. This value is saved to the nlmConfigGlobalEntryLimit object in the SNMP Notification Log MIB.

The default global log size is 500 log entries. The default log size for each individual log (such as the "default log") is 500 log entries. The maximum size for all logs combined is 15,000 log entries.

Examples

In the following example, the system is configured to delete older log entries when there are more than 600 log entries in all SNMP notification logs on the system:

```
Router(config)# snmp mib notification-log globalsize 600
```

Related Commands

Command	Description
show snmp mib notification-log	Provides a summary of logs.
snmp mib notification-log default	Creates the default log in the MIB.
snmp mib notification-log globalageout	Sets the maximum age for a notification.

snmp mib persist

To enable MIB persistence, use the **snmp mib persist** command in global configuration mode. To disable MIB persistence, use the **no** form of this command.

snmp mib persist [**event** | **expression** | **circuit** | **cbqos**]

no snmp mib persist [**event** | **expression** | **circuit** | **cbqos**]

Syntax Description

event	(Optional) Enables Event MIB persistence.
expression	(Optional) Enables Expression MIB persistence.
circuit	(Optional) Enables Circuit MIB persistence.
cbqos	(Optional) Enables class-based (CB) quality of service (QoS) MIB persistence.

Command Default

MIB persistence is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(4)T3	Support for event and expression MIBs was added.
12.4(4)T	The **cbqos** keyword was added.
12.0(32)S	This command was integrated into Cisco IOS Release 12.0(32)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

After entering the **snmp mib persist** command, you must enter the **write mib-data** command to save MIB persistence configuration data to NVRAM.

The Circuit Interface MIB provides a MIB object (cciDescr) that can be used to identify individual circuit-based interfaces for Simple Network Management Protocol (SNMP) monitoring. Circuit interface identification persistence maintains the user-defined name of the circuit across reboots by retaining the value of the cciDescr object in the Circuit Interface MIB (CISCO-CIRCUIT-INTERFACE-MIB). A consistent value for specific circuits is useful for network management applications that use SNMP. Circuit interface identification persistence is enabled using the **snmp mib persist circuit** global configuration command. This command is disabled by default because it uses NVRAM memory.

To enable MIB persistence for all available MIB types, use the **snmp mib persist** command without keywords.

Examples

The following example shows how to enable Event MIB persistence:

```
Router(config)# snmp mib persist event
Router(config)# end
Router# write mib-data
```

Related Commands

Command	Description
snmp ifindex persist	Enables SNMP interface index values that remain constant across reboots only on a specific interface.
snmp-server ifindex persist	Globally enables SNMP interface index values that remain constant across reboots.
write mib-data	Saves MIB persistence configuration data to NVRAM.

snmp mib target list

To create a list of target virtual private network (VPN) routing and forwarding (VRF) instance and hosts to associate with a Simple Network Management Protocol (SNMP) community, use the **snmp mib target list** command in global configuration mode. To delete the list of VRF instances and hosts or to delete a particular VRF or host from the list, use the **no** form of this command.

snmp mib target list *vpn-list-name* {**vrf** *vrf-name* | **host** *ip-address*}

no snmp mib target list *vpn-list-name* {**vrf** *vrf-name* | **host** *ip-address*}

Syntax Description

vpn-list-name	Name of the target list.
vrf	Adds a specified VRF to the target list.
vrf-name	Name of a VRF to include in the list.
host	Adds a specified host to the target list.
ip-address	IP address of the host.

Command Default

No target list is created.

Command Modes

Global configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31) SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use this command when using SNMPv1 or SNMPv2 in a VPN environment to configure a list of VRFs or hosts for source address validation. Configuring the target list ensures that the community is valid only if the incoming packet is received from a VRF or host on the target list.

- Only the following MIBs are context aware and all the tables in these MIBs can be polled:
  - CISCO-IPSEC-FLOW-MONITOR-MIB (Cisco IOS Release 12.4T and later)
  - CISCO-IPSEC-MIB (Cisco IOS Release 12.4T and later)
  - CISCO-PING-MIB
  - IP-FORWARD-MIB
  - MPLS-LDP-MIB

- Currently, two SNMP variables in the IP-FORWARD-MIB can be polled: 1.3.6.1.2.1.4.24.3 (ipCidrRouteNumber - Scalar) and 1.3.6.1.2.1.4.24.4.1 (ipCidrRouteEntry - Table).

Note It is recommended that you use SNMPv3 with the authNoPriv or higher level of security when using SNMP in a VPN environment.

Examples

The following example shows how to add a target list named target1 and add a VRF named vrf1 to the newly created target list:

```
Router(config)# snmp mib target list target1 vrf vrf1
```

Related Commands

Command	Description
snmp mib community-map	Associates an SNMP community with an SNMP context, engine ID, or security name.

snmp trap link-status

To enable Simple Network Management Protocol (SNMP) link trap generation, use the **snmp trap link-status** command in interface configuration mode. To disable SNMP link traps, use the **no** form of this command.

snmp trap link-status [**permit duplicates**]

no snmp trap link-status [**permit duplicates**]

Syntax Description.

permit duplicates	(Optional) Permits duplicate SNMP linkup and linkdown traps.

Command Default

SNMP link traps are sent when an interface goes up or down.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(30)S	The **permit duplicates** keyword pair was added in Cisco IOS Release 12.2(30)S.
12.3(8)T	Support for the **permit duplicates** keyword pair was integrated in Cisco IOS Release 12.3(8)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

By default, SNMP link traps are sent when an interface goes up or down. For interfaces expected to go up and down during normal usage, such as ISDN interfaces, the output generated by these traps may not be useful. The **no** form of this command disables these traps.

The **permit** and **duplicates** keywords are used together and cannot be used individually. Use the **permit duplicates** keyword pair when an interface is not generating SNMP linkup traps, linkdown traps, or both. When the **snmp trap link-status permit duplicates** command is configured, more than one trap may be sent for the same linkup or linkdown transition.

The **permit duplicates** keyword pair does not guarantee that SNMP link traps will be generated nor should configuring these keywords be required to receive traps.

Examples

The following example shows how to disable the sending of SNMP link traps related to the ISDN BRI 0 interface:

```
Router(config)# interface bri 0
Router(config-if)# no snmp trap link-status
```

snmp-server cache

To enable the Simple Network Management Protocol (SNMP) cache and configure the SNMP cache expiry interval, use the **snmp-server cache** command in global configuration mode. To disable the cache for MIBs that are kept by the SNMP engine, use the **no** form of this command.

snmp-server cache [**interval** *seconds*]

no snmp-server cache

Syntax Description

interval *seconds*	(Optional) Specifies the SNMP cache interval; valid values are from 1 to 300 seconds.

Command Default

The defaults are as follows:

- Disabled
- If enabled, the interval is 10 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

This command is for distributed or modular environments. The SNMP engine cache maintains the cache for MIBs.

Examples

This example shows how to enable the SNMP cache and configure the SNMP cache expiry interval:

```
Router(config)# snmp-server cache interval 200
```

This example shows how to disable the SNMP cache:

```
Router(config)# no snmp-server cache
```

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 *text*

no snmp-server chassis-id

Syntax Description

text	Message that identifies the chassis serial number.

Command Default

On hardware platforms where the serial number can be machine read, the default is the serial number. For example, a Cisco 7000 router has a default chassis-id value of its serial number.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Cisco MIB provides a chassis MIB variable that enables the SNMP manager to gather data on system card descriptions, chassis type, chassis hardware version, chassis ID string, software version of ROM monitor, software version of system image in ROM, bytes of processor RAM installed, bytes of NVRAM installed, bytes of NVRAM in use, current configuration register setting, and the value of the configuration register at the next reload. The following installed card information is provided: type of card, serial number, hardware version, software version, and chassis slot number.

The chassis ID message can be seen with the **show snmp** command.

Examples

In the following example, the chassis serial number specified is 1234456:

```
Router(config)# snmp-server chassis-id 1234456
```

Related Commands

Command	Description
show snmp	Checks the status of SNMP communications.

snmp-server community

To set up 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 *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number*]

no snmp-server community *string*

Syntax Description

string	Community string that consists of 1 to 32 alphanumeric characters and functions much like a password, permitting access to SNMP. Blank spaces are not permitted in the community string. **Note** The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.
view	(Optional) Specifies a previously defined view. The view defines the objects available to the SNMP community.
view-name	(Optional) Name of a previously defined view.
ro	(Optional) Specifies read-only access. Authorized management stations can retrieve only MIB objects.
rw	(Optional) Specifies read-write access. Authorized management stations can both retrieve and modify MIB objects.
ipv6	(Optional) Specifies an IPv6 named access list.
nacl	(Optional) IPv6 named access list.
access-list-number	(Optional) Integer from 1 to 99 that specifies a standard access list of IP addresses or a string (not to exceed 64 characters) that is the name of a standard access list of IP addresses allowed access to the SNMP agent. Alternatively, an integer from 1300 to 1999 that specifies a list of IP addresses in the expanded range of standard access list numbers that are allowed to use the community string to gain access to the SNMP agent.

Command Default

An SNMP community string permits read-only access to all objects.

Note If the **snmp-server community** command is not used during the SNMP configuration session, the command will automatically be added to the configuration after the **snmp host** command is used. In this case, the default password (*string*) for the **snmp-server community** command will be taken from the **snmp host** command.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.0(17)S	This command was integrated into Cisco IOS Release 12.0(17)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The access list values were enhanced to support the expanded range of standard access list values and to support named standard access lists.
12.0(27)S	The **ipv6** *nacl* keyword and argument pair was added to support assignment of IPv6 named access lists. This keyword and argument pair is not supported in Cisco IOS 12.2S releases.
12.3(14)T	The **ipv6** *nacl* keyword and argument pair was integrated into Cisco IOS Release 12.3(14)T to support assignment of IPv6 named access lists. This keyword and argument pair is not supported in Cisco IOS 12.2S releases.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **no snmp-server** command disables all versions of SNMP (SNMPv1, SNMPv2C, SNMPv3).

The first **snmp-server** command that you enter enables all versions of SNMP.

To configure SNMP community strings for the MPLS LDP MIB, use the **snmp-server community** command on the host network management station (NMS).

The **snmp-server community** command can be used to specify only an IPv6 named access list, only an IPv4 access list, or both. For you to configure both IPv4 and IPv6 access lists, the IPv6 access list must appear first in the command statement.

Note The @ symbol is used as a delimiter between the community string and the context in which it is used. For example, specific VLAN information in BRIDGE-MIB may be polled using community@VLAN_ID (for example, public@100) where 100 is the VLAN number. Avoid using the @ symbol as part of the SNMP community string when configuring this command.

Examples

The following example shows how to set the read/write community string to newstring:

```
Router(config)# snmp-server community newstring rw
```

The following example shows how to allow read-only access for all objects to members of the standard named access list lmnop that specify the comaccess community string. No other SNMP managers have access to any objects.

```
Router(config)# snmp-server community comaccess ro lmnop
```

The following example shows how to assign the string comaccess to SNMP, allow read-only access, and specify that IP access list 4 can use the community string:

```
Router(config)# snmp-server community comaccess ro 4
```

The following example shows how to assign the string manager to SNMP and allow read-write access to the objects in the restricted view:

```
Router(config)# snmp-server community manager view restricted rw
```

The following example shows how to remove the community comaccess:

```
Router(config)# no snmp-server community comaccess
```

The following example shows how to disable all versions of SNMP:

```
Router(config)# no snmp-server
```

The following example shows how to configure an IPv6 access list named list1 and links an SNMP community string with this access list:

```
Router(config)# ipv6 access-list list1
Router(config-ipv6-acl)# permit ipv6 any any
Router(config-ipv6-acl)# exit
Router(config)# snmp-server community comaccess rw ipv6 list1
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
snmp-server enable traps	Enables the router to send SNMP notification messages to a designated network management workstation.
snmp-server host	Specifies the targeted recipient of an SNMP notification operation.
snmp-server view	Creates or updates a view entry.

snmp-server contact

To set the system contact (sysContact) string, 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 *text*

no snmp-server contact

Syntax Description

text	String that describes the system contact information.

Command Default

No system contact string is set.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is an example of a system contact string:

```
Router(config)# snmp-server contact Dial System Operator at beeper # 27345
```

Related Commands

Command	Description
snmp-server location	Sets the system location string.

snmp-server context

To create a Simple Network Management Protocol (SNMP) context, use the **snmp-server context** command in global configuration mode. To delete 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 being created.

Command Default

No SNMP contexts are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

When you use the **no snmp-server context** command, all SNMP instances in that context are deleted.

A route distinguisher (RD) is required when you configure an SNMP context. An RD creates routing and forwarding tables and specifies the default route distinguisher for a VPN. The RD is added to the beginning of a IPv4 prefix to make it globally unique. An RD is either ASN relative, which means it is composed of an autonomous system number and an arbitrary number, or it is IP address relative and composed of an IP address and an arbitrary number.

Examples

The following example shows how to create an SNMP context named contextA and associate it with a virtual private network (VPN) routing and forwarding (VRF) instance named CustomerA:

```
Router(config)# snmp-server context contextA
Router(config)# ip vrf CustomerA
Router(config-vrf)# rd 100:120
Router(config-vrf)# context contextA
```

Related Commands

Command	Description
context	Associates an SNMP context with a particular VRF.

snmp-server enable informs

This command has no functionality. To enable the sending of Simple Network Management Protocol (SNMP) inform notifications, use one of the **snmp-server enable traps** *notification-type* commands in global configuration mode combined with the **snmp-server host** *host-address* **informs** commands in global configuration mode.

snmp-server enable traps

To enable all Simple Network Management Protocol (SNMP) notification types that are available on your system, use the **snmp-server enable traps** command in global configuration mode. To disable all available SNMP notifications, use the **no** form of this command.

snmp-server enable traps [*notification-type*] [**vrrp**]

no snmp-server enable traps [*notification-type*] [**vrrp**]

Syntax Description

notification-type	(Optional) Type of notification (trap or inform) to enable or disable. If no type is specified, all notifications available on your device are enabled or disabled (if the **no** form is used). The notification type can be one of the following keywords: **alarms**—Enables alarm filtering to limit the number of syslog messages generated. Alarms are generated for the severity configured as well as for the higher severity values. • The *severity* argument is an integer or string value that identifies the severity of an alarm. Integer values are from 1 to 4. String values are critical, major, minor, and informational. The default is 4, or informational. Severity levels are defined as follows: – 1—Critical. The condition affects service. – 2—Major. Immediate action is needed. – 3—Minor. Minor warning conditions. – 4—Informational. No action is required. This is the default. • **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. • **dot1x**—Enables IEEE 802.1x traps. This notification type is defined in the CISCO PAE MIB. • **ds0-busyout**—Sends notification when the busyout of a DS0 interface changes state (Cisco AS5300 platform only). This notification is defined in the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2), and the notification type is (1) cpmDS0BusyoutNotification. • **ds1-loopback**—Sends notification when the DS1 interface goes into loopback mode (Cisco AS5300 platform only). This notification type is defined in the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2) as (2) cpmDS1LoopbackNotification. • **dsp**—Enables SNMP digital signal processing (DSP) traps. This notification type is defined in the CISCO-DSP-MGMT-MIB. • **dsp oper-state**—Sends a DSP notification made up of both a DSP ID that indicates which DSP is affected and an operational state that indicates whether the DSP has failed or recovered. • **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.

	• **hsrp**—Controls Hot Standby Routing Protocol (HSRP) notifications, as defined in the CISCO-HSRP-MIB (enterprise 1.3.6.1.4.1.9.9.106.2). The notification type is (1) cHsrpStateChange. • **ipmulticast**—Controls IP multicast notifications. • **modem-health**—Controls modem-health notifications. • **rsvp**—Controls Resource Reservation Protocol (RSVP) flow change notifications. • **tty**—Controls TCP connection notifications. • **xgcp**—Sends External Media Gateway Control Protocol (XGCP) notifications. This notification is from the XGCP-MIB-V1SMI.my, and the notification is enterprise 1.3.6.1.3.90.2 (1) xgcpUpDownNotification. **Note** For additional notification types, see the Related Commands table.
vrrp	(Optional) Specifies the Virtual Router Redundancy Protocol (VRRP).

Command Default

No notifications controlled by this command are sent.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
12.0(2)T	The **rsvp** notification type was added in Cisco IOS Release 12.0(2)T.
12.0(3)T	The **hsrp** notification type was added in Cisco IOS Release 12.0(3)T.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(14)SX	Support for this command was implemented on the Supervisor Engine 720.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was integrated into Cisco IOS Release 12.2(17d)SXB.
12.3(11)T	The **vrrp** notification type was added in Cisco IOS Release 12.3(11)T.
12.4(4)T	Support for the **alarms** notification type and *severity* argument was added in Cisco IOS Release 12.4(4)T. Support for the **dsp** and **dsp oper-state** notification types was added in Cisco IOS Release 12.4(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **dot1x** notification type was added in Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

For additional notification types, see the Related Commands table for this command.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. To specify whether the notifications should be sent as traps or informs, use the **snmp-server host** [**traps** | **informs**] command.

To configure the router to send these SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled. To enable multiple types of notifications, you must issue a separate **snmp-server enable traps** command for each notification type and notification option.

Most notification types are disabled by default but some cannot be controlled with the **snmp-server enable traps** command.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send notifications, you must configure at least one **snmp-server host** command.

Examples

The following 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:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

The following example shows how to configure an alarm severity threshold of 3:

```
Router# snmp-server enable traps alarms 3
```

The following example shows how to enable the generation of a DSP operational state notification from from the command-line interface (CLI):

```
Router(config)# snmp-server enable traps dsp oper-state
```

The following example shows how to enable the generation of a DSP operational state notification from a network management device:

```
setany -v2c 1.4.198.75 test cdspEnableOperStateNotification.0 -i 1
cdspEnableOperStateNotification.0=true(1)
```

The following example shows how to send no traps to any host. The Border Gateway Protocol (BGP) traps are enabled for all hosts, but the only traps enabled to be sent to a host are ISDN traps (which are not enabled in this example).

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host user1 public isdn
```

The following example shows how to enable the router to send all inform requests to the host at the address myhost.cisco.com, using the community string defined as public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example shows how to send HSRP MIB traps to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps hsrp
Router(config)# snmp-server host myhost.cisco.com traps version 2c public hsrp
```

The following example shows that VRRP will be used as the protocol to enable the traps:

```
Router(config)# snmp-server enable traps vrrp
Router(config)# snmp-server host myhost.cisco.com traps version 2c vrrp
```

The following example shows how to send IEEE 802.1x MIB traps to the host “myhost.example.com” using the community string defined as public:

```
Router(config)# snmp-server enable traps dot1x
Router(config)# snmp-server host myhost.example.com traps public
```

Related Commands

Command	Description
snmp-server enable traps atm pvc	Enables ATM PVC SNMP notifications.
snmp-server enable traps atm pvc extension	Enables extended ATM PVC SNMP notifications.
snmp-server enable traps bgp	Enables BGP server state change SNMP notifications.
snmp-server enable traps calltracker	Enables Call Tracker callSetup and callTerminate SNMP notifications.
snmp-server enable traps envmon	Enables environmental monitor SNMP notifications.
snmp-server enable traps frame-relay	Enables Frame Relay DLCI link status change SNMP notifications.
snmp-server enable traps ipsec	Enables IPsec SNMP notifications.
snmp-server enable traps isakmp	Enables IPsec ISAKMP SNMP notifications.
snmp-server enable traps isdn	Enables ISDN SNMP notifications.
snmp-server enable traps memory	Enables memory pool and buffer pool SNMP notifications.
snmp-server enable traps mpls ldp	Enables MPLS LDP SNMP notifications.
snmp-server enable traps mpls traffic-eng	Enables MPLS TE tunnel state-change SNMP notifications.
snmp-server enable traps mpls vpn	Enables MPLS VPN specific SNMP notifications.
snmp-server enable traps repeater	Enables RFC 1516 hub notifications.
snmp-server enable traps snmp	Enables RFC 1157 SNMP notifications.
snmp-server enable traps syslog	Enables the sending of system logging messages via SNMP.
snmp-server host	Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the destination host (recipient) for the notifications.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) from which an SNMP trap should originate.
snmp trap illegal-address	Issues an SNMP trap when a MAC address violation is detected on an Ethernet hub port of a Cisco 2505, Cisco 2507, or Cisco 2516 router.
vrrp shutdown	Disables a VRRP group.

snmp-server enable traps (MPLS)

To enable a label switch router (LSR) to send Simple Network Management Protocol (SNMP) notifications or informs to an SNMP host, use the **snmp-server enable traps** command in global configuration mode. To disable notifications or informs, use the **no** form of this command.

snmp-server enable traps [*notification-type*] [*notification-option*]

no snmp-server enable traps [*notification-type*] [*notification-option*]

Syntax Description

notification-type	(Optional) Specifies the particular type of SNMP notification(s) to be enabled on the LSR. If a notification type is not specified, all SNMP notifications applicable to the LSR are enabled and sent to the SNMP host. Any one or all of the following keywords can be specified in any combination as the *notification-type* (family name) in the **snmp-server enable traps** command: • **bgp**—Sends Border Gateway Protocol (BGP) state change notifications. • **config**—Sends configuration notifications. • **entity**—Sends entity MIB modification notifications. • **envmon**—Sends Cisco enterprise-specific environmental monitor notifications whenever certain environmental thresholds are exceeded. *Notification-option* arguments (below) can be specified in combination with this keyword. • **frame-relay**—Sends Frame Relay notifications. • **hsrp**—Sends Hot Standby Routing Protocol (HSRP) notifications. • **isdn**—Sends ISDN notifications. *Notification-option* arguments (see examples below) can be specified in combination with this keyword. • **repeater**—Sends Ethernet repeater (hub) notifications. *Notification-option* arguments (see examples below) can be specified in combination with this keyword. • **rsvp**—Sends Resource Reservation Protocol (RSVP) notifications. • **rtr**—Sends Service Assurance Agent/Response Time Reporter (RTR) notifications. • **snmp** [**authentication**]—Sends RFC 1157 SNMP notifications. Using the **authentication** keyword produces the same effect as not using it. Both the **snmp-server enable traps snmp** and the **snmp-server enable traps snmp authentication** forms of this command globally enable the following SNMP notifications (or, if you are using the **no** form of the command, disables such notifications): **authenticationFailure**, **linkUp**, **linkDown**, and **warmstart**. • **syslog**—Sends system error message (syslog) notifications. You can specify the level of messages to be sent using the **logging history level** command.

notification-type (continued)

- **mpls ldp**—Sends notifications about status changes in LDP sessions. Note that this keyword is specified as ***mpls ldp***. This syntax, which the CLI interprets as a two-word construct, has been implemented in this manner to maintain consistency with other MPLS commands. *Notification-option* arguments (below) can be specified in combination with this keyword.
- **mpls traffic-eng**—Sends notifications about status changes in MPLS label distribution tunnels. This keyword is specified as ***mpls traffic-eng***. This syntax, which the CLI interprets as a two-word construct, has been implemented in this manner to maintain consistency with other MPLS commands. *Notification-option* arguments (below) can be specified in combination with this keyword.

notification-option

(Optional) Defines the particular options associated with the specified *notification-type* that are to be enabled on the LSR.

- **envmon** [**voltage** | **shutdown** | **supply** | **fan** | **temperature**]

  When you specify the **envmon** keyword, you can enable any one or all of the following environmental notifications in any combination: **voltage**, **shutdown**, **supply**, **fan**, or **temperature**. If you do not specify an argument with the **envmon** keyword, all types of system environmental notifications are enabled on the LSR.

- **isdn** [**call-information** | **isdn u-interface**]

  When you specify the **isdn** keyword, you can use either the **call-information** argument (to enable an SNMP ISDN call information option for the ISDN MIB subsystem) or the **isdn u-interface** argument (to enable an SNMP ISDN U interface option for the ISDN U Interfaces MIB subsystem), or both. If you do not specify an argument with the **isdn** keyword, both types of isdn notifications are enabled on the LSR.

- **repeater** [**health** | **reset**]

  When you specify the **repeater** keyword, you can use either the **health** argument or the **reset** argument, or both (to enable the IETF Repeater Hub MIB [RFC 1516] notification). If you do not specify an argument with the **repeater** keyword, both types of notifications are enabled on the LSR.

- **mpls ldp** [**session-up** | **session-down** | **pv-limit** | **threshold**]

  When you specify the **mpls ldp** keyword, you can use any one or all of the following arguments in any combination to indicate status changes in LDP sessions: **session-up**, **session-down**, **pv-limit**, or **threshold**. If you do not specify an argument with the **mpls ldp** keyword, all four types of LDP session notifications are enabled on the LSR.

- **mpls traffic-eng** [**up** | **down** | **reroute**]

  When you specify the **mpls traffic-eng** keyword, you can use any one or all of the following arguments in any combination to enable the sending of notifications regarding status changes in MPLS label distribution tunnels: **up**, **down**, or **reroute**. If you do not specify an argument with the **mpls traffic-eng** keyword, all three types of tunnel notifications are enabled on the LSR.

Defaults

If you issue this command on an LSR without specifying any *notification-type* keywords, the default behavior of the LSR is to enable all notification types controlled by the command (some notification types cannot be controlled by means of this command).

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
11.3	The **snmp-server enable traps snmp authentication** form of this command was introduced to replace the **snmp-server trap-authentication** command.
12.0(17)ST	The **mpls traffic-eng** keyword was added to define a class or family of specific SNMP notifications for use with the *notification-type* and *notification-option* parameters of the **snmp-server enable traps** command.
12.0(21)ST	The **mpls ldp** keyword was added to define a class or family of specific SNMP notifications for use with the *notification-type* and *notification-option* parameters of the **snmp-server enable traps** command.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

To configure an LSR to send SNMP LDP notifications, you must issue at least one **snmp-server enable traps** command on the router.

To configure an LSR to send either notifications (traps) or informs to a designated network management station (NMS), you must issue the **snmp-server host** command on that device, using the keyword (**traps** or **informs**) that suits your purposes.

If you issue the **snmp-server enable traps** command without keywords, all SNMP notification types are enabled on the LSR. If you issue this command with specific keywords, only the notification types associated with those particular keywords are enabled on the LSR.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. You use the latter command to specify the NMS host (or hosts) targeted as the recipient(s) of the SNMP notifications generated by SNMP-enabled LSRs in the network. To enable an LSR to send such notifications, you must issue at least one **snmp-server host** command on the LSR.

Examples

In the following example, the router is enabled to send all notifications to the host specified as myhost.cisco.com. The community string is defined as public.

