System Management Commands

This section 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 *Router Products Command Reference* publication.

[**no**] **buffers** {**small** | **middle** | **big** | **large** | **huge**} {**permanent** | **max-free** | **min-free** | **initial**} *number*

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.

small	Small buffer size.
middle	Medium buffer size.
big	Big buffer size.
large	Large buffer size.
huge	Huge buffer size.
permanent	Number of permanent buffers that the system tries to allocate. Permanent buffers are normally not deallocated by the system.
max-free	Maximum number of free or unallocated buffers in a buffer pool.
min-free	Minimum number of free or unallocated buffers in a buffer pool.
initial	Number of additional temporary buffers that should be allocated when the system is reloaded. This can be used to ensure that the system has necessary buffers immediately after reloading in a high-traffic environment.

number	Number of buffers to be allocated.

[**no**] **buffers huge size** *number*

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.

number	Number of buffers to be allocated.

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

To set the Cisco 7000 series system calendar, use the **calendar se**t EXEC command.

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)

[**no**] **clock calendar-valid**

To configure the Cisco 7000 series 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 router so that the calendar is not an authoritative time source.

clock read-calendar

To manually read the calendar into the Cisco 7000 series system clock, use the **clock read-calendar** EXEC command.

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

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

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 *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

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 router not to automatically switch to summer time.

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

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

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

clock update-calendar

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

custom-queue-list *list*
no custom-queue-list [***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.

list	Number of the custom queue list you want to assign to the interface. An integer from 1 to 10.

[**no**] **enable last-resort** {**password** | **succeed**}

To specify what happens if the TACACS servers used by the **enable** command do not respond, use the **enable last-resort** global configuration command. The **no** form of this command restores the default.

password	Allows you to enable by entering the privileged command level password.
succeed	Allows you to enable without further question.

enable password *password*

To assign a password for the privileged command level, use the **enable password** global configuration command. The commands **enable password** and **enable-password** are synonymous.

password	Case-sensitive character string that specifies the line password prompted for in response to the EXEC command **enable**. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the *password* in the format *number-space-anything*. The space after the number causes problems.

[**no**] **enable use-tacacs**

To enable use of the TACACS to determine whether a user can access the privileged command level, use the **enable use-tacacs** global configuration command. Use the **no** form of this command to disable TACACS verification.

hostname *name*

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.

name	New host name for the network server; the name is case sensitive.

[**no**] **logging** *host*

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.

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

[**no**] **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 console *level*
no logging console

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

level	Limits the logging of messages displayed on the console terminal to the named level. See the error message logging priorities table in the *Router Products Command Reference* publication for a list of the *level* keywords.

logging facility *facility-type*
no 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 logging facility** global configuration command.

facility-type	See the logging facility facility-type keywords table in the *Router Products Command Reference* publication.

logging monitor *level*
no 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 logging monitor command disables logging to terminal lines other than the console line.

level	One of the *level* keywords listed in the error message logging priorities table in the *Router Products Command Reference* publication.

[**no**] **logging on**

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

logging trap *level*
no 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. The **no** form of this command disables logging to syslog servers.

level	One of the *level* keywords listed in the error message logging priorities table in the *Router Products Command Reference* publication.

ntp access-group {**query-only** | **serve-only** | **serve** | **peer**}
access-list-number
no ntp access-group {**query-only** | **serve-only** | **serve** | **peer**}

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.

query-only	Allows only NTP control queries. See RFC 1305 (NTP version 3).

serve-only	Allows only time requests.
serve	Allows time requests and NTP control queries, but does not allow the system to synchronize to the remote system.
peer	Allows time requests and NTP control queries and allows the system to synchronize to the remote system.
number	Number (1 to 99) of a standard IP access list.

[**no**] **ntp authenticate**

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

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

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.

number	Key number (1 to 4294967295)
value	Key value (an arbitrary string of up to eight characters)

ntp broadcast [**version** *number*]
no 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.

