# 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 *Router Products Command Reference* publication.

**aaa accounting** {**system** | **network** | **connection** | **exec** |
**command** *level*} {**start-stop** |
**wait-start** | **stop-only**} **tacacs+**
**no aaa accounting** {**system** | **network** | **connection** | **exec** |
**command** *level*}

To enable AAA accounting of requested services for billing or security purposes when using TACACS+, use the **aaa accounting** global configuration command. Use the **no** form of this command to disable accounting.

| | |
|---|---|
| **system** | Performs accounting for all system-level events not associated with users, such as reloads. |
| **network** | Runs accounting for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARAP. |
| **connection** | Runs accounting for outbound Telnet and rlogin. |
| **exec** | Runs accounting for Execs (user shells). This keyword might return user profile information such as **autocommand** information. |
| **command** | Runs accounting for all commands at the specified privilege level. |
| *level* | Command level that should be accounted. Valid entries are 0 through 15. |

| | |
|---|---|
| **start-stop** | Sends a start record accounting notice at the beginning of a process and a stop record is sent at the end of a process. The start accounting record is sent in the background. The requested user process begins regardless of whether or not the start accounting record was received by the accounting server. |
| **wait-start** | As in **start-stop**, sends both a start and a stop accounting record to the accounting server. However, if you use the **wait-start** keyword, the requested user service does not begin until the start accounting record is acknowledged. A stop accounting record is also sent. |
| **stop-only** | Sends a stop record accounting notice at the end of the requested user process. |

[**no**] **aaa authentication arap** {**default** | *list-name*} *method1* [...[*method4*]]

To enable an AAA authentication method for ARA users using TACACS+, use the **aaa authentication arap** global configuration command. Use the **no** form of the command to disable this authentication.

| | |
|---|---|
| **default** | Uses the listed methods that follow this argument as the default list of methods when a user logs in. |
| *list-name* | Character string used to name the following list of authentication methods tried when a user logs in. |
| *method* | At least one and up to four of the keywords described in the table “AAA Authentication ARAP Method Descriptions.” See this command in the *Router Products Command Reference* publication for the keywords table. |

[**no**] **aaa authentication enable default** *method1* [...[*method4*]]

To enable AAA authentication to determine if a user can access the privileged command level with TACACS+, use the **aaa authentication enable default** global configuration command. Use the **no** form of the command to disable this authorization method.

| | |
|---|---|
| *method* | At least one and up to four of the keywords described in the table "AAA Authentication Enable Default Method Descriptions." See this command in the *Router Products Command Reference* publication for the keywords table. |

[**no**] **aaa authentication local-override**

To have the router check the local user database for authentication before attempting another form of authentication, use the **aaa authentication local-override** global configuration command. Use the **no** form of the command to disable the override.

[**no**] **aaa authentication login** {**default** | *list-name*} *method1* [...[*method4*]]

To set AAA authentication at login when using TACACS+, use the **aaa authentication login** global configuration command. Use the **no** form of the command to disable AAA authentication.

| | |
|---|---|
| **default** | Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in. |
| *list-name* | Character string used to name the following list of authentication methods tried when a user logs in. |
| *method* | At least one and up to four of the methods described in the keywords table "AAA Authentication Login Method Descriptions." See this command in the *Router Products Command Reference* publication for the keywords table. |

[**no**] **aaa authentication ppp** {**default** | *list-name*} *method1* [...[*method4*]]

To specify one or more AAA authentication methods for use on serial interfaces running PPP when using TACACS+, use the **aaa authentication ppp** global configuration command. Use the **no** form of the command to disable authentication.

| | |
|---|---|
| **default** | Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in. |
| *list-name* | Character string used to name the following list of authentication methods tried when a user logs in. |
| *method* | At least one and up to four of the methods described in the methods keyword table "AAA Authentication PPP Method Descriptions." See this command in the *Router Products Command Reference* publication for the keywords table. |

**aaa authorization** {**network** | **connection** | **exec** | **command** *level*} *methods*
**no aaa authorization** {**network** | **connection** | **exec** | **command** *level*}

To set parameters that restrict a user's network access based on TACACS+ authorization, use the **aaa authorization** global configuration command. To disable authorization for a function, use the **no** form of the command.

| | |
|---|---|
| **network** | Performs authorization for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARAP. |
| **connection** | Runs authorization for outbound Telnet and rlogin. |
| **exec** | Runs authorization to determine if the user is allowed to run an EXEC shell. This keyword might return user profile information such as **autocommand** information. |

| | |
|---|---|
| **command** | Runs authorization for all commands at the specified privilege level. |
| *level* | Specific command level that should be authorized. Valid entries are 0 through 15. |
| *methods* | The table "AAA Authorization Method Descriptions" lists the *methods* keywords. See this command in the *Router Products Command Reference* publication for the keywords table. |

[**no**] **aaa new-model**

To enable the AAA access control model that includes TACACS+, issue the **aaa new-model** global configuration command. Use the **no** form of the command to disable this functionality.

