

# System Management Commands

---

This chapter describes the function and displays the syntax of commands used to manage the router system and its performance on the network. For more information about defaults and usage guidelines, see the corresponding chapter of the *Configuration Fundamentals Command Reference*.

## access-enable

To enable the router to create a temporary access list entry in a dynamic access list, use the **access-enable** EXEC command.

**access-enable** [**host**] [**timeout** *minutes*]

- host** (Optional) Tells the software to enable access only for the host from which the Telnet session originated. If not specified, the software allows all hosts on the defined network to gain access. The dynamic access list contains the network mask to use for enabling the new network.
- timeout** *minutes* (Optional) Specifies an idle timeout for the temporary access list entry. If the access list entry is not accessed within this period, it is automatically deleted and requires the user to authenticate again. The default is for the entries to remain permanently. It is recommended that this value equal the idle timeout set for the WAN connection.

## access-template

To manually place a temporary access list entry on a router to which you are connected, use the **access-template** EXEC command.

**access-template** [*access-list-number*] [*dynamic-name*] [*source*] [*destination*] [**timeout** *minutes*]

- access-list-number* (Optional) Number of the dynamic access list.
- dynamic-name* (Optional) Name of a dynamic access list.
- source* (Optional) Source address in a dynamic access list. The keywords **host** and **any** are allowed. All other attributes are inherited from the original access-list entry.
- destination* (Optional) Destination address in a dynamic access list. The keywords **host** and **any** are allowed. All other attributes are inherited from the original access-list entry.

**timeout** *minutes* (Optional) Specifies a maximum time limit for each entry within this dynamic list. This is an absolute time, from creation, that an entry can reside in the list. The default is an infinite time limit and allows an entry to remain permanently.

## alias

To create a command alias, use the **alias** global configuration command. Use the **no alias** command to delete all aliases in a command mode or to delete a specific alias, and to revert to the original command syntax.

**alias** *mode alias-name alias-command-line*

**no alias** *mode [alias-name]*

*mode* Command mode of the original and alias commands. Values are:

- **controller**—Controller configuration
- **exec**—EXEC
- **hub**—Hub configuration
- **interface**—Interface configuration
- **ipx-router**—IPX router configuration
- **line**—Line configuration
- **map-class**—Map-class configuration
- **map-list**—Map list configuration
- **route-map**—Route map configuration
- **router**—Router configuration

*alias-name* Command alias.

*alias-command-line* Original command syntax.

## buckets-of-history-kept

To set the number of history buckets that are kept during the response time reporter probe's lifetime, use the **buckets-of-history-kept** response time reporter configuration command. Use the **no** form of this command to return to the default value.

**buckets-of-history-kept** *size*

**no buckets-of-history-kept**

*size* Number of history buckets kept during the response time reporter probe's lifetime. The default is 50 buckets.

## buffers

Use the **buffers** global configuration command to make adjustments to initial buffer pool settings and to the limits at which temporary buffers are created and destroyed. Use the **no** form of this command to return the buffers to their default size.

```
buffers {small | middle | big | verybig | large | huge | type number} {permanent | max-free
| min-free | initial} number
no buffers {small | middle | big | verybig | large | huge | type number} {permanent | max-free
| min-free | initial} number
```

<b>small</b>	Buffer size of this public buffer pool is 104 bytes.
<b>middle</b>	Buffer size of this public buffer pool is 600 bytes.
<b>big</b>	Buffer size of this public buffer pool is 1524 bytes.
<b>verybig</b>	Buffer size of this public buffer pool is 4520 bytes.
<b>large</b>	Buffer size of this public buffer pool is 5024 bytes.
<b>huge</b>	Default buffer size of this public buffer pool is 18024 bytes. This value can be configured with the <b>buffers huge size</b> command.
<i>type number</i>	Interface type and interface number of the interface buffer pool. The type value cannot be <b>fdi</b> .
<b>permanent</b>	Number of permanent buffers that the system tries to create and keep. Permanent buffers are normally not trimmed by the system.
<b>max-free</b>	Maximum number of free or unallocated buffers in a buffer pool.
<b>min-free</b>	Minimum number of free or unallocated buffers in a buffer pool.
<b>initial</b>	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.
<i>number</i>	Number of buffers to be allocated.

## buffers huge size

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

```
buffers huge size number
no buffers huge size number
```

<i>number</i>	Number of buffers to be allocated.
---------------	------------------------------------

## calendar set

To set the system calendar for a Cisco 7000 series, Cisco 7200 series, or Cisco 4500 system, use the **calendar set** EXEC command.

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

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

*hh:mm:ss* Current time in hours (military format), minutes, and seconds.

*day* Current day (by date) in the month.

*month* Current month (by name).

*year* Current year (no abbreviation).

## cdp enable

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

**cdp enable**

**no cdp enable**

## cdp holdtime

To specify the amount of time the receiving device should hold a CDP packet from your router before discarding it, use the **cdp holdtime** global configuration command. Use the **no** form of this command to revert to the default setting.

**cdp holdtime** *seconds*

**no cdp holdtime**

*seconds* Specifies the hold time to be sent in the CDP update packets.

## cdp run

To enable CDP, use the **cdp run** global configuration command. Use the **no** form of this command to disable CDP.

**cdp run**

**no cdp run**

## cdp timer

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

**cdp timer** *seconds*

**no cdp timer**

*seconds* Specifies how often the Cisco IOS software sends CDP updates.

## clear cdp counters

To reset CDP traffic counters to zero (0), use the **clear cdp counters** privileged EXEC command.

**clear cdp counters**

## clear cdp table

To clear the table that contains CDP information about neighbors, use the **clear cdp table** privileged EXEC command.

**clear cdp table**

## clock calendar-valid

To configure the Cisco 7000 series or the Cisco 4500 as a time source for a network based on its calendar, use the **clock calendar-valid** global configuration command. Use the **no** form of this command to set the Cisco IOS software so that the calendar is not an authoritative time source.

**clock calendar-valid**

**no clock calendar-valid**

## clock read-calendar

To manually read the calendar into either the Cisco 7000, Cisco 7200 series, or Cisco 4500 series clock, use the **clock read-calendar** EXEC command.

**clock read-calendar**

## clock set

To manually set the system clock, use the **clock set** EXEC command.

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

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

*hh:mm:ss* Current time in hours (military format), minutes, and seconds.

*day* Current day (by date) in the month.

*month* Current month (by name).

*year* Current year (no abbreviation).

## clock summer-time

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

**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**

<i>zone</i>	Name of the time zone (PDT,...) to be displayed when summer time is in effect.
<i>week</i>	Week of the month (1 to 5 or <b>last</b> ).
<i>day</i>	Day of the week (Sunday, Monday,...).
<i>date</i>	Date of the month (1 to 31).
<i>month</i>	Month (January, February,...).
<i>year</i>	Year (1993 to 2035).
<i>hh:mm</i>	Time (military format) in hours and minutes.
<i>offset</i>	(Optional) Number of minutes to add during summer time (default is 60).

## clock timezone

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

**clock timezone zone hours** [*minutes*]  
**no clock timezone**

<i>zone</i>	Name of the time zone to be displayed when standard time is in effect.
<i>hours</i>	Hours offset from UTC.
<i>minutes</i>	(Optional) Minutes offset from UTC.

## clock update-calendar

To set the Cisco 7000, Cisco 7200, or Cisco 4500 calendar from the system clock, use the **clock update-calendar EXEC** command.

**clock update-calendar**

## custom-queue-list

To assign a custom queue list to an interface, use the **custom-queue-list** interface configuration command. To remove a specific list or all list assignments, use the **no** form of the command.

**custom-queue-list** *list*  
**no custom-queue-list** [*list*]

*list*                      Number of the custom queue list you want to assign to the interface. An integer from 1 to 16.

## distributions-of-statistics-kept

To set the number of statistic distributions kept per hop during the response time reporter probe's lifetime, use the **distributions-of-statistics-kept** response time reporter configuration command. Use the **no** form of this command to return to the default value.

**distributions-of-statistics-kept** *size*  
**no distributions-of-statistics-kept**

*size*                      Number of statistic distributions kept per hop. The default is 1 distribution.

## downward-compatible-config

To generate a configuration that is compatible with an earlier Cisco IOS release, use the **downward-compatible-config** global configuration command. To remove this feature, use the **no** form of this command.

**downward-compatible-config** *version*  
**no downward-compatible-config**

*version*                      Cisco IOS Release number, not earlier than 10.2.

## fair-queue

To enable weighted fair queueing for an interface, use the **fair-queue** interface configuration command. To disable weighted fair queueing for an interface, use the **no** form of this command.

**fair-queue** [*congestive-discard-threshold* [*dynamic-queues* [*reservable-queues*]]]  
**no fair-queue**

*congestive-discard-threshold*      (Optional) Number of messages allowed in each queue in the range 1 to 512. The default is 64 messages. When the number of messages in the queue for a high-bandwidth conversation reaches the specified threshold, new high-bandwidth messages are discarded.

*dynamic-queues*                      (Optional) Number of dynamic queues used for best-effort conversations (that is, a normal conversation not requiring any special network services). Values are 16, 32, 64, 128, 256, 512, 1024, 2048, and 4096. The default is 256.

*reservable-queues* (Optional) Number of reservable queues used for reserved conversations in the range 0 to 1000. The default is 0. Reservable queues are used for interfaces configured for the Resource Reservation Protocol (RSVP) feature.

## filter-for-history

To define the type of information kept in the history table for the response time reporter probe, use the **filter-for-history** response time reporter configuration command. Use the **no** form of this command to return to the default value.

**filter-for-history** { **none** | **all** | **overThreshold** | **failures** }  
**no filter-for-history** { **none** | **all** | **overThreshold** | **failures** }

<b>none</b>	No history kept. This is the default.
<b>all</b>	All probe operations attempted are kept in the history table.
<b>overThreshold</b>	Only packets that are over the threshold are kept in the history table.
<b>failures</b>	Only packets that fail for any reason are kept in the history table.

## frequency

To set the rate at which the response time reporter probe starts a response time operation, use the **frequency** response time reporter configuration command. Use the **no** form of this command to return to the default value.