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

ntp broadcast client
no 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 broadcastdelay *microseconds*
no ntp broadcastdelay

To set the estimated round-trip delay between the router 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.

microseconds	Estimated round-trip time (in microseconds) for NTP broadcasts. The range is from 1 to 999999. The default is 3000.

ntp clock-period *value*
no ntp clock-period

Do not enter this command; it is documented for informational purposes only. As NTP compensates for the error in the system clock, it keeps track of the correction factor for this error. The system will automatically save 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.

value	Amount to add to the system clock for each clock hardware tick (in units of 2^{-32} seconds). The default is 17179869 (4 milliseconds).

[**no**] **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 ntp disable** interface configuration command.

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

To configure the router as an NTP master clock to which peers synchronize themselves when an external NTP source is not available, use the **ntp maste**r global configuration command. To disable the master clock function, use the **no** form of this command.

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

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

To configure the router's 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.

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) Identifies the interface from which to pick the IP source address.
interface	(Optional) Name of the interface from which to pick the IP source address.
prefer	(Optional) Makes this peer the preferred peer that provides synchronization.

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

To allow the router's 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.

ip address	IP address of the time server providing 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) Identifies the interface from which to pick the IP source address.
interface	(Optional) Name of the interface from which to pick the IP source address.
prefer	(Optional) Makes this server the preferred server that provides synchronization.

ntp source *interface*
no 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.

interface	Any valid system interface name.

[**no**] **ntp trusted-key** *key-number*

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.

key-number	Key number of authentication key to be trusted.

[**no**] **ntp update-calendar**

To periodically update the Cisco 7000 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.

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

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

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

priority-group *list*
no priority-group

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

list	Priority list number assigned to the interface

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

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.

list-number	Arbitrary integer between 1 and 10 that identifies the priority list selected by the user
high | **medium** | **normal** | **low**	Priority queue level

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

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.

list-number	Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.
interface-type	Name of the interface.
interface-number	Number of the specified interface.
high | **medium** | **normal** | **low**	Priority queue level.

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

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**, **ip**, **ipx**, **pad**, **rsrb**, **stun**, **vines**, **xns**, and **x25**.
high | **medium** | **normal** | **low**	Priority queue level.
queue-keyword keyword-value	Possible queue keywords are **fragments**, **gt**, **lt**, **list**, **tcp**, and **udp**. See the queue keywords table for this command in the *Router Products Command Reference* publication.

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

list-number	Arbitrary integer between 1 and 10 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.

[**no**] **priority-list** *list-number* **stun** {**high** | **medium** | **normal** | **low**} **address** *group-number address*

To establish queuing priorities based on the address of the serial link on a STUN connection, use the **priority-list stun** global configuration command. Use the **no** form of this command with the appropriate arguments to remove an entry from the list.

list-number	Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.
high | **medium** | **normal** | **low**	Priority queue level.
address	Required keyword.
group-number	Group number used in the **stun group** command.
address	Address of the serial link. The format of the address is either a 1-byte hex value (for example, C1) for an SDLC link or one that is specified by the **stun schema** global configuration command.

[**no**] **queue-list** *list* **default** *queue-number*

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.

list	Number of the queue list. An integer from 1 to 10.
queue-number	Number of the queue. An integer from 1 to 10.

queue-list *list-number* **interface** *interface-type interface-number queue-number*
no queue-list *list-number* **interface** *queue-number*

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.

list-number	Number of the queue list. An integer from 1 to 10.
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 10.

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

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

list-number	Number of the queue list. An integer from 1 to 10.
protocol-name	Required argument that specifies the protocol type: **aarp**, **arp**, **apollo**, **appletalk**, **bridge** (transparent), **clns**, **clns_es**, **clns_is**, **compressedtcp**, **cmns**, **decnet**, **decnet_node**, **decnet_router**, **ip**, **ipx**, **pad**, **rsrb**, **stun**, **vines**, **xns**, and **x25**.
queue-number	Number of the queue. An integer from 1 to 10.

queue-keyword keyword-value	Possible keywords are **gt**, **lt**, **list**, **tcp**, and **udp**. See the protocol priority queue values table in the *Router Products Command Reference* publication.