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

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

| | |
|---|---|
| *mode* | Command mode of the original and alias commands. See this command in the *Router Products Command Reference* publication for the mode argumnet options keywords table. |
| *alias-name* | Command alias. |
| *alias-command-line* | Original command syntax. |

[**no**] **arap authentication** {**default** | *list-name*}

To enable TACACS+ authentication for ARA on a line, use the **arap authentication** line configuration command. Use the **no** form of the command to disable authentication for an ARA line.

| | |
|---|---|
| **default** | Use the default list created with the **aaa authentication arap** command. |
| *list-name* | Use the indicated list created with the **aaa authentication arap** command. |

**buffers** {**small** | **middle** | **big** | **verybig** | **large** | **huge** | *type number***}** {**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** | Buffer size of this public buffer pool is 104 bytes. |
| **middle** | Buffer size of this public buffer pool is 600 bytes. |
| **big** | Buffer size of this public buffer pool is 1524 bytes. |
| **verybig** | Buffer size of this public buffer pool is 4520 bytes. |
| **large** | Buffer size of this public buffer pool is 5024 bytes. |
| **huge** | Default buffer size of this public buffer pool is 18024 bytes. This value can be configured with the **buffers huge size** command. |
| *type* | Interface type of the interface buffer pool. Value cannot be **fddi**. |
| *number* | Interface number of the interface buffer pool. |
| **permanent** | Number of permanent buffers that the system tries to create and keep. Permanent buffers are normally not trimmed 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 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. |
| *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 or Cisco 4500 series system calendar, use the **calendar 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). |

**cdp enable**

To enable 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 holdtime** *seconds*
**no 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.

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

**cdp run**

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

**cdp timer** *seconds*
**no cdp timer**

To specify how often your router will send CDP updates, use the **cdp timer** global configuration command. Use the **no** form of this command to revert to the default setting.

| | |
|---|---|
| *seconds* | Specifies how often your router will send CDP updates. |

**clear cdp counters**

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

**clear cdp table**

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

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

To configure the Cisco 7000 series or Cisco 4500 series router 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 or Cisco 4500 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 or Cisco 4500 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 this command.

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

**enable** [*level*]

To log onto the router at a specified level, use the **enable** EXEC command.

| | |
|---|---|
| *level* | (Optional) Privilege level to log in to on the router. |

[**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** [**level** *level*] [*encryption-type*] *password*
**no enable password** [**level** *level*]

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.

| | |
|---|---|
| **level** *level* | (Optional) Level for which the password applies. |
| *encryption-type* | (Optional) Type of password encryption. Can be 0 or 7. 0 indicates that the password that follows has not yet been encrypted. 7 indicates that the password has been encrypted using Cisco-proprietary encryption. |
| *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 secret** *password*

To specify an additional layer of security over the **enable password** command, use the **enable secret** command. Use the **no** form of the command to turn off the enable secret function.

| | |
|---|---|
| *password* | The **enable secret** password. This password should be different from the password created with the **enable password** command for additional security. |

[**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.

**fair-queue** *congestive-discard-threshold-number*
**no fair-queue**

To enable weighted fair queueing for an interface and to set the congestion threshold after which messages for high-bandwidth conversations are dropped, use the **fair-queue** interface configuration command. To disable weighted fair queueing for an interface, use the **no** form of this command.

| | |
|---|---|
| *congestive-discard-threshold-number* | Number of messages creating a congestion threshold after which new messages for high-bandwidth conversations are no longer enqueued. Valid values are 1 to 512 inclusive. The congestive-discard threshold default is 64 messages. |

**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] load-interval** *seconds*

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.

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

[**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** form of this command disables logging to the console terminal.

| | |
|---|---|
| *level* | Limits the logging of messages displayed on the console terminal to the named level. See the *level* keywords table for this command in the *Router Products Command Reference* publication. |

**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** form of this global configuration command.

| | |
|---|---|
| *facility-type* | Syslog facility. See the *facility-type* keywords table for this command 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** form of this command disables logging to terminal lines other than the console line.

| | |
|---|---|
| *level* | One of the *level* keywords. See the **logging console** command in the *Router Products Command Reference* publication for a list of supported values. |

[**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.

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

To synchronize unsolicited messages and debug output with solicited router output and prompts for a specific console port line, auxiliary port line, or virtual terminal line, use the **logging synchronous** line configuration command. The **no** form of this command disables the synchronizing of messages.

| | |
|---|---|
| **level** *severity-level* | (Optional) 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. |
| **all** | (Optional) Specifies that all messages are printed asynchronously, regardless of the severity level. |

| | |
|---|---|
| **limit** *number-of-buffers* | (Optional) Number of buffers to be queued for the terminal after which new messages are dropped. The default value is 20. |

**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. See this command in the *Router Products Command Reference* publication for a list of supported values. |

[**no**] **login authentication** {**default** | *list-name*}

To enable TACACS+ authentication for logins, use the **login authentication** line configuration command. Use the **no** form of the command to return to the default.

| | |
|---|---|
| **default** | Uses the default list created with the **aaa authentication login** command. |
| *list-name* | Uses the indicated list created with the **aaa authentication login** command. |

**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. |
| *access-list-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. |

[**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*

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.