**frequency** *second*  
**no frequency**

<i>second</i>	Number of seconds between the probe's response time reporter operations. The default value is 60 seconds.
---------------	---

## hops-of-statistics-kept

To set the number of hops for which statistics are maintained per path for the response time reporter probe, use the **hops-of-statistics-kept** response time reporter configuration command. Use the **no** form of this command to return to the default value.

**hops-of-statistics-kept** *size*  
**no hops-of-statistics-kept**

<i>size</i>	Number of hops for which statistics are maintained per path. The default is 16 hops for type <b>pathecho</b> and 1 hop for type <b>echo</b> .
-------------	---

## hostname

To specify or modify the host name for the network server, use the **hostname** global configuration command. The host name is used in prompts and default configuration filenames. The **setup** command facility also prompts for a host name at startup.

**hostname** *name*

*name*                                      New host name for the network server.

## hours-of-statistics-kept

To set the number of hours for which statistics are maintained for the response time reporter probe, use the **hours-of-statistics-kept** response time reporter configuration command. Use the **no** form of this command to return to the default value.

**hours-of-statistics-kept** *hours*  
**no hours-of-statistics-kept**

*hours*                                      Number of hours that the router maintains statistics. The default is 2 hours.

## ip bootp server

To access the BOOTP service available from hosts on the network, use the **ip bootp server** global configuration command. Use the **no** form of the command to disable these services.

**ip bootp server**  
**no ip bootp server**

## ip telnet source-interface

Use the **ip telnet source-interface** global configuration command to allow a user to select an address of an interface as the source address for Telnet connections.

**ip telnet source-interface** *interface*  
**no ip telnet source-interface**

*interface*                                      The interface whose address is to be used as the source for Telnet connections.

## ip tftp source-interface

Use the **ip tftp source-interface** global configuration command to allow a user to select the interface whose address will be used as the source address for TFTP connections.

**ip tftp source-interface** *interface*  
**no ip tftp source-interface**

*interface*                                      The interface whose address is to be used as the source for TFTP connections.

## lives-of-history-kept

To set the number of lives maintained in the history table for the response time reporter probe, use the **lives-of-history-kept** response time reporter configuration command. Use the **no** form of this command to return to the default value.

**lives-of-history-kept** *lives*  
**no lives-of-history-kept**

*lives*                      Number of lives maintained in the history table for the probe. The default is 0 lives.

## load-interval

To change the length of time for which data is used to compute load statistics, use the **load-interval** interface configuration command. Use the **no** form of this command to revert to the default setting.

**load-interval** *seconds*  
**no load-interval** *seconds*

*seconds*                      Length of time for which data is used to compute load statistics. A value that is a multiple of 30, from 30 to 600 (30, 60, 90, 120, and so forth).

## logging

To log messages to a syslog server host, use the **logging** global configuration command. The **no** form of this command deletes the syslog server with the specified address from the list of syslogs.

**logging** *host*  
**no logging** *host*

*host*                      Name or IP address of the host to be used as a syslog server.

## logging buffered

To log messages to an internal buffer, use the **logging buffered** global configuration command. The **no** form of this command cancels the use of the buffer and writes messages to the console terminal, which is the default.

**logging buffered** [*size*]  
**no logging buffered**

*size*                      (Optional) Size of the buffer from 4096 to 4294967295 bytes. The default is 4096 bytes (4K).

## logging console

To limit messages logged to the console based on severity, use the **logging console** global configuration command. The **no** form of this command disables logging to the console terminal.

**logging console** *level*

**no logging console**

<i>level</i>	Limits the logging of messages displayed on the console terminal to a specified level. Values are: <ul style="list-style-type: none"> <li>• <b>emergencies</b> (level 0)—System unusable (LOG_EMERG)</li> <li>• <b>alerts</b> (level 1)—Immediate action needed (LOG_ALERT)</li> <li>• <b>critical</b> (level 2)—Critical conditions (LOG_CRIT)</li> <li>• <b>errors</b> (level 3)—Error conditions (LOG_ERR)</li> <li>• <b>warnings</b> (level 4)—Warning conditions (LOG_WARNING)</li> <li>• <b>notifications</b> (level 5)—Normal but significant condition (LOG_NOTICE)</li> <li>• <b>informational</b> (level 6)—Informational messages only (LOG_INFO)</li> <li>• <b>debugging</b> (level 7)—Debugging messages (LOG_DEBUG)</li> </ul>
--------------	--

## logging facility

To configure the syslog facility in which error messages are sent, use the **logging facility** global configuration command. To revert to the default of **local7**, use the **no** form of this command.

**logging facility** *facility-type*

**no logging facility**

<i>facility-type</i>	Syslog facility. Values are: <b>auth</b> , <b>cron</b> , <b>daemon</b> , <b>kern</b> , <b>local0–7</b> , <b>lpr</b> , <b>mail</b> , <b>news</b> , <b>sys9</b> , <b>sys10</b> , <b>sys11</b> , <b>sys12</b> , <b>sys13</b> , <b>sys14</b> , <b>syslog</b> , <b>user</b> , and <b>uucp</b> .
----------------------	--

## logging history

To limit syslog messages sent to the router's history table and the SNMP network management station based on severity, use the **logging history** global configuration command. The **no** form of this command returns the logging of syslog messages to the default level.

**logging history** *level*

**no logging history**

<i>level</i>	Limits the messages saved in the history table and sent to the SNMP network management station to the specified set of levels. Values are: <ul style="list-style-type: none"> <li>• <b>emergencies</b> (level 0)—System unusable (LOG_EMERG)</li> <li>• <b>alerts</b> (level 1)—Immediate action needed (LOG_ALERT)</li> <li>• <b>critical</b> (level 2)—Critical conditions (LOG_CRIT)</li> <li>• <b>errors</b> (level 3)—Error conditions (LOG_ERR)</li> </ul>
--------------	--

- **warnings** (level 4)—Warning conditions (LOG\_WARNING)
- **notifications** (level 5)—Normal but significant condition (LOG\_NOTICE)
- **informational** (level 6)—Informational messages only (LOG\_INFO)
- **debugging** (level 7)—Debugging messages (LOG\_DEBUG)

## logging history size

To change the number of syslog messages stored in the router's history table, use the **logging history size** global configuration command. The **no** form of this command returns the number of messages to the default value.

**logging history size** *number*  
**no logging history size**

*number*                      Number from 1 to 500 that indicates the maximum number of messages stored in the history table.

## logging monitor

To limit messages logged to the terminal lines (monitors) based on severity, use the **logging monitor** global configuration command. This command limits the logging messages displayed on terminal lines other than the console line to messages with a level at or above *level*. The **no** form of this command disables logging to terminal lines other than the console line.

**logging monitor** *level*  
**no logging monitor**

*level*                      One of the *level* keywords. Values are:

- **emergencies** (level 0)—System unusable (LOG\_EMERG)
- **alerts** (level 1)—Immediate action needed (LOG\_ALERT)
- **critical** (level 2)—Critical conditions (LOG\_CRIT)
- **errors** (level 3)—Error conditions (LOG\_ERR)
- **warnings** (level 4)—Warning conditions (LOG\_WARNING)
- **notifications** (level 5)—Normal but significant condition (LOG\_NOTICE)
- **informational** (level 6)—Informational messages only (LOG\_INFO)
- **debugging** (level 7)—Debugging messages (LOG\_DEBUG)

## logging on

To control logging of error messages, use the **logging on** global configuration command. This command enables or disables message logging to all destinations except the console terminal. The **no** form of this command enables logging to the console terminal only.

**logging on**  
**no logging on**

## logging synchronous

To synchronize unsolicited messages and **debug** output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or virtual terminal line, use the **logging synchronous** line configuration command. Use the **no** form of this command to disable synchronization of unsolicited messages and debug output.

**logging synchronous** [**level** *severity-level* | **all**] [**limit** *number-of-buffers*]  
**no logging synchronous** [**level** *severity-level* | **all**] [**limit** *number-of-buffers*]

<b>level</b> <i>severity-level</i>	(Optional) Specifies the message severity level. Messages with a severity level equal to or higher than this value are printed asynchronously. When specifying a severity level number, consider that for the logging system, low numbers indicate greater severity and high numbers indicate lesser severity. The default value is 2.
<b>all</b>	(Optional) Specifies that all messages are printed asynchronously, regardless of the severity level.
<b>limit</b> <i>number-of-buffers</i>	(Optional) Specifies the number of buffers to be queued for the terminal after which new messages are dropped. The default value is 20.

## logging trap

To limit messages logged to the syslog servers based on severity, use the **logging trap** global configuration command. The command limits the logging of error messages sent to syslog servers to only those messages at the specified level. Use the **no** form of this command to disable logging to syslog servers.

**logging trap** *level*  
**no logging trap**

<i>level</i>	One of the <i>level</i> keywords. Values are: <ul style="list-style-type: none"> <li>• <b>emergencies</b> (level 0)—System unusable (LOG_EMERG)</li> <li>• <b>alerts</b> (level 1)—Immediate action needed (LOG_ALERT)</li> <li>• <b>critical</b> (level 2)—Critical conditions (LOG_CRIT)</li> <li>• <b>errors</b> (level 3)—Error conditions (LOG_ERR)</li> <li>• <b>warnings</b> (level 4)—Warning conditions (LOG_WARNING)</li> <li>• <b>notifications</b> (level 5)—Normal but significant condition (LOG_NOTICE)</li> </ul>
--------------	---

- **informational** (level 6)—Informational messages only (LOG\_INFO)
- **debugging** (level 7)—Debugging messages (LOG\_DEBUG)

## ntp access-group

To control access to the system's Network Time Protocol (NTP) services, use the **ntp access-group** global configuration command. To remove access control to the system's 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 }
```

<b>query-only</b>	Allows only NTP control queries. See RFC 1305 (NTP version 3).
<b>serve-only</b>	Allows only time requests.
<b>serve</b>	Allows time requests and NTP control queries, but does not allow the system to synchronize to the remote system.
<b>peer</b>	Allows time requests and NTP control queries and allows the system to synchronize to the remote system.
<i>access-list-number</i>	Number (1 to 99) of a standard IP access list.

## ntp authenticate

To enable Network Time Protocol (NTP) authentication, use the **ntp authenticate** global configuration command. Use the **no** form of this command to disable the feature.