```
Router(config)# snmp-server enable traps

Router(config)# snmp-server host myhost.cisco.com public
```

In the following example, the router is enabled to send Frame Relay and environmental monitor notifications to the host specified as myhost.cisco.com. The community string is defined as public:

```
Router(config)# snmp-server enable traps frame-relay

Router(config)# snmp-server enable traps envmon temperature

Router(config)# snmp-server host myhost.cisco.com public
```

In the following example, notifications are not sent to any host. BGP notifications are enabled for all hosts, but the only notifications enabled to be sent to a host are ISDN notifications (which are not enabled in this example).

```
Router(config)# snmp-server enable traps bgp

Router(config)# snmp-server host host1 public isdn
```

In the following example, the router is enabled to send all inform requests to the host specified as myhost.cisco.com. The community string is defined as public.

```
Router(config)# snmp-server enable traps

Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

In the following example, HSRP MIB notifications are sent to the host specified as myhost.cisco.com. The community string is defined as public.

```
Router(config)# snmp-server enable hsrp

Router(config)# snmp-server host myhost.cisco.com traps version 2c public hsrp
```

Related Commands

Command	Description
snmp-server host	Specifies the intended recipient of an SNMP notification (that is, the designated NMS workstation in the network).

snmp-server enable traps aaa_server

To enable authentication, authorization, and accounting (AAA) server state-change Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps aaa_server** command in global configuration mode. To disable AAA server state-change SNMP notifications, use the **no** form of this command.

snmp-server enable traps aaa_server

no snmp-server enable traps aaa_server

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced for the Cisco AS5300 and Cisco AS5800.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) AAA Server state change (casServerStateChange) notifications. ServerStateChange notifications, when enabled, will be sent when the server moves from an “up” to “dead” state or when a server moves from a “dead” to “up” state.

The Cisco AAA Server State is defined by the casState object in the Cisco AAA Server MIB. The possible values are as follows:

- up(1)—Server is responding to requests.
- dead(2)—Server failed to respond to requests.

A server is marked "dead" if it does not respond after maximum retransmissions. A server is marked "up" again either after a waiting period or if some response is received from it. The initial value of casState is "up(1)" at system startup. This will only transition to "dead(2)" if an attempt to communicate fails.

For a complete description of this notification and additional MIB functions, see the CISCO-AAA-SERVER-MIB.my file, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

The **snmp-server enable traps aaa_sever** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables the router to send AAA server up/down informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps aaa_server
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
aaa session-mib disconnect	Allows a remote network management system to perform Set operations and disconnect users on the configured device using SNMP.
show caller	Displays caller information for async, dialer, and serial interfaces.
show radius statistics	Displays AAA server MIB statistics for AAA functions.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps atm pvc

To enable the sending of ATM permanent virtual circuit (PVC) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps atm pvc** command in global configuration mode. To disable ATM PVC-specific SNMP notifications, use the **no** form of this command.

snmp-server enable traps atm pvc [**interval** *seconds*] [**fail-interval** *seconds*]

no snmp-server enable traps atm pvc [**interval** *seconds*] [**fail-interval** *seconds*]

Syntax Description

interval *seconds*	(Optional) Specifies a minimum period between successive traps. Generation of PVC traps is dampened by the notification interval to prevent trap storms. No traps are sent until the interval lapses. The *seconds* argument is an integer in the range from 1 to 3600. The default is 30.
fail-interval *seconds*	(Optional) Specifies a minimum period for storing the failed time stamp. The *seconds* argument is an integer in the range from 0 to 3600. The default is 0.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced for the platforms that support ATM PVC Management.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. ATM notifications are defined in the CISCO-IETF-ATM2-PVCTRAP-MIB.my file, available from the Cisco FTP site at ftp://ftp.cisco.com/pub/mibs/v2/.

ATM PVC failure notifications are sent when a PVC on an ATM interface fails or leaves the UP operational state. Only one trap is generated per hardware interface, within the specified interval defined by the **interval** keyword (stored as the atmIntfPvcNotificationInterval in the MIB). If other PVCs on the same interface go DOWN during this interval, traps are generated and held until the fail interval has elapsed. When the interval has elapsed, the traps are sent if the PVCs are still DOWN.

No notifications are generated when a PVC returns to the UP state after having been in the DOWN state. If you need to detect the recovery of PVCs, you must use the SNMP management application to regularly poll your router.

The **snmp-server enable traps atm pvc** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows the enabling of ATM PVC traps on a router, so that if PVC 0/1 goes down, host 172.16.61.90 will receive the notifications:

```
!For ATM PVC Trap Support to work on your router, you must first have SNMP support and
!an IP routing protocol configured on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 172.16.61.90 public
Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.16.0.0
!
!Enable ATM PVC Trap Support and OAM management:
Router(config)# snmp-server enable traps atm pvc interval 40 fail-interval 10
Router(config)# interface atm 1/0.1
Router(config-if)# pvc 0/1
Router(config-if-atm-vc)# oam-pvc manage
```

Related Commands

Command	Description
show atm pvc	Displays all ATM PVCs and traffic information.
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps atm pvc extension

To enable the sending of extended ATM permanent virtual circuit (PVC) SNMP notifications and SNMP notifications for ATM Operation, Administration, and Maintenance (OAM) F5 continuity check (CC), ATM OAM F5 alarm indication signals/remote defect indications (AIS/RDI), and loopback failures, use the **snmp-server enable traps atm pvc extension** command in global configuration mode. To disable these SNMP notifications, use the **no** form of this command.

snmp-server enable traps atm pvc extension {**up** | **down** | **oam failure** [**aisrdi** | **endCC** | **loopback** | **segmentCC**]}

no snmp-server enable traps atm pvc extension {up | **down** | **oam failure** [**aisrdi** | **endCC** | **loopback** | **segmentCC**]}

Syntax Description

up	Enables ATM PVC up traps. These notifications are generated when a PVC changes from the DOWN to the UP state.
down	Enables ATM PVC failure traps. These notifications are generated when a PVC changes from the UP to the DOWN state.
oam failure	Enables ATM PVC OAM failure traps. These notifications are generated when any type of OAM failure occurs on the PVC.
aisrdi	(Optional) Enables AIS/RDI OAM failure traps. These notifications are generated when AIS/RDI OAM failure occurs on the PVC.
endCC	(Optional) Enables end-to-end OAM CC failure traps. These notifications are generated when end-to-end CC failures occur on the PVC.
loopback	(Optional) Enables OAM failure loopback traps. These notifications are generated when OAM loopback failure occurs on the PVC.
segmentCC	(Optional) Enables segment OAM CC failure traps. These notifications are generated when segment CC failures occur on the PVC.

Command Default

SNMP notifications are disabled.
The interval between successive traps is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced for those platforms that support ATM PVC management.
12.2(13)T	This command was modified to configure SNMP notification support for ATM OAM F5 CC and ATM OAM F5 AIS/RDI failures.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

For PVCs that are not part of a range, extended ATM PVC traps include virtual path identifier/virtual channel identifier (VPI/ VCI) information, the number of state transitions a PVC goes through in an interval, and the timestamp for the start and end of the transitions. For PVCs that are part of a range, extended ATM PVC traps include the first and last VPI/VCI of the range and the timestamp for the first failure and the last failure within the same range.

Extended ATM PVC and ATM OAM F5 CC traps cannot be used at the same time as the legacy ATM PVC trap. The legacy ATM PVC trap must be disabled by using the **no snmp-server enable traps atm pvc** command before extended ATM PVC traps can be configured.

The extended ATM PVC failure trap (which is enabled by the **snmp-server enable traps atm pvc extension down** command) is the same trap as the legacy ATM PVC failure trap (which is enabled by the **snmp-server enable traps atm pvc** command), but with the following differences:

- The extended ATM PVC failure trap contains information in the form of VPI/VCI ranges.
- The extended ATM PVC failure trap contains timestamps for when PVCs go down.
- The legacy ATM PVC failure trap contains only one VPI/VCI per trap.

Note You must configure the **snmp-server enable traps atm pvc extension mibversion 2** command before you can enable the ATM OAM F5 AIS/RDI failure traps, the end-to-end ATM OAM F5 CC failure traps, the OAM failure loopback traps, and the segment ATM OAM F5 CC failure traps. This command enables the MIB that supports these traps.

OAM management must be enabled on the PVC before you can use ATM PVC traps. To generate F5 loopback failure traps, enable OAM management using the **oam-pvc manage** command. To generate segment F5 CC failure traps, enable segment OAM CC management by using the **oam-pvc manage cc segment** command. To generate end-to-end F5 CC failure traps, enable end-to-end OAM CC management by using the **oam-pvc manage cc end** command. To generate OAM F5 AIS/RDI failure traps, enable any of the three types of OAM management listed above.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types.

The extended ATM PVC notifications for MIB version 1 are defined in the CISCO-IETF-ATM2-PVCTRAP-MIB.my file.The extended ATM PVC notifications for MIB version 2 are defined in the CISCO-ATM-PVCTRAP-EXTN-MIB.my file. Both of these MIB files are available from the Cisco FTP site at ftp://ftp.cisco.com/pub/mibs/v2/.

ATM PVC traps are generated at the end of the notification interval. It is possible to generate all three types of ATM PVC traps (the ATM PVC failure trap, ATM PVC up trap, and ATM PVC OAM failure trap) at the end of the same notification interval; however, only one type of trap will be generated for each PVC.

The **snmp-server enable traps atm pvc extension** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

When the ATM OAM F5 loopback, AIS/RDI, or CC failure trap is enabled, the PVC remains in the UP state when an OAM loopback, AIS/RDI, or CC failure is detected, so that the flow of data will still be possible. If one of these traps is not enabled, the PVC will be placed in the DOWN state when an OAM loopback, AIS/RDI, or CC failure is detected.

Examples

Extended ATM PVC Notifications Example

The following example shows all three of the extended ATM PVC traps enabled on a router. If PVC 0/1 leaves the UP state, leaves the DOWN state, or has an OAM loopback failure, host 172.16.61.90 will receive the SNMP notifications:

```
! Configure SNMP support and an IP routing protocol on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 172.16.61.90 public
Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.16.0.0
!
! Enable extended ATM PVC trap support and OAM management:
Router(config)# snmp-server enable traps atm pvc extension down
Router(config)# snmp-server enable traps atm pvc extension up
Router(config)# snmp-server enable traps atm pvc extension oam failure loopback
Router(config)# interface atm 1/0.1
Router(config-if)# pvc 0/1
Router(config-if-atm-vc)# oam-pvc manage
```

Extended ATM PVC Failure Trap Output: Example

The following example shows output for extended ATM PVC failure trap for PVCs 1/100, 1/102, and 1/103. Note that only one trap is generated for all the PVCs associated with the same interface or subinterface (in contrast to the legacy ATM PVC failure trap, which generates a separate trap for each PVC). The VPI/VCI information and timing information are located in the objects associated with the trap.

```
00:23:56:SNMP:Queuing packet to 1.1.1.1
00:23:56:SNMP:V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 143636
snmpTrapOID.0 = atmIntfPvcFailuresTrap
ifEntry.1.19 = 19
atmIntfPvcFailures.2 = 7
atmIntfCurrentlyFailingPVcls.2 = 3
atmPVclLowerRangeValue.19.1.2 = 102
atmPVclHigherRangeValue.19.1.2 = 103
atmPVclRangeStatusChangeStart.19.1.2 = 140643
atmPVclRangeStatusChangeEnd.19.1.2 = 140698
atmPVclStatusTransition.19.1.100 = 1
atmPVclStatusChangeStart.19.1.100 = 140636
atmPVclStatusChangeEnd.19.1.100 = 140636
00:23:56:SNMP:Packet sent via UDP to 1.1.1.1
```

Extended ATM PVC Up Trap Output: Example

The following example shows output for the extended ATM PVC up trap for PVCs 1/100, 1/102, and 1/103:

```
00:31:29:SNMP:Queuing packet to 1.1.1.1
00:31:29:SNMP:V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 188990
snmpTrapOID.0 = atmIntfPvcUpTrap
ifEntry.1.19 = 19
atmIntfCurrentlyDownToUpPVcls.2 = 3
atmPVclLowerRangeValue.19.1.2 = 102
atmPVclHigherRangeValue.19.1.2 = 103
atmPVclRangeStatusChangeStart.19.1.2 = 186005
atmPVclRangeStatusChangeEnd.19.1.2 = 186053
atmPVclStatusTransition.19.1.100 = 1
atmPVclStatusChangeStart.19.1.100 = 185990
atmPVclStatusChangeEnd.19.1.100 = 185990
00:31:30:SNMP:Packet sent via UDP to 1.1.1.1
```

ATM OAM F5 CC Notifications Example

In the following example, the ATM OAM CC notifications and an extended ATM PVC notification are enabled. If connectivity failures are detected on PVC 0/1, host 172.16.61.90 will receive the SNMP notifications:

```
! Configure SNMP support and an IP routing protocol on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 172.16.61.90 public
Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.16.0.0
!
! Enable extended ATM PVC trap support and OAM management:
Router(config)# snmp-server enable traps atm pvc extension mibversion 2
Router(config)# snmp-server enable traps atm pvc extension oam failure aisrdi
Router(config)# snmp-server enable traps atm pvc extension oam failure endcc
Router(config)# snmp-server enable traps atm pvc extension oam failure segmentcc
Router(config)# snmp-server enable traps atm pvc extension oam failure loopback
Router(config)# snmp-server enable traps atm pvc extension up
Router(config)# interface atm 0
Router(config-if)# pvc 0/1
Router(config-if-atm-vc)# oam-pvc manage cc end
```

Related Commands

Command	Description
oam-pvc manage	Enables end-to-end F5 OAM loopback cell generation and OAM management.
oam-pvc manage cc	Configures ATM OAM F5 CC management.
show atm pvc	Displays all ATM PVCs and traffic information.
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server enable traps atm pvc	Enables the sending of legacy ATM PVC failure traps.
snmp-server enable traps atm pvc extension mibversion	Specifies the MIB that supports extended ATM PVC SNMP notifications or the MIB that supports SNMP notifications for ATM OAM F5 CC, F5 AIS/RDI, and F5 loopback failures.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps atm pvc extension mibversion

To specify the MIB that supports extended ATM permanent virtual circuit (PVC) Simple Network Management Protocol (SNMP) notifications or the MIB that supports SNMP notifications for ATM Operation, Administration, and Maintenance (OAM) F5 continuity check (CC) management, ATM OAM F5 AIS/RDI management, and F5 loopback failure management, use the **snmp-server enable traps atm pvc extension mibversion** command in global configuration mode. To remove the MIB specification, use the **no** form of this command.

snmp-server enable traps atm pvc extension mibversion {**1** | **2**}

no snmp-server enable traps atm pvc extension mibversion {**1** | **2**}

Syntax Description

1	Specifies the MIB that supports the extended ATM permanent virtual circuit (PVC) SNMP notifications. This is the default.
2	Specifies the MIB that supports ATM OAM F5 CC and ATM OAM F5 AIS/RDI SNMP notifications, in addition to the notifications supported by MIB version 1.

Command Default

The default is MIB version **1.**

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

MIB version 1 specifies the MIB that supports legacy extended ATM PVC traps and is defined in the file CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN.my. MIB version 1 is implemented by default. Use the **snmp-server enable traps atm pvc extension mibversion 1** command or the **no snmp-server enable traps atm pvc extension mibversion 2** command to reenable this MIB if it was previously disabled with the **snmp-server enable traps atm pvc extension mibversion 2** command.

Use the **snmp-server enable traps atm pvc extension mibversion 2** command to specify the MIB that supports ATM OAM F5 CC and ATM OAM AID/RDI failure notifications. This MIB is defined in the file CISCO-ATM-PVCTRAP-EXTN-MIB.my.

To enable the SNMP notifications that support ATM OAM F5 continuity checking, use the **snmp-server enable traps atm pvc extension** command in global configuration mode. These SNMP notifications are defined in the file CISCO-ATM-PVCTRAP-EXTN-MIB.my, available from the Cisco FTP site at ftp://ftp.cisco.com/pub/mibs/v2/.

OAM management and support for OAM F5 continuity checking must be enabled on the PVC by using the **oam-pvc manage cc** command before you can use the ATM OAM continuity check SNMP notifications.

Examples

In the following example, the MIB that supports the SNMP notifications for ATM OAM continuity checking is implemented, and the ATM OAM continuity checking notifications are enabled. Support for end-to-end OAM F5 continuity checking is enabled on PVC 0/1:

```
Router(config)# snmp-server enable traps atm pvc extension mibversion 2
Router(config)# snmp-server enable traps atm pvc extension oam failure aisrdi
Router(config)# snmp-server enable traps atm pvc extension oam failure endcc
Router(config)# snmp-server enable traps atm pvc extension oam failure segmentcc
Router(config)# snmp-server enable traps atm pvc extension oam failure loopback
Router(config)# snmp-server enable traps atm pvc extension up
Router(config)# interface atm 0
Router(config-if)# pvc 0/40
Router(config-if-atm-vc)# oam-pvc manage cc end
```

Related Commands

Command	Description
debug atm oam cc	Displays ATM OAM F5 CC management activity.
oam-pvc manage cc	Configures ATM OAM F5 CC management.
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server enable traps atm pvc	Enables the sending of legacy ATM PVC DOWN traps.
snmp-server enable traps atm pvc extension	Enables the sending of extended ATM PVC SNMP notifications and SNMP notifications for ATM OAM F5 CC, ATM OAM F5 AIS/RDI, and loopback failures.

snmp-server enable traps atm subif

To enable the sending of ATM subinterface Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps atm subif** command in global configuration mode. To disable ATM subinterface-specific SNMP notifications, use the **no** form of this command.

snmp-server enable traps atm subif [**interval** *seconds* [**count** *number-of-traps*]] | [**count** *number-of-traps*]

no snmp-server enable traps atm subif [**interval** *seconds* [**count** *number-of-traps*]] | [**count** *number-of-traps*]

Syntax Description

interval	(Optional) Specifies the minimum period between successive traps.
seconds	(Optional) Integer in the range from 0 to 3600. The default is 10.
count	(Optional) Specifies the maximum number of traps that will be sent in the specified interval.
number-of-traps	(Optional) Integer in the range from 1 to 1000. The default is 10.

Command Default

ATM subinterface SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **snmp-server trap link ietf** command must be configured in order to use the **snmp-server enable traps atm subif** command. The **snmp-server trap link ietf** command is used to configure a router to use the RFC 2233 IETF standards-based implementation of linkUp/linkDown traps. The default Cisco object definitions do not generate linkUp/linkDown traps correctly for subinterfaces.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types.

ATM subinterface traps are sent to the network management system (NMS) when a subinterface enters or leaves the down state.

To prevent trap storms, the **count** and **interval** keywords can be configured to limit the number of traps and the frequency at which they are sent. Configuring an interval of 0 seconds causes all ATM subinterface traps to be sent.

You can disable ATM subinterface traps by using the **no snmp-server enable traps atm subif** command. When traps are disabled, you can use the SNMP management application to poll your router for subinterface status information.

The **snmp-server enable traps atm subif** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send notifications, you must configure at least one **snmp-server host** command.

By default (when the **snmp-server enable traps atm subif** command is not configured), the ifLinkUpDownTrapEnable object returns disabled(2), and no traps are generated for the subinterfaces.

When the **snmp-server enable traps atm subif** command is configured, the ifLinkUpDownTrapEnable object is set to enabled(1) for all the ATM aal5 layers of the subinterfaces. To verify that the traps are generated (with the **debug snmp packets** command enabled), enter the **shutdown** or **no shutdown** commands to display the traps.

Configuring the **snmp trap link-status** command on a subinterface generates the traps and sets the ifLinkUpDownTrapEnable object to enabled(1). If the **snmp trap link-status** command is not configured on the subinterface, then the ifLinkUpDownTrapEnable object is set to disabled(2) for that subinterface, and the **shutdown** or **no shutdown** commands no longer generate traps for that subinterface.

Examples

The following example shows how to enable ATM subinterface traps on a router. If an ATM subinterface on this router changes state, host 172.16.61.90 will receive the notifications:

```
!For ATM subinterface trap to work on your router, you must first have SNMP support and
!an IP routing protocol configured on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 172.16.61.90 public
Router(config)# snmp-server trap link ietf
Router(config)# snmp-server enable traps snmp
Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.16.0.0

!Enable ATM subinterface trap support:
Router(config)# snmp-server enable traps atm subif interval 60 count 5
```

Related Commands

Command	Description
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server enable traps atm pvc	Enables the sending of ATM PVC SNMP notifications.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap link ietf	Enables linkUp/linkDown SNMP traps that are compliant with RFC 2233.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps bgp

To enable Border Gateway Protocol (BGP) support for Simple Network Management Protocol (SNMP) operations on a router, use the **snmp-server enable traps bgp** command in global configuration mode. To disable BGP support for SNMP operations, use the **no** form of this command.

snmp-server enable traps bgp [**state-changes** [**all**] [**backward-trans**] [**limited**] | **threshold prefix**]

no snmp-server enable traps bgp [**state-changes** [**all**] [**backward-trans**] [**limited**] | **threshold prefix**]

Syntax Description

state-changes	(Optional) Enables traps for finite state machine (FSM) state changes.
all	(Optional) Enables Cisco specific traps for all FSM state changes
backward-trans	(Optional) Enables Cisco specific traps for backward transition events.
limited	(Optional) Enables traps for standard backward transition and established events.
threshold prefix	(Optional) Enables Cisco-specific trap for prefix threshold events.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced for the Cisco AS5300 and Cisco AS5800.
12.0(26)S	The following keywords were added in Cisco IOS Release 12.0(26)S: **state-changes**, **all**, **backward-trans**, **limited**, and **threshold prefix**.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was implemented on the Cisco 7304.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was implemented on the following platforms: Cisco 7301, Cisco 7200 series, and Cisco 10000 series.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests and this command enables both notification types. If this command is entered with no keywords specified, support for all configurable options is enabled.

Using this command you can enable or disable BGP server state change notifications for the BGP4-MIB (enterprise 1.3.6.1.2.1.15.7). The notifications types are:

- *bgpEstablished*
- *bgpBackwardsTransition*

For a complete description of BGP notifications and additional MIB functions, see the BGP4-MIB.my file, available through the Cisco FTP site at ftp://ftp.cisco.com/pub/mibs/v2/.

Note You may notice incorrect BGP trap object ID (OID) output when using the SNMP version 1 BGP4-MIB that is available for download at ftp://ftp.cisco.com/pub/mibs/v1/BGP4-MIB-V1SMI.my. When a router sends out BGP traps (notifications) about state changes on an SNMP version 1 monitored BGP peer, the enterprise OID is incorrectly displayed as .1.3.6.1.2.1.15 (bgp) instead of .1.3.6.1.2.1.15.7 (bgpTraps). This problem occurs because the BGP4-MIB does not follow RFC 1908 rules for version 1 and version 2 trap compliance. The problem is not due to an error in Cisco IOS software.This MIB is controlled by IANA under the guidance of the IETF, and work is currently in progress by the IETF to replace this MIB with a new version that represents the current state of the BGP protocol. In the meantime, we recommend that you use the SNMP version 2 BGP4-MIB or the CISCO-BGP4-MIB to avoid an incorrect trap OID.

The **snmp-server enable traps bgp** command also can be enabled to control BGP server state change notifications for the CISCO-BGP4-MIB. This MIB contains support the following SNMP operations:

- Notification for all BGP FSM transition changes.
- Notifications to query for total number of routes received by a BGP peer.
- Notifications for the maximum prefix-limit threshold on a BGP peer.
- GET operations for VPNv4 unicast routes.

For a complete description of BGP notifications and additional MIB functions, see the CISCO-BGP4-MIB.my file, available through the Cisco FTP site at ftp://ftp.cisco.com/pub/mibs/v2/.

The **snmp-server enable traps bgp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to enable the router to send BGP state change informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps bulkstat

To enable the sending of Simple Network Management Protocol (SNMP) bulk statistics collection and transfer SNMP notifications, use the **snmp-server enable traps bulkstat** command in global configuration mode. To disable bulk statistics SNMP notifications, use the **no** form of this command.

snmp-server enable traps bulkstat [**collection** | **transfer**]

no snmp-server enable traps bulkstat [**collection** | **transfer**]

Syntax Description

collection	(Optional) Controls bulk statistics collection notifications, which are sent when data collection cannot be carried out successfully. (Defined as cdcVFileCollectionError in the CISCO-DATA-COLLECTION-MIB.)
transfer	(Optional) Controls bulk statistics transfer notifications, which are sent when a transfer attempt is successful or when a transfer attempt fails. (Defined as cdcFileXferComplete in the CISCO-DATA-COLLECTION-MIB. The varbind cdcFilXferStatus object in the trap indicates if the transfer is successful or not.)