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

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 this command.

list-number	Number of the queue list. An integer from 1 to 10.
queue-number	Number of the queue. An integer from 1 to 10.
byte-count-number	Specifies the lower boundary on how many bytes the system allows to be delivered from a given queue during a particular cycle.

[**no**] **queue-list** *list-number* **queue** *queue-number* **limit** *limit-number*

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 this command.

list-number	Number of the queue list. An integer from 1 to 10.
queue-number	Number of the queue. An integer from 1 to 10.
limit-number	Maximum number of packets which can be queued at any time. Range is 0 to 32767 queue entries.

[**no**] **queue-list** *list-number* **stun** *queue-number* **address** *group-number address-number*

To establish queuing priorities based on the address of the serial link on a STUN connection, use the **queue-list stun** global configuration command. Use the **no** form of this command with the appropriate arguments to remove an entry from the list.

list-number	Number of the queue list. An integer from 1 to 10.
queue-number	Queue number in the range from 1 to 10.
address	Required keyword.
group-number	Group number used in the **stun group** command.
address-number	Address of the serial link. The format of the address is either a 1-byte hex value (for example, C1) for an SDLC link or one that is specified by the **stun schema** configuration command.

scheduler-interval *milliseconds*
no scheduler-interval

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

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

[**no**] **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.

[**no**] **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.

[**no**] **service password-encryption**

To encrypt passwords, use the **service password-encryption** global configuration command. Use the **no** form of this command to disable this service.

[**no**] **service tcp-keepalives** {**in** | **out**}

To generate keepalive packets on idle network connections, use the **service tcp-keepalives** global configuration command. The **no** form of this command with the appropriate keyword disables the keepalives.

in	Generates keepalives on incoming connections (initiated by remote host).
out	Generates keepalives on outgoing connections (initiated by a user).

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

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.

type	(Optional) Type of message to timestamp: **debug** or **log**.

uptime	(Optional) Timestamp with time since the system was rebooted.
datetime	Timestamp with the date and time.
msec	(Optional) Add milliseconds to the date and time.
localtime	(Optional) Timestamp relative to the local time zone.
show-timezone	(Optional) Include the time zone name in the timestamp.

show buffers [*interface*]

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

The network server has one pool of queuing elements and five pools of packet buffers of different sizes. For each pool, the network server keeps counts of the number of buffers outstanding, the number of buffers in the free list, and the maximum number of buffers allowed in the free list.

interface	(Optional) Causes a search of all buffers that have been associated with that interface for longer than one minute. The contents of these buffers are printed to the screen. This option is useful in diagnosing problems where the input queue count on an interface is consistently nonzero.

show calendar

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

show clock [**detail**]

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

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

show environment

Use the **show environment** EXEC command to display temperature and voltage information on the AGS+ and Cisco 7000 series console.

show environment all

Use the **show environment all** EXEC command to display temperature and voltage information on the Cisco 7000 series console.

show environment last

If a shutdown occurs due to detection of fatal environmental margins, the CSC-ENVM (on the AGS+) or the route processor (RP) (on the Cisco 7000 series) logs the last measured value from each of the six test points to internal nonvolatile memory. Only one set of measurements may be stored at any one time.