```
ntp authenticate  
no ntp authenticate
```

## ntp authentication-key

To define an authentication key for Network Time Protocol (NTP), use the **ntp authentication-key** global configuration command. Use the **no** form of this command to remove the authentication key for NTP.

```
ntp authentication-key number md5 value  
no ntp authentication-key number
```

<i>number</i>	Key number (1 to 4294967295).
<b>md5</b>	Authentication key. Message authentication support is provided using the Message Digest (MD5) algorithm. The key type <b>md5</b> is currently the only key type supported.
<i>value</i>	Key value (an arbitrary string of up to eight characters).

## ntp broadcast

To specify that a specific interface should send Network Time Protocol (NTP) broadcast packets, use the **ntp broadcast** interface configuration command. Use the **no** form of this command to disable this capability.

```
ntp broadcast [version number]  
no ntp broadcast
```

*version number* (Optional) Number from 1 to 3 indicating the NTP version.

## ntp broadcast client

To allow the system to receive NTP broadcast packets on an interface, use the **ntp broadcast client** command. Use the **no** form of this command to disable this capability.

```
ntp broadcast client  
no ntp broadcast client
```

## 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** global configuration command. Use the **no** form of this command to revert to the default value.

```
ntp broadcastdelay microseconds  
no ntp broadcastdelay
```

*microseconds* Estimated round-trip time (in microseconds) for NTP broadcasts. The range is from 1 to 999999.

## 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 system clock, it keeps track of the correction factor for this error. The system automatically saves this value into the system configuration using the **ntp clock-period** global configuration command. The system uses the **no** form of this command to revert to the default.

```
ntp clock-period value  
no ntp clock-period
```

*value* Amount to add to the system clock for each clock hardware tick (in units of 2-32 seconds).

## ntp disable

To prevent an interface from receiving Network Time Protocol (NTP) packets, use the **ntp disable** interface configuration command. To enable receipt of NTP packets on an interface, use the **no** form of this command.

**ntp disable**  
**no ntp disable**

## ntp master



**Caution** Use this command with *extreme* caution. It is very easy to override valid time sources using this command, especially if a low stratum number is configured. Configuring multiple machines in the same network with the **ntp master** command can cause instability in keeping time if the machines do not agree on the time.

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** global configuration command. To disable the master clock function, use the **no** form of this command.

**ntp master** [*stratum*]  
**no ntp master** [*stratum*]

*stratum* (Optional) Number from 1 to 15. Indicates the NTP stratum number that the system will claim.

## ntp peer

To configure the system clock to synchronize a peer or to be synchronized by a peer, use the **ntp peer** global configuration command. To disable this capability, use the **no** form of this command.

**ntp peer** *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]  
**no ntp peer** *ip-address*

*ip-address* IP address of the peer providing, or being provided, the clock synchronization.

**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.

## ntp server

To allow the system clock to be synchronized by a time server, use the **ntp server** global configuration command. To disable this capability, use the **no** form of this command.

```
ntp server ip-address [version number] [key keyid] [source interface] [prefer]  
no ntp server ip-address
```

<i>ip-address</i>	IP address of the time server providing the clock synchronization.
<b>version</b>	(Optional) Defines the Network Time Protocol (NTP) version number.
<i>number</i>	(Optional) NTP version number (1 to 3).
<b>key</b>	(Optional) Defines the authentication key.
<i>keyid</i>	(Optional) Authentication key to use when sending packets to this peer.
<b>source</b>	(Optional) Identifies the interface from which to pick the IP source address.
<i>interface</i>	(Optional) Name of the interface from which to pick the IP source address.
<b>prefer</b>	(Optional) Makes this server the preferred server that provides synchronization.

## ntp source

To use a particular source address in Network Time Protocol (NTP) packets, use the **ntp source** global configuration command. Use the **no** form of this command to remove the specified source address.

```
ntp source type number  
no ntp source
```

<i>type</i>	Type of interface.
<i>number</i>	Number of the interface.

## ntp trusted-key

To authenticate the identity of a system to which Network Time Protocol (NTP) will synchronize, use the **ntp trusted-key** global configuration command. Use the **no** form of this command to disable authentication of the identity of the system.

```
ntp trusted-key key-number  
no ntp trusted-key key-number
```

<i>key-number</i>	Key number of authentication key to be trusted.
-------------------	---

## ntp update-calendar

To periodically update the Cisco 7000 series or Cisco 7200 series calendar from Network Time Protocol (NTP), use the **ntp update-calendar** global configuration command. Use the **no** form of this command to disable this feature.

**ntp update-calendar**  
**no ntp update-calendar**

## owner

To configure the SNMP owner of the response time reporter probe, use the **owner** response time reporter configuration command. Use the **no** form of this command to return to the default value.

**owner** *text*  
**no owner**

*text* Name of the SNMP owner from 0 to 255 ASCII characters. The default is none.

## paths-of-statistics-kept

To set the number of paths for which statistics are maintained per hour for the response time reporter probe, use the **paths-of-statistics-kept** response time reporter configuration command. Use the **no** form of this command to return to the default value.

**paths-of-statistics-kept** *size*  
**no paths-of-statistics-kept**

*size* Number of paths for which statistics are maintained per hour. The default is 5 paths for type **pathEcho** and 1 path for type **echo**.

## ping (privileged)

Use the **ping** (packet internet groper) privileged EXEC command to diagnose basic network connectivity on Apollo, AppleTalk, Connectionless Network Service (CLNS), DECnet, IP, Novell IPX, VINES, or XNS networks.

**ping** [*protocol*] {*host* | *address*}

*protocol* (Optional) Protocol keyword, one of **apollo**, **appletalk**, **clns**, **decnet**, **ip**, **ipx**, **vines**, or **xns**.

*host* Host name of system to ping.

*address* Address of system to ping.

## ping (user)

Use the **ping** (packet internet groper) user EXEC command to diagnose basic network connectivity on AppleTalk, CLNS, IP, Novell, Apollo, VINES, DECnet, or XNS networks.

**ping** [*protocol*] {*host* | *address*}

<i>protocol</i>	(Optional) Protocol keyword, one of <b>apollo</b> , <b>appletalk</b> , <b>clns</b> , <b>decnet</b> , <b>ip</b> , <b>ipx</b> , <b>vines</b> , or <b>xns</b> .
<i>host</i>	Host name of system to ping.
<i>address</i>	Address of system to ping.

## priority-group

To assign the specified priority list to an interface, use the **priority-group** interface configuration command. Use the **no** form of this command to remove the specified priority group assignment.

**priority-group** *list*  
**no priority-group**

<i>list</i>	Priority list number assigned to the interface.
-------------	---

## priority-list default

To assign a priority queue for those packets that do not match any other rule in the priority list, use the **priority-list default** global configuration command. Use the **no** form of this command to return to the default or assign **normal** as the default.

**priority-list** *list-number* **default** {**high** | **medium** | **normal** | **low**}  
**no priority-list** *list-number* **default** {**high** | **medium** | **normal** | **low**}

<i>list-number</i>	Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.
<b>high</b>   <b>medium</b>   <b>normal</b>   <b>low</b>	Priority queue level.

## priority-list interface

To establish queuing priorities on packets entering from a given interface, use the **priority-list interface** global configuration command. Use the **no** form of this command with the appropriate arguments to remove an entry from the list.

**priority-list** *list-number* **interface** *interface-type* *interface-number* {**high** | **medium** | **normal** | **low**}  
**no priority-list** *list-number* **interface** *interface-type* *interface-number* {**high** | **medium** | **normal** | **low**}

<i>list-number</i>	Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.
<i>interface-type</i>	Specifies the name of the interface.

*interface-number*                      Number of the specified interface.

**high** | **medium** | **normal** | **low**    Priority queue level.

## priority-list protocol

To establish queuing priorities based upon the protocol type, use the **priority-list protocol** global configuration command. Use the **no** form of this command with the appropriate list number to remove an entry from the list.

**priority-list** *list number* **protocol** *protocol-name* {**high** | **medium** | **normal** | **low**}  
*queue-keyword* *keyword-value*  
**no priority-list** *list-number* **protocol**

*list-number*                              Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.

*protocol-name*                          Specifies the protocol type: **aarp**, **arp**, **apollo**, **appletalk**, **bridge** (transparent), **clns**, **clns\_es**, **clns\_is**, **compressedtcp**, **cmns**, **decnet**, **decnet\_node**, **decnet\_router-11**, **decnet\_router-12**, **ip**, **ipx**, **pad**, **rsrb**, **stun**, **vines**, **xns**, and **x25**.

**high** | **medium** | **normal** | **low**      Priority queue level.

*queue-keyword* *keyword-value*      Possible keywords are **fragments**, **gt**, **lt**, **list**, **tcp**, and **udp**.

## priority-list queue-limit

To specify the maximum number of packets that can be waiting in each of the priority queues, use the **priority-list queue-limit** global configuration command. The **no** form of this command selects the normal queue.

**priority-list** *list-number* **queue-limit** *high-limit* *medium-limit* *normal-limit* *low-limit*  
**no priority-list** *list-number* **queue-limit**

*list-number*                              Arbitrary integer between 1 and 16 that identifies the priority list selected by the user.

*high-limit* *medium-limit*  
*normal-limit* *low-limit*                  Priority queue maximum length. A value of 0 for any of the four arguments means that the queue can be of unlimited size for that particular queue.

## prompt

To customize the prompt, use the **prompt** global configuration command. To revert to the default prompt, use the **no** form of this command.

```
prompt string
no prompt [string]
```

*string* Prompt. It can consist of all printing characters and the following escape sequences:

- **%h**—Host name. This is either Router or the name defined with the `hostname` global configuration command.
- **%n**—Physical terminal line (TTY) number of the EXEC user.
- **%p**—Prompt character itself. It is either an angle bracket (>) for EXEC mode or a pound sign (#) for privileged EXEC mode.
- **%s**—Space.
- **%t**—Tab.
- **%%**—Percent sign (%).

## queue-list default

To assign a priority queue for those packets that do not match any other rule in the queue list, use the **queue-list default** global configuration command. To restore the default value, use the **no** form of this command.