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps bulkstat** command enables both traps and inform requests for the specified notification types. Use this command with the **snmp-server host** [**bulkstat**] command.

The optional **collection** keyword controls bulk statistics collection notifications that are sent when data collection cannot be carried out successfully. One possible reason for this condition is insufficient memory on the device.

If the optional keywords are not used, all bulk statistics notification types are enabled (or disabled, if the **no** form of the command is used).

Examples

In the following example, bulk statistics collection and transfer notifications are configured to be sent to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps bulkstat
Router(config)# snmp-server host myhost.cisco.com traps version 2c public bulkstat
```

Related Commands

Command	Description
snmp mib bulkstat transfer	Names a bulk statistics transfer configuration and enters Bulk Statistics Transfer configuration mode.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps calltracker

To enable Call Tracker CallSetup and Call Terminate Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps calltracker** command in global configuration mode. To disable Call Tracker SNMP notifications, use the **no** form of this command.

snmp-server enable traps calltracker

no snmp-server enable traps calltracker

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced for the Cisco AS5300 and Cisco AS580 access servers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) Call Tracker CallSetup and CallTerminate notifications. CallSetup notifications are generated at the start of each call, when an entry is created in the active table (cctActiveTable), and CallTerminate notifications are generated at the end of each call, when an entry is created in the history table (cctHistoryTable).

For a complete description of these notifications and additional MIB functions, refer to the CISCO-CALL-TRACKER-MIB.my file, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

The **snmp-server enable traps calltracker** command is used in conjunction with the **snmp-server host** global configuration command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables the router to send call-start and call-stop informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps calltracker
Router(config)# snmp-server host myhost.cisco.com informs version 2c public calltracker
```

Related Commands

Command	Description
calltracker call-record	Enables call record SYSLOG generation for the purpose of debugging, monitoring, or externally saving detailed call record information.
calltracker enable	Enables the Call Tracker feature on an access server.
isdn snmp busyout b-channel	Enables PRI B channels to be busied out via SNMP.
show call calltracker	Displays Call Tracker activity and configuration information such as the number of active calls and the history table attributes.
show modem calltracker	Displays all of the information stored within the Call Tracker Active or History Database for the latest call assigned to specified modem.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps cpu

To enable a device to send CPU thresholding violation notifications, use the **snmp-server enable traps cpu** command in global configuration mode. To stop a device from sending CPU thresholding notifications, use the **no** form of this command.

snmp-server enable traps cpu threshold

no snmp-server enable traps cpu

Syntax Description

threshold	Enables notifications of CPU threshold violations.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests and controls CPU thresholding notifications, as defined in the Process MIB (CISCO-PROCESS-MIB).

This command enables the following notifications:

- cpmCPURisingThreshold—Indicates that CPU usage has risen and remains above the configured CPU threshold settings.
- cpmCPUFallingThreshold—Indicates that CPU usage has fallen and remains below the configured CPU threshold settings.

For a complete description of these notification types, and for information about the other MIB functions, see the CISCO-PROCESS-MIB.my file available from Cisco.com at http://www.cisco.com/go/mibs.

The **snmp-server enable traps cpu** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to enable the router to send CPU threshold related informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps cpu threshold
Router(config)# snmp-server host myhost.cisco.com informs version 2c public cpu
```

Related Commands

Command	Description
snmp-server host	Specifies the destination NMS and transfer parameters for SNMP notifications.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps dhcp

To enable DHCP Simple Network Management Protocol (SNMP) trap notifications, use the **snmp-server enable traps dhcp** command in global configuration mode. To disable DHCP trap notifications, use the **no** form of this command.

snmp-server enable traps dhcp [**duplicate**] [**interface**] [**pool**] [**subnet**] [**time**]

no snmp-server enable traps dhcp [**duplicate**] [**interface**] [**pool**] [**subnet**] [**time**]

Syntax Description

duplicate	(Optional) Sends notification about duplicate IP addresses.
interface	(Optional) Sends notification that a per interface lease limit is exceeded.
pool	(Optional) Sends notification when address utilization for an address pool has risen above or fallen below a configurable threshold.
subnet	(Optional) Sends notification when address utilization for a subnet has risen above or fallen below a configurable threshold.
time	(Optional) Sends notification that the DHCP server has started or stopped.

Command Default

DHCP trap notifications are not sent.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

If you do not specify any of the optional keywords, all DHCP trap notifications are enabled.

Examples

The following example shows how to send SNMP trap notifications to the SNMP manager when the secondary subnet utilization falls below or exceeds the configured threshold:

```
Router(config)# ip dhcp pool pool2
Router(dhcp-config)# utilization mark high 80 log
Router(dhcp-config)# utilization mark low 70 log
Router(dhcp-config)# network 192.0.2.0 255.255.255.0
Router(dhcp-config)# network 192.0.4.0 255.255.255.252 secondary
Router(config-dhcp-subnet-secondary)# override utilization high 40
Router(config-dhcp-subnet-secondary)# override utilization low 30
!
Router(config)# snmp-server enable traps dhcp subnet
```

In the following example, all DHCP trap notifications will be sent to the SNMP manager in response to DHCP server events:

```
Router(config)# snmp-server enable traps dhcp
```

snmp-server enable traps director

To enable DistributedDirector Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps director** command in global configuration mode. To disable DistributedDirector SNMP notifications, use the **no** form of this command.

snmp-server enable traps director [**server-up** | **server-down**]

no snmp-server enable traps director [**server-up** | **server-down**]

Syntax Description

server-up	(Optional) Enables the DistributedDirector notification that the server has changed to the "up" state.
server-down	(Optional) Enables the DistributedDirector notification that the server has changed to the "down" state.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) DistributedDirector status notifications for systems. If none of the optional keywords is specified, all available environmental notifications are enabled.

Examples

In the following example, both ciscoDistDirEventServerUp and ciscoDistDirEventServerDown notifications are enabled:

```
Router(config)# snmp-server enable traps director

Router# show running-config

ip host myhost 172.20.2.10 172.20.2.20 172.20.2.30
.
.
.
ip director host myhost
ip dns primary myhost soa myhost myhost@com
ip director host myhost priority boomerang 1
no ip director drp synchronized
snmp-server enable traps director server-up server-down
```

Related Commands

Command	Description
snmp-server enable traps	Enables the router to send SNMP traps.
snmp-server host	Specifies the recipient of an SNMP notification.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) from which an SNMP trap should originate.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.
snmp trap link-status	Enables SNMP trap notifications to be generated when a specific port is brought up or down.

snmp-server enable traps dlsw

To enable the sending of Data Link Switch (DLSw) circuit and peer connection Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp-server enable traps dlsw** command in global configuration mode. To disable DLSw notifications, use the **no** form of this command.

snmp-server enable traps dlsw [**circuit** | **tconn**]

no snmp-server enable traps dlsw [**circuit** | **tconn**]

Syntax Description

circuit	(Optional) Enables DLSw circuit traps: • (5) ciscoDlswTrapCircuitUp • (6) ciscoDlswTrapCircuitDown
tconn	(Optional) Enables DLSw peer transport connection traps: • (1) ciscoDlswTrapTConnPartnerReject • (2) ciscoDlswTrapTConnProtViolation • (3) ciscoDlswTrapTConnUp • (4) ciscoDlswTrapTConnDown

Command Default

SNMP notifications are disabled.

If the optional keywords are not used, all DLSw notification types are enabled (or disabled, if the **no** form of the command is used).

Command Modes

Global configuration

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests. Use this command in conjunction with the **snmp-server host** command.

This command controls (enables or disables) SNMP notifications for Data Link Switch (DLSw) circuit and connection activity. DLSw objects are defined in the Cisco DLSw MIB module (CISCO-DLSW-MIB.my) and the DLSw+ (Cisco Specific Features) MIB module (CISCO-DLSW-EXT-MIB.my), available through Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Examples

In the following example the device is configured to send DLSw circuit state change informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps dlsw circuit
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps eigrp

To enable support for Enhanced Interior Gateway Routing Protocol (EIGRP) notifications on a Cisco router, use the **snmp-server enable traps eigrp** command in global configuration mode. To disable EIGRP notification support, use the **no** form of this command.

snmp-server enable traps eigrp

no snmp-server enable traps eigrp

Syntax Description

This command has no keywords or arguments.

Command Default

EIGRP notification support is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

The **snmp-server enable traps eigrp** command is used to enable notifications (traps) for stuck-in-active (SIA) and neighbor authentication failure events. Support for trap events is not activated until a trap destination is configured with the **snmp-server host** command and until a community string is defined with the **snmp-server community** command.

Examples

In the following example, an SNMP server host is specified, a community string is configured, and support for EIGRP notifications is enabled:

```
Router(config)# snmp-server host 10.0.0.1 traps version 2c NETMANAGER eigrp
Router(config)# snmp-server community EIGRP1NET1A
Router(config)# snmp-server enable traps eigrp
```

Related Commands

Command	Description
snmp-server community	Configures a community access string to permit SNMP access to the local router by the remote SNMP software client.
snmp-server host	Specifies the destination host or address for SNMP notifications.

snmp-server enable traps envmon

To enable environmental monitor Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps envmon** command in global configuration mode. To disable environmental monitor SNMP notifications, use the **no** form of this command.

snmp-server enable traps envmon [**shutdown**] [**voltage**] [**temperature**] [**fan**] [**supply**]

no snmp-server enable traps envmon [**shutdown**] [**voltage**] [**temperature**] [**fan**] [**supply**]

Syntax Description

shutdown	(Optional) Controls shutdown notifications.
voltage	(Optional) Controls voltage notifications.
temperature	(Optional) Controls temperature notifications.
fan	(Optional) Controls fan failure notifications.
supply	(Optional) Controls Redundant Power Supply (RPS) failure notifications.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
11.3(6)AA	Support for this command was introduced for the Cisco AS5300 access server.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command enables or disables Environmental Monitor (EnvMon) status notifications for supported systems. Cisco enterprise EnvMon notifications are triggered when an environmental threshold is exceeded. If none of the optional keywords are specified, all available environmental notifications are enabled.

When the **shutdown** keyword is used, a ciscoEnvMonShutdownNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.1) is sent if the environmental monitor detects a testpoint reaching a critical state and is about to initiate a shutdown.

When the **voltage** keyword is used, a ciscoEnvMonVoltageNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.2) is sent if the voltage measured at a given testpoint is outside the normal range for the testpoint (that is, at the warning, critical, or shutdown stage). For access servers, this notification is defined as the caemVoltageNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.61.2.2).

When the **temperature** keyword is used, a ciscoEnvMonTemperatureNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.3) is sent if the temperature measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the warning, critical, or shutdown stage). For access servers, this notification is defined as the caemTemperatureNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.61.2.1).

When the **fan** keyword is used, a ciscoEnvMonFanNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.4) is sent if any one of the fans in a fan array fails.

When the **supply** keyword is used, a ciscoEnvMonRedundantSupplyNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.2.5) is sent if a redundant power supply fails.

For a complete description of these notifications and additional MIB functions, see the CISCO-ENVMON-MIB.my and CISCO-ACCESS-ENVMON-MIB.my files, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

Status of the Environmental Monitor can be viewed using the **show environment** command.

The **snmp-server enable traps envmon** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to enable a Cisco 12000 GSR to send environmental failure informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps envmon
Router(config)# snmp-server host myhost.cisco.com informs version 2c public envmon
```

Related Commands

Command	Description
show environment	Displays environmental conditions on the system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps firewall

To enable the router to send firewall Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps firewall** command in global configuration mode. To disable firewall SNMP notifications, use the **no** form of this command.

snmp-server enable traps firewall serverstatus

no snmp-server enable traps firewall serverstatus

Syntax Description

serverstatus	Displays the status of configured servers.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

SNMP notifications are sent as traps by the agent. Currently, only one URL filtering trap is generated.

For a complete description of the notification types and additional MIB functions, refer to the CISCO-UNIFIED-FIREWALL-MIB.my and CISCO-FIREWALL-TC.my files, available on Cisco.com through:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

The **snmp-server enable traps firewall** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

In the following example, the router is configured to send firewall MIB inform notifications to the host nms.cisco.com using the community string named “public”:

```
snmp-server enable traps firewall serverstatus
snmp-server host nms.cisco.com informs public firewall
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.

snmp-server enable traps flash

To enable Flash device insertion and removal Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps flash** command in global configuration mode. To disable Flash device SNMP notifications, use the **no** form of this command.

snmp-server enable traps flash [**insertion**] [**removal**]

no snmp-server enable traps flash [**insertion**] [**removal**]

Syntax Description

insertion	(Optional) Controls Flash card insertion notifications.
removal	(Optional) Controls Flash card removal notifications.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.0(23)S	This command was integrated in Cisco IOS Release 12.0 S.
12.1(13)E4	This command was implemented on the Cisco Catalyst 6000 Series.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command enables or disables Flash card insertion and removal notifications, as defined by the ciscoFlashDeviceInsertedNotif and ciscoFlashDeviceRemovedNotif objects in the Cisco Flash MIB.

When the **insertion** keyword is used, a ciscoFlashDeviceInsertedNotif (OID 1.3.6.1.4.1.9.9.10.1.3.0.5) is sent whenever a removable Flash device is inserted.

When the **removal** keyword is used, a ciscoFlashDeviceRemovedNotif (OID 1.3.6.1.4.1.9.9.10.1.3.0.6) notification is sent whenever a removable Flash device is removed.

For a complete description of these notifications and additional MIB functions, see the CISCO-FLASH-MIB.my file, available on Cisco.com at http://www.cisco.com/go/mibs.

The **snmp-server enable traps flash** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to enable the router to send Flash card insertion and removal informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps flash insertion removal
Router(config)# snmp-server host myhost.cisco.com informs version 2c public flash
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps frame-relay

To enable Frame Relay Data Link Connection Identifier (DLCI) and subinterface Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps frame-relay** command in global configuration mode. To disable Frame Relay DLCI and subinterface SNMP notifications, use the **no** form of this command.

snmp-server enable traps frame-relay

no snmp-server enable traps frame-relay

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(13)T	This command was modified to enable Frame Relay subinterface traps in addition to DLCI traps.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) DLCI Frame Relay notifications, as defined in the RFC1315-MIB (enterprise 1.3.6.1.2.1.10.32).

This trap indicates that the indicated virtual circuit (VC) or subinterface has changed state, meaning that the VC or subinterface has either been created or invalidated, or has toggled between the active and inactive states.

To enable only Frame Relay subinterface traps, use the **snmp-server enable traps frame-relay subif** command.

Note For large scale configurations (systems containing hundreds of Frame Relay point-to-point subinterfaces), note that having Frame Relay notifications enabled could potentially have a negative impact on network performance when there are line status changes.

For a complete description of this notification and additional MIB functions, see the RFC1315-MIB.my file and the CISCO-FRAME-RELAY-MIB.my file, available in the “v1” and “v2” directories, respectively, at the Cisco.com MIB web site at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

The **snmp-server enable traps frame-relay** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

In the following example, the router is configured to send Frame Relay DLCI and subinterface state change informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps frame-relay
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps frame-relay multilink bundle-mismatch

To enable multilink Frame Relay Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps frame-relay multilink bundle-mismatch** command in global configuration mode. To disable these notifications, use the **no** form of this command.

snmp-server enable traps frame-relay multilink bundle-mismatch

no snmp-server enable traps frame-relay multilink bundle-mismatch

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the multilink Frame Relay MIB to manage devices that are configured with multilink Frame Relay.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

Although the bundle-mismatch trap is one of five traps defined in RFC 3020, Cisco IOS supports only the bundle-mismatch trap.

For a complete description of MIB functions, see the CISCO-FRAME-RELAY-MIB.my file, which is available in the "SNMP v2 MIBs" directory found at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Examples

In the following example, multilink Frame Relay is configured on the host router with one bundle, and the peer router is configured with zero bundle links.

On the host router:

```
Router(config)# interface MFR1
Router(config)# ip address 209.165.200.225 255.255.255.224
Router(config)# frame-relay multilink bid UUT_BUNDLE_ONE
Router(config)# frame-relay interface-dlci 100
!
Router(config)# snmp-server community public RW
Router(config)# snmp-server enable traps frame-relay multilink bundle-mismatch
Router(config)# snmp-server host 10.0.47.4 public
```

On the peer router:

```
Router(config)# interface MFR1
Router(config)# ip address 209.165.200.226 255.255.255.224
Router(config)# frame-relay multilink bid PEER_BUNDLE_ONE
Router(config)# frame-relay interface-dlci 100
Router(config)# frame-relay intf-type dce

Router(config)# snmp-server enable traps frame-relay multilink bundle-mismatch
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps frame-relay subif

To enable Frame Relay subinterface Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps frame-relay subif** command in global configuration mode. To disable Frame Relay subinterface SNMP notifications, use the **no** form of this command.

snmp-server enable traps frame-relay subif [[**interval** *seconds*] **count** *number-of-traps*]

no snmp-server enable traps frame-relay subif [[**interval** *seconds*] **count** *number-of-traps*]

Syntax Description

interval	(Optional) Specifies a minimum period between successive traps,
seconds	(Optional) Integer in the range from 0 to 3600. The default is 10.
count	(Optional) Specifies a maximum number of traps that will be sent in the specified interval.
number-of-traps	(Optional) Integer in the range from 1 to 1000. The default is 10.

Command Default

Frame Relay subinterface SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

Frame Relay subinterface traps are sent to the network management system (NMS) when a subinterface enters or leaves the down state.

To prevent trap storms, the **count** and **interval** keywords can be configured to limit the number of traps and the frequency at which they are sent. Configuring an interval of 0 seconds causes all Frame Relay subinterface traps to be sent.

Note The **snmp-server enable traps frame-relay** command enables both Frame Relay data-link connection identifier (DLCI) and subinterface traps. The **snmp-server enable traps frame-relay subif** command enables only Frame Relay subinterface traps.

You can disable Frame Relay subinterface traps by using the **no snmp-server enable traps frame-relay subif** command. When traps are disabled, you can use the SNMP management application to poll your router for subinterface status information.

The **snmp-server enable traps frame-relay subif** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

The **snmp-server trap link ietf** command must be configured in order to use the **snmp-server enable traps frame-relay subif** command. The **snmp-server trap link ietf** command is used to configure your router to use the RFC 2233 IETF standards-based implementation of linkUp/linkDown traps. The default Cisco object definitions do not generate linkUp/linkDown traps correctly for subinterfaces.

Examples

The following example shows how to enable Frame Relay subinterface traps on a router. If a Frame Relay subinterface on this router changes state, host 172.16.61.90 will receive the notifications:

```
! For Frame Relay subinterface traps to work on your router, you must first have SNMP
! support and an IP routing protocol configured on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 172.16.61.90 public
Router(config)# snmp-server trap link ietf
Router(config)# snmp-server enable traps snmp
Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.16.0.0

!Enable Frame Relay subinterface trap support:
Router(config)# snmp-server enable traps frame-relay subif interval 60 count 5
```

Related Commands

Command	Description
snmp-server enable traps frame-relay	Enables Frame Relay DLCI link status SNMP notifications.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap link ietf	Enables linkUp/linkDown SNMP traps that are compliant with RFC 2233.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps ip local pool

To enable the sending of local IP pool Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps ip local pool** command in global configuration mode. To disable local IP pool notifications, use the **no** form of this command.

snmp-server enable traps ip local pool

no snmp-server enable traps ip local pool

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled; no notifications are sent.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following example shows how to enable the sending of local IP SNMP notifications:

```
Router(config)# snmp-server enable traps ip local pool
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.

snmp-server enable traps isdn

To enable the sending of Integrated Services Digital Network (ISDN) specific Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps isdn** command in global configuration mode. To disable ISDN-specific SNMP notifications, use the **no** form of this command.

snmp-server enable traps isdn [**call-information**] [**chan-not-avail**] [**isdnu-interface**] [**layer2**]

no snmp-server enable traps isdn [**call-information**] [**chan-not-avail**] [**isdnu-interface**] [**layer2**]

Syntax Description

call-information	(Optional) Controls SNMP ISDN call information notifications, as defined in the CISCO-ISDN-MIB (enterprise 1.3.6.1.4.1.9.9.26.2). Notification types are: • demandNbrCallInformation (1) This notification is sent to the manager whenever a successful call clears, or a failed call attempt is determined to have ultimately failed. In the event that call retry is active, then this is after all retry attempts have failed. However, only one such notification is sent in between successful call attempts; subsequent call attempts do not generate notifications of this type. • demandNbrCallDetails (2) This notification is sent to the manager whenever a call connects, or clears, or a failed call attempt is determined to have ultimately failed. In the event that call retry is active, then this is after all retry attempts have failed. However, only one such notification is sent in between successful call attempts; subsequent call attempts do not generate notifications of this type.
chan-not-avail	(Optional) Controls SNMP ISDN channel-not-available notifications. ISDN PRI channel-not-available traps are generated when a requested DS-0 channel is not available, or when there is no modem available to take the incoming call. These notifications are available only for ISDN PRI interfaces.
isdnu-interface	(Optional) Controls SNMP ISDN U interface notifications.
layer2	(Optional) Controls SNMP ISDN layer2 transition notifications.

Defaults

SNMP notifications are disabled by default.

If you enter this command with none of the optional keywords, all available notifications are enabled.

Command Modes

Global configuration

Command History

Release	Modification
10.3	The **snmp-server enable traps isdn** command was introduced.
11.3	The **call-information** and **isdnu-interface** keywords were added for the Cisco 1600 series router.

Release	Modification
12.0	Support for the **call-information** and **isdnu-interface** keywords was introduced for most voice platforms.
12.1(5)T	Support for the **isdn chan-not-available** option was added for the Cisco AS5300, Cisco AS5400, and Cisco AS5800 access servers only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. ISDN notifications are defined in the CISCO-ISDN-MIB.my and CISCO-ISDNU-IF-MIB.my files, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

Availability of notifications will depend on your platform. To see what notifications are available, use the **snmp-server enable traps isdn ?** command.

If you do not enter an **snmp-server enable traps isdn** command, no notifications controlled by this command are sent. In order to configure the router to send these SNMP notifications, you must enter at least one **snmp-server enable traps isdn** command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.

The **snmp-server enable traps snmp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows the checking of what notification types are available on a Cisco AS5300, and the enabling of channel-not-available and layer2 informs:

```
NAS(config)# snmp-server enable traps isdn ?
  call-information  Enable SNMP isdn call information traps
  chan-not-avail    Enable SNMP isdn channel not avail traps
  layer2            Enable SNMP isdn layer2 transition traps
  <cr>

NAS(config)# snmp-server enable traps isdn chan-not-avail layer2
NAS(config)# snmp-server host myhost.cisco.com informs version 2c public isdn
```

Related Commands

Command	Description
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps l2tun pseudowire status

To enable the sending of Simple Network Management Protocol (SNMP) notifications when a pseudowire changes state, use the **snmp-server enable traps l2tun pseudowire status** command in global configuration mode. To disable SNMP notifications of pseudowire state changes, use the **no** form of this command.

snmp-server enable traps l2tun pseudowire status

no snmp-server enable traps l2tun pseudowire status

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(31)S	This command was introduced.
12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) notification of pseudowire state changes. For a complete description of these notification types, and for information about the other MIB functions, see the VPDN MIB, available through the Cisco Technical Assistance Center (TAC) SNMP Object Navigator tool at http://www.cisco.com/go/mibs.

The **snmp-server enable traps l2tun pseudowire status** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Use the **snmp-server enable traps** command without any additional syntax to disable all SNMP notification types supported on your system.

Examples

The following example enables the router to send pseudowire state change informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps l2tun pseudowire status
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server enable traps	Enables all SNMP notifications (traps or informs) available on your system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
xconnect logging pseudowire status	Enables syslog reporting of pseudowire status events.

snmp-server enable traps l2tun session

To enable Simple Network Management Protocol (SNMP) notifications (traps or inform requests) for Layer 2 Tunnel Protocol Version 3 (L2TPv3) sessions, use the **snmp-server enable traps l2tun session** command in global configuration mode. To disable SNMP notifications, use the **no** form of this command.

snmp-server enable traps l2tun session

no snmp-server enable traps l2tun session

Syntax Description

This command has no arguments or keywords.

Command Default

No SNMP notifications for L2TPv3 sessions are sent.

Command Modes

Global configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

In this command **l2tun** indicates "layer 2 tunneling." Layer 2 tunneling session notifications are defined by the cvpdnNotifSession object { ciscoVpdnMgmtMIBNotifs 3 } in the Cisco VPDN Management MIB (CISCO-VPDN-MGMT-MIB.my). MIB files are available from Cisco.com at http://www.cisco.com/go/mibs.

SNMP notifications can be sent as traps or inform requests and this command enables both types of notifications for L2TP sessions. To specify whether the notifications should be sent as traps or informs, and to specify which host or hosts receive SNMP notifications, use the **snmp-server host** [**traps** | **informs**] command.

Use the **snmp-server enable traps** command without any additional syntax to disable all SNMP notification types supported on your system.

Examples

The following example shows how to enable a router to send L2TP session traps to the host specified by the name myhost.example.com, using the community string defined as public:

```
Router(config)# snmp-server enable traps l2tun session
Router(config)# snmp-server host myhost.example.com public l2tun-session
```

Related Commands

Command	Description
snmp-server enable traps	Enables all SNMP notifications available on your system.
snmp-server host	Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the recipient (host) of the notifications.

snmp-server enable traps memory

To enable a device to send Simple Network Management Protocol (SNMP) notifications when memory pool buffer usage reaches a new peak, use the **snmp-server enable traps memory** command in global configuration mode. To stop notifications from being generated, use the **no** form of this command.

snmp-server enable traps memory [**bufferpeak**]

no snmp-server enable traps memory [**bufferpeak**]

Syntax Description

bufferpeak	(Optional) Specifies memory buffer peak notifications.

Command Default

SNMP notifications in the MEMPOOL-MIB are not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command enables or disables memory buffer peak (cempMemBufferNotify) notifications.When they are enabled, these notifications are sent when the value of the maximum number of buffer objects changes.

In current releases of Cisco IOS software, this command has the same behavior whether you use or omit the **bufferpeak** keyword.

The cempMemBufferNotify notification type is defined as {cempMIBNotifications 1} in the CISCO-ENHANCED-MEMPOOL-MIB. For a complete description of this notification and additional MIB functions, see the CISCO-ENHANCED-MEMPOOL-MIB.my file, available on Cisco.com at http://www.cisco.com/go/mibs/.

Examples

In the following example all available memory related SNMP notifications are enabled and configured to be sent as informs to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps memory
Router(config)# snmp-server host myhost.cisco.com informs version 3 public memory
```

Related Commands

Command	Description
show buffers	Displays memory buffer pool related information.
show memory	Displays memory pool related information.
snmp-server host	Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the recipient (host) of the notifications.

snmp-server enable traps mpls ldp

To enable the sending of Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) SNMP notifications, use the **snmp-server enable traps mpls ldp** command in global configuration mode. To disable the sending of MPLS LDP notifications, use the **no** form of this command.

snmp-server enable traps mpls ldp [**session-down** | **session-up** | **pv-limit** | **threshold**]

no snmp-server enable traps mpls ldp [**session-down** | **session-up** | **pv-limit** | **threshold**]

Syntax Description

session-down	(Optional) Enables or disables LDP session down notifications (mplsLdpSessionDown).
session-up	(Optional) Enables or disables LDP session up notifications (mplsLdpSessionUp).
pv-limit	(Optional) Enables or disables path-vector (PV) Limit notifications (mplsLdpPathVectorLimitMismatch).
threshold	(Optional) Enables or disables PV Limit notifications (mplsLdpFailedInitSessionThresholdExceeded).