Use the **show environment last** EXEC command to display these test points.

show environment table

Use the **show environment table** EXEC command to display environmental measurements and a table that lists the ranges of environment measurement that are within specification.This command is available on the Cisco 7000 series only.

show logging

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

This command displays the state of syslog error and event logging, including host addresses, and whether console logging is enabled. This command also displays Simple Network Management Protocol (SNMP) configuration parameters and protocol activity.

show memory [*type*] [**free**]

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

type	(Optional) Memory type to display (**processor**, **multibus**, **io**, **sram**). If *type* is not specified, statistics for all memory types present in the router will be displayed.
free	(Optional) Displays free memory statistics.

show ntp associations [**detail**]

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

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 processes [**cpu**]

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

cpu	(Optional) Displays detailed CPU utilization statistics.

show processes memory

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

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 queueing [**custom** | **priority**]

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

custom	(Optional) Shows status of custom queue lists.
priority	(Optional) Shows status of priority lists.

show snmp

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

show stacks

Use the **show stacks** EXEC command to monitor the stack utilization of processes and interrupt routines. Its display includes the reason for the last system reboot. If the system was reloaded because of a system failure, a saved system stack trace is displayed. This information is of use only to Cisco engineers analyzing crashes in the field. It is included here in case you need to read the displayed statistics to an engineer over the phone.

[**no**] **snmp-server access-list** *list-number*

To set up an access list that determines which hosts can send requests to the network server, use the snmp-server access-list global configuration command. Use the **no** form of this command to remove the specified access list.

list-number	Integer from 1 to 99 that specifies an IP access list number.

snmp-server chassis-id *text*
no 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 remove the message line.

text	Message you want to enter to identify the chassis serial number.

snmp-server community [*string* [**RO** | **RW**] [*number*]]
no snmp-server [**community** [*string*]]

To set up the community access string, use the snmp-server community global configuration command. This command enables SNMP server operation on the router. The **no** form of this command removes the specified community string or access list.

string	(Optional) Community string that acts like a password and permits access to the SNMP protocol.
RO	(Optional) Specifies read-only access.
RW	(Optional) Specifies read-write access.
number	(Optional) Integer from 1 to 99 that specifies an access list of IP addresses that might use the community string.

snmp-server contact *text*
no snmp-server contact

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

text	String that describes the system contact information.

snmp-server host *address community-string* [**snmp**] [**tty**]
no snmp-server host *address community-string*

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.

address	Name or IP address of the host.
community-string	Password-like community string to send with the trap operation.

snmp	(Optional) Enables the SNMP traps defined in RFC 1157.
tty	(Optional) Enables Cisco enterprise-specific traps when a TCP connection closes.

snmp-server location *text*
no 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.

text	String that describes the system location information.

snmp-server packetsize *byte-count*
no snmp-server packetsize

To specify 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.

byte-count	Integer byte count from 484 to 8192

snmp-server queue-length *length*

To establish the message queue length for each trap host, use the snmp-server queue-length global configuration command. This command defines the length of the message queue for each trap host. Once a trap message is successfully transmitted, software will continue to empty the queue, but never faster than at a rate of four trap messages per second.

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

[**no**] **snmp-server system-shutdown**

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

[**no**] **snmp-server trap-authentication**

To establish trap message authentication, use the snmp-server trap-authentication global configuration command. This command enables the network server to send a trap message when it receives a packet with an incorrect community string. Use the no snmp-server trap-authentication command to remove message authentication.

snmp-server trap-source *interface*
no 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 this command to remove the source designation.

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

snmp-server trap-timeout *seconds*

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

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

tacacs-server attempts *count*
no tacacs-server attempts

To control the number of login attempts that can be made on a line set up for TACACS verification, use the **tacacs-server attempts** global configuration command. Use the **no** form of this command to remove this feature and restore the default.

count	Integer that sets the number of attempts.

tacacs-server authenticate {**connection** | **enable**}

The **tacacs-server authenticate** global configuration command requires a response from the network or router to indicate whether the user may perform the indicated action. Enter one of the keywords to specify the action (when a user makes TCP connection, for example).

connection	Configures a required response when a user makes a TCP connection.
enable	Configures a required response when a user enters the **enable** command.

[**no**] **tacacs-server extended**

To enable an extended TACACS mode, use the **tacacs-server extended** global configuration command. Use the no tacacs-server extended command to disable the mode.