```
queue-list list-number default queue-number
no queue-list list-number default queue-number
```

*list-number* Number of the queue list. An integer from 1 to 16.

*queue-number* Number of the queue. An integer from 1 to 16.

## queue-list interface

To establish queuing priorities on packets entering on an interface, use the **queue-list interface** global configuration command. To remove an entry from the list, use the **no** form of the command.

```
queue-list list-number interface interface-type interface-number queue-number
no queue-list list-number interface queue-number
```

*list-number* Number of the queue list. An integer from 1 to 16.

*interface-type* Required argument that specifies the name of the interface.

*interface-number* Number of the specified interface.

*queue-number* Number of the queue. An integer from 1 to 16.

## queue-list protocol

To establish queuing priority based upon the protocol type, use the **queue-list protocol** global configuration command. Use the **no** form of this command with the appropriate list number to remove an entry from the list.

**queue-list** *list-number* **protocol** *protocol-name* *queue-number* *queue-keyword* *keyword-value*  
**no queue-list** *list-number* **protocol** *protocol-name*

<i>list-number</i>	Number of the queue list. An integer from 1 to 16.
<i>protocol-name</i>	Required argument that specifies the protocol type: <b>aarp</b> , <b>arp</b> , <b>apollo</b> , <b>appletalk</b> , <b>bridge</b> (transparent), <b>clns</b> , <b>clns_es</b> , <b>clns_is</b> , <b>compressedtcp</b> , <b>cmns</b> , <b>decnet</b> , <b>decnet_node</b> , <b>decnet_router11</b> , <b>decnet_router12</b> , <b>ip</b> , <b>ipx</b> , <b>pad</b> , <b>rsrb</b> , <b>stun</b> , <b>vines</b> , <b>xns</b> , and <b>x25</b> .
<i>queue-number</i>	Number of the queue. An integer from 1 to 16.
<i>queue-keyword</i> <i>keyword-value</i>	Possible keywords are <b>gt</b> , <b>lt</b> , <b>list</b> , <b>tcp</b> , and <b>udp</b> .

## queue-list queue byte-count

To designate the byte size allowed per queue, use the **queue-list queue byte-count** global configuration command. To return the byte size to the default value, use the **no** form of the command.

**queue-list** *list-number* **queue** *queue-number* **byte-count** *byte-count-number*  
**no queue-list** *list-number* **queue** *queue-number* **byte-count** *byte-count-number*

<i>list-number</i>	Number of the queue list. An integer from 1 to 16.
<i>queue-number</i>	Number of the queue. An integer from 1 to 16.
<i>byte-count-number</i>	Specifies the lower boundary on how many bytes the system allows to be delivered from a given queue during a particular cycle.

## queue-list queue limit

To designate the queue length limit for a queue, use the **queue-list queue limit** global configuration command. To return the queue length to the default value, use the **no** form of the command.

**queue-list** *list-number* **queue** *queue-number* **limit** *limit-number*  
**no queue-list** *list-number* **queue** *queue-number* **limit** *limit-number*

<i>list-number</i>	Number of the queue list. An integer from 1 to 16.
<i>queue-number</i>	Number of the queue. An integer from 1 to 16.
<i>limit-number</i>	Maximum number of packets which can be enqueued at any time. Range is 0 to 32767 queue entries.

## random-detect

To enable random early detection on an interface, use the **random-detect** interface configuration command. Use the **no** form of this command to disable random early detection on the interface.

**random-detect** [*weighting*]  
**no random-detect**

*weighting* (Optional) Exponential weighting constant in the range 1 to 16 used to determine the rate that packets are dropped when congestion occurs. The default is 10 (that is, drop 1 packet every  $2^{10}$ ).

## request-data-size

To set the protocol data size in the payload of the response time reporter probe's request packet, use the **request-data-size** response time reporter configuration command. Use the **no** form of this command to return to the default value.

**request-data-size** *byte*  
**no request-data-size**

*byte* Size of the protocol data in the payload of the probe's request packet. Range is 0 to the protocol's maximum. The default is 1 byte.

## response-data-size

To set the protocol data size in the payload of the response time reporter probe's response packet, use the **response-data-size** response time reporter configuration command. Use the **no** form of this command to return to the default value.

**response-data-size** *byte*  
**no response-data-size**

*byte* Size of the protocol data in the payload in the probe's response packet. For "appl" protocols, the default is 0 byte. For all others, the default is the same value as the **request-data-size**.

## rmon

To enable Remote Network Monitoring (RMON) on an Ethernet interface, use the **rmon** interface configuration command. Use the **no** form of this command to disable RMON on the interface.

**rmon** {**native** | **promiscuous**}  
**no rmon**

**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.

## rmon alarm

To set an alarm on any MIB object, use the **rmon alarm** configuration command. Use the **no** form of this command to disable the alarm.

```
rmon alarm number variable interval { delta | absolute } rising-threshold value [event-number]
falling-threshold value [event-number] [owner string]
no rmon alarm number
```

<i>number</i>	Alarm number, which is identical to the <i>alarmIndex</i> in the <i>alarmTable</i> in the Remote Network Monitoring (RMON) MIB.
<i>variable</i>	MIB object to monitor, which translates into the <i>alarmVariable</i> used in the <i>alarmTable</i> of the RMON MIB.
<i>interval</i>	Time in seconds the alarm monitors the MIB variable, which is identical to the <i>alarmValue</i> used in the <i>alarmTable</i> of the RMON MIB.
<b>delta</b>	Tests the change between MIB variables, which affects the <i>alarmSampleType</i> in the <i>alarmTable</i> of the RMON MIB.
<b>absolute</b>	Tests each MIB variable directly, which affects the <i>alarmSampleType</i> in the <i>alarmTable</i> of the RMON MIB.
<b>rising-threshold</b> <i>value</i>	Value at which the alarm is triggered.
<i>event-number</i>	(Optional) Event number to trigger when the rising or falling threshold exceeds its limit. This value is identical to the <i>alarmRisingEventIndex</i> or the <i>alarmFallingEventIndex</i> in the <i>alarmTable</i> of the RMON MIB.
<b>falling-threshold</b> <i>value</i>	Value at which the alarm is reset.
<b>owner</b> <i>string</i>	(Optional) Specifies an owner for the alarm, which is identical to the alarm owner in the <i>alarmTable</i> of the RMON MIB.

## rmon event

To add or remove an event in the RMON event table that is associated with an RMON event number, use the **rmon event** global configuration command. Use the **no** form of this command to disable RMON on the interface.

```
rmon event number [log] [trap community] [description string] [owner string]
no rmon event number
```

<i>number</i>	Assigned event number, which is identical to the <i>eventIndex</i> in the <i>eventTable</i> in the RMON MIB.
<b>log</b>	(Optional) Generates an RMON log entry when the event is triggered and sets the <i>eventType</i> in the RMON MIB to <i>log</i> or <i>log-and-trap</i> .

<b>trap</b> <i>community</i>	(Optional) SNMP community string used for this trap. Configures the setting of the <i>eventType</i> in the RMON MIB for this row as either <i>snmp-trap</i> or <i>log-and-trap</i> . This value is identical to the <i>eventCommunityValue</i> in the <i>eventTable</i> in the RMON MIB.
<b>description</b> <i>string</i>	(Optional) Specifies a description of the event, which is identical to the event description in the <i>eventTable</i> of the RMON MIB.
<b>owner</b> <i>string</i>	(Optional) Owner of this event, which is identical to the <i>eventDescription</i> in the <i>eventTable</i> of the RMON MIB.

## rmon queuesize

To change the size of the queue that holds packets for analysis by the Remote Network Monitoring (RMON) process, use the **rmon queuesize** global configuration command. Use the **no** form of this command to restore the default value.

**rmon queuesize** *size*  
**no rmon queuesize**

*size*                      Number of packets allowed in the queue awaiting RMON analysis. Default queue size is 64 packets.

## rtr

To configure a response time reporter probe, use the **rtr** global configuration command. Use the **no** form of this command to remove all configuration information for a probe including the probe's schedule, reaction configuration, and reaction triggers.

**rtr** *probe*  
**no rtr** *probe*

*probe*                      Number of the response time reporter probe (instance) to configure.

## rtr reaction-configuration

To configure certain actions to occur based on events under the control of the response time reporter, use the **rtr reaction-configuration** global configuration command. Use the **no** form of this command to return to the probe's default values.

**rtr reaction-configuration** *probe* [**connection-loss-enable**] [**timeout-enable**]  
 [**threshold-falling** *milliseconds*] [**threshold-type** *option*] [**action-type** *option*]  
**no rtr reaction-configuration** *probe*

*probe*                      Number of the response time reporter probe to configure.

**connection-loss-enable** (Optional) Enable checking for connection loss in connection-oriented protocols. The default is disabled.

<b>timeout-enable</b>	(Optional) Enable checking for response time reporting operation timeouts based on the timeout value configured for the probe with the <b>timeout</b> response time reporter configuration command. The default is disabled.
<b>threshold-falling</b> <i>milliseconds</i>	(Optional) Set the falling threshold (standard RMON-type hysteresis mechanism) in milliseconds. When the falling threshold is met, generate a resolution reaction event. The probe's rising over threshold is set with the <b>threshold</b> response time reporter configuration command. The default value is 3000 ms.
<b>threshold-type</b> <i>option</i>	<p>(Optional) Specify the algorithm used by the response time reporter to calculate over and falling threshold violations. Option can be one of the following keywords:</p> <ul style="list-style-type: none"><li>• <b>never</b>—Do not calculate threshold violations (the default).</li><li>• <b>immediate</b>—When the response time exceeds the rising over threshold or drops below the falling threshold, immediately perform the action defined by <b>action-type</b>.</li><li>• <b>consecutive</b> [<i>occurrences</i>]—When the response time exceeds the rising threshold consecutively 5 times or drops below the falling threshold consecutively 5 times, perform the action defined by <b>action-type</b>. Optionally specify the number of consecutive occurrences. The default is 5.</li><li>• <b>xofy</b> [<i>x-value y-value</i>]—When the response time exceeds the rising threshold 5 out of the last 5 times or drops below the falling threshold 5 out of the last 5 times, perform the action defined by <b>action-type</b>. Optionally specify the number of violations that must occur and the number that must occur within a specified number. The default is 5 for both x-value and y-value.</li><li>• <b>average</b> [<i>attempts</i>]—When the average of the last 5 response times exceeds the rising threshold or when the average of the last 5 response times drops below the falling threshold, perform the action defined by <b>action-type</b>. Optionally specify the number of operations to average. The default is the average of the last 5 response time operations. For example: if the probe's threshold is 5000 ms and the probe's last 3 attempts results are 6000, 6000, and 5000 ms, the average would be <math>6000+6000+5000=17000/3&gt;5000</math>, thus violating the 5000-ms threshold.</li></ul>
<b>action-type</b> <i>option</i>	<p>(Optional) Specify what action or combination of actions the probe performs when you configure <b>connection-loss-enable</b> or <b>timeout-enable</b>, or threshold events occur. For the <b>action-type</b> to occur for threshold events, the <b>threshold-type</b> must be defined to anything other than <b>never</b>. Option can be one of the following keywords:</p> <ul style="list-style-type: none"><li>• <b>none</b>—No action is taken.</li><li>• <b>trapOnly</b>—Send an SNMP trap on both over and falling threshold violations.</li><li>• <b>nmvtOnly</b>—Send an SNA NMVT Alert on over threshold violation and an SNA NMVT Resolution on falling threshold violations.</li></ul>

- **triggerOnly**—Transition one or more target probe’s operational state from “pending” to “active” on over (and falling) threshold violations. The target probes are defined with the **rtr reaction-trigger** command. A target probe will continue until its life expires as specified by the target probe’s life value configured with the **rtr schedule** global configuration command. After a target probe is triggered, it must finish its life before it can be triggered again.
- **trapAndMmvt**—Send a combination of **trapOnly** and **nmvtOnly**.
- **trapAndTrigger**—Send a combination of **trapOnly** and **triggerOnly**.
- **nmvtAndTrigger**—Send a combination of **nmvtOnly** and **triggerOnly**.
- **trapNmvtAndTrigger**—Send a combination of **trapOnly**, **nmvtOnly**, and **triggerOnly**.

## rtr reaction-trigger

To define a second response time reporter probe to make the transition from a “pending” state to an “active” state when one of the trigger action-type options are defined with the **rtr reaction-configuration** global configuration command, use the **rtr reaction-trigger** global configuration command. Use the **no** form of this command to remove the trigger combination.