Command Default

The sending of SNMP notifications is disabled. If you do not specify an optional keyword, all four types of LDP notifications are enabled on the label switching router (LSR).

Command Modes

Global configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.0(30)S	This command was integrated into Cisco IOS Release 12.0(30)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The MPLS LDP **pv-limit** (mplsLdpPathVectorLimitMismatch) notification provides a warning message that can be sent to the network management station (NMS) when two routers engaged in LDP operations have a dissimilar path vector limits. We recommend that all LDP-enabled routers in the network be configured with the same path vector limits.

The value of the path vector limit can range from 0 to 255; a value of 0 indicates that loop detection is off; any value other than 0 up to 255 indicates that loop detection is on and, in addition, specifies the maximum number of hops through which an LDP message can pass before a loop condition in the network is sensed.

The MPLS LDP **threshold** (mplsLdpFailedInitSessionThresholdExceeded) notification object provides a warning message that can be sent to a NMS when a local Label Switching Router (LSP) and an adjacent Label Distribution Protocol (LDP) peer attempt to set up an LDP session between them, but fail to do so after a specified number of attempts. The default number of attempts is 8. This default value is implemented in Cisco IOS and cannot be changed using either the CLI or an SNMP agent.

In general, Cisco routers support the same features across multiple platforms. Therefore, the most likely incompatibility to occur between Cisco LSRs is a mismatch of their respective ATM VPI/VCI label ranges. For example, if you specify a range of valid labels for an LSR that does not overlap the range of its adjacent LDP peer, the routers will try eight times to create an LDP session between themselves before the mplsLdpFailedInitSessionThresholdExceeded notification is generated.

The LSRs whose label ranges do not overlap continue their attempt to create an LDP session between themselves after the eight retry threshold is exceeded. In such cases, the LDP threshold exceeded notification alerts the network administrator to the existence of a condition in the network that may warrant attention.

RFC 3036, *LDP Specification*, details the incompatibilities that can exist between Cisco routers and/or other vendor LSRs in an MPLS network. Among these incompatibilities, for example, are the following:

- Nonoverlapping ATM VPI/VCI ranges (as noted above) or nonoverlapping Frame-Relay DLCI ranges between LSRs attempting to set up an LDP session
- Unsupported label distribution method
- Dissimilar protocol data unit (PDU) sizes
- Dissimilar LDP feature support

The **snmp-server enable traps mpls ldp** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

If the **session-down** keyword is used, a session-down message is generated when an LDP session between the router and its adjacent LDP peer is terminated.

If the **session-up** keyword is used, a message is generated when the router establishes an LDP session with another LDP entity (an adjacent LDP peer in the network).

If the **pv-limit** keyword is used, a message is generated when the router establishes an LDP session with its adjacent peer LSR, but the two LSRs have dissimilar path vector limits.

If the **threshold** keyword is used, a message is generated after eight failed attempts to establish an LDP session between the router and an LDP peer. The failures can be caused by any type of incompatibility between the devices.

Examples

In the following example, LDP-specific informs are enabled and will be sent to the host myhost.cisco.com through use of community string defined as public:

```
Router(config)# snmp-server enable traps mpls ldp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public mpls-ldp
```

Related Commands

Command	Description
snmp-server host	Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the recipient (host) of the notifications.

snmp-server enable traps mpls traffic-eng

To enable Multiprotocol Label Switching (MPLS) traffic engineering tunnel state-change Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps mpls traffic-eng** command in global configuration mode. To disable MPLS traffic engineering tunnel state-change SNMP notifications, use the **no** form of this command.

snmp-server enable traps mpls traffic-eng [**up** | **down** | **reroute**]

no snmp-server enable traps mpls traffic-eng [**up** | **down** | **reroute**]

Syntax Description

up	(Optional) Enables only mplsTunnelUp notifications { mplsTeNotifyPrefix 1 }.
down	(Optional) Enables only mplsTunnelDown notifications { mplsTeNotifyPrefix 2 }.
reroute	(Optional) Enables or disables only mplsTunnelRerouted notifications { mplsTeNotifyPrefix 3 }.

Command Default

SNMP notifications are disabled.

When this command is used without keywords, all available trap types (up, down, reroute) are enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.0(17)ST	This command was integrated into Cisco IOS Release 12.0(17)ST.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command enables or disables MPLS traffic engineering tunnel notifications. MPLS Tunnel StateChange notifications, when enabled, will be sent when the connection moves from an “up” to “down” state, when a connection moves from a “down” to “up” state, or when a connection is rerouted.

If you do not specify a specific argument in conjunction with this command, all three types of MPLS traffic engineering tunnel notifications are sent.

When the **up** keyword is used, MplsTunnelUp notifications are sent to a network management system (NMS) when an MPLS traffic engineering tunnel is configured and the tunnel transitions from an operationally “down” state to an “up” state.

When the **down** keyword is used, MplsTunnelDown notifications are generated and sent to the NMS when an MPLS traffic engineering tunnel transitions from an operationally “up” state to a “down” state.

When the **reroute** keyword is used, MplsTunnelRerouted notifications are sent to the NMS under the following conditions:

- The signaling path of an existing MPLS traffic engineering tunnel fails and a new path option is signaled and placed into effect (that is, the tunnel is rerouted).
- The signaling path of an existing MPLS traffic engineering tunnel is fully operational, but a better path option can be signaled and placed into effect (that is, the tunnel can be reoptimized). This reoptimization can be triggered by: a) a timer, b) the issuance of an **mpls traffic-eng reoptimize** command, or c) a configuration change that requires the resignaling of a tunnel.

The **snmp-server enable traps mpls traffic-eng** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to enable the router to send MPLS notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps mpls traffic-eng
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps mpls vpn

To enable the router to send Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN)-specific Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp-server enable traps mpls vpn** command in global configuration mode. To disable MPLS VPN specific SNMP notifications, use the **no** form of this command.

snmp-server enable traps mpls vpn [**illegal-label**] [**max-thresh-cleared**] [**max-threshold**] [**mid-threshold**] [**vrf-down**] [**vrf-up**]

no snmp-server enable traps mpls vpn [**illegal-label**] [**max-thresh-cleared**] [**max-threshold**] [**mid-threshold**] [**vrf-down**] [**vrf-up**]

Syntax Description

illegal-label	(Optional) Enables a notification for any illegal labels received on a VPN routing/forwarding instance (VRF) interface.
max-thresh-cleared	(Optional) Enables a notification when the number of routes attempts to exceed the maximum limit and then drops below the maximum number of routes.
max-threshold	(Optional) Enables a notification that a route creation attempt was unsuccessful because the maximum route limit was reached.
mid-threshold	(Optional) Enables a warning that the number of routes created has exceeded the warning threshold.
vrf-down	(Optional) Enables a notification for the removal of a VRF from an interface or the transition of an interface to the down state.
vrf-up	(Optional) Enables a notification for the assignment of a VRF to an interface that is operational or for the transition of a VRF interface to the operationally up state.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.0(30)S	This command was updated with the **max-thresh-cleared** keyword.
12.2(28)SB2	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

If this command is used without any of the optional keywords, all MPLS VPN notification types are enabled.

The **illegal-label** keyword enables a notification for illegal labels received on a VRF interface. Labels are illegal if they are outside the legal range, do not have a Label Forwarding Information Base (LFIB) entry, or do not match table IDs for the label.

When the **max-thresh-cleared** keyword is used and you attempt to create a route on a VRF that already contains the maximum number of routes, the mplsNumVrfRouteMaxThreshExceeded notification is sent (if enabled). **When you remove routes from the VRF so that the number of routes falls below the set limit, the** cMplsNumVrfRouteMaxThreshCleared notification is sent. You can clear all routes from the VRF by using the **clear ip route vrf** command.

The **max-threshold** keyword enables a notification that a route creation attempt was unsuccessful because the maximum route limit was reached. Another notification is not sent until the number of routes falls below the maximum threshold and reaches the maximum threshold again. The max-threshold value is determined by the **maximum routes** command in VRF configuration mode.

The warning that the **mid-threshold** keyword enables is sent only at the time the warning threshold is exceeded.

For the **vrf-up** (mplsVrfIfUp) or **vrf-down** (mplsVrfIfDown) notifications to be issued from an ATM or Frame Relay subinterface, you must first configure the **snmp-server traps atm subif** command or the **snmp-server traps frame-relay subif** command on the subinterfaces, respectively.

The values for the **mid-threshold** and **max-threshold** keywords are set using the **maximum routes** *limit* {*warn-threshold* | **warning-only**} VRF command in configuration mode.

The **maximum routes** command gives you two options:

- **maximum routes** *limit* **warning-only**—generates a warning message when you attempt to exceed the limit. The specified limit is not enforced.

  If you use the **maximum routes** *limit* **warning-only** command with the **snmp-server enable traps mpls vpn** command, a mid-threshold SNMP notification is generated when the *limit* value is reached or exceeded. No max-threshold SNMP notification is generated.

- **maximum routes** *limit warn-threshold*—generates a warning message when the *warn-threshold* is reached. The specified limit is enforced.

  If you use the **maximum routes** *limit warn-threshold* command with the **snmp-server enable traps mpls vpn** command, a mid-threshold SNMP notification is generated when the *warn-threshold* value is reached. A max-threshold notification is generated when the *limit* value is reached.

The notification types described are defined in the following MIB objects of the PPVPN-MPLS-VPN-MIB:

- mplsVrfIfUp
- mplsVrfIfDown
- mplsNumVrfRouteMidThreshExceeded
- mplsNumVrfRouteMaxThreshExceeded
- mplsNumVrfSecIllegalLabelThreshExceeded

The cMplsNumVrfRouteMaxThreshCleared notification type is defined in the CISCO-IETF-PPVPN-MPLS-VPN-MIB.

Examples

In the following example, MPLS VPN trap notifications are sent to the host specified as 172.31.156.34 using the community string named public if a VRF transitions from an up or down state:

```
Router(config)# snmp-server host 172.31.156.34 traps public mpls-vpn
Router(config)# snmp-server enable traps mpls vpn vrf-down vrf-up
```

Related Commands

Command	Description
maximum routes	Sets the warning threshold and route maximum for VRFs.
snmp-server enable traps atm subif	Enables ATM subinterface SNMP notifications.
snmp-server enable traps frame-relay subif	Enables Frame Relay subinterface SNMP notifications.
snmp-server host	Specifies the recipient of SNMP notifications.

snmp-server enable traps ospf cisco-specific errors config-error

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) nonvirtual interface mismatch errors, use the **snmp-server enable traps ospf cisco-specific errors config-error** command in global configuration mode. To disable OSPF nonvirtual interface mismatch error SNMP notifications, use the **no** form of this command.

snmp-server enable traps ospf cisco-specific errors config-error

no snmp-server enable traps ospf cisco-specific errors config-error

Syntax Description

This command has no keywords or arguments.

Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF nonvirtual interface mismatch errors are not created.

Command Modes

Global configuration

Command History

Release	Modification
12.3(5)	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

To enable the cospfShamLinkConfigError trap, you must first enter the **snmp-server enable traps ospf cisco-specific errors config-error** command in global configuration mode. The **snmp-server enable traps ospf cisco-specific errors config-error** command enables the cospfConfigError trap, so that both traps can be generated at the same place and maintain consistency with a similar case for configuration errors across virtual links.

If you try to enable the cospfShamLinkConfigError trap before configuring the cospfospfConfigError trap you will receive an error message stating you must first configure the cospfConfigError trap.

Examples

The following example enables the router to send nonvirtual interface mismatch error notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps ospf cisco-specific errors config-error
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server enable traps ospf cisco-specific errors shamlink	Enables SNMP notifications for OSPF sham-link errors.
snmp-server enable traps ospf cisco-specific retransmit	Enables SNMP notifications for OSPF retransmission errors.
snmp-server enable traps ospf cisco-specific state-change	Enables SNMP notifications for OSPF transition state changes.

snmp-server enable traps ospf cisco-specific errors shamlink

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) sham-link errors, use the **snmp-server enable traps ospf cisco-specific errors shamlink** command in global configuration mode. To disable OSPF sham-link error SNMP notifications, use the **no** form of this command.

snmp-server enable traps ospf cisco-specific errors shamlink [**authentication** [**bad-packet**] [[**config**] | **config** [**bad-packet**]]]

no snmp-server enable traps ospf cisco-specific errors shamlink [**authentication** [**bad-packet**] [[**config**] | **config** [**bad-packet**]]]

Syntax Description

authentication	(Optional) Enables SNMP notifications only for authentication failures on OSPF sham-link interfaces.
bad-packet	(Optional) Enables SNMP notifications only for packet parsing failures on OSPF sham-link interfaces.
config	(Optional) Enables SNMP notifications only for configuration mismatch errors on OSPF sham-link interfaces.

Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF sham-link errors are not created.

Command Modes

Global configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

To enable the cospfShamLinkConfigError trap, you must first enter the **snmp-server enable traps ospf cisco-specific errors config-error** command in global configuration mode. The **snmp-server enable traps ospf cisco-specific errors config-error** command enables the cospfConfigError trap, so that both traps can be generated at the same place and maintain consistency with a similar case for configuration errors across virtual links.

If you try to enable the cospfShamLinkConfigError trap before configuring the cospfospfConfigError trap you will receive an error message stating you must first configure the cospfConfigError trap.

Examples

The following example enables the router to send OSPF sham-link error notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps ospf cisco-specific errors config-error
Router(config)# snmp-server enable traps ospf cisco-specific errors shamlink
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server enable traps ospf cisco-specific errors config-error	Enables SNMP notifications for OSPF nonvirtual interface mismatch errors.
snmp-server enable traps ospf cisco-specific retransmit	Enables SNMP notifications for OSPF retransmission errors.
snmp-server enable traps ospf cisco-specific state-change	Enables SNMP notifications for OSPF transition state changes.

snmp-server enable traps ospf cisco-specific retransmit

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) retransmission errors, use the **snmp-server enable traps ospf cisco-specific retransmit** command in global configuration mode. To disable OSPF sham-link error SNMP notifications, use the **no** form of this command.

snmp-server enable traps ospf cisco-specific retransmit [**packets** [**shamlink** | **virt-packets**] | **shamlink** [**packets** | **virt-packets**] | **virt-packets** [**shamlink**]]

no snmp-server enable traps ospf cisco-specific retransmit [**packets** [**shamlink** | **virt-packets**] | **shamlink** [**packets** | **virt-packets**] | **virt-packets** [**shamlink**]]

Syntax Description

packets	(Optional) Enables SNMP notifications only for packet retransmissions on nonvirtual interfaces.
shamlink	(Optional) Enables SNMP notifications only for sham-link retransmission notifications.
virt-packets	(Optional) Enables SNMP notifications only for packet retransmissions on virtual interfaces.

Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF retransmission errors are not created.

Command Modes

Global configuration

Command History

Release	Modification
12.3(5)	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.0(30)S	The **shamlink** keyword and related options were added.
12.3(14)T	Support was added for the **shamlink** keyword and related options.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following example enables the router to send OSPF sham-link retransmission notifications:

```
Router(config)# snmp-server enable traps ospf cisco-specific retransmit shamlink
```

Related Commands

Command	Description
snmp-server enable traps ospf cisco-specific errors config-error	Enables SNMP notifications for OSPF nonvirtual interface mismatch errors.
snmp-server enable traps ospf cisco-specific errors shamlink	Enables SNMP notifications for OSPF sham-link errors.
snmp-server enable traps ospf cisco-specific state-change	Enables SNMP notifications for OSPF transition state changes.

snmp-server enable traps ospf cisco-specific state-change

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) transition state changes, use the **snmp-server enable traps ospf cisco-specific state-change** command in global configuration mode. To disable OSPF transition state change SNMP notifications, use the **no** form of this command.

snmp-server enable traps ospf cisco-specific state-change [**nssa-trans-change** | **shamlink** [**interface** | **interface-old** | **neighbor**]]

no snmp-server enable traps ospf cisco-specific state-change [**nssa-trans-change** | **shamlink** [**interface** | **interface-old** | **neighbor**]]

Syntax Description

nssa-trans-change	(Optional) Enables only not-so-stubby area (NSSA) translator state changes trap for the OSPF area.
shamlink	(Optional) Enables only the sham-link transition state changes trap for the OSPF area.
interface	(Optional) Enables only the sham-link interface state changes trap for the OSPF area.
interface-old	(Optional) Enables only the replaced interface transition state changes trap for the OSPF area.
neighbor	(Optional) Enables only the sham-link neighbor transition state changes trap for the OSPF area.

Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF transition state changes are not created.

Command Modes

Global configuration

Command History

Release	Modification
12.3(5)	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.0(30)S	The **shamlink**, **interface-old**, and **neighbor** keywords were added.
12.3(14)T	Support was added for the **shamlink**, **interface-old**, and **neighbor** keywords.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

You cannot enter both the **interface** and **interface-old** keywords because you cannot enable both the new and replaced sham-link interface transition state change traps. You can configure only one of the two traps, but not both.

Examples

The following example enables the router to send OSPF sham-link transition state change notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps ospf cisco-specific state-change shamlink
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server enable traps ospf cisco-specific errors config-error	Enables SNMP notifications for OSPF nonvirtual interface mismatch errors.
snmp-server enable traps ospf cisco-specific errors shamlink	Enables SNMP notifications for OSPF sham-link errors.
snmp-server enable traps ospf cisco-specific retransmit	Enables SNMP notifications for OSPF retransmission errors.

snmp-server enable traps pim

To enable Protocol Independent Multicast (PIM) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps pim** command in global configuration mode. To disable PIM-specific SNMP notifications, use the **no** form of this command.

snmp-server enable traps pim [**neighbor-change** | **rp-mapping-change** | **invalid-pim-message**]

no snmp-server enable traps pim

Syntax Description

neighbor-change	(Optional) Enables notifications indicating when the PIM interface on a router is disabled or enabled, or when the PIM neighbor adjacency on a router expires or is established.
rp-mapping-change	(Optional) Enables notifications indicating a change in the rendezvous point (RP) mapping information due to either Auto-RP or bootstrap router (BSR) messages.
invalid-pim-message	(Optional) Enables invalid PIM message traps. For example, an invalid PIM message could result when a router receives a join or prune message for which the RP specified in the packet is not the RP for the multicast group.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files, available from Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Examples

The following example shows how to configure a router to generate notifications indicating that a PIM interface on the router has been enabled:

```
! Configure PIM traps to be sent as SNMPv2c traps to host with IP address 10.0.0.1.
Router(config)# snmp-server host 10.0.0.1 traps version 2c public pim
```

```
! Configure router to send the neighbor-change class of notifications to host.
Router(config)# snmp-server enable traps pim neighbor-change

! Enable PIM sparse-dense mode on Ethernet interface 0/0.
Router(config)# interface ethernet0/0
Router(config-if)# ip pim sparse-dense-mode
```

Related Commands

Command	Description
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps pppoe

To enable Point-to-Point Protocol over Ethernet (PPPoE) session count Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps pppoe** command in global configuration mode. To disable PPPoE session count SNMP notifications, use the **no** form of this command.

snmp-server enable traps pppoe

no snmp-server enable traps pppoe

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)DC	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

This command enables SNMP traps only. It does not support inform requests.

To configure the PPPoE session-count thresholds at which SNMP notifications will be sent, use the **pppoe limit max-sessions** or **pppoe max-sessions** commands.

For a complete description of this notification and additional MIB functions, see the CISCO-PPPOE-MIB.my file, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

Examples

The following example enables the router to send PPPoE session-count SNMP notifications to the host at the address 10.64.131.20:

```
snmp-server community public RW
snmp-server enable traps pppoe
snmp-server host 10.64.131.20 version 2c public udp-port 1717
```

Related Commands

Command	Description
pppoe limit max-sessions	Sets the maximum number of PPPoE sessions that will be permitted on a router, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.
pppoe max-sessions	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps repeater

To enable or disable standard repeater (hub) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps repeater** command in global configuration mode. To disable repeater notifications, use the **no** form of this command.

snmp-server enable traps repeater [**health**] [**reset**]

no snmp-server enable traps repeater [**health**] [**reset**]

Syntax Description

health	(Optional) Enables the rptrHealth trap, which conveys information related to the operational status of the repeater.
reset	(Optional) Sends the rptrResetEvent trap on completion of a repeater reset action (triggered by the transition to a START state by a manual command).

Command Default

SNMP notifications are disabled.

If no option keywords are specified when entering this command, all repeater notifications available on your system are enabled or disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command enables or disables Repeater MIB notifications, as defined in RFC 1516. RFC 1516 defines objects for managing IEEE 802.3 10 Mbps baseband repeaters, also known as hubs.

Two sets of notifications are available for this command. The following notification is defined in the CISCO-REPEATER-MIB (enterprise 1.3.6.1.4.1.9.9.22.3):

- 1 ciscoRptrIllegalSrcAddrTrap (illegal source address trap)

The following notifications are defined in the CISCO-REPEATER-MIB-V1SMI (enterprise 1.3.6.1.2.1.22):

- 1 rptrHealth
- 2 rptrGroupChange
- 3 rptrResetEvent

For a complete description of the repeater notifications and additional MIB functions, refer to the CISCO-REPEATER-MIB.my and CISCO-REPEATER-MIB-V1SMI.my files, available on Cisco.com at

http://www.cisco.com/public/mibs/.

When the optional **health** keyword is used, the rptrHealth trap is sent when the value of rptrOperStatus changes, or upon completion of a nondisruptive test.

The rptrOperStatus object indicates the operational state of the repeater. Status values are as follows:

- other(1)—undefined or unknown status
- ok(2)—no known failures
- rptrFailure(3)—repeater-related failure
- groupFailure(4)—group-related failure
- portFailure(5)—port-related failure
- generalFailure(6)—failure, unspecified type

When the optional **reset** keyword is used, the rptrResetEvent trap is not sent when the agent restarts and sends an SNMP coldStart or warmStart trap.