[**no**] **tacacs-server host** *name*

To specify a TACACS host, use the tacacs-server host global configuration command. You can use multiple tacacs-server host commands to specify multiple hosts. The software searches for the hosts in the order you specify them. The **no** form of this command deletes the specified name or address.

name	Name or IP address of the host.

[**no**] **tacacs-server last-resort** {**password** | **succeed**}

To cause the network server to request the privileged password as verification, or to force successful login without further input from the user, use the tacacs-server last-resort global configuration command. The **no** form of this command restores the system to the default behavior.

password	Allows the user to access the EXEC command mode by entering the password set by the **enable** command.
succeed	Allows the user to access the EXEC command mode without further question.

tacacs-server notify {**connection** | **enable** | **logout**}

Use the **tacacs-server notify** global configuration command to cause a message to be transmitted to the TACACS server, with retransmission being performed by a background process for up to 5 minutes. The terminal user, however, receives an immediate response allowing access to the feature specified. Enter one of the keywords to specify notification of the TACACS server upon the corresponding action (when user logs out, for example).

connection	Specifies that a message be transmitted when a user makes a TCP connection.
enable	Specifies that a message be transmitted when a user enters the **enable** command.
logout	Specifies that a message be transmitted when a user logs out.

[**no**] **tacacs-server optional-passwords**

To specify that the first TACACS request to a TACACS server be made *without* password verification, use the **tacacs-server optional-passwords** global configuration command. Use the **no** form of this command to restore the default.

tacacs-server retransmit *retries*
no tacacs-server retransmit

To specify the number of times the router software will search the list of TACACS server hosts before giving up, use the tacacs-server retransmit global configuration command. The router software will try all servers, allowing each one to time out before increasing the retransmit count. The no tacacs-server retransmit command restores the default.

retries Integer that specifies the retransmit count.

tacacs-server timeout *seconds*
no tacacs-server timeout

To set the interval that the server waits for a server host to reply, use the **tacacs-server timeout** global configuration command. The **no** form of this command restores the default.

seconds Integer that specifies the timeout interval in seconds.

test flash

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

test interfaces

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

test memory

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

trace [*protocol*] [*destination*]

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

protocol	(Optional) Protocols that can be used are **appletalk**, **clns**, **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.

username *name* [**nopassword** | **password** *encryption-type* **password**]
username *name* **password** *secret*
username *name* [**access-class** *number*]
username *name* [**autocommand** *command*]
username *name* [**noescape**] [**nohangup**]

To establish a username-based authentication system at login, even though your network cannot support a TACACS service, use the **username** global configuration command.

name	Host name, server name, user ID, or command name.
nopassword	(Optional) Specifies that no password is required for this user to log in. This is usually most useful in combination with the **autocommand** keyword.
password	Specifies a possibly encrypted password for this username.
encryption-type	(Optional) A single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Currently defined encryption types are 0, which means that the text immediately following is not encrypted, and 7, which means that the text is encrypted using a Cisco-defined encryption algorithm.

password	(Optional) A password can contain embedded spaces and must be the last option specified in the **username** command.
secret	For CHAP authentication: specifies the secret for the local router or the remote device. The secret is encrypted when it is stored on the local router. This prevents the secret from being stolen. The secret can consist of any string of up to 11 printable ASCII characters. There is no limit to the number of username/password combinations that can be specified, allowing any number of remote devices to be authenticated.
access-class	(Optional) Specifies an outgoing access list that overrides the access list specified in the **access-class** line configuration command. It is used for the duration of the user's session.
number	(Optional) The access list number.
autocommand	(Optional) Causes the specified command to be issued automatically after the user logs in. When the command is complete, the session is terminated. As the command can be any length and contain imbedded spaces, commands using the **autocommand** keyword must be the last option on the line.
command	(Optional) The command string.
noescape	(Optional) Prevents a user from using an escape character on the host to which that user is connected.
nohangup	(Optional) Prevents the router /from disconnecting the user after an automatic command (set up with the **autocommand** keyword) has completed. Instead, the user gets another login prompt.