```
rtr reaction-trigger probe target-probe
no rtr reaction-trigger probe
```

<i>probe</i>	Number of the probe in the “active” state that has the <b>action-type</b> set with the <b>rtr reaction-configuration</b> global configuration command.
<i>target-probe</i>	Number of the probe in the “pending” state that is waiting to be triggered with the <b>rtr</b> global configuration command.

## rtr reset

To perform a shutdown and restart of the response time reporter, use the **rtr reset** global configuration command.

```
rtr reset
```

## rtr schedule

To configure the time parameters for a response time reporter probe, use the **rtr schedule** global configuration command. Use the **no** form of this command to stop the probe and restart it with the default parameters (that is, pending).

```
rtr schedule probe [life seconds] [start-time {pending | now | hh:mm [month day | day month]}] [ageout seconds]
no rtr schedule probe
```

<i>probe</i>	Number of the response time reporter probe to schedule.
--------------	---

<b>life</b> <i>seconds</i>	(Optional) Number of seconds the probe actively collects information. The default is 3600 seconds (one hour).
<b>start-time</b>	(Optional) Time when the probe starts collecting information. If the <b>start-time</b> is not specified, no information is collected until the <b>start-time</b> is configured or a trigger occurs that performs a <b>start-time now</b> .
<b>pending</b>	No information is collected. This is the default value.
<b>now</b>	Information is immediately collected.
<i>hh:mm</i>	Information is collected at the specified time (use a 24-hour clock). The time is the current day if you do not specify the month and day.
<i>month</i>	(Optional) Name of the month, any characters in a unique string. If month is not specified, the current month is used. This requires a day.
<i>day</i>	(Optional) Number of the day in the range 1 to 31. If day is not specified, the current day is used. This requires a month.
<b>ageout</b> <i>seconds</i>	(Optional) Number of seconds to keep the probe when it is not actively collecting information. The default is 0 seconds (never ages out).

## samples-of-history-kept

To set the number of entries kept in the history table per bucket for the response time reporter probe, use the **samples-of-history-kept** response time reporter configuration command. Use the **no** form of this command to return to the default value.

**samples-of-history-kept** *samples*  
**no samples-of-history-kept**

*samples* Number of entries kept in the history table per bucket. The default is 16 entries for type **pathecho** and 1 entry for type **echo**.

## scheduler allocate

To guarantee CPU time for processes, use the **scheduler allocate** global configuration command on the Cisco 7200 series and Cisco 7500 series. The no form of this command restores the default.

**scheduler allocate** *interrupt-time process-time*  
**no scheduler allocate**

*interrupt-time* Integer (in microseconds) that limits the maximum number of microseconds to spend on fast switching within any one network interrupt context. The range is 400 to 60000 microseconds. The default is 4000 microseconds.

*process-time* Integer (in microseconds) that guarantees the minimum number of microseconds to spend at the process level when network interrupts are disabled. The range is 100 to 4000. The default is 200 microseconds.

## scheduler interval

To control the maximum amount of time that can elapse without running the system processes, use the **schedule interval** global configuration command. The **no** form of this command restores the default.

**scheduler-interval** *milliseconds*  
**no scheduler-interval**

*milliseconds* Integer that specifies the interval, in milliseconds. The minimum interval that you can specify is 500 milliseconds; there is no maximum value.

## service decimal-tty

To specify that line numbers be displayed and interpreted as decimal numbers rather than octal numbers, use the **service decimal-tty** global configuration command. Use the **no** form of this command to restore the default.

**service decimal-tty**  
**no service decimal-tty**

## service exec-wait

To delay the startup of the EXEC on noisy lines, use the **service exec-wait** global configuration command. Use the **no** form of this command to disable this feature.

**service exec-wait**  
**no service exec-wait**

## service finger

To allow Finger protocol requests (defined in RFC 742) to be made of the network server, use the **service finger** global configuration command. This service is equivalent to issuing a remote **show users** command. Use the **no** form of this command to remove this service.

**service finger**  
**no service finger**

## service hide-telnet-address

To hide addresses while trying to establish a Telnet session, use the **service hide-telnet-address** global configuration command. Use the **no** form of this command to remove this service.

**service hide-telnet-address**  
**no service hide-telnet-address**

## service nagle

To enable the Nagle congestion control algorithm, use the **service nagle** global configuration command. Use the **no** form of this command to disable this feature.

**service nagle**  
**no service nagle**

## service prompt config

To display the configuration prompt (config), use the **service prompt config** global configuration command. Use the **no** form of this command to remove the configuration prompt.

```
service prompt config
no service prompt config
```

## service tcp-keepalives-in

To generate keepalive packets on idle incoming network connections (initiated by the remote host), use the **service tcp-keepalives-in** global configuration command. The **no** form of this command with the appropriate keyword disables the keepalives.

```
service tcp-keepalives-in
no service tcp-keepalives-in
```

## service tcp-keepalives-out

To generate keepalive packets on idle outgoing network connections (initiated by a user), use the **service tcp-keepalives-out** global configuration command. The **no** form of this command with the appropriate keyword disables the keepalives.

```
service tcp-keepalives-out
no service tcp-keepalives-out
```

## service tcp-small-servers

To access minor TCP/IP services available from hosts on the network, use the **service tcp-small-servers** command. Use the **no** form of the command to disable these services.

```
service tcp-small-servers
no service tcp-small-servers
```

## service telnet-zero-idle

To set the TCP window to zero (0) when the Telnet connection is idle, use the **service telnet-zero-idle** global configuration command. Use the **no** form of this command to disable this feature.

```
service telnet-zero-idle
no service telnet-zero-idle
```

## service timestamps

To configure the system to timestamp debugging or logging messages, use one of the **service timestamps** global configuration commands. Use the **no** form of this command to disable this service.

```
service timestamps type [uptime]
service timestamps type datetime [msec] [localtime] [show-timezone]
no service timestamps type
```

<i>type</i>	Type of message to timestamp: <b>debug</b> or <b>log</b> .
<b>uptime</b>	(Optional) Timestamp with time since the system was rebooted.
<b>datetime</b>	Timestamp with the date and time.
<b>msec</b>	(Optional) Include milliseconds in the date and timestamp.
<b>localtime</b>	(Optional) Timestamp relative to the local time zone.
<b>show-timezone</b>	(Optional) Include the time zone name in the timestamp.

## service udp-small-servers

To access minor User Datagram Protocol (UDP) services available from hosts on the network, use the **service udp-small-servers** command. Use the **no** form of the command to disable these services.

```
service udp-small-servers
no service udp-small-servers
```

## show aliases

To display all alias commands, or the alias commands in a specified mode, use the **show aliases EXEC** command.