The **snmp-server enable traps repeater** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to enable the router to send repeater inform notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps repeater
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps resource-policy

To enable ERM-MIB notification traps, use the **snmp-server enable traps resource-policy** command in global configuration mode. To disable the ERM-MIB notification traps, use the **no** form of this command.

snmp-server enable traps resource-policy

no snmp-server enable traps resource-policy

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled (notification traps will be sent to the host that is configured to receive traps).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Examples

The following example shows how to configure the router to send SNMP notifications for ERM to a host:

```
Router(config)# snmp-server enable traps resource policy
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification message.
snmp-server community	Permits access to SNMP by setting up the community access string.

snmp-server enable traps rtr

To enable the sending of Cisco IOS IP Service Level Agreements (SLAs) Simple Network Management Protocol (SNMP) trap notifications, use the **snmp-server enable traps rtr** command in global configuration mode. To disable IP SLAs SNMP notifications, use the **no** form of this command.

snmp-server enable traps rtr

no snmp-server enable traps rtr

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command controls (enables or disables) Cisco IOS IP SLAs notifications, as defined in the Response Time Monitor MIB (CISCO-RTTMON-MIB).

The **snmp-server enable traps rtr** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to enable the router to send IP SLAs SNMP traps to the host at the address myhost.cisco.com using the community string defined as public:

```
snmp-server enable traps rtr
snmp-server host myhost.cisco.com informs version 2c public rtr
```

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.

Command	Description
snmp-server host	Specifies the destination NMS and transfer parameters for SNMP notifications.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps snmp

To enable the sending of RFC 1157 Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps snmp** command in global configuration mode. To disable RFC 1157 SNMP notifications, use the **no** form of this command.

snmp-server enable traps snmp [**authentication**] [**linkup**] [**linkdown**] [**coldstart**] [**warmstart**]

no snmp-server enable traps snmp [**authentication**] [**linkup**] [**linkdown**] [**coldstart**] [**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.

When you enter this command without any optional keywords, all RFC 1157 SNMP notifications are enabled (or disabled, if using the **no** form of the command).

Command Modes

Global configuration

Command History

Release	Modification
11.3	The **snmp-server enable traps snmp authentication** command was introduced. This command replaced the **snmp-server trap-authentication** command.
12.1(3)T	The following keywords were added: • **linkup** • **linkdown** • **coldstart**
12.1(5)T	The **warmstart** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types.

If you do not enter an **snmp-server enable traps snmp** command, no notifications controlled by this command are sent. To configure the router to send these SNMP notifications, you must enter at least one **snmp-server enable traps snmp** command. When you enter the command with no keywords, all notification types are enabled. When you enter the command with a keyword, only the types of notifications related to that keyword are enabled.

When the optional **authentication** keyword is used, the authenticationFailure(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 SNMPv2c, authentication failure occurs for packets with an incorrect community string. For SNMPv3, authentication failure occurs for packets with an incorrect SHA/MD5 authentication key or for a packet that is outside the authoritative SNMP engine's window (for example, outside configured access lists or time ranges).

When the optional **linkup** keyword is used, the linkUp(3) trap signifies that the sending device recognizes that one of the communication links represented in the agent's configuration has come up.

When the optional **linkdown** keyword is used, 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 enable traps snmp** [**linkup**] [**linkdown**] form of this command globally enables or disables SNMP linkUp and linkDown traps. After enabling either of these traps globally, you can disable them on specific interfaces using the **no snmp trap link-status** command in interface configuration mode. On the interface level, linkUp and linkDown traps are enabled by default, which means that these notifications do not have to be enabled on a per-interface basis. However, linkUp and linkDown notifications will not be sent unless you enable them globally using the **snmp-server enable traps snmp** command.

When the optional **coldstart** keyword is used, 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.

When the optional **warmstart** keyword is used, 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.

The **snmp-server enable traps snmp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

For a host to receive a notification controlled by this command, both the **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled. If the notification type is not controlled by this command, just the appropriate **snmp-server host** command must be enabled.

Examples

The following example shows how to enable the router to send all traps to the host `myhost.cisco.com`, using the community string defined as public:

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server host myhost.cisco.com public snmp
```

The following example shows how to enable the router to send all inform notifications to the host `myhost.cisco.com` using the community string defined as `public`:

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public snmp
```

The following example shows the enabling all SNMP trap types, then the disabling of only the linkUp and linkDown trap:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server enable traps snmp
Router(config)# end
Router# more system:running-config | include traps snmp
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart

Router# configure terminal
Router(config)# no snmp-server enable traps snmp linkup linkdown
Router(config)# end
Router# more system:running-config | include traps snmp
snmp-server enable traps snmp authentication coldstart warmstart
```

Related Commands

Command	Description
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server informs	Specifies inform request options.
snmp-server trap authentication vrf	Disables or reenables SNMP authentication notifications specific to VPN context mismatches.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps srp

To enable the sending of Intelligent Protection Switching (IPS) Spatial Reuse Protocol (SRP) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps srp** command in global configuration mode. To disable SRP notifications, use the **no** form of this command.

snmp-server enable traps srp

no snmp-server enable traps srp

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced to support DPT-OC12 Port Adapters.

Usage Guidelines

The Cisco SRP MIB module (CISCO-SRP-MIB.my) provides objects for monitoring IP-over-SONET IPS SRP traffic using the SNMP. When IPS is enabled, if a node or fiber facility failure is detected, traffic going toward or coming from the failure direction is wrapped (looped) back to go in opposite direction on the other ring.

The **snmp-server enable traps srp** command enables SRP state change notifications (traps or informs). SRP state change notifications are generated whenever one of the two sides of an SRP interface ring enters or leaves the wrapped state (when a ring wraps, or when a ring is restored).

Specifically, the srpMACIpsWrapCounter object in the CISCO-SRP-MIB increments when a Ring wraps, and the value of the rpMACIpsLastUnWrapTimeStamp object changes when a ring unwraps. (An “unwrap” event happens when the original ring is restored.)

The **snmp-server enable traps srp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

In the following example, SRP-specific informs are enabled and will be sent to the host “myhost.cisco.com” using the community string defined as public:

```
Router(config)# snmp-server enable traps srp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public srp
```

snmp-server enable traps syslog

To enable the sending of system logging message Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps syslog** command in global configuration mode. To disable system logging message SNMP notifications, use the **no** form of this command.

snmp-server enable traps syslog

no snmp-server enable traps syslog

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) system logging message notifications. System logging messages (also called system error messages, or syslog messages) are status notification messages that are generated by the routing device during operation. These messages are typically logged to a destination (such as the terminal screen, to a system buffer, or to a remote “syslog” host).

If your software image supports the Cisco Syslog MIB, these messages can also be sent via SNMP to a network management station (NMS). To determine which software images support the Cisco Syslog MIB, used the Cisco MIB Locator tool at http://www.cisco.com/go/mibs/ .(At the time of writing, the Cisco Syslog MIB is only supported in “Enterprise” images.)

Unlike other logging processes on the system, debug messages (enabled using CLI debug commands) are not included with the logging messages sent via SNMP.

To specify the severity level at which notifications should be generated, use the **logging history** global configuration command. For additional information about the system logging process and severity levels, see the description of the **logging** commands.

The syslog notification is defined by the clogMessageGenerated NOTIFICATION-TYPE object in the Cisco Syslog MIB (CISCO-SYSLOG-MIB.my). When a syslog message is generated by the device a clogMessageGenerated notification is sent to the designated NMS. The clogMessageGenerated notification includes the following objects: clogHistFacility, clogHistSeverity, clogHistMsgName, clogHistMsgText, clogHistTimestamp.

For a complete description of these objects and additional MIB information, see the text of CISCO-SYSLOG-MIB.my, available on Cisco.com using the SNMP Object Navigator tool at http://www.cisco.com/go/mibs . See also the CISCO-SYSLOG-EXT-MIB and the CISCO-SYSLOG-EVENT-EXT-MIB.

The **snmp-server enable traps syslog** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables the router to send system logging messages at severity levels 0 (emergencies) through 2 (critical) to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps syslog
Router(config)# logging history 2
Router(config)# snmp-server host myhost.cisco.com traps version 2c public
```

Related Commands

Command	Description
logging history	Limits syslog messages sent to the router's history table and to an SNMP NMS based on severity.
snmp-server host	Specifies the destination NMS and transfer parameters for SNMP notifications.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps transceiver type all

To enable all supported SNMP transceiver traps for all transceiver types in the global configuration mode, use the **snmp-server enable traps transceiver type all** command. Use the **no** form of this command to disable the transceiver SNMP trap notifications.

snmp-server enable traps transceiver type all

no snmp-server enable traps transceiver type all

Syntax Description

The command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **snmp-server enable 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. To send notifications, you must configure at least one **snmp-server host** command.

Examples

This example shows how to enable all supported SNMP transceiver traps for all transceiver types:

```
Router(config)# snmp-server enable traps transceiver type all
Router(config)#
```

Related Commands

Command	Description
show interfaces transceiver	Displays information about the optical transceivers that have DOM enabled.

snmp-server enable traps voice

To enable Simple Network Management Protocol (SNMP) voice notifications, use the **snmp-server enable traps voice** command in global configuration mode. To disable SNMP voice notifications, use the **no** form of this command.

snmp-server enable traps voice [**poor-qov**] [**fallback**]

no snmp-server enable traps voice

Syntax Description

poor-qov	(Optional) Enables poor-quality-of-voice SNMP notifications.
fallback	(Optional) Enables SNMP fallback voice notifications.

Command Default

If you enter this command without any of the optional keywords, both available notifications are enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.3(14)T	The **fallback** keyword was added.

Usage Guidelines

SNMP notifications can be sent as traps (notifications) or inform requests. This command enables both traps and inform requests.

The **poor-qov** keyword enables or disables poor-quality-of-voice notifications. The poor quality-of-voice notification is defined in CISO-VOICE-DIAL-CONTROL-MIB as follows:

enterprise 1.3.6.1.4.1.9.9.63.2

(1) cvdcPoorQoVNotification

The **fallback** keyword enables or disables public switched telephone network (PSTN) fallback notifications. The fallback notification is defined in CISCO-VOICE-DIAL-CONTROL-MIB as follows:

(1) cvVoIPCallHistoryConnectionId

(2) cvVoIPCallHistoryFallbackIcpif

(2) cvVoIPCallHistoryFallbackLoss

(3) cvVoIPCallHistoryFallbackDelay

(4) cvVoIPCallHistoryRemSigIPAddrT

(5) cvVoIPCallHistoryRemSigIPAddr

(6) cvVoIPCallHistoryRemMediaIPAddrT

(7) cvVoIPCallHistoryRemMediaIPAddr

(8) cCallHistoryCallOrigin

(9) cvCommonDcCallHistoryCoderTypeRate

For a complete description of these notifications and additional MIB functions, see the CISCO-VOICE-DIAL-CONTROL-MIB.my file, available on Cisco.com at http://www.cisco.com/go/mibs.

The **snmp-server enable traps voice** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to enable the router to send poor-quality-of-voice informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps voice poor-qov
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example shows how to enable the router to send PSTN fallback messages at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps voice fallback
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server enable traps voice poor-qov	Enables poor quality-of-voice SNMP notifications.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface which an SNMP trap should originate from.

snmp-server enable traps voice poor-qov

The **snmp-server enable traps voice poor-qov** command is replaced by the **snmp-server enable traps voice** command. See the **snmp-server enable traps voice** command for more information.

snmp-server engineID local

To specify the Simple Network Management Protocol (SNMP) engine ID on the local device, use the **snmp-server engineID local** command in global configuration mode. To remove the configured engine ID, use the **no** form of this command.

snmp-server engineID local *engineid-string*

no snmp-server engineID local *engineid-string*

Syntax Description

engineid-string	String of a maximum of 24 characters that identifies the engine ID.

Command Default

An SNMP engine ID is generated automatically but is not displayed or stored in the running configuration. You can display the default or configured engine ID by using the **show snmp engineID** command.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The SNMP engine ID is a unique string used to identify the device for administration purposes. You do not need to specify an engine ID for the device; a default string is generated using Cisco's enterprise number (1.3.6.1.4.1.9) and the mac address of the first interface on the device. For further details on the SNMP engine ID, see RFC 2571.

If you wish to specify your own ID, note that you need not specify the entire 24-character engine ID if it contains trailing zeros. Specify only the portion of the Engine ID up until the point where only zeros remain in the value. For example, to configure an engine ID of 123400000000000000000000, you can specify **snmp-server engineID local 1234**.

Changing the value of snmpEngineID has important side-effects. A user's password (entered on the command line) is converted to an MD5 or SHA security digest. This digest is based on both the password and the local engine ID. The command line password is then destroyed, as required by RFC 2274. Because of this deletion, if the local value of engineID changes, the security digests of SNMPv3 users will be invalid, and the users will have to be reconfigured.

Similar restrictions require the reconfiguration of community strings when the engine ID changes. A remote engine ID is required when an SNMPv3 inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

Related Commands

Command	Description
show snmp engineID	Displays the identification of the local SNMP engine and all remote engines that have been configured on the router.
snmp-server host	Specifies the recipient (SNMP manager) of an SNMP trap notification.

snmp-server engineID remote

To specify the Simple Network Management Protocol (SNMP) engine ID of a remote SNMP device, use the **snmp-server engineID remote** command in global configuration mode. To remove a specified SNMP engine ID from the configuration, use the **no** form of this command.

snmp-server engineID remote {*ipv4-ip-address* | *ipv6 address*}[**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engineid-string*

no snmp-server engineID remote {*ipv4-ip-address* | *ipv6 address*} [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engineid-string*

Syntax Description

ipv4-ip-address | *ipv6-address*	IPv4 or IPv6 address of the device that contains the remote copy of SNMP.
udp-port	(Optional) Specifies a User Datagram Protocol (UDP) port of the host to use.
udp-port-number	(Optional) Socket number on the remote device that contains the remote copy of SNMP. The default is 161.
vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
engineid-string	String of a maximum of 24 characters that identifies the engine ID.

Command Default

UDP port: 161

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(2)T	The **vrf** keyword and *vrf-name* argument were added.
12.0(27)S	Support for configuring an IPv6 notification server was added.
12.3(14)T	Support for configuring an IPv6 notification server was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Specifying the entire 24-character engine ID if it contains trailing zeros is not required. Specify only the portion of the engine ID up to where the trailing zeros start. For example, to configure an engine ID of 123400000000000000000000, specify the value 1234 as the *engineid-string* argument.

A remote engine ID is required when an SNMP version 3 inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

Examples

The following example specifies the SNMP engine ID and configures the VRF name traps-vrf for SNMP communications with the remote device at 172.16.20.3:

```
Router(config)# snmp-server engineID remote 172.16.20.3 vrf traps-vrf
80000009030000B064EFE100
```

Related Commands

Command	Description
show snmp engineID	Displays the identification of the local SNMP engine and all remote engines that have been configured on the router.
snmp-server host	Specifies the recipient (SNMP manager) of an SNMP trap notification.

snmp-server file-transfer access-group

To associate an access list to the transfer protocols TFTP, FTP, Remote Copy Protocol (RCP), Secure Copy Protocol (SCP), and Secured File Transfer Protocol (SFTP), use the **snmp-server file-transfer access-group** command in global configuration mode. To disassociate an access list, use **no** form of this command.

snmp-server file-transfer access-group {*acl-number* | *acl-name*} [**protocol** *p-name*]

no snmp-server file-transfer access-group {*acl-number* | *acl-name*}

Syntax Description

acl-number	Integer from 1 to 99 that specifies a standard ACL.
acl-name	String that specifies a standard ACL.
protocol	(Optional) Enables the user to associate a named protocol with an access group.
p-name	(Optional) Name of a transfer protocol. Valid values are: **ftp**, **rcp**, **scp**, **sftp**, and **tftp**.

Command Default

If a protocol is not specified, all protocols are associated with the access list.

Command Modes

Global configuration

Command History

Release	Modification
12.4(12)	This command was introduced. This command replaces the **snmp-server tftp-server-list** command.

Usage Guidelines

The **snmp-server tftp-server-list** command is still supported in Cisco IOS software, but if it is configured as **snmp-server tftp-server-list 10**, it will be substituted with the **snmp-server file-transfer access-group 10 protocol tftp** command.

Use the **snmp-server file-transfer access-group** command to restrict configuration transfers that are initiated via Simple Network Management Protocol (SNMP). You can restrict transfers for specific transfer protocols by associating an access list to the protocol.

Examples

The following example associates access group 10 to the transfer protocols FTP and RCP:

```
Router(config)# snmp-server file-transfer access-group 10 protocol ftp
Router(config)# snmp-server file-transfer access-group 10 protocol rcp
```

Related Commands

Command	Description
snmp-server tftp-server-list	Associates TFTP servers used via SNMP controlled TFTP operations to the servers specified in an access list.

snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, 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 *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [**ipv6** *named-access-list*] [*acl-number* | *acl-name*]]

no snmp-server group *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*]

Syntax Description

group-name	Name of the group.
v1	Specifies that the group is using the SNMPv1 security model. SNMPv1 is the least secure of the possible SNMP security models.
v2c	Specifies that the group is using the SNMPv2c security model. The SNMPv2c security model allows informs to be transmitted and supports 64-character strings.
v3	Specifies that the group is using the SNMPv3 security model. SMNPv3 is the most secure of the supported security models. It allows you to explicitly configure authentication characteristics.
auth	Specifies authentication of a packet without encrypting it.
noauth	Specifies no authentication of a packet.
priv	Specifies authentication of a packet with encryption.
context	(Optional) Specifies the SNMP context to associate with this SNMP group and its views.
context-name	(Optional) Context name.
read	(Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent.
read-view	(Optional) String of a maximum of 64 characters that is the name of the view. The default is that the read-view is assumed to be every object belonging to the Internet object identifier (OID) space (1.3.6.1), unless the **read** option is used to override this state.
write	(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.
write-view	(Optional) String of a maximum of 64 characters that is the name of the view. The default is that nothing is defined for the write view (that is, the null OID). You must configure write access.
notify	(Optional) Specifies a notify view for the SNMP group. This view enables you to specify a notify, inform, or trap.

notify-view	(Optional) String of a maximum of 64 characters that is the name of the view. By default, nothing is defined for the notify view (that is, the null OID) until the **snmp-server host** command is configured. If a view is specified in the **snmp-server group** command, any notifications in that view that are generated will be sent to all users associated with the group (provided a SNMP server host configuration exists for the user). Cisco recommends that you let the software autogenerate the notify view. See the "Configuring Notify Views" section in this document.
access	(Optional) Specifies a standard access control list (ACL) to associate with the group.
ipv6	(Optional) Specifies an IPv6 named access list. If both IPv6 and IPv4 access lists are indicated, the IPv6 named access list must appear first in the list.
named-access-list	(Optional) Name of the IPv6 access list.
acl-number	(Optional) The *acl-number* argument is an integer from 1 to 99 that identifies a previously configured standard access list.
acl-name	(Optional) The *acl-name* argument is a string of a maximum of 64 characters that is the name of a previously configured standard access list.

Command Default

No SNMP server groups are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.(3)T	This command was introduced.
12.0(23)S	The **context** *context-name* keyword and argument pair was added.
12.3(2)T	The **context** *context-name* keyword and argument pair was integrated into Cisco IOS Release 12.3(2)T, and support for standard named access lists (acl-name) was added.
12.0(27)S	The **ipv6** *named-access-list* keyword and argument pair was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	The **ipv6** *named-access-list* keyword and argument pair was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

When a community string is configured internally, two groups with the name public are autogenerated, one for the v1 security model and the other for the v2c security model. Similarly, deleting a community string will delete a v1 group with the name public and a v2c group with the name public.

No default values exist for authentication or privacy algorithms when you configure the **snmp-server group** command. Also, no default passwords exist. For information about specifying a Message Digest 5 (MD5) password, see the documentation of the **snmp-server user** command.

Configuring Notify Views

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, you must either reconfigure the **snmp-server host** command, or specify the appropriate notify view.

Specifying a notify view when configuring an SNMP group is not recommended, 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 group's notify view will affect all users associated with that group.

Instead of specifying the notify view for a group as part of the **snmp-server group** command, use the following commands in the order specified:

1. **snmp-server user**—Configures an SNMP user.
2. **snmp-server group**—Configures an SNMP group, without adding a notify view.
3. **snmp-server host**—Autogenerates the notify view by specifying the recipient of a trap operation.

SNMP Contexts

SNMP contexts provide 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.

Use this command with the **context** *context-name* keyword and argument to associate a read, write, or notify SNMP view with an SNMP context.

Examples

Create an SNMP Group

The following example shows how to create the SNMP server group "public," allowing read-only access for all objects to members of the standard named access list "lmnop":

```
Router(config)# snmp-server group public v2c access lmnop
```

Remove an SNMP Server Group

The following example shows how to remove the SNMP server group "public" from the configuration:

```
Router(config)# no snmp-server group public v2c
```

Associate an SNMP Server Group with Specified Views

The following example shows SNMP context "A" associated with the views in SNMPv2c group "GROUP1":

```
Router(config)# snmp-server context A
Router(config)# snmp mib community commA
Router(config)# snmp mib community-map commA context A target-list commAVpn
Router(config)# snmp-server group GROUP1 v2c context A read viewA write viewA notify viewB
```

Related Commands

Command	Description
show snmp group	Displays the names of groups on the router and the security model, the status of the different views, and the storage type of each group.
snmp mib community-map	Associates a SNMP community with an SNMP context, engine ID, security name, or VPN target list.
snmp-server host	Specifies the recipient of a SNMP notification operation.
snmp-server user	Configures a new user to a SNMP group.

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 from the configuration, use the **no** form of this command.

snmp-server host {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]

no snmp-server host {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]

Syntax Description

hostname	The SNMP notification host is typically a network management station (NMS) or SNMP manager. This host is the recipient of the SNMP traps or informs.
ip-address	Name, IP address, or IPv6 address of the SNMP notification host. The *ip-address* can be an IP or IPv6 address.
vrf	(Optional) Specifies that a Virtual Private Network (VPN) routing and forwarding (VRF) instance should be used to send SNMP notifications.
vrf-name	(Optional) VPN VRF instance used to send SNMP notifications.
traps	(Optional) Specifies that notifications should be sent as traps. This is the default.
informs	(Optional) Specifies that notifications should be sent as informs.
version	(Optional) Version of the SNMP that is used to send the traps or informs. The default is 1. If you use the **version** keyword, one of the following keywords must be specified: • **1**—SNMPv1. This option is not available with informs. • **2c**—SNMPv2C. • **3**—SNMPv3. The most secure model because it allows packet encryption with the **priv** keyword. The default is **noauth**. One of the following three optional security level keywords can follow the **3** keyword: – **auth**—Enables Message Digest 5 (MD5) 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 is sent with the notification operation. **Note** You can set this string using the **snmp-server host** command by itself, but Cisco recommends that you define the string using the **snmp-server community** command prior to using the **snmp-server host** command. **Note** The "at" sign (@) is used for delimiting the context information.
udp-port	(Optional) Specifies that SNMP traps or informs are to be sent to an NMS host.
port	(Optional) UDP port number of the NMS host. The default is 162.
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 the following keywords: • **bgp**—Sends Border Gateway Protocol (BGP) state change notifications. • **calltracker**—Sends Call Tracker call-start/call-end notifications. • **cef** — Sends notifications related to Cisco Express Forwarding. • **config**—Sends configuration change notifications. • **cpu**—Sends CPU-related notifications. • **director**—Sends notifications related to DistributedDirector. • **dspu**—Sends downstream physical unit (DSPU) notifications. • **eigrp**—Sends Enhanced Interior Gateway Routing Protocol (EIGRP) stuck-in-active (SIA) and neighbor authentication failure notifications. • **entity**—Sends Entity MIB modification notifications. • **envmon**—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded. • **flash**—Sends flash media insertion and removal notifications. • **frame-relay**—Sends Frame Relay notifications. • **hsrp**—Sends Hot Standby Routing Protocol (HSRP) notifications. • **iplocalpool**—Sends IP local pool notifications. • **ipmobile**—Sends Mobile IP notifications. • **ipsec**—Sends IP Security (IPsec) notifications. • **isdn**—Sends ISDN notifications. • **l2tun-pseudowire-status**—Sends pseudowire state change notifications. • **l2tun-session**—Sends Layer 2 tunneling session notifications. • **llc2**—Sends Logical Link Control, type 2 (LLC2) notifications. • **memory**—Sends memory pool and memory buffer pool notifications. • **mpls-ldp**—Sends Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) notifications indicating status changes in LDP sessions.

- **mpls-traffic-eng**—Sends MPLS traffic engineering notifications indicating changes in the status of MPLS traffic engineering tunnels.
- **mpls-vpn**—Sends MPLS VPN notifications.
- **ospf**—Sends Open Shortest Path First (OSPF) sham-link notifications.
- **pim**—Sends Protocol Independent Multicast (PIM) notifications.
- **repeater**—Sends standard repeater (hub) notifications.
- **rsrb**—Sends remote source-route bridging (RSRB) notifications.
- **rsvp**—Sends Resource Reservation Protocol (RSVP) notifications.
- **rtr**—Sends Response Time Reporter (RTR) notifications.
- **sdlc**—Sends Synchronous Data Link Control (SDLC) notifications.
- **sdllc**—Sends SDLC Logical Link Control (SDLLC) notifications.
- **snmp**—Sends any enabled RFC 1157 SNMP linkUp, linkDown, authenticationFailure, warmStart, and coldStart notifications.

Note To enable RFC 2233 compliant link up/down notifications, you should use the **snmp server link trap** command.

- **srp**—Sends Spatial Reuse Protocol (SRP) notifications.
- **stun**—Sends serial tunnel (STUN) notifications.
- **syslog**—Sends error message notifications (Cisco Syslog MIB). Use the **logging history level** command to specify the level of messages to be sent.
- **tty**—Sends Cisco enterprise-specific notifications when a TCP connection closes.
- **voice**—Sends SNMP poor quality of voice traps, when used with the **snmp enable peer-trap poor qov** command.
- **vrrp**—Sends Virtual Router Redundancy Protocol (VRRP) notifications.
- **vsimaster**—Sends Virtual Switch Interface (VSI) Master notifications.
- **x25**—Sends X.25 event notifications.

Command Default

This command is disabled by default. A recipient is not specified to receive notifications.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
Cisco IOS Release 12 Mainline/T Train	
12.0(3)T	• The **version 3** [**auth** | **noauth** | **priv**] syntax was added as part of the SNMPv3 Support feature. • The **hsrp** notification-type keyword was added. • The **voice** notification-type keyword was added.
12.1(3)T	The **calltracker** notification-type keyword was added for the Cisco AS5300 and AS5800 platforms.
12.2(2)T	• The **vrf** *vrf-name* keyword/argument combination was added. • The **ipmobile** notification-type keyword was added. • Support for the **vsimaster** notification-type keyword was added for the Cisco 7200 and Cisco 7500 series.
12.2(4)T	• The **pim** notification-type keyword was added. • The **ipsec** notification-type keyword was added.
12.2(8)T	• The **mpls-traffic-eng** notification-type keyword was added. • The **director** notification-type keyword was added.
12.2(13)T	• The **srp** notification-type keyword was added. • The **mpls-ldp** notification-type keyword was added.
12.3(2)T	• The **flash** notification-type keyword was added. • The **l2tun-session** notification-type keyword was added.
12.3(4)T	• The **cpu** notification-type keyword was added. • The **memory** notification-type keyword was added. • The **ospf** notification-type keyword was added.
12.3(8)T	The **iplocalpool** notification-type keyword was added for the Cisco 7200 and 7301 series routers.
12.3(11)T	The **vrrp** keyword was added.
12.3(14)T	• Support for SNMP over IPv6 transport was integrated into Cisco IOS Release 12.3(14)T. Either an IP or IPv6 Internet address can be specified as the *hostname* argument. • The **eigrp** notification-type keyword was added.
Cisco IOS Release 12.0S	
12.0(17)ST	The **mpls-traffic-eng** notification-type keyword was integrated into Cisco IOS Release 12.0(17)ST.
12.0(21)ST	The **mpls-ldp** notification-type keyword was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	• All features in the Cisco IOS Release 12.0ST train were integrated into Cisco IOS Release 12.0(22)S. • The **mpls-vpn** notification-type keyword was added.
12.0(23)S	The **l2tun-session** notification-type keyword was added.
12.0(26)S	The **memory** notification-type keyword was added.

Release	Modification
12.0(27)S	• Support for SNMP over IPv6 transport was added. Either an IP or IPv6 Internet address can be specified as the *hostname* argument. • The **vrf** *vrf-name* keyword argument pair was integrated into Cisco IOS Release 12.0(27)S to support multiple Lightweight Directory Protocol (LDP) contexts for VPNs.
12.0(31)S	The **l2tun-pseudowire-status** notification-type keyword was added.
Release 12.2S	
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(25)S	• The **cpu** notification-type keyword was added. • The **memory** notification-type keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	The **cef** notification-type keyword was added.
12.2(31)SB3	This command was implemented on the Cisco 10000 series.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

If you enter this command with no optional keywords, the default is to send all notification-type traps to the host. No informs will be sent to the host.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

Note If a community string is not defined using the **snmp-server community** command prior to using this command, the default form of the **snmp-server community** command will automatically be inserted into the configuration. The password (community string) used for this automatic configuration of the **snmp-server community** will be the same as specified in the **snmp-server host** command. This automatic command insertion and use of passwords is the default behavior for Cisco IOS Release 12.0(3) and later releases.

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with a SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely than traps to reach their intended destination.

Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter a **snmp-server host** command, no notifications are sent. To configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no optional keywords, all trap types are enabled for the host.

To enable multiple hosts, you must 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 or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

Some notification types cannot be controlled with the **snmp-server enable** command. Some notification types are always enabled, and others are enabled by a different command. For example, the **linkUpDown** notifications are controlled by the **snmp trap link-status** command. These notification types do not require an **snmp-server enable** command.

The availability of a notification-type options depends on the router type and the Cisco IOS software features supported on the router. For example, the **envmon** notification type is available only if the environmental monitor is part of the system. To see what notification types are available on your system, use the command help **?** at the end of the **snmp-server host** command.

The **vrf** keyword allows you to specify the notifications being sent to a specified IP address over a specific VRF. The VRF defines a VPN membership of a user so data is stored using the VPN.

Notification-Type Keywords

The *notification-type* keywords used in the **snmp-server host** command do not always match the keywords used in the corresponding **snmp-server enable traps** command. For example, the notification keyword applicable to Multiprotocol Label Switching Protocol (MPLS) traffic engineering tunnels is specified as **mpls-traffic-eng** (containing two hyphens and no embedded spaces). The corresponding parameter in the **snmp-server enable traps** command is specified as **mpls traffic-eng** (containing an embedded space and a hyphen).

This syntax difference is necessary to ensure that the command-line interface (CLI) interprets the *notification-type* keyword of the **snmp-server host** command as a unified, single-word construct, which preserves the capability of the **snmp-server host** command to accept multiple *notification-type* keywords in the command line. The **snmp-server enable traps** commands, however, often use two-word constructs to provide hierarchical configuration options and to maintain consistency with the command syntax of related commands. Table 83 maps some examples of **snmp-server enable traps** commands to the keywords used in the **snmp-server host** command.

Table 83 SNMP-server enable traps Commands and Corresponding Notification Keywords

snmp-server enable traps Command	snmp-server host Command Keyword
snmp-server enable traps l2tun session	**l2tun-session**
snmp-server enable traps mpls ldp	**mpls-ldp**
snmp-server enable traps mpls traffic-eng[1]	**mpls-traffic-eng**
snmp-server enable traps mpls vpn	**mpls-vpn**

[1] See the *Cisco IOS Multiprotocol Label Switching Command Reference* for documentation of this command.

Examples

If you want to configure a unique SNMP community string for traps but prevent SNMP polling access with this string, the configuration should include an access list. The following example shows how to name a community string comaccess and number an access list 10:

```
Router(config)# snmp-server community comaccess ro 10
Router(config)# snmp-server host 172.20.2.160 comaccess
Router(config)# access-list 10 deny any
```

Note The “at” sign (@) is used as a delimiter between the community string and the context in which it is used. For example, specific VLAN information in BRIDGE-MIB may be polled using *community@VLAN_ID* (for example, public@100), where 100 is the VLAN number.

The following example shows how to send RFC 1157 SNMP traps to a specified host named myhost.cisco.com. Other traps are enabled, but only SNMP traps are sent because only **snmp** is specified in the **snmp-server host** command. The community string is defined as comaccess.

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com comaccess snmp
```

The following example shows how to send the SNMP and Cisco environmental monitor enterprise-specific traps to address 172.30.2.160 using the community string public:

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server enable traps envmon
Router(config)# snmp-server host 172.30.2.160 public snmp envmon
```

The following example shows how to enable the router to send all traps to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but only the ISDN traps are enabled to be sent to a host. The community string is defined as public.

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host myhost.cisco.com public isdn
```

The following example shows how to enable the router to send all inform requests to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example shows how to send HSRP MIB informs to the host specified by the name myhost.cisco.com. The community string is defined as public.

```
Router(config)# snmp-server enable traps hsrp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public hsrp
```

The following example shows how to send all SNMP notifications to company.com over the VRF named trap-vrf using the community string public:

```
Router(config)# snmp-server host company.com vrf trap-vrf public
```

The following example shows how to configure an IPv6 SNMP notification server with the IPv6 address 2001:0DB8:0000:ABCD:1 using the community string public:

```
Router(config)# snmp-server host 2001:0DB8:0000:ABCD:1 version 2c public udp-port 2012
```

The following example shows how to specify VRRP as the protocol using the community string public:

```
Router(config)# snmp-server enable traps vrrp
Router(config)# snmp-server host myhost.cisco.com traps version 2c public vrrp
```

The following example shows how to send all Cisco Express Forwarding informs to the notification receiver with the IP address 10.56.125.47 using the community string public:

```
Router(config)# snmp-server enable traps cef
Router(config)# snmp-server host 10.56.125.47 informs version 2c public cef
```

Related Commands

Command	Description
snmp-server enable peer-trap poor qov	Enables poor quality of voice notifications for applicable calls associated with a specific voice dial peer.
snmp-server enable traps	Enables SNMP notifications (traps and informs).
snmp-server informs	Specifies inform request options.
snmp-server link trap	Enables linkUp/linkDown SNMP trap that are compliant with RFC 2233.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.

snmp-server informs

To specify inform request options, use the **snmp-server informs** command in global configuration mode. To return settings to their default values, use the **no** form of this command.

snmp-server informs [**retries** *retries*] [**timeout** *seconds*] [**pending** *pending*]

no snmp-server informs [**retries** *retries*] [**timeout** *seconds*] [**pending** *pending*]

Syntax Description

retries	(Optional) Specifies a maximum number of times to resend an inform request.
retries	(Optional) Integer. The default value is 3.
timeout	(Optional) Specifies a number of seconds to wait for an acknowledgment before resending.
seconds	(Optional) Integer. The default is 30.
pending	(Optional) Specifies a maximum number of informs waiting for acknowledgment at any one time. When the maximum is reached, older pending informs are discarded.
pending	(Optional) Integer. The default is 25.

Command Default

Inform requests are resent three times. Informs are resent after 30 seconds if no response is received. The maximum number of informs waiting for acknowledgment at any one time is 25.

Command Modes

Global configuration

Command History

Release	Modification
11.3T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to increase the pending queue size when several informs drop:

```
Router(config)# snmp-server informs pending 50
```

The following example shows how to increase the default timeout when you send informs over slow network links. Because informs will remain in the queue longer than other types of messages, you also may need to increase the pending queue size.

```
snmp-server informs timeout 60 pending 40
```

The following example shows how to decrease the default timeout when you send informs over very fast links:

```
Router(config)# snmp-server informs timeout 5
```

The following example shows how to increase the retry count when you send informs over unreliable links. Because informs will remain in the queue longer than other types of messages, you may need to increase the pending queue size.

```
Router(config)# snmp-server informs retries 10 pending 45
```

Related Commands

Command	Description
snmp-server enable traps	Enables a router to send SNMP traps and informs.

snmp-server location

To set the system location string, 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 *text*

no snmp-server location

Syntax Description

text	String that describes the system location information.

Command Default

No system location string is set.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to set a system location string:

```
Router(config)# snmp-server location Building 3/Room 214
```

Related Commands

Command	Description
snmp-server contact	Sets the system contact (sysContact) string.

snmp-server manager

To start the Simple Network Management Protocol (SNMP) manager process, use the **snmp-server manager** command in global configuration mode. To stop the SNMP manager process, use the **no** form of this command.

snmp-server manager

no snmp-server manager

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The SNMP manager process sends SNMP requests to agents and receives SNMP responses and notifications from agents. When the SNMP manager process is enabled, the router can query other SNMP agents and process incoming SNMP traps.

Most network security policies assume that routers will be accepting SNMP requests, sending SNMP responses, and sending SNMP notifications. With the SNMP manager functionality enabled, the router may also be sending SNMP requests, receiving SNMP responses, and receiving SNMP notifications. The security policy implementation may need to be updated prior to enabling this functionality.

SNMP requests are typically sent to UDP port 161. SNMP responses are typically sent from UDP port 161. SNMP notifications are typically sent to UDP port 162.

Examples

The following example enables the SNMP manager process:

```
Router(config)# snmp-server manager
```

Related Commands

Command	Description
show snmp	Checks the status of SNMP communications.
show snmp pending	Displays the current set of pending SNMP requests.

Command	Description
show snmp sessions	Displays the current SNMP sessions.
snmp-server manager session-timeout	Sets the amount of time before a nonactive session is destroyed.

snmp-server manager session-timeout

To set the amount of time before a nonactive session is destroyed, use the **snmp-server manager session-timeout** command in global configuration mode. To return the value to its default, use the **no** form of this command.

snmp-server manager session-timeout *seconds*

no snmp-server manager session-timeout

Syntax Description

seconds	Number of seconds before an idle session is timed out. The default is 600 seconds.

Command Default

Idle sessions time out after 600 seconds (10 minutes).

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Sessions are created when the SNMP manager in the router sends SNMP requests, such as inform requests, to a host or receives SNMP notifications from a host. One session is created for each destination host. If there is no further communication between the router and host within the session timeout period, the session will be deleted.

The router tracks statistics, such as the average round-trip time required to reach the host, for each session. Using the statistics for a session, the SNMP manager in the router can set reasonable timeout periods for future requests, such as informs, for that host. If the session is deleted, all statistics are lost. If another session with the same host is later created, the request timeout value for replies will return to the default value.

However, sessions consume memory. A reasonable session timeout value should be large enough such that regularly used sessions are not prematurely deleted, yet small enough such that irregularly used, or one-shot sessions, are purged expeditiously.

Examples

The following example sets the session timeout to a larger value than the default:

```
Router(config)# snmp-server manager
Router(config)# snmp-server manager session-timeout 1000
```

Related Commands

Command	Description
show snmp pending	Displays the current set of pending SNMP requests.
show snmp sessions	Displays the current SNMP sessions.
snmp-server manager	Starts the SNMP manager process.

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 *byte-count*

no snmp-server packetsize

Syntax Description

byte-count	Integer from 484 to 8192. The default is 1500.

Command Default

Packet size is not configured.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example establishes a packet filtering of a maximum size of 1024 bytes:

```
Router(config)# snmp-server packetsize 1024
```

Related Commands

Command	Description
snmp-server queue-length	Establishes the message queue length for each trap host.

snmp-server queue-length

To establish the message queue length for each trap host, use the **snmp-server queue-length** command in global configuration mode.

snmp-server queue-length *length*

Syntax Description

length	Integer that specifies the number of trap events that can be held before the queue must be emptied. The default is 10.

Command Default

The queue length is set to 10.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command defines the length of the message queue for each trap host. When a trap message is successfully transmitted, Cisco IOS software will continue to empty the queue but never faster than at a rate of four trap messages per second.

During device bootup, some traps could be dropped because of trap queue overflow on the device. If you think that traps are being dropped, you can increase the size of the trap queue (for example, to 100) to determine if traps can then be sent during bootup.

Examples

The following example shows how to set the Simple Network Management Protocol (SNMP) notification queue to 50 events:

```
Router(config)# snmp-server queue-length 50
```

Related Commands

Command	Description
snmp-server packetsize	Establishes control over the largest SNMP packet size permitted when the SNMP server is receiving a request or generating a reply.

snmp-server source-interface

To specify the interface from which a Simple Network Management Protocol (SNMP) trap originates the informs or traps, use the **snmp-server source-interface** command in global configuration mode. To remove the source designation, use the **no** form of this command.

snmp-server source-interface {**traps** | **informs**} *interface*

no snmp-server source-interface {**traps** | **informs**} [*interface*]

Syntax Description

traps	Specifies SNMP traps.
informs	Specifies SNMP informs.
interface	The interface type and the module and port number of the source interface.

Command Default

No interface is designated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXB2	This command was introduced.
12.2(18)SXF6	The **informs** keyword was added. This command replaced the **snmp-server trap-source** command.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command replaced the **snmp-server trap-source** command.

Note The **snmp-server trap-source** command is available in other versions of Cisco IOS software for backward compatibility.

The source interface must have an IP address. Enter the *interface* argument in the following format: *interface-type module/port*.

An SNMP trap or inform sent from a Cisco SNMP server has a notification IP address of the interface it went out of at that time. Use this command to monitor notifications from a particular interface.

Examples

The following example shows how to specify that Gigabit Ethernet interface 5/2 is the source for all informs:

```
snmp-server source-interface informs gigabitethernet5/2
```

The following example shows how to specify that the Gigabit Ethernet interface 5/3 is the source for all traps:

```
snmp-server source-interface traps gigabitethernet5/3
```

The following example shows how to remove the source designation for all traps for a specific interface:

```
no snmp-server source-interface traps gigabitethernet5/3
```

Related Commands

Command	Description
snmp-server enable traps	Enables a router to send SNMP traps and informs.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which a SNMP trap should originate.

snmp-server system-shutdown

To use the Simple Network Management Protocol (SNMP) message reload feature, the router configuration must include the **snmp-server system-shutdown** command in global configuration mode. To prevent an SNMP system-shutdown request (from an SNMP manager) from resetting the Cisco agent, use the **no** form of this command.

snmp-server system-shutdown

no snmp-server system-shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

This command is not included in the configuration file.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example enables the SNMP message reload feature:

```
Router(config)# snmp-server system-shutdown
```

snmp-server tftp-server-list

Note This command was replaced with the **snmp-server file-transfer access-group** command in Cisco IOS Release 12.4(12). Use the **snmp-server file-transfer access-group** command in Cisco IOS Release 12.4(12) and in later releases.

To limit the TFTP servers used via Simple Network Management Protocol (SNMP) controlled TFTP operations (saving and loading configuration files) to the servers specified in an access list, use the **snmp-server tftp-server-list** command in global configuration mode. To disable this function, use the **no** form of this command.

snmp-server tftp-server-list {*acl-number* | *acl-name*}

no snmp-server tftp-server-list {*acl-number* | *acl-name*}

Syntax Description

acl-number	Integer from 1 to 99 that specifies a standard access control list (standard ACL).
acl-name	String (not to exceed 64 characters) that specifies a standard ACL.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.2	This command was introduced.
12.3(2)T	Support for standard named access lists was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to limit the TFTP servers that can be used for saving and loading configuration files via SNMP to the servers specified in the standard named access list lmnop:

```
Router(config)# snmp-server tftp-server-list lmnop
```

The following example shows how to limit the TFTP servers that can be used for copying configuration files via SNMP to the servers in access list 44:

```
Router(config)# snmp-server tftp-server-list 44
```

snmp-server trap authentication unknown-context

To enable the Simple Network Management Protocol (SNMP) authorization failure (authFail) traps during an unknown context error, use the **snmp-server trap authentication unknown-context** command in global configuration mode. To disable the authFail traps, use the **no** form of this command.

snmp-server trap authentication unknown-context

no snmp-server trap authentication unknown-context

Syntax Description

This command has no arguments or keywords.

Defaults

No authFail traps are generated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXF5	This command was introduced on the Supervisor Engine 720 and the Supervisor Engine 32.

Examples

The following example shows how to enable the authorization failure traps during an unknown context error:

```
Router(config)# snmp-server trap authentication unknown-context
Router(config)#
```

The following example shows how to disable the authorization failure traps during an unknown context error:

```
Router(config)# no snmp-server trap authentication unknown-context
Router(config)#
```

snmp-server trap authentication vrf

To enable virtual private network (VPN) routing and forwarding (VRF) instance context authentication notifications, use the **snmp-server trap authentication vrf** command in global configuration mode. To suppress authentication notifications for Simple Network Management Protocol (SNMP) packets dropped due specifically to VRF context mismatches while keeping all other SNMP authentication notifications enabled, use the **no** form of this command.

snmp-server trap authentication vrf

no snmp-server trap authentication vrf

Syntax Description

This command has no arguments or keywords.

Command Default

No VRF-specific authentication notifications are enabled when SNMP authentication notifications are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **snmp-server enable traps snmp authentication** command controls SNMP authentication traps and the **no** form of this command disables all SNMP authentication failure notifications. The **snmp-server trap authentication vrf** command provides more granular control of these notifications.

With context-based MIB access, SNMP requests on each VRF are tied to a specific context. This context is used for access control. If SNMP contexts are configured for VPNs, any SNMP request not matching the configured context will generate an SNMP authentication failure notification.The **no snmp-server trap authentication vrf** command allows you to suppress the authentication failure notifications that are specific to these VRF contexts, while keeping all other SNMP authentication failure notifications enabled.

The **no snmp-server trap authentication vrf** command has no effect if the **snmp-server enable traps snmp authentication** command has not been configured..

Examples

The following example shows how to enable a router to send SNMP authentication traps to host myhost.cisco.com using the community string public while disabling all VRF authentication traps:

```
Router(config)# snmp-server enable traps snmp authentication
Router(config)# no snmp-server trap authentication vrf
Router(config)# snmp-server host myhost.cisco.com public
```

Related Commands

Command	Description
snmp-server enable traps snmp	Enables the sending of RFC 1157 SNMP notifications.
snmp-server host	Specifies the recipient of an SNMP notification operation.

snmp-server trap link

To enable linkUp/linkDown Simple Network Management Protocol (SNMP) traps that are compliant with RFC2233, use the **snmp-server trap link** command in global configuration mode. To disable IETF-compliant functionality and revert to the default Cisco implementation of linkUp/linkDown traps, use the **no** form of this command.

snmp-server trap link ietf

no snmp-server trap link ietf

Syntax Description

ietf	Notifies the command parser to link functionality of SNMP linkUp/linkDown traps to the Internet Engineering Task Force (IETF) standard (instead of the previous Cisco implementation).

Command Default

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **snmp-server trap link ietf** command is used to configure your router to use the RFC2233 IETF standards-based implementation of linkUp/linkDown traps. This command is disabled by default to allow you to continue using the earlier Cisco implementation of linkUp/linkDown traps if you so choose.

However, please note that when using the default Cisco object definitions, linkUp/linkDown traps are not generated correctly for sub-interfaces. In the default implementation an arbitrary value is used for the *locIfReason* object in linkUp/linkDown traps for sub-interfaces, which may give you unintended results. This is because the *locIfReason* object is not defined for sub-interfaces in the current Cisco implementation, which uses OLD-CISCO-INTERFACES-MIB.my.

If you do not enable this functionality, the link trap varbind list will consist of {ifIndex, ifDescr, ifType, locIfReason}. After you enable this functionality with the **snmp-server trap link ietf** command, the varbind list will consist of {inIndex, ifAdminStatus,ifOperStatus, if Descr, ifType}. The *locIfReason* object will also be conditionally included in this list depending on whether meaningful information can be retrieved for that object. A configured sub-interface will generate retrievable information. On non-HWIDB interfaces, there will be no defined value for *locIfReason*, so it will be omitted from the trap message.

Examples

The following example shows the enabling of the RFC 2233 linkUp/linkDown traps, starting in privileged EXEC mode:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# snmp-server trap link ietf
Router(config)# end
Router# more system:running configuration
.
.
.
!
snmp-server engineID local 00000009000000A1616C2056
snmp-server community public RO
snmp-server community private RW
snmp-server trap link ietf
!
.
.
.
```

Related Commands

Command	Description
debug snmp packets	Displays information about every SNMP packet sent or received by the router for the purposes of troubleshooting.

snmp-server trap link switchover

To enable sending a linkdown trap followed by a linkup trap for every interface in the switch during a switch failover, use the **snmp-server trap link switchover** command in global configuration mode. To disable linkdown during a switch failover, use the **no** form of this command.

snmp-server trap link switchover

no snmp-server trap link switchover

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXF2	This command was introduced on the Supervisor Engine 720 and the Supervisor Engine 32.

Usage Guidelines

By default, no link traps are generated during a switchover.

Examples

This example shows how to enable sending a linkdown trap followed by a linkup trap for every interface in the switch during a switch failover:

```
snmp-server trap link switchover
```

This example shows how to disable linkdown followed by a linkup trap for every interface in the switch during a switch failover:

```
no snmp-server trap link switchover
```

snmp-server trap retry

To define the number of times the Simple Network Management Protocol (SNMP) agent on a device tries to find a route before it sends traps, use the **snmp-server trap retry** command in global configuration mode.

snmp-server trap retry *number*

Syntax Description

number	Integer from 0 to 10 that sets the number of times the message will be retransmitted. The default is 3.

Command Default

Messages are not retransmitted.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRA	This command was introduced.

Usage Guidelines

The SNMP agent looks for a configured route in the system before sending a trap out to a destination. If a route is not present, traps are queued in the trap queue and discarded when the queue becomes full. When the **snmp-server trap retry** command is configured, the route search retry number tells the agent how many times to look for the route before sending the trap out.

Configuring the **snmp-server trap retry** command also ensures that policy-based routing traps are sent and not discarded. Policy-based traps must be sent immediately and routes are not needed. The number of retries must be set to 0 so that policy-based traps are sent immediately.

Examples

The following example shows how to set the number of times a SNMP agent on a device tries to find a route to 10:

```
Router(config)# snmp-server trap retry 10
```

Related Commands

Command	Description
snmp-server trap timeout	Defines an interval of time between retransmissions of traps on a retransmission queue.

snmp-server trap timeout

To define an interval of time between retransmissions of trap messages on a retransmission queue, use the **snmp-server trap timeout** command in global configuration mode.

snmp-server trap timeout *seconds*

Syntax Description

seconds	Integer from 1 to 1000 that sets the interval, in seconds, for resending messages. The default is 30.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRA	This command was introduced. This command replaces the **snmp-server trap-timeout** command in Cisco IOS Release 12.2SR only.

Usage Guidelines

Before a trap is sent, the SNMP agent looks for a route to the destination address. If there is no known route, the trap is saved in a retransmission queue. Issue the **snmp-server trap timeout** command to configure the number of seconds between retransmission attempts.

Examples

The following example shows how to set an interval of 20 seconds between retransmissions of traps:

```
Router(config)# snmp-server trap timeout 20
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server queue-length	Establishes the message queue length for each trap host.

snmp-server trap-authentication

The **snmp-server trap-authentication** command has been replaced by the **snmp-server enable traps snmp authentication** command. See the description of the **snmp-server enable traps snmp** command in this chapter for more information.

snmp-server trap-source

Note Effective with Cisco IOS Release 12.2(18)SXB6, the **snmp-server trap-sourc**e command is replaced by the **snmp-server source-interface** command. See the **snmp-server source-interface** command for more information.

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 the command.

snmp-server trap-source *interface*

no snmp-server trap-source

Syntax Description

interface	Interface from which the SNMP trap originates. Includes the interface type and number in platform-specific syntax (for example, *type slot/port*).

Command Default

No interface is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated in to Cisco IOS Release 12.2(33)SRA.
12.2(18)SXB6	This command was replaced by the **snmp-server source-interface** command in Cisco IOS Release 12.2(18)SXB6.

Usage Guidelines

An SNMP trap or inform sent from a Cisco SNMP server has a notification address of the interface it went out of at that time. Use this command to monitor notifications from a particular interface.

Examples

The following example shows how to set the IP address for Ethernet interface 0 as the source for all SNMP notifications:

```
Router(config)# snmp-server trap-source ethernet 0
```

The following example shows how to set the IP address for the Ethernet interface in slot 2, port 1 as the source for all SNMP notifications:

```
Router(config)# snmp-server trap-source ethernet 2/1
```

Related Commands

Command	Description
snmp-server enable traps	Enables a router to send SNMP traps and informs.
snmp-server host	Specifies the recipient of a SNMP notification operation.

snmp-server trap-timeout

Note This command is not supported in Cisco IOS Release 12.2SR. For Cisco IOS Release12.2SR, use the **snmp-server trap timeout** command.

To define an interval of time before resending trap messages on the retransmission queue, use the **snmp-server trap-timeout** command in global configuration mode.

snmp-server trap-timeout *seconds*

Syntax Description

seconds	Integer from 1 to 1000 that sets the interval, in seconds, for resending messages. The default is 30.

Defaults

30 seconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was replaced by the **snmp-server trap timeout** command in Cisco IOS Release 12.2SR.

Usage Guidelines

The **snmp-server trap-timeout** command remains in Cisco IOS software for compatibility but is written in the configuration as **snmp-server trap timeout**.

Before the Cisco IOS 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. The **snmp-server trap-timeout** command determines the number of seconds between retransmission attempts.

Examples

The following example shows how to set an interval of 20 seconds between resending trap messages on the retransmission queue:

```
Router(config)# snmp-server trap-timeout 20
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server queue-length	Establishes the message queue length for each trap host.

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 group-name* [**remote** *host* [**udp-port** *port*]]
{**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** [**ipv6** *nacl*]
[**priv** {**des** | **3des** | **aes** {**128** | **192** |**256**}} *privpassword*] {*acl-number* | *acl-name*}]

no snmp-server user *username group-name* [**remote** *host* [**udp-port** *port*]]
{**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** [**ipv6** *nacl*]
[**priv** {**des** | **3des** | **aes** {**128** | **192** |**256**}} *privpassword*] {*acl-number* | *acl-name*}]

Syntax Description

username	Name of the user on the host that connects to the agent.
group-name	Name of the group to which the user belongs.
remote	(Optional) Specifies a remote SNMP entity to which the user belongs, and the hostname or IPv6 address or IPv4 IP address of that entity. If both an IPv6 address and IPv4 IP address are being specified, the IPv6 host must be listed first.
host	(Optional) Name or IP address of the remote SNMP host.
udp-port	(Optional) Specifies the UDP port number of the remote host. The default is UDP port 162.
port	(Optional) Integer value that identifies the UDP port.
v1	Specifies that SNMPv1 should be used.
v2c	Specifies that SNMPv2c should be used.
v3	Specifies that the SNMPv3 security model should be used. Allows the use of the **encrypted** or **auth** keywords or both.
encrypted	(Optional) Specifies whether the password appears in encrypted format.
auth	(Optional) Specifies which authentication level should be used.
md5	(Optional) Specifies the HMAC-MD5-96 authentication level.
sha	(Optional) Specifies the HMAC-SHA-96 authentication level.
auth-password	(Optional) String (not to exceed 64 characters) that enables the agent to receive packets from the host.
access	(Optional) Specifies an access control list (ACL) to be associated with this SNMP user.
ipv6	(Optional) Specifies an IPv6 named access list to be associated with this SNMP user. Either IPv4, IPv6, or both IPv4 and IPv6 access lists may be specified. If both are specified, the IPv6 named access list must appear first in the statement.
nacl	(Optional) Name of the ACL.
priv	(Optional) Specifies the use of the User-based Security Model (USM) for SNMP version 3 for SNMP message level security.
des	(Optional) Specifies the use of the 56-bit Digital Encryption Standard (DES) algorithm for encryption.
3des	(Optional) Specifies the use of the 168-bit 3DES algorithm for encryption.

aes	(Optional) Specifies the use of the Advanced Encryption Standard (AES) algorithm for encryption.
128	(Optional) Specifies the use of a 128-bit AES algorithm for encryption.
192	(Optional) Specifies the use of a 192-bit AES algorithm for encryption.
256	(Optional) Specifies the use of a 256-bit AES algorithm for encryption.
privpassword	(Optional) String (not to exceed 64 characters) that specifies the privacy user password.
acl-number	(Optional) Integer in the range from 1 to 99 that specifies a standard access list of IP addresses.
acl-name	(Optional) String (not to exceed 64 characters) that is the name of a standard access list of IP addresses.

Command Default

See Table 84 in the "Usage Guidelines" section for default behaviors for encryption, passwords, and access lists.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.3(2)T	Support for named standard access lists was added.
12.0(27)S	The **ipv6** *nacl* keyword/argument pair was added to allow for configuration of IPv6 named access lists and IPv6 remote hosts.
12.3(14)T	The **ipv6** *nacl* keyword/argument pair to allow for configuration of IPv6 named access lists and IPv6 remote hosts was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **priv** keyword and associated arguments were added to enable the use of the User-based Security Model (USM) for SNMP version 3 for SNMP message level security.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the **snmp-server engineID** command with the **remote** option. The remote agent's SNMP engine ID is needed when computing the authentication and privacy digests from the password. If the remote engine ID is not configured first, the configuration command will fail.

For the *privpassword* and *auth-password* arguments, the minimum length is one character; the recommended length is at least eight characters, and should include both letters and numbers.

Table 84 describes the default user characteristics for encryption, passwords, and access lists.

Table 84 snmp-server user Default Descriptions

Characteristic	Default
encryption	Not present by default. The **encrypted** keyword is used to specify that the passwords are MD5 digests and not text passwords.
passwords	Assumed to be text strings.
access lists	Access from all IP access lists is permitted.
remote users	All users are assumed to be local to this SNMP engine unless you specify they are remote with the **remote** keyword.

SNMP passwords are localized using the SNMP engine ID of the authoritative SNMP engine. For informs, the authoritative SNMP agent is the remote agent. You need to configure the remote agent's SNMP engine ID in the SNMP database before you can send proxy requests or informs to it.

Working with Passwords and Digests

No default values exist for authentication or privacy algorithms when you configure the command. Also, no default passwords exist. The minimum length for a password is one character, although Cisco recommends using at least eight characters for security. If you forget a password, you cannot recover it and will need to reconfigure the user. You can specify either a plain-text password or a localized message digest 5 (MD5) digest.

If you have the localized MD5 or SHA digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd where aa, bb, and cc are hex values. Also, the digest should be exactly 16 octets long.

Examples

The following example shows how to add the user abcd to the public SNMP server group. In this example, no access list is specified for the user, so the standard named access list applied to the group applies to the user.

```
Router(config)# snmp-server user abcd public v2c
```

The following example shows how to add the user abcd to the public group. In this example, access rules from the standard named access list qrst apply to the user.

```
Router(config)# snmp-server user abcd public v2c access qrst
```

In the following example, the plain-text password "cisco123" is configured for the user "abcd" in the SNMPv3 group "public":

```
Router(config)# snmp-server user abcd public v3 auth md5 cisco123
```

When you enter a **show running-config** command, a line for this user will be displayed. To learn if this user has been added to the configuration, type the **show snmp user** command.

If you have the localized MD5 or Secure Hash Algorithm (SHA) digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd where aa, bb, and cc are hex values. Also, the digest should be exactly 16 octets long.

In the following example, the MD5 digest string is used instead of the plain text password:

```
Router(config)# snmp-server user abcd public v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

In the following example, the user "abcd" is removed from the SNMP group "public":

```
Router(config)# no snmp-server user abcd public v2c
```

In the following example, the user "abcd" from the SNMP group "public" specifies the use of the 168-bit 3DES algorithm for privacy encryption with "secure3des" as the password.

```
Router(config)# snmp-server user abcd public priv 3des secure3des
```

Related Commands

Command	Description
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.
show snmp user	Displays information on each SNMP username in the group username table.
snmp-server engineID	Displays the identification of the local SNMP engine and all remote engines that have been configured on the router.

snmp-server view

To create or update a view entry, use the **snmp-server view** command in global configuration mode. To remove the specified Simple Network Management Protocol (SNMP) server view entry, use the **no** form of this command.

snmp-server view *view-name oid-tree* {**included** | **excluded**}

no snmp-server view *view-name*

Syntax Description

view-name	Label for the view record that you are updating or creating. The name is used to reference the record.
oid-tree	Object identifier 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.
included	Configures the OID (and subtree OIDs) specified in *oid-tree* argument to be included in the SNMP view.
excluded	Configures the OID (and subtree OIDs) specified in *oid-tree* argument to be explicitly excluded from the SNMP view.

Command Default

No view entry exists.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command was modified to exclude USM, VACM, and Community MIBs from any parent OIDs in a configured view by default.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Other SNMP commands require an SMP view as an argument. You use this command to create a view to be used as arguments for other commands.

Two standard predefined views can be used when a view is required, instead of defining a view. One is *everything*, which indicates that the user can see all objects. The other is *restricted,* which indicates that the user can see three groups: system, snmpStats, and snmpParties. The predefined views are described in RFC 1447.

Note Beginning in Release 12.0(26)S and 12.2(2)T, the USM, VACM, and Community MIBs are excluded from any parent OIDs in a configured view by default. If you wish to include these MIBs in a view, you must now explicitly include them.

The first **snmp-server** command that you enter enables SNMP on your routing device.

Examples

The following example creates a view that includes all objects in the MIB-II subtree:

```
snmp-server view mib2 mib-2 included
```

The following example creates a view that includes all objects in the MIB-II system group and all objects in the Cisco enterprise MIB:

```
snmp-server view root_view system included
snmp-server view root_view cisco included
```

The following example creates 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:

```
snmp-server view agon system included
snmp-server view agon system.7 excluded
snmp-server view agon ifEntry.*.1 included
```

In the following example, the USM, VACM, and Community MIBs are explicitly included in the view “test” with all other MIBs under the root parent “internet”:

```
! -- include all MIBs under the parent tree “internet”
snmp-server view test internet included
! -- include snmpUsmMIB
snmp-server view test 1.3.6.1.6.3.15 included
! -- include snmpVacmMIB
snmp-server view test 1.3.6.1.6.3.16 included
! -- exclude snmpCommunityMIB
snmp-server view test 1.3.6.1.6.3.18 excluded
```

Related Commands

Command	Description
snmp-server community	Sets up the community access string to permit access to the SNMP protocol.

snmp trap ip verify drop-rate

To configure the router to send a simple network management protocol (SNMP) notification when the unicast reverse path forwarding (URPF) drop rate exceeds the configured threshold, use the **snmp trap ip verify drop-rate** command in interface configuration mode. To disable SNMP notification, use the **no** form of this command.

snmp trap ip verify drop-rate

no snmp trap ip verify drop-rate

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled (no SNMP notifications are sent).

Command Modes

Interface configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS 12.2(33)SRC.

Usage Guidelines

This command enables **cipUrpfIfDropRateNotify** notification. This notification is sent when the URPF drop rate exceeds the threshold.

Examples

The following example shows how to configure SNMP notification for the URPF drop rate:

```
snmp trap ip verify drop-rate
```

Related Commands

Command	Description
ip verify drop-rate compute window	Configures the interval of time over which the URPF drop count used in the drop rate computation is collected.
ip verify unicast notification threshold	Configures the URPF drop count threshold which, when exceeded, triggers a notification.

snmp trap link-status

To enable Simple Network Management Protocol (SNMP) link trap generation, use the **snmp trap link-status** command in interface configuration mode. To disable SNMP link traps, use the **no** form of this command.

snmp trap link-status [**permit duplicates**]

no snmp trap link-status [**permit duplicates**]

Syntax Description.

permit duplicates	(Optional) Permits duplicate SNMP linkup and linkdown traps.

Command Default

SNMP link traps are sent when an interface goes up or down.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(30)S	The **permit duplicates** keyword pair was added in Cisco IOS Release 12.2(30)S.
12.3(8)T	Support for the **permit duplicates** keyword pair was integrated in Cisco IOS Release 12.3(8)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

By default, SNMP link traps are sent when an interface goes up or down. For interfaces expected to go up and down during normal usage, such as ISDN interfaces, the output generated by these traps may not be useful. The **no** form of this command disables these traps.

The **permit** and **duplicates** keywords are used together and cannot be used individually. Use the **permit duplicates** keyword pair when an interface is not generating SNMP linkup traps, linkdown traps, or both. When the **snmp trap link-status permit duplicates** command is configured, more than one trap may be sent for the same linkup or linkdown transition.

The **permit duplicates** keyword pair does not guarantee that SNMP link traps will be generated nor should configuring these keywords be required to receive traps.

Examples

The following example shows how to disable the sending of SNMP link traps related to the ISDN BRI 0 interface:

```
Router(config)# interface bri 0
Router(config-if)# no snmp trap link-status
```

sntp broadcast client

To use the Simple Network Time Protocol (SNTP) to accept Network Time Protocol (NTP) traffic from any broadcast server, use the **sntp broadcast client** command in global configuration mode to configure a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router. To prevent the router from accepting broadcast traffic, use the **no** form of this command.

sntp broadcast client

no sntp broadcast client

Syntax Description

This command has no arguments or keywords.

Defaults

The router does not accept SNTP traffic from broadcast servers.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNTP is a compact, client-only version of the NTP. SNMP can only receive the time from NTP servers; it cannot be used to provide time services to other systems.

SNTP typically provides time within 100 milliseconds of the accurate time, but it does not provide the complex filtering and statistical mechanisms of NTP. In addition, SNTP does not authenticate traffic, although you can configure extended access lists to provide some protection.

You must configure the router with either this command or the **sntp server** global configuration command to enable SNTP.

Examples

The following example enables the router to accept broadcast NTP packets and shows sample **show sntp** command output:

```
Router(config)# sntp broadcast client
Router(config)# end
Router#
%SYS-5-CONFIG: Configured from console by console
Router# show sntp
```

```
SNTP server     Stratum   Version    Last Receive
172.21.28.34       4         3        00:00:36    Synced  Bcast

Broadcast client mode is enabled.
```

Related Commands

Command	Description
show sntp	Displays information about SNTP on a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router.
sntp server	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to request and accept NTP traffic from a time server.

sntp logging

To enable Simple Network Time Protocol (SNTP) message logging, use the **sntp logging** command in global configuration mode. To disable SNTP logging, use the **no** form of this command.

sntp logging

no sntp logging

Syntax Description

This command has no arguments or keywords.

Defaults

SNTP message logging is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use the **sntp logging** command to control the display of SNTP logging messages.

SNTP is a compact, client-only version of Network Time Protocol (NTP). SNTP can be used only to receive the time from NTP servers; SNTP cannot be used to provide time services to other systems. You should consider carefully the use of SNTP rather than NTP in primary servers.

Examples

The following example shows how to enable SNTP message logging, configure the IP address of the SNTP server as 10.107.166.3, and verify that SNTP logging is enabled:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# sntp logging

Router(config)# sntp server 10.107.166.3

Router(config)# end

Router#
04:02:54: %SYS-5-CONFIG_I: Configured from console by console
Router#

Router# show running-config | include ntp

sntp logging
sntp server 10.107.166.3
```

The “sntp logging” entry in the configuration file verifies that SNTP message logging is enabled.

The following example shows how to disable SNTP message logging and verify that it is disabled:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# no sntp logging

Router(config)# end

Router#
04:04:34: %SYS-5-CONFIG_I: Configured from console by console

Router# show running-config | include ntp

sntp server 10.107.166.3
```

The “sntp logging” entry no longer appears in the configuration file, which verifies that SNTP message logging is disabled.

Related Commands

Command	Description
show sntp	Displays information about SNTP on a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router.
sntp broadcast client	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to accept NTP traffic from any broadcast server.
sntp server	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to request and accept NTP traffic from a time server.

sntp server

To configure a Cisco 800, Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use the Simple Network Time Protocol (SNTP) to request and accept Network Time Protocol (NTP) traffic from a stratum 1 time server, use the **sntp server** command in global configuration mode. To remove a server from the list of NTP servers, use the **no** form of this command.

sntp server {*address* | *hostname*} [**version** *number*]

no sntp server {*address* | *hostname*}

Syntax Description

address	IP address of the time server.
hostname	Host name of the time server.
version *number*	(Optional) Version of NTP to use. The default is 1.

Defaults

The router does not accept SNTP traffic from a time server.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNTP is a compact, client-only version of the NTP. SNMP can only receive the time from NTP servers; it cannot be used to provide time services to other systems.

SNTP typically provides time within 100 milliseconds of the accurate time, but it does not provide the complex filtering and statistical mechanisms of NTP. In addition, SNTP does not authenticate traffic, although you can configure extended access lists to provide some protection.

Enter this command once for each NTP server.

You must configure the router with either this command or the **sntp broadcast client** global configuration command in order to enable SNTP.

SNTP time servers should operate only at the root (stratum 1) of the subnet, and then only in configurations where no other source of synchronization other than a reliable radio or modem time service is available. A stratum 2 server cannot be used as an SNTP time server. The use of SNTP rather than NTP in primary servers should be carefully considered.

Examples

The following example enables the router to request and accept NTP packets from the server at 172.21.118.9 and displays sample **show sntp** command output:

```
Router(config)# sntp server 172.21.118.9
Router(config)# end
Router#
%SYS-5-CONFIG: Configured from console by console
Router# show sntp

SNTP server     Stratum   Version    Last Receive
172.21.118.9       5         3        00:01:02    Synced
```

Related Commands

Command	Description
show sntp	Displays information about SNTP on a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router.
sntp broadcast client	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to accept NTP traffic from any broadcast server.

sntp source-interface

To use a particular source address in Simple Network Time Protocol (SNTP) packets, use the **sntp source-interface** command in global configuration mode. To remove the specified source address, use the **no** form of this command.

sntp source-interface *type number*

no sntp source-interface

Syntax Description

type	Type of interface.
number	Number of the interface.

Command Default

The source address is determined by the outgoing interface.

Command Modes

Global configuration

Command History

Release	Modification
12.4(10)	This command was introduced.

Usage Guidelines

Use this command to specify a particular source IP address for all SNTP packets. The address is taken from the named interface. This command is useful if the address on an interface cannot be used as the destination for reply packets. The **no** form of the command only replaces the default; that is, the source address of the SNTP request sent is determined by the outgoing interface.

If this command is the last one issued and you then remove it, the SNTP process stops.

Examples

The following example shows how to configure a router to use the IP address of interface Ethernet 0 as the source address for all outgoing SNTP packets:

```
Router(config)# sntp source-interface ethernet 0
```

The following example shows how to remove a configured SNTP option:

```
Router(config)# no sntp source-interface
```

system (ERM policy)

To configure system level resource owners (ROs), use the **system** command in Embedded Resource Manager (ERM) policy configuration mode.

system

Syntax Description

This command has no arguments or keywords.

Command Default

No system level ROs are configured.

Command Modes

ERM policy configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Examples

The following example shows how to configure system level ROs:

```
Router(config-erm-policy)# system
```

Related Commands

Command	Description
buffer public	Enters the buffer owner configuration mode and sets thresholds for buffer usage.
cpu interrupt	Enters the CPU owner configuration mode and sets thresholds for interrupt level CPU utilization.
cpu process	Enters the CPU owner configuration mode and sets thresholds for processor level CPU utilization.
cpu total	Enters the CPU owner configuration mode and sets thresholds for total CPU utilization.
critical rising	Sets the critical level threshold values for the buffer, CPU, and memory ROs.
major rising	Sets the major level threshold values for the buffer, CPU, and memory ROs.
memory io	Enters the memory owner configuration mode and sets threshold values for I/O memory.
memory processor	Enters the memory owner configuration mode and sets threshold values for processor memory.
minor rising	Sets the minor level threshold values for the buffer, CPU, and memory ROs.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.

tclsafe

To enable the interactive Tool Command Language (Tcl) shell untrusted safe mode, use the **tclsafe** command in privileged EXEC mode. To exit from the safe mode, use the **exit** or the **tclquit** command.

tclsafe

exit | **tclquit**

Syntax Description

This command has no arguments or keywords.

Command Default

The Tcl shell untrusted safe mode is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the **tclsafe** command when you want to manually run Tcl commands from the Cisco IOS command-line interface (CLI) in untrusted safe mode. When you use the **tclsafe** command and enter the interactive Tcl shell safe mode, you can explore the safe mode Tcl commands that are available. When a script fails the signature check for a configured trustpoint name, it is determined to be untrusted. Untrusted Tcl scripts execute in limited safe mode, if **scripting tcl trustpoint untrusted safe-execute** command is configured. In order to get a better understanding of what is available in this limited safe mode, use the **tclsafe** Exec command to explore the options.

After Tcl commands are entered they are sent to a Tcl interpreter. If the commands are recognized as valid Tcl commands, the command is executed and the result is sent to the tty. If a command is not a recognized Tcl command, it is sent to the Cisco IOS CLI parser. If the command is not a Tcl or Cisco IOS command, two error messages are displayed.

A predefined Tcl script can be created outside of Cisco IOS software, transferred to flash or disk memory, and run within Cisco IOS software. It is also possible to create a Tcl script and precompile the code before running it under Cisco IOS software. To exit from this mode, use the **exit** or the **tclquit** command to disable the use of the Tcl shell and return to privileged EXEC mode.

You can also use the **tclsafe** command with a script name such as **tclsafe disk0:hello.tcl**. The script **hello.tcl** executes immediately and allows you to exit from the untrusted safe mode and return to privileged EXEC mode.

Examples

The following example shows how to enable the Tcl shell untrusted safe mode and run **info commands**:

```
Router# tclsafe
Router(safe)(tcl)# info commands
info commands
```

```
tell socket subst open eof glob list pid time eval lrange tcl_trace fblocked lsearch gets
case lappend proc break variable llength return linsert error catch clock info split array
if fconfigure concat join lreplace source fcopy global switch update close cd for file
append format read package set binary namespace scan seek while flush after vwait uplevel
continue hostname foreach rename fileevent regexp upvar unset encoding expr load regsub
interp history puts incr lindex lsort string
```

The following example shows how to execute the script **hello.tcl** to exit from the untrusted safe mode and return to privileged EXEC mode.

```
Router# tclsafe disk0:hello.tcl
```

Related Commands

Command	Description
scripting tcl trustpoint untrusted	Allows the interactive Tcl scripts to run regardless of the scripts failing the signature check.
tclquit	Quits Tcl shell.
tclsh	Enables the interactive Tcl shell and enters Tcl configuration mode.

tclsh

To enable the interactive Tool Command Language (Tcl) shell, use the **tclsh** command in privileged EXEC mode.

tclsh

Syntax Description

This command has no arguments or keywords.

Defaults

The Tcl shell is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **tclsh** command when you want to run Tcl commands from the Cisco IOS command-line interface (CLI). When the interactive Tcl shell is enabled and Tcl configuration mode is entered, Tcl commands can be entered line by line or a predefined Tcl script can be run. After Tcl commands are entered they are sent to a Tcl interpreter. If the commands are recognized as valid Tcl commands, the command is executed and the result is sent to the tty. If a command is not a recognized Tcl command, it is sent to the Cisco IOS CLI parser. If the command is not a Tcl or Cisco IOS command, two error messages will be displayed.

A predefined Tcl script can be created outside of Cisco IOS software, transferred to Flash or disk memory, and run within Cisco IOS software. It is also possible to create a Tcl script and precompile the code before running it under Cisco IOS.

Use the Cisco IOS CLI **exit** or the Tcl **tclquit** command to disable the use of the Tcl shell and return to privileged EXEC mode.

Examples

The following example shows how to enable the Tcl interactive shell:

```
Router# tclsh
Router(tcl)#
```

template (cns)

To specify a list of Cisco Networking Services (CNS) connect templates within a CNS connect profile to be applied to a router's configuration, use the **template** command in CNS connect configuration mode. To disable this CNS connect template, use the **no** form of this command.

template *name* [...*name*]

no template *name* [...*name*]

Syntax Description

name	Name of the CNS connect template to be applied to a router's configuration.
[...*name*]	Multiple *name* arguments, which are delimited by a single space. The ellipsis (...) in the command syntax indicates that the command input can include multiple names.

Command Default

No CNS connect templates are specified.

Command Modes

CNS connect configuration

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9).

Usage Guidelines

First use the **cns connect** command to enter CNS connect configuration mode and define the parameters of a CNS connect profile for connecting to the CNS configuration engine. Then use the following CNS connect commands to create a CNS connect profile:

- **discover**
- **template**

A CNS connect profile specifies the **discover** commands and associated **template** commands that are to be applied to a router's configuration. The **template** command specifies the list of CNS connect templates that is to be applied to a router's configuration. The templates in the list are applied one at a time. That is, when the **template** command is processed, the first template in the list is applied to the router's configuration. The router then tries to ping the CNS configuration engine. If the ping fails, then the first template in the list is removed from the router's configuration and the second template in the list is applied and so on.

The configuration mode in which the CNS connect templates are applied is specified by the immediately preceding **discover** command. (If there are no preceding **discover** commands, the templates are applied in global configuration mode.) When multiple **discover** and **template** commands are configured in a CNS connect profile, they are processed in the order in which they are entered.

Examples

The following example shows how to create a CNS connect profile named profile-1:

```
Router(config)# cns connect profile-1
Router(config-cns-conn)# discover interface Serial
Router(config-cns-conn)# template temp-A1 temp-A2
Router(config-cns-conn)# template temp-B1 temp-B2
Router(config-cns-conn)# exit
Router(config)#
```

In this example, the following sequence of events occur for all serial interfaces when the **cns connect profile-1** command is processed. Assume all ping attempts to the CNS configuration engine are unsuccessful.

1. Enter interface configuration mode and apply all commands in the temp-A1 template to the router's configuration.
2. Enter interface configuration mode and apply all commands in the temp-B1 template to the router's configuration.
3. Try to ping the CNS configuration engine.
4. Enter interface configuration mode and remove all commands in the temp-B1 template from the router's configuration.
5. Enter interface configuration mode and apply all commands in the temp-B2 template to the router's configuration.
6. Try to ping the CNS configuration engine.
7. Enter interface configuration mode and remove all commands in the temp-B2 template from the router's configuration.
8. Enter interface configuration mode and remove all commands in the temp-A1 template from the router's configuration.
9. Enter interface configuration mode and apply all commands in the temp-A2 template to the router's configuration.
10. Enter interface configuration mode and apply all commands in the temp-B1 template to the router's configuration.
11. Try to ping the CNS configuration engine.
12. Enter interface configuration mode and remove all commands in the temp-B1 template from the router's configuration.
13. Enter interface configuration mode and apply all commands in the temp-B2 template to the router's configuration.
14. Try to ping the CNS configuration engine.
15. Enter interface configuration mode and remove all commands in the temp-B2 template from the router's configuration.
16. Enter interface configuration mode and remove all commands in the temp-A2 template from the router's configuration.