```
show aliases [mode]
```

<i>mode</i>	(Optional) Command mode. Values are: <ul style="list-style-type: none"> <li>• <b>controller</b>—Controller configuration</li> <li>• <b>exec</b>—EXEC</li> <li>• <b>hub</b>—Hub configuration</li> <li>• <b>interface</b>—Interface configuration</li> <li>• <b>ipx-router</b>—IPX router configuration</li> <li>• <b>line</b>—Line configuration</li> <li>• <b>map-class</b>—Map class configuration</li> <li>• <b>map-list</b>—Map list configuration</li> <li>• <b>route-map</b>—Route map configuration</li> <li>• <b>router</b>—Router configuration</li> </ul>
-------------	---

## show buffers

Use the **show buffers** EXEC command to display statistics for the buffer pools on the network server.

**show buffers** [*type number* | **alloc** [**dump**]]

*type number* (Optional) Displays interface pool information. If the specified interface *type* and *number* has its own buffer pool, displays information for that pool. Value of *type* can be **ethernet**, **serial**, **tokenring**, **fdi**, **bri**, **atm**, **e1**, **t1**.

**alloc** (Optional) Displays a brief listing of all allocated buffers.

**dump** (Optional) Dumps all allocated buffers. This keyword must be used with the **alloc** keyword, not by itself.

## show c7200

Use the **show c7200** EXEC command to display information about the CPU and midplane for Cisco 7200 series routers.

**show c7200**

## show calendar

To display the calendar hardware setting for the Cisco 7000 series, Cisco 7200 series, or Cisco 4500 series, use the **show calendar** EXEC command.

**show calendar**

## show cdp

To display global CDP information, including timer and hold-time information, use the **show cdp** privileged EXEC command.

**show cdp**

## show cdp entry

To display information about a neighbor device listed in the CDP table, use the **show cdp entry** privileged EXEC command.

**show cdp entry** *entry-name* [**protocol** | **version**]

*entry-name* Name of neighbor about which you want information.

**protocol** (Optional) Limits the display to information about the protocols enabled on a router.

**version** (Optional) Limits the display to information about the version of software running on the router.

## show cdp interface

To display information about the interfaces on which CDP is enabled, use the **show cdp interface** command.

**show cdp interface** [*type number*]

*type* (Optional) Type of interface about which you want information.

*number* (Optional) Number of the interface about which you want information.

## show cdp neighbors

To display information about neighbors, use the **show cdp neighbors** privileged EXEC command.

**show cdp neighbors** [*type number*] [**detail**]

*type* (Optional) Type of the interface connected to the neighbors about which you want information.

*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.

## show cdp traffic

To display traffic information from the CDP table, use the **show cdp traffic** privileged EXEC command.

**show cdp traffic**

## show clock

To display the system clock, use the **show clock** EXEC command.

**show clock** [**detail**]

**detail** (Optional) Indicates the clock source (NTP, VINES, 7000 calendar, and so forth) and the current summer-time setting (if any).

## show debugging

To display information about the types of CDP debugging that are enabled for your router, use the **show debugging** privileged EXEC command.

**show debugging**

## show environment

Use the **show environment** EXEC command to display temperature and voltage information on the Cisco 7000 series, Cisco 7200 series, and Cisco 7500 series routers.

**show environment** [**all** | **last** | **table**]

- all** (Optional) Displays a detailed listing of the power supplies, temperature readings, and voltage readings.
- last** (Optional) Displays the reason for the last system shutdown that was related to voltage or temperature and the environmental status at that time.
- table** (Optional) Displays the temperature and voltage thresholds and a table that lists the ranges of environmental measurements that are within specification.

## show gt64010

Use the **show gt64010** EXEC command to display all GT64010 internal registers and interrupt status on the Cisco 7200 series routers.

**show gt64010**

## show logging

Use the **show logging** EXEC command to display the state of logging (syslog).

**show logging** [**history**]

- history** (Optional) Display information in the syslog history table only.

## show memory

Use the **show memory** EXEC command to show statistics about memory, including memory free pool statistics.

**show memory** [*memory-type*] [**free**] [**summary**]

- memory-type* (Optional) Memory type to display (**processor**, **multibus**, **io**, **sram**). If *type* is not specified, statistics for all memory types present are displayed.
- free** (Optional) Displays free memory statistics.
- summary** (Optional) Displays a summary of memory usage including the size and number of blocks allocated for each address of the system call that allocated the block.

## show ntp associations

To show the status of Network Time Protocol (NTP) associations, use the **show ntp associations** EXEC command.

**show ntp associations [detail]**

**detail** (Optional) Shows detailed information about each NTP association.

## show ntp status

To show the status of Network Time Protocol (NTP), use the **show ntp status** EXEC command.

**show ntp status**

## show pci

Use the **show pci** EXEC command to display information about the peripheral component interconnect (PCI) hardware registers or bridge registers for the Cisco 7200 series routers.

**show pci {hardware | bridge [register]}**

**hardware** Display PCI hardware registers.

**bridge** Display PCI bridge registers.

*register* (Optional) Number of a specific bridge register in the range 0 to 7. If not specified, this command displays information about all registers.

## show processes

Use the **show processes** EXEC command to display information about the active processes.

**show processes [cpu]**

**cpu** (Optional) Displays detailed CPU utilization statistics.

## show processes memory

Use the **show processes memory** EXEC command to show memory used.

**show processes memory**

## show protocols

Use the **show protocols** EXEC command to display the configured protocols.

This command shows the global and interface-specific status of any configured Level 3 protocol; for example, IP, DECnet, IPX, AppleTalk, and so forth.

**show protocols**

## show queueing

To list the current state of the queue lists, use the **show queueing** privileged EXEC command.

**show queueing** [**custom** | **fair** | **priority**]

- custom** (Optional) Shows status of custom queuing list configuration.
- fair** (Optional) Shows status of the fair queuing configuration. This is the default.
- priority** (Optional) Shows status of priority queuing list configuration.

## show rmon

Use the **show rmon** EXEC command to display the current RMON agent status on the router.

**show rmon** [**alarms** | **capture** | **events** | **filter** | **history** | **hosts** | **matrix** | **statistics** | **task** | **topn**]

- alarms** (Optional) Displays the RMON alarm table.
- capture** (Optional) Displays the RMON buffer capture table. Available on Cisco 2500 series and Cisco AS5200 only.
- events** (Optional) Displays the RMON event table.
- filter** (Optional) Displays the RMON filter table. Available on Cisco 2500 series and Cisco AS5200 only.
- history** (Optional) Displays the RMON history table. Available on Cisco 2500 series and Cisco AS5200 only.
- hosts** (Optional) Displays the RMON hosts table. Available on Cisco 2500 series and Cisco AS5200 only.
- matrix** (Optional) Displays the RMON matrix table. Available on Cisco 2500 series and Cisco AS5200 only.
- statistics** (Optional) Displays the RMON statistics table. Available on Cisco 2500 series and Cisco AS5200 only.
- task** (Optional) Displays general RMON statistics.
- topn** (Optional) Displays the RMON top-n hosts table. Available on Cisco 2500 series and Cisco AS5200 only.

## show rmon alarms

Use the **show rmon alarms** EXEC command to display the contents of the router's RMON alarm table.

**show rmon alarms**

## show rmon capture

Use the **show rmon capture** EXEC command to display the contents of the router's RMON capture table.

```
show rmon capture
```

## show rmon events

Use the **show rmon events** EXEC command to display the contents of the router's RMON event table.

```
show rmon events
```

## show rmon filter

Use the **show rmon filter** EXEC command to display the contents of the router's RMON filter table.

```
show rmon filter
```

## show rmon history

Use the **show rmon history** EXEC command to display the contents of the router's RMON history table.

```
show rmon history
```

## show rmon hosts

Use the **show rmon hosts** EXEC command to display the contents of the router's RMON hosts table.

```
show rmon hosts
```

## show rmon matrix

Use the **show rmon matrix** EXEC command to display the contents of the router's RMON matrix table.

```
show rmon matrix
```

## show rmon statistics

Use the **show rmon statistics** EXEC command to display the contents of the router's RMON statistics table.

```
show rmon statistics
```

## show rmon topn

Use the **show rmon topn** EXEC command to display the contents of the router's RMON Top-N host table.

```
show rmon topn
```

## show rtr application

Use the **show rtr application** EXEC command to display global information about the response time reporter feature.

**show rtr application** [**tabular** | **full**]

<b>tabular</b>	(Optional) Display information in a column format reducing the number of screens required to display the information.
<b>full</b>	(Optional) Display all information using identifiers next to each displayed value. This is the default.

## show rtr collection-statistics

Use the **show rtr collection-statistics** EXEC command to display statistical errors for all response time reporter probes or the specified probe.

**show rtr collection-statistics** [*probe*] [**tabular** | **full**]

<i>probe</i>	(Optional) Number of the response time reporter probe to display.
<b>tabular</b>	(Optional) Display information in a column format reducing the number of screens required to display the information.
<b>full</b>	(Optional) Display all information using identifiers next to each displayed value. This is the default.

## show rtr configuration

Use the **show rtr configuration** EXEC command to display configuration values including all defaults for all response time reporter probes or the specified probe.

**show rtr configuration** [*probe*] [**tabular** | **full**]

<i>probe</i>	(Optional) Number of the response time reporter probe to display.
<b>tabular</b>	(Optional) Display information in a column format reducing the number of screens required to display the information.
<b>full</b>	(Optional) Display all information using identifiers next to each displayed value. This is the default.

## show rtr distribution-statistics

Use the **show rtr distribution-statistics** EXEC command to display statistic distribution information (captured response times) for all response time reporter probes or the specified probe.

**show rtr distribution-statistics** [*probe*] [**tabular** | **full**]

<i>probe</i>	(Optional) Number of the response time reporter probe to display.
<b>tabular</b>	(Optional) Display information in a column format reducing the number of screens required to display the information. This is the default.

**full** (Optional) Display all information using identifiers next to each displayed value.

## show rtr history

Use the **show rtr history** EXEC command to display history collected for all response time reporter probes or the specified probe.

**show rtr history** [*probe*] [**tabular** | **full**]

*probe* (Optional) Number of the response time reporter probe to display.

**tabular** (Optional) Display information in a column format reducing the number of screens required to display the information. This is the default.

**full** (Optional) Display all information using identifiers next to each displayed value.

## show rtr operational-state

Use the **show rtr operational-state** EXEC command to display the operational state of all response time reporter probes or the specified probe.

**show rtr operational-state** [*probe*] [**tabular** | **full**]

*probe* (Optional) Number of the response time reporter probe to display.

**tabular** (Optional) Display information in a column format reducing the number of screens required to display the information.

**full** (Optional) Display all information using identifiers next to each displayed value. This is the default.

## show rtr reaction-trigger

Use the **show rtr reaction-trigger** EXEC command to display the reaction trigger information for all response time reporter probes or the specified probe.

**show rtr reaction-trigger** [*probe*] [**tabular** | **full**]

*probe* (Optional) Number of the response time reporter probe to display.

**tabular** (Optional) Display information in a column format reducing the number of screens required to display the information.

**full** (Optional) Display all information using identifiers next to each displayed value. This is the default.

## show rtr totals-statistics

Use the **show rtr totals-statistics** EXEC command to display the total statistical values (accumulation of error counts and completions) for all response time reporter probes or the specified probe.

**show rtr totals-statistics** [*probe*] [**tabular** | **full**]

- probe* (Optional) Number of the response time reporter probe to display.
- tabular** (Optional) Display information in a column format reducing the number of screens required to display the information.
- full** (Optional) Display all information using identifiers next to each displayed value. This is the default.

## show snmp

To check the status of communications between the SNMP agent and SNMP manager, use the **show snmp** EXEC command.

**show snmp**

## show stacks

Use the **show stacks** EXEC command to monitor the stack utilization of processes and interrupt routines.

**show stacks**

## show tcp

Use the **show tcp** EXEC command to display the status of TCP connections.

**show tcp** [*line-number*]

- line-number* (Optional) Absolute line number of the line for which you want to display Telnet connection status

## show tcp brief

To display a concise description of TCP connection endpoints, use the **show tcp brief** EXEC command.

**show tcp brief** [**all**]

- all** (Optional) Displays status for all endpoints. Without this keyword, endpoints in the LISTEN state are not shown.

## show tech-support

To display general information about the router when reporting a problem, use the **show tech-support** privileged EXEC command.

**show tech-support** [**page**] [**password**]

<b>page</b>	(Optional) Causes the output to display a page of information at a time. Use the return key to display the next line of output or use the space bar to display the next page of information. If not used, the output scrolls (that is, does not stop for page breaks).
<b>password</b>	(Optional) Leaves passwords and other security information in the output. If not used, passwords and other security-sensitive information in the output are replaced with the word “<removed>” (this is the default).

## snmp-server access-policy

To create or update an access policy, use the **snmp-server access-policy** global configuration command. To remove the specified access policy, use the **no** form of this command.

**snmp-server access-policy** *destination-party source-party context privileges*  
**no snmp-server access-policy** *destination-party source-party context*

<i>destination-party</i>	Name of a previously defined party identified as the destination party or target for this access policy. This name serves as a label used to reference a record defined for this party through the <b>snmp-server party</b> command.
<i>source-party</i>	Name of a previously defined party identified as the source party or subject for this access policy. This name serves as a label used to reference a record defined for this party through the <b>snmp-server party</b> command.
<i>context</i>	Name of a previously defined context that defines the resources for the access policy. This name serves as a label used to reference a record defined for this context through the <b>snmp-server context</b> command.
<i>privileges</i>	Bit mask representing the access privileges that govern the management operations that the source party can ask the destination party to perform.

## snmp-server chassis-id

To provide a message line identifying the SNMP server serial number, use the **snmp-server chassis-id** global configuration command. Use the **no** form of this command to restore the default value, if any.

**snmp-server chassis-id** *text*  
**no snmp-server chassis-id**

<i>text</i>	Message you want to enter to identify the chassis serial number.
-------------	--

## snmp-server community

To set up the community access string to permit access to the SNMPv1 protocol, use the **snmp-server community** global configuration command. The **no** form of this command removes the specified community string.

```
snmp-server community string [view view-name] [ro | rw] [number]  
no snmp-server community string
```

<i>string</i>	Community string that acts like a password and permits access to the SNMP protocol.
<b>view</b> <i>view-name</i>	(Optional) Name of a previously defined view. The view defines the objects available to the community.
<b>ro</b>	(Optional) Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
<b>rw</b>	(Optional) Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.
<i>number</i>	(Optional) Integer from 1 to 99 that specifies an access list of IP addresses that are allowed to use the community string to gain access to the SNMP v.1 agent.

## snmp-server contact

To set the system contact (syscontact) string, use the **snmp-server contact** global configuration command. Use the **no** form to remove the system contact information.

```
snmp-server contact text  
no snmp-server contact
```

<i>text</i>	String that describes the system contact information.
-------------	---

## snmp-server context

To create or update a context record, use the **snmp-server context** global configuration command. To remove a specific context entry, use the **no** form of this command.

```
snmp-server context context-name context-oid view-name  
no snmp-server context context-name
```

<i>context-name</i>	Name of the context to be created or updated. This name serves as a label used to reference a record for this context.
<i>context-oid</i>	Object identifier to assign to the context. Specify this value in dotted decimal notation, with an optional text identifier; for example, 1.3.6.1.6.3.3.1.4.192.180.45.11.1(== initialContextId.192.180.45.11.1).
<i>view-name</i>	Name of a previously defined view. The view defines the objects available to the context.

## snmp-server enable

To enable the router to send SNMP traps, use the **snmp-server enable** global configuration command. The **no** form of this command disables sending SNMP traps.

```
snmp-server enable traps [trap-type] [trap-option]  
no snmp-server enable traps [trap-type] [trap-option]
```

<b>traps</b>	Enables all traps.
<i>trap-type</i>	<p>(Optional) Type of trap to enable. If no type is specified, all traps are sent (including <b>envmon</b> and <b>repeater</b>). It can be one of the following values:</p> <ul style="list-style-type: none"> <li>• <b>bgp</b>—Send Border Gateway Protocol (BGP) state change traps.</li> <li>• <b>config</b>—Send configuration traps.</li> <li>• <b>frame-relay</b>—Send Frame Relay traps.</li> <li>• <b>isdn</b>—Send ISDN traps.</li> <li>• <b>envmon</b>—Send Cisco enterprise-specific environmental monitor traps when an environmental threshold is exceeded. When <b>envmon</b> is selected, you can specify a <i>trap-option</i>.</li> <li>• <b>repeater</b>—Send Ethernet hub repeaters. When <b>repeater</b> is selected, you can specify a <i>trap-option</i>.</li> <li>• <b>syslog</b>—Send error message traps (Cisco Syslog MIB). Specify the level of messages to be sent with the <b>logging history level</b> command.</li> </ul>
<i>trap-option</i>	<p>(Optional) When <b>envmon</b> is used, you can enable a specific environmental trap type, or accept all trap types from the environmental monitor system. If no option is specified, all environmental types are enabled. It can be one or more of the following values: <b>voltage</b>, <b>shutdown</b>, <b>supply</b>, <b>fan</b>, and <b>temperature</b>.</p> <p>When <b>repeater</b> is used, you can specify the repeater option. If no option is specified, all repeater types are enabled. It can be one or more of the following values:</p> <ul style="list-style-type: none"> <li>• <b>health</b>—enable IETF Repeater Hub MIB (RFC 1516) health trap.</li> <li>• <b>reset</b>—enable IETF Repeater Hub MIB (RFC 1516) reset trap.</li> </ul>

## snmp-server host

To specify the recipient of an SNMP trap operation, use the **snmp-server host** global configuration command. The **no** form of this command removes the specified host.

```
snmp-server host host community-string [trap-type]  
no snmp-server host host community-string [trap-type]
```

<i>host</i>	Name or Internet address of the host.
<i>community-string</i>	Password-like community string to send with the trap operation.

- trap-type* (Optional) Type of trap to be sent to the trap receiver *host*. If no type is specified, all traps are sent. It can be one or more of the following values:
- **bgp**—Send Border Gateway Protocol (BGP) state change traps.
  - **config**—Send configuration traps.
  - **dspu**—Send downstream physical unit (DSPU) traps.
  - **envmon**—Send Cisco enterprise-specific environmental monitor traps when an environmental threshold is exceeded.
  - **frame-relay**—Send Frame Relay traps.
  - **isdn**—Send ISDN traps.
  - **llc2**—Send Logical Link Control, type 2 (LLC2) traps.
  - **rprr**—Send standard repeater (hub) traps.
  - **rsrb**—Send remote source route bridging (RSRB) traps.
  - **sdlc**—Send Synchronous Data Link Control (SDLC) traps.
  - **sdllc**—Send SDLLC traps.
  - **snmp**—Send SNMP traps defined in RFC 1157.
  - **stun**—Send serial tunnel (STUN) traps.
  - **syslog**—Send error message traps (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history level** command.
  - **tty**—Send Cisco enterprise-specific traps when a TCP connection closes.
  - **x25**—Send X.25 event traps.

## snmp-server location

To set the system location string, use the **snmp-server location** global configuration command. Use the **no** form of this command to remove the location string.

```
snmp-server location text  
no snmp-server location
```

*text* String that describes the system location information.

## snmp-server packetsize

To establish control over the largest SNMP packet size permitted when the SNMP server is receiving a request or generating a reply, use the **snmp-server packetsize** global configuration command. Use the **no** form of this command to restore the default value.

```
snmp-server packetsize byte-count  
no snmp-server packetsize
```

*byte-count* Integer byte count from 484 to 8192.

## snmp-server party

To create or update a party record, use the **snmp-server party** global configuration command. To remove a specific party entry, use the **no** form of this command.