Related Commands

Command	Description
cli (cns)	Specifies the command lines of a CNS connect template.
cns connect	Enters CNS connect configuration mode and defines the parameters of a CNS connect profile for connecting to the CNS configuration engine.

Command	Description
cns template connect	Enters CNS template connect configuration mode and defines the name of a CNS connect template.
discover (cns)	Defines the interface parameters within a CNS connect profile for connecting to the CNS configuration engine.

time-period

To set the time increment for automatically saving an archive file of the current running configuration in the Cisco IOS configuration archive, use the **time-period** command in archive configuration mode. To disable this function, use the **no** form of this command.

time-period *minutes*

no time-period *minutes*

Syntax Description

minutes	Specifies how often, in minutes, to automatically save an archive file of the current running configuration in the Cisco IOS configuration archive.

Command Default

By default, no time increment is set.

Command Modes

Archive configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was implemented on the Cisco 10000 series router.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Note Before using this command, you must configure the **path** command to specify the location and filename prefix for the files in the Cisco IOS configuration archive.

If this command is configured, an archive file of the current running configuration is automatically saved after the given time specified by the *minutes* argument. Archive files continue to be automatically saved at this given time increment until this function is disabled. Use the **maximum** command to set the maximum number of archive files of the running configuration to be saved.

Note This command saves the current running configuration to the configuration archive whether or not the running configuration has been modified since the last archive file was saved.

Examples

In the following example, a value of 20 minutes is set as the time increment for which to automatically save an archive file of the current running configuration in the Cisco IOS configuration archive:

```
Router# configure terminal
!
Router(config)# archive
Router(config-archive)# path disk0:myconfig
Router(config-archive)# time-period 20
Router(config-archive)# end
```

Related Commands

Command	Description
archive config	Saves a copy of the current running configuration to the Cisco IOS configuration archive.
configure confirm	Confirms replacement of the current running configuration with a saved Cisco IOS configuration file.
configure replace	Replaces the current running configuration with a saved Cisco IOS configuration file.
maximum	Sets the maximum number of archive files of the running configuration to be saved in the Cisco IOS configuration archive.
path	Specifies the location and filename prefix for the files in the Cisco IOS configuration archive.
show archive	Displays information about the files saved in the Cisco IOS configuration archive.

time-range

To enable time-range configuration mode and define time ranges for functions (such as extended access lists), use the **time-range** command in global configuration or webvpn context configuration mode. To remove the time limitation, use the **no** form of this command.

time-range *time-range-name*

no time-range *time-range-name*

Syntax Description

time-range-name	Desired name for the time range. The name cannot contain either a space or quotation mark, and it must begin with a letter.

Command Default

None

Command Modes

Global configuration
Webvpn context configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(17a)SX	Support for this command was implemented on the Cisco 7600 series routers.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was available in webvpn context configuration mode.

Usage Guidelines

The **time-range** entries are identified by a name, which is referred to by one or more other configuration commands. Multiple time ranges can occur in a single access list or other feature.

Note In Cisco IOS 12.2SX releases, IP and IPX-extended access lists are the only types of access lists that can use time ranges.

After the **time-range** command, use the **periodic** time-range configuration command, the **absolute** time-range configuration command, or some combination of them to define when the feature is in effect. Multiple **periodic** commands are allowed in a time range; only one **absolute** command is allowed.

Tip To avoid confusion, use different names for time ranges and named access lists.

Examples

The following example denies HTTP traffic on Monday through Friday from 8:00 a.m. to 6:00 p.m. The example allows UDP traffic on Saturday and Sunday from noon to midnight only.

```
time-range no-http
 periodic weekdays 8:00 to 18:00
!
time-range udp-yes
 periodic weekend 12:00 to 24:00
!
ip access-list extended strict
 deny tcp any any eq http time-range no-http
 permit udp any any time-range udp-yes
!
interface ethernet 0
 ip access-group strict in
```

Related Commands

Command	Description
absolute	Specifies an absolute start and end time for a time range.
ip access-list	Defines an IP access list by name.
periodic	Specifies a recurring (weekly) start and end time for a time range.
permit (IP)	Sets conditions under which a packet passes a named IP access list.

track stub

To create a stub object that can be tracked by Embedded Event Manager (EEM) and to enter tracking configuration mode, use the **track stub** command in global configuration mode. To remove the stub object, use the **no** form of this command.

track *object-number* **stub**

no track *object-number* **stub**

Syntax Description

object-number	Object number that represents the object to be tracked. The range is from 1 to 500.

Command Default

No stub objects are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(31)SB3	This command was integrated into Cisco IOS Release 12.2(31)SB3.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use the **track stub** command to create a stub object, which is an object that can be tracked and manipulated by an external process, EEM. After the stub object is created, the **default-state** command can be used to set the default state of the stub object.

EEM is a distributed, scalable, and customized approach to event detection and recovery offered directly in a Cisco IOS device. EEM offers the ability to monitor events and take informational or corrective action when the monitored events occur or when a threshold is reached. An EEM policy is an entity that defines an event and the actions to be taken when that event occurs.

Examples

In the following example, stub object 1 is created and configured with a default state of up.

```
track 1 stub
 default-state up
```

Related Commands

Command	Description
default-state	Sets the default state for a stub object.
show track	Displays tracking information.

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 (config-bulk-tr)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

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 will still be initiated, and bulk statistics MIB data will be collected into a new file in the system buffer.

Examples

The following example shows how to configure a transfer interval of 20 minutes for the bulk statistics configuration bulkstat1:

```
Router(config)# snmp mib bulkstat transfer bulkstat1

Router(config-bulk-tr)# transfer-interval 20
```

Related Commands

Command	Description
snmp mib bulkstat transfer	Names a bulk statistics transfer configuration and enters Bulk Statistics Transfer configuration mode.

transport event

To specify that inventory events are sent out by the CNS inventory agent, use the **transport event** command in CNS inventory configuration mode. To disable the transport of inventory events, use the **no** form of this command.

transport event

no transport event

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

CNS inventory configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to send out inventory requests with each CNS inventory agent message. When configured, the routing device will respond to queries from the CNS event bus. Online insertion and removal (OIR) events on the routing device will be reported to the CNS event bus.

Examples

The following example shows how to enable the CNS inventory agent and configure it to send out inventory events:

```
Router(config)# cns inventory
Router(cns_inv)# transport event
```

Related Commands

Command	Description
cns inventory	Enables the CNS inventory agent and enters CNS inventory configuration mode.

ttl dns

To configure the number of seconds for which an answer received from the boomerang client will be cached by the Domain Name System (DNS) client, use the **ttl dns** command in boomerang configuration mode. To remove this 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.

ttl dns *seconds*

no ttl dns *seconds*

Syntax Description

seconds	Integer in the range from 10 to 2147483647 that specifies the number of seconds for which an answer received from the boomerang client will be cached by the DNS client.

Command Default

No default behavior or values.

Command Modes

Boomerang configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **ttl dns** command can be used only on a Director Response Protocol (DRP) agent. The boomerang client is the DRP agent.

The **ttl dns** command configures the number of seconds for which the DNS client can cache a boomerang reply from a boomerang client.

Examples

In the following example, the number of seconds for which the DNS client can cache a boomerang reply from a boomerang client is configured as 10:

```
Router(config)# ip drp domain www.boom1.com
Router(config-boomerang)# ttl dns 10

Router# show running-config
.
.
.
ip drp domain www.boom1.com
dns-ttl 10
```

Related Commands

Command	Description
alias (boomerang configuration)	Configures an alias name for a specified domain.
ip drp domain	Adds a new domain to the DistributedDirector client or configures an existing domain and puts the client in boomerang configuration mode.
server (boomerang configuration)	Configures the server address for a specified boomerang domain.
show ip drp	Displays DRP statistics on DistributedDirector or a DRP server agent.
show ip drp boomerang	Displays boomerang information on the DRP agent.
ttl ip	Configures the IP TTL value for the boomerang response packets sent from the boomerang client to the DNS client in number of hops.

ttl ip

To configure the IP time-to-live (TTL) value for the boomerang response packets sent from the boomerang client to the DNS client, use the **ttl ip** command in boomerang configuration mode. To remove this 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.

ttl ip *hops*

no ttl ip *hops*

Syntax Description

hops	Integer in the range from 1 to 255 that specifies the number of hops that occur between the boomerang client and the DNS client before the boomerang response packet fails.

Command Default

No default behavior or values.

Command Modes

Boomerang configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **ttl ip** command can be used only on a Director Response Protocol (DRP) agent. The boomerang client is the DRP agent.

The **ttl ip** command configures the maximum number of hops allowed between the boomerang client and the DNS client, after which the boomerang response packet fails. If the user wants to restrict the contending proxies only to nearby ones, the value of the **ttl ip** command can be set to a specific number within the allowed range. Any proxy outside of this range will be automatically disqualified in the boomerang race because its replies will never reach the DNS client. Because the **ttl ip** command specifies the number of hops for which a response from a client will live, it allows faraway proxies to avoid wasting bandwidth.

Examples

In the following example, the number of hops that occur between the boomerang client and the DNS client before the boomerang response packet fails is configured as 2:

```
Router(config)# ip drp domain www.boom1.com
Router(config-boomerang)# ttl ip 2

Router# show running-config
.
.
.
ip drp domain www.boom1.com
ip-ttl 2
```

Related Commands

Command	Description
alias (boomerang)	Configures an alias name for a specified domain.
ip drp domain	Adds a new domain to the DistributedDirector client or configures an existing domain and puts the client in boomerang configuration mode.
server (boomerang)	Configures the server address for a specified boomerang domain.
show ip drp	Displays DRP statistics on DistributedDirector or a DRP server agent.
show ip drp boomerang	Displays boomerang information on the DRP agent.
ttl dns	Configures the number of seconds for which an answer received from the boomerang client will be cached by the DNS client.

url (bulkstat)

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, RCP, or TFTP. The Cisco IOS File System (IFS) syntax for these URLs is as follows: • **ftp:**[[[//*username* [:*password*]@]*location*]/*directory*]/*filename* • **rcp:**[[[//*username*@]*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 (config-bulk-tr)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

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.

Examples

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.

```
Router(config)# snmp mib bulkstat transfer ifMibTesting
Router(config-bulk-tr)# schema carMibTesting1
Router(config-bulk-tr)# schema carMibTesting2
Router(config-bulk-tr)# format bulkBinary
Router(config-bulk-tr)# transfer-interval 60
Router(config-bulk-tr)# buffer-size 10000
Router(config-bulk-tr)# url primary ftp://user2:pswd@192.168.10.5/functionality/
Router(config-bulk-tr)# url secondary tftp://user2@192.168.10.8/tftpboot/
Router(config-bulk-tr)# buffer-size 2500000
Router(config-bulk-tr)# enable
Router(config-bulk-tr)# exit
```

Related Commands

Command	Description
retry (bulkstat)	Configures the number of retries that should be attempted for sending bulk statistics files.
snmp mib bulkstat transfer	Names a bulk statistics transfer configuration and enters Bulk Statistics Transfer configuration mode.

user (ERM)

To apply a global policy, create a resource group, or add resource users (RUs) to a resource group, use the **user** command in Embedded Resource Manager (ERM) configuration mode. To disable applying the policy, use the **no** form of this command.

user {*resource-instance-name resource-user-type resource-policy-name* | **global** *global-policy-name* | **group** *resource-group-name* **type** *resource-user-type*}

no user {*resource-instance-name resource-user-type resource-policy-name* | **global** *global-policy-name* | **group** *resource-group-name* **type** *resource-user-type*}

Syntax Description

resource-instance-name	Name of the RU to which you are applying a policy.
resource-user-type	Name of the RU type.
resource-policy-name	Name of the policy you are applying to the specified RU.
global	Applies a global policy.
global-policy-name	Name of the global policy you are applying.
group	Specifies a resource group to which the policy is being applied.
resource-group-name	Name of the resource group to which the policy is being applied.
type	Specifies the type of the RU to which the policy is being applied.
resource-user-type	Name of the RU type to which the policy is being applied.

Command Default

No policy is configured.

Command Modes

ERM configuration (config-erm)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command helps you to apply the various policies (system global, per-user local, and user global) to resource owners (ROs), RUs, or a group of RUs.

Use the **user** *resource-instance-name resource-user-type resource-policy-name* command to apply a specified policy to a RU. This policy is also known as a per-user local policy or per-user template.

Use the **user global** *global-policy-name* command to apply a global thresholding policy to all the users.

Use the **user group** *resource-group-name* **type** *resource-user-type* command to create a resource group and to enter resource group configuration mode. After you create the resource group, you can add RUs using the **instance** *instance-name* command and apply the same thresholding policy to all the RUs against the resource group using the **policy** *policy-name* command in resource group configuration mode.

For example, you created a resource group named lowPrioUsers with a type of iosprocess. You have low-priority RUs or tasks such as HTTP and Simple Network Management Protocol (SNMP), and you want to set a threshold for all the low-priority RUs as a group. You must add the RUs to the resource group using the **instance** *instance-name* command and then apply a resource policy. If the resource policy you apply sets a minor rising threshold value of 10 percent for the resource group, when the accumulated usage of both HTTP and SNMP RUs crosses the 10 percent mark, a notification is sent to the RUs in the resource group lowPrioUsers. That is, if HTTP usage is 4 percent and SNMP usage is 7 percent, a notification is sent to lowPrioUsers.

Examples

The following example shows how to apply a per-user thresholding policy for the resource instance EXEC, resource user type iosprocess, and resource policy name policy-test1:

```
Router(config-erm)# user EXEC iosprocess policy-test1
```

The following example shows how to apply a global thresholding policy with policy name global-global-test1:

```
Router(config-erm)# user global global-global-test1
```

The following example shows how to create a resource group with the resource group name lowPrioUsers and RU type as iosprocess, and how to add the RU HTTP to the resource group and apply a thresholding policy group-policy1:

```
Router(config-erm)# user group lowPrioUsers type iosprocess
Router(config-res-group)# instance http
Router(config-res-group)# policy group-policy1
```

Related Commands

Command	Description
instance (resource group)	Adds RUs to a resource group.
policy (ERM)	Configures an ERM resource policy.
policy (resource group)	Applies the same policy to all the RUs in a resource group.
resource policy	Enters ERM configuration mode.
show resource all	Displays resource details for all RUs.

write mib-data

To save MIB data to system memory (NVRAM) for MIB Data Persistence, use the **write mib-data** command in EXEC mode.

write mib-data

Syntax Description

This command has no arguments or keywords.

Command Modes

Exec

Command History

Release	Modification
12.2(2)T	This command was introduced as part of the "Circuit Interface Identification Persistence for SNMP" feature.
12.2(4)T	MIB Data Persistence for the Event and Expression MIBs was introduced as part of the "Distributed Management Event and Expression MIB Persistence" feature.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The MIB Data Persistence feature allows the SNMP data of a MIB to be persistent across reloads; that is, the values of certain MIB objects are retained even if your networking device reboots.

To determine which MIBs support "MIB Persistence" in your release, use the **snmp mib persist ?** command in global configuration mode.

Any modified MIB data must be written to NVRAM memory using the **write mib-data** command. If the **write mib-data** command is not used, modified MIB data is not saved automatically, even if MIB Persistence is enabled. Executing the **write mib-data** command saves only the current MIB data; if the MIB object values are changed, you should reenter the **write mib-data** command to ensure that those values are persistent across reboots.

Examples

In the following example. Event MIB Persistence and Circuit MIB persistence are enabled, and any currenly set object values for those MIBs are saved to NVRAM:

```
Router# configure terminal
Router(config)# snmp mib persist circuit
Router(config)# snmp mib persist event
Router(config)# end
Router# write mib-data
```

Related Commands

Command	Description
snmp mib persist	Enables MIB data persistence.

xsm

To enable XML Subscription Manager (XSM) client access to the device, use the **xsm** command in global configuration mode. To disable XSM client access to the device, use the **no** form of this command.

xsm

no xsm

Syntax Description

This command has no arguments or keywords.

Command Default

XSM client access to the device is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command requires that the **ip http server** command is enabled. Enabling the **xsm** command also enables the **xsm vdm** and **xsm edm** commands. This command must be enabled for the XSM client (such as VPN Device Manager [VDM]) to operate.

Examples

In the following example, access by remote XSM clients to XSM data on the device is disabled:

```
Router# no xsm
```

Related Commands

Command	Description
ip http server	Enables a device to be reconfigured through the Cisco browser interface.
show xsm status	Displays information and status about clients subscribed to the XSM server.
show xsm xrd-list	Displays all XRDs for clients subscribed to the XSM server.
xsm dvdm	Grants access to switch operations.

Command	Description
xsm edm	Grants access to EDM monitoring and configuration data.
xsm vdm	Grants access to VPN-specific monitoring and configuration data.

xsm dvdm

To enable switch-specific configuration data (for example, configuring switch ports and VLANs) when running VPN Device Manager (VDM) on a switch, use the **xsm dvdm** command in global configuration mode. To disable switch-specific configuration data for VDM, use the **no** form of this command.

xsm dvdm

no xsm dvdm

Syntax Description

This command has no arguments or keywords.

Command Default

Access to switch-specific configuration data is enabled when XSM is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(9)YO1	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Access to switch-specific configuration data (dVDM) is enabled by default when XSM is enabled.

The **no xsm dvdm** command allows you to disable only switch-specific XSM data. Note however that disabling dVDM will prevent the VDM application from communicating properly with the device (switch). There is minimal performance impact associated with leaving dVDM enabled.

Examples

In the following example, access to switch-specific configuration data is disabled in XSM:

```
Router(config)# no xsm dvdm
```

Related Commands

Command	Description
xsm	Enables XSM client access to the router.
xsm edm	Grants access to EDM monitoring and configuration data.
xsm history vdm	Enables specific VPN statistics collection on the XSM server.
xsm vdm	Grants access to VPN-specific monitoring and configuration data.

xsm edm

To grant access to Embedded Device Manager (EDM) monitoring and configuration data, use the **xsm edm** command in global configuration mode. To cancel access to EDM monitoring and configuration data, use the **no** form of this command.

xsm edm

no xsm edm

Syntax Description

This command has no arguments or keywords.

Command Default

Access to EDM monitoring and configuration data is granted by default if XSM is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command exists to allow you to disable EDM using the **no xsm edm** form of the command. EDM is enabled by default when XSM is enabled.

EDM provides the following generic information to the VPN Device Manager (VDM):

- Relevant interfaces
- IP routing
- Access-list details
- Basic device health

Note that disabling EDM prevents XSM clients (such as VDM) from working properly and also disables the **xsm history edm** command. There is minimal performance impact associated with leaving EDM enabled.

Examples

In the following example, access to EDM data is disabled:

```
Router(config)# xsm
Router(config)# no xsm edm
```

Related Commands

Command	Description
xsm	Enables XSM client access to the router.
xsm dvdm	Grants access to switch operations.
xsm history edm	Enables statistics collection for the EDM on the XSM server.
xsm vdm	Grants access to VPN-specific monitoring and configuration data.

xsm history edm

To enable statistics collection for the Embedded Device Manager (EDM) on the XML Subscription Manager (XSM) server, use the **xsm history edm** command in global configuration mode. To disable statistics collection for the EDM on the XSM server, use the **no** form of this command.

xsm history edm

no xsm history edm

Syntax Description

This command has no arguments or keywords.

Command Default

EDM statistics collection is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to save up to five days of data. Historical information on items such as RAM and CPU utilization is gathered and made available, thus enabling XSM clients (such as VPN Device Manager [VDM]) to display charts and data. Use of this command consumes resources on the device. Disabling this command clears all your historical data, as the XSM server does not save this data between reloads.

Examples

In the following example, statistics collection for the EDM is enabled on the XSM server:

```
Router(config)# xsm
Router(config)# xsm history edm
```

Related Commands

Command	Description
xsm	Enables XSM client access to the router.

Command	Description
xsm edm	Grants access to EDM monitoring and configuration data.
xsm history vdm	Enables specific VPN statistics collection on the XSM server.

xsm history vdm

To enable specific VPN statistics collection on the XML Subscription Manager (XSM) server, use the **xsm history vdm** command in global configuration mode. To disable collection of specific selected VPN statistics on the XSM server, use the **no** form of this command.

xsm history vdm

no xsm history vdm

Syntax Description

This command has no arguments or keywords.

Command Default

VPN statistics collecting is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

With this command enabled, you can save up to five days of data. Historical information on items such as the number of active IKE tunnels, IPSec tunnels, total crypto throughput, and total throughput is gathered and made available, thus enabling XSM clients (such as VPN Device Manager [VDM]) to display charts and data. Use of this command consumes resources on the device. Disabling this command clears all your historical data. The XSM server does not save history data across reloads.

Examples

The following example shows how to enable specific VPN statistics collection on the XSM server:

```
Router(config)# xsm
Router(config)# xsm history vdm
```

Related Commands

Command	Description
xsm	Enables XSM client access to the router.
xsm history edm	Enables statistics collection for the EDM on the XSM server.
xsm vdm	Grants access to VPN-specific monitoring and configuration data.

xsm privilege configuration level

To enable the XML Subscription Manager (XSM) configuration privilege level required to subscribe to XML Request Descriptors (XRDs), use the **xsm privilege configuration level** command in global configuration mode. To remove a previously configured XSM configuration privilege level, use the **no** form of this command.

xsm privilege configuration level *number*

no xsm privilege configuration level *number*

Syntax Description

number	Integer in the range from 1 to 15 that identifies the privilege level. The default is 15.

Command Default

The default level is 15.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The privilege level for the **xsm privilege configuration level** command must be greater than or equal to the privilege level for the **xsm privilege monitor level** command. For example, if the **xsm privilege configuration 7** command is enabled, you need a minimum privilege level of 7 to subscribe to configuration XRDs. The higher the number the higher the privilege level. Trying to set a conflicting range of privilege settings will force the Cisco device to display the following message:

```
Attempt to set monitor privilege greater than configuration. Privilege denied.
```

You can check the XSM privilege level settings by using the **show xsm status** command. Use the **show xsm xrd-list** command to check which privilege level is required for each XRD.

Note The initial login set by your system administrator determines whether you have the necessary IOS privilege level for actually configuring the Cisco router. Ask your system administrator for more information about privilege levels.

Examples

The following example shows how to set a configuration privilege level of 15, and a monitor privilege level of 11 for subscription to XRDs. Users with a privilege level below 11 are denied access.

```
Router(config)# xsm privilege configuration level 15
Router(config)# xsm privilege monitor level 11
```

Related Commands

Command	Description
privilege	Configures IOS privilege parameters.
xsm privilege monitor level	Enables monitor privilege level to subscribe to XRDs.

xsm privilege monitor level

To enable the XML Subscription Manager (XSM) monitoring privilege level required to subscribe to XML Request Descriptors (XRDs), use the **xsm privilege monitor level** command in global configuration mode. To remove a previously configured XSM monitoring privilege level, use the **no** form of this command.

xsm privilege monitor level *number*

no xsm privilege monitor level *number*

Syntax Description

number	Integer in the range from 1 to 15 that identifies the privilege level. The default is 15.

Command History

The default is level 1.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The privilege level for the **xsm privilege monitor level** command must be less than or equal to the privilege level for the **xsm privilege configuration level** command. For example, if the **xsm privilege monitor 7** command is enabled, you need a minimum privilege level of 7 to subscribe to monitor XRDs. The higher the number the higher the privilege level. Trying to set a conflicting range of privilege settings will force the Cisco device to display the following message:

```
Attempt to set monitor privilege greater than configuration. Privilege denied.
```

You can check the XSM privilege level settings by using the **show xsm status** command. Use the **show xsm xrd-list** command to check which privilege level is required for each XRD.

Note The initial login set by your system administrator determines whether you have the necessary IOS privilege level for actually configuring the Cisco router. Ask your system administrator for more information about privilege levels.

Examples

The following example shows how to set a configuration privilege level of 15 and a monitor privilege level of 11 for subscription to XRDs. Users with a privilege level below 11 are denied access.

```
Router(config)# xsm privilege configuration level 15
Router(config)# xsm privilege monitor level 11
```

Related Commands

Command	Description
privilege	Configures IOS privilege parameters.
xsm privilege configuration level	Enables configuration privilege level to subscribe to XRDs.

xsm vdm

To grant access to VPN-specific monitoring and configuration data for the VPN Device Manager (VDM), use the **xsm vdm** command in global configuration mode. To cancel access to VPN-specific monitoring and configuration data for VDM, use the **no** form of this command.

xsm vdm

no xsm vdm

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled (Access to VPN-specific monitoring and configuration data for the VDM is granted when XSM is enabled.)

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command enables access to the following VPN-specific information:

- IPSec
- IKE
- Tunneling
- Encryption
- Keys and certificates

If XSM is enabled, this command is enabled by default. Access to VPN-specific monitoring and configuration data within XSM can be disabled by using the **no** form of the command. However, disabling this command will prevent VDM from working properly and will also disable the **xsm history vdm** command. Leaving this command enabled has minimal performance impact.

Examples

In the following example, access to VPN-specific monitoring and configuration data is disabled:

```
Router(config)# xsm
Router(config)# no xsm dvm
```

Related Commands

Command	Description
xsm	Enables XSM client access to the router.
xsm dvdm	Grants access to switch operations.
xsm edm	Grants access to EDM monitoring and configuration data.
xsm history vdm	Enables specific VPN statistics collection on the XSM server.