```
snmp-server party party-name party-oid [protocol-address] [packetsize size]
    [local | remote] [authentication {md5 key [clock clock]
    [lifetime lifetime] | snmpv1 string}
no snmp-server party party-name
```

<i>party-name</i>	Name of the party characterized by the contents of the record. This name serves as a label used to reference the party record that you are creating or modifying.
<i>party-oid</i>	Object identifier to assign to the party. Specify this value in dotted decimal notation, with an optional text identifier; for example, 1.3.6.1.6.3.3.1.3.192.180.34.54.1 (= initialPartyId.192.180.34.54.1).
<i>protocol-address</i>	(Optional) Address of the protocol that the party record pertains to. Currently the only supported protocol is UDP, so this value specifies a UDP address in the format <i>a.b.c.d port</i> .  In future releases, additional protocols will be supported. This value is used to specify the destination of trap messages.
<b>packetsize</b> <i>size</i>	(Optional) Maximum size in bytes of a message that this party is able to receive. By default, the packet size set through the <b>snmp-server packetsize</b> command is used.
<b>local</b>   <b>remote</b>	(Optional) Indicates that the party is local or remote. If neither <b>local</b> nor <b>remote</b> is specified, a default value of local is assumed.
<b>authentication</b>	(Optional) Indicates that the party uses an authentication protocol. If specified, either <b>md5</b> or <b>snmpv1</b> is required.
<b>md5</b> <i>key</i>	(Optional) Indicates that the party uses the Message Digest algorithm MD5 for message authentication. If <b>md5</b> is specified, you must also specify a 16-byte hexadecimal ASCII string representing the MD5 authentication key for the party. All messages sent to this party will be authenticated using the SNMP v2 MD5 authentication method with the key specified by <i>key</i> .
<b>clock</b> <i>clock</i>	(Optional) Initial value of the authentication clock.
<b>lifetime</b> <i>lifetime</i>	(Optional) Lifetime, in seconds, that represents the upper bound on acceptable delivery delay for messages generated by the party.
<b>snmpv1</b> <i>string</i>	(Optional) Community string. The keyword <b>snmpv1</b> indicates that the party uses community-based authentication. All messages sent to this party will be authenticated using the SNMP v1community string specified by <i>string</i> instead of MD5.

## snmp-server queue-length

To establish the message queue length for each trap host, use the **snmp-server queue-length** global configuration command.

**snmp-server queue-length** *length*

*length* Integer that specifies the number of trap events that can be held before the queue must be emptied.

## snmp-server system-shutdown

To use the SNMP message reload feature, the router configuration must include the **snmp-server system-shutdown** global configuration command. The **no** form of this command prevents an SNMP system-shutdown request (from an SNMP manager) from resetting the Cisco agent.

**snmp-server system-shutdown**  
**no snmp-server system-shutdown**

## snmp-server trap-authentication

To establish trap message authentication, use the **snmp-server trap-authentication** global configuration command. To remove message authentication, use the **no** form of this command.

**snmp-server trap-authentication** [**snmpv1** | **snmpv2**]  
**no snmp-server trap-authentication** [**snmp1** | **snmp2**]

**snmpv1** (Optional) Indicates that SNMP authentication traps will be sent to SNMPv1 management stations only.

**snmpv2** (Optional) Indicates that SNMP authentication traps will be sent to SNMPv2 management stations only.

## snmp-server trap-source

To specify the interface (and hence the corresponding IP address) that an SNMP trap should originate from, use the **snmp-server trap-source** global configuration command. Use the **no** form of the command to remove the source designation.

**snmp-server trap-source** *interface*  
**no snmp-server trap-source**

*interface* Interface from which the SNMP trap originates. The argument includes the interface type and number in platform-specific syntax.

## snmp-server trap-timeout

To define how often to try resending trap messages on the retransmission queue, use the **snmp-server trap-timeout** global configuration command.

**snmp-server trap-timeout** *seconds*

*seconds* Integer that sets the interval, in seconds, for resending the messages.

## snmp-server view

To create or update a view entry, use the **snmp-server view** global configuration command. To remove the specified 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
```

<i>view-name</i>	Label for the view record that you are updating or creating. The name is used to reference the record.
<i>oid-tree</i>	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 <i>1.3.6.2.4</i> , or a word, such as <i>system</i> . Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example <i>1.3.*.4</i> .
<b>included</b>   <b>excluded</b>	Type of view. You must specify either <b>included</b> or <b>excluded</b> .

## statistics-distribution-interval

To set the time interval for each statistics distribution kept for the response time reporter, use the **statistics-distribution-interval** response time reporter configuration command. Use the **no** form of this command to return to the default value.

```
statistics-distribution-interval milliseconds
no statistics-distribution-interval
```

<i>milliseconds</i>	Number of milliseconds used for each statistics distribution kept. The default is 20 ms.
---------------------	--

## tag

To create a user-specified identifier for a response time reporter probe, use the **tag** response time reporter configuration command. It is normally used to logically link probes together in a group. Use the **no** form of this command to remove a tag from a probe.

```
tag text
no tag
```

<i>text</i>	Name of a group that this probe belongs to. From 0 to 16 ASCII characters.
-------------	--

## test flash

To test Flash memory on MCI and envm Flash EPROM interfaces, use the **test flash EXEC** command.

```
test flash
```

## test interfaces

To test the system interfaces on the modular router, use the **test interfaces EXEC** command.

**test interfaces**

## test memory

To perform a test of Multibus memory (including nonvolatile memory) on the modular router, use the **test memory EXEC** command.

**test memory**

## threshold

To set the rising threshold (hysteresis) that generates a reaction event and stores history information for the response time reporter probe, use the **threshold** response time reporter configuration command. Use the **no** form of this command to return to the default value.

**threshold** *millisecond*

**no threshold**

*millisecond*                      Number of milliseconds required for a rising threshold to be declared. The default value is 5000 ms.

## timeout

To set the amount of time the response time reporter probe waits for a response from its request packet, use the **timeout** response time reporter configuration command. Use the **no** form of this command to return to the default value.

**timeout** *millisecond*

**no timeout**

*millisecond*                      Number of milliseconds the probe waits to receive a response from its request packet. The default is 5000 ms.

## trace (privileged)

Use the **trace EXEC** command to discover the routes that packets will actually take when traveling to their destination.

**trace** [*protocol*] [*destination*]

*protocol*                      (Optional) Protocols that can be used are **appletalk**, **cns**, **ip** and **vines**.

*destination*                      (Optional) Destination address or host name on the command line. The default parameters for the appropriate protocol are assumed and the tracing action begins.

## trace (user)

Use the **trace EXEC** command to discover the IP routes that packets will actually take when traveling to their destination.

**trace** [*protocol*] [*destination*]

<i>protocol</i>	(Optional) Protocols that can be used are <b>appletalk</b> , <b>clns</b> , <b>ip</b> and <b>vines</b> .
<i>destination</i>	(Optional) Destination address or host name on the command line. The default parameters for the appropriate protocol are assumed and the tracing action begins.

## traffic-shape adaptive

To configure a Frame Relay subinterface to estimate the available bandwidth when backward explicit congestion notifications (BECNs) are received, use the **traffic-shape adaptive** interface configuration command. Use the **no** form of this command to stop adapting to congestion signals.

**traffic-shape adaptive** [*bit-rate*]  
**no traffic-shape adaptive**

<i>bit-rate</i>	(Optional) Lowest bit rate that traffic is shaped to in kbps. The default is half the value specified for the <b>traffic-shape rate</b> or <b>traffic-shape group</b> <i>bit-rate</i> option.
-----------------	---

## traffic-shape group

To enable traffic shaping based on a specific access list for outbound traffic on an interface, use the **traffic-shape group** interface configuration command. Use the **no** form of this command to disable traffic shaping on the interface for the access list.

**traffic-shape group** *access-list* *bit-rate* [*burst-size* [*excess-burst-size*]]  
**no traffic-shape group** *access-list*

<i>access-list</i>	Number of the access list that controls the packets that traffic shaping is applied to on the interface.
<i>bit-rate</i>	Bit rate that traffic is shaped to in bps. This is the access bit rate that you contract with your service provider or the service level you intend to maintain.
<i>burst-size</i>	(Optional) Sustained number of bits that can be transmitted per interval. On Frame Relay interfaces, this is the committed burst size contracted with your service provider. The default is the <i>bit-rate</i> divided by 8.
<i>excess-burst-size</i>	(Optional) Maximum number of bits that can exceed the burst size in the first interval in a congestion event. On Frame Relay interfaces, this is the excess burst size contracted with your service provider. The default is equal to the <i>burst-size</i> .

## traffic-shape rate

To enable traffic shaping for outbound traffic on an interface, use the **traffic-shape rate** interface configuration command. Use the **no** form of this command to disable traffic shaping on the interface.

**traffic-shape rate** *bit-rate* [*burst-size* [*excess-burst-size*]]

**no traffic-shape rate**

<i>bit-rate</i>	Bit rate that traffic is shaped to in kbps. This is the access bit rate that you contract with your service provider or the service level you intend to maintain.
<i>burst-size</i>	(Optional) Sustained number of bits that can be transmitted per interval. On Frame Relay interfaces, this is the committed burst size contracted with your service provider. The default is the <i>bit-rate</i> divided by 8.
<i>excess-burst-size</i>	(Optional) Maximum number of bits that can exceed the burst size in the first interval in a congestion event. On Frame Relay interfaces, this is the excess burst size contracted with your service provider. The default is equal to the <i>burst-size</i> .

## type

To configure the type of response time reporter probe, use the **type** response time reporter configuration command. You must configure the probe's type before you can configure any of the other characteristics of the probe. Use the **no** form of this command to remove all response time reporter configuration information for a probe and return all other response time reporter configuration commands to their default values.

**type** {**echo** | **pathEcho**} **protocol** *type* *type-target*

**no rtr** *probe*

<b>echo</b>	Perform end-to-end response time reporter operations only.
<b>pathEcho</b>	Perform response time reporter operations by using a route discovery algorithm to find a path to the destination and echo each device on the path.

**protocol** *type type-target* Protocol used by the probe. Type can be one of the following keywords (whether the keyword is available depends on the Cisco IOS software features installed on your router) followed by the required type parameter:

- **ipIcmpEcho** {*ip-address* | *ip-host-name*}—IP/ICMP Echo that requires a destination IP address or IP host name.
- **snaRUEcho** *sna-host-name*—SNA's SSCP Native Echo that requires the host name defined for the SNA's Physical Unit connection to VTAM.
- **snaLU0EchoAppl** *sna-host-name* [*sna-application*] [*sna-mode*]—An SNA LU Type 0 connection to Cisco's NSPECHO host application that requires the host name defined for the SNA's Physical Unit connection to VTAM. Optionally specify the host application name (the default is NSPECHO) and SNA mode to access the application.
- **snaLU2EchoAppl** *sna-host-name* [*sna-application*] [*sna-mode*]—An SNA LU Type 2 connection to Cisco's NSPECHO host application that requires the host name defined for the SNA's Physical Unit connection to VTAM. Optionally specify the host application name (the default is NSPECHO), and SNA mode to access the application.

## verify-data

To cause the response time reporter probe to check each response for corruption, use the **verify-data** response time reporter configuration command. Use the **no** form of this command to return to the default value.

**verify-data**  
**no verify-data**