[**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** form of this 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. |

**ppp authentication** {**chap** | **pap**} [**if-needed**] [*list-name*]
**no ppp authentication**

To enable Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) and to enable an AAA authentication method on an interface, use the **ppp authentication** interface configuration command. Use the **no** form of the command to disable this authentication.

| | |
|---|---|
| **chap** | Enables CHAP on a serial interface. |
| **pap** | Enables PAP on a serial interface. |

| | |
|---|---|
| **if-needed** | (Optional) Used with TACACS and extended TACACS. Does not perform CHAP or PAP authentication if the user has already provided authentication. This option is available only on asynchronous interfaces. |
| *list-name* | (Optional) Used with AAA/TACACS+. Specifies the name of a list of AAA methods of authentication to use. If no listname is specified, the system uses the default. Lists and default are created with the **aaa authentication ppp** command. |

**ppp use-tacacs** [**single-line**]
**no ppp use-tacacs**

To enable TACACS for PPP authentication, use the **ppp use-tacacs** interface configuration command. Use the **no** form of this command to disable TACACS for PPP authentication.

| | |
|---|---|
| **single-line** | (Optional) Accept the username and password in the username field. This option applies only when using CHAP authentication. |

**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** form of this 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-l1**, **decnet_router-l2**, **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 this command in the *Router Products Command Reference* publication for a list of supported values. |

**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**] **privilege** *mode* **level** *level command*

To set the privilege level for a command, use the **privilege level** global configuration command. Use the no form of this command to revert to default privileges for a given command.

| | |
|---|---|
| *mode* | Configuration mode. See the mode argument options table in the description of the **alias** command in the *Router Products Command Reference* publication for a list of acceptable options. |
| *level* | Privilege level to be associated with the specified command. You can specify up to sixteen privilege levels, using numbers 0 through 15. |
| *command* | Command to which privilege level is associated. |

[**no**] **privilege level** *level*

To set the default privilege level for a line, use the **privilege level** line configuration command. Use the **no** form of this command to restore the default user privilege level to the line.

| | |
|---|---|
| *level* | Privilege level to be associated with the specified line. |

[**no**] **prompt** *string*

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

| | |
|---|---|
| *string* | Router prompt. See this command in the *Router Products Command Reference* publication for a list of supported values. |

[**no**] **queue-list** *list-number* **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* | 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 this 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** form of this 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-l1**, **decnet_router-l2**, **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 **priority-list protocol** command in the *Router Products Command Reference* publication for a list of supported values. |

[**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 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. The **no service finger** command removes this service.

[**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) Include milliseconds with 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 aliases** [*mode*]

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

| | |
|---|---|
| *mode* | (Optional) Command mode. See the mode argument options table in the description of the **alias** command for acceptable options for the *mode* argument. |

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

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

| | |
|---|---|
| *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, fddi, 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 calendar**

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

**show cdp**

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

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

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

| | |
|---|---|
| *entry-name* | Name of neighbor about which you want information. |
| **protocol** | (Optional) Limits the display to information about the protocols enabled on a device. |
| **version** | (Optional) Limits the display to information about the version of software running on the device. |

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

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

| | |
|---|---|
| *type* | (Optional) Type of interface about which you want information. |
| *number* | (Optional) Number of the interface about which you want information. |

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

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

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

After a shutdown occurs due to detection of fatal environmental margins, use the **show environment last** EXEC command to display the last measured value from each of six test points on the CSC-ENVM (on the AGS+) or the route processor (RP) (on the Cisco 7000 series).

### 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 syslog error and event logging, including host addresses, and whether console logging is enabled, and also to display 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 privilege**

To display your current level of privilege, use the **show privilege** 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 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, including the reason for the last system reboot; if the system was reloaded because of a system failure, a saved system stack trace is displayed.

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

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.

| | |
|---|---|
| *destination-party* | 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 **snmp-server party** command. A destination party performs management operations that are requested by a source party. |
| *source-party* | 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 **snmp-server party** command. A source party sends communications to a destination party requesting the destination party to perform management operations. |
| *context* | 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 **snmp-server context** command. A context identifies object resources accessible to a party. |

*privileges* Bit mask representing the access privileges that govern the management operations that the source party can ask the destination party to perform. Use decimal or hexadecimal format to specify privileges as a sum of values in which each value specifies an SNMP PDU type that the source party can use to request an operation. The decimal values are defined as follows:

- Get =1
- GetNext = 2
- Response = 4
- Set = 8
- SNMPv1-Trap = 16
- GetBulk = 32
- SNMPv2-Trap = 128

**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 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. The **no snmp-server** command disables both versions of SNMP (SNMPv1 and SNMPv2).

| | |
|---|---|
| *string* | Community string that acts like a password and permits access to the SNMP protocol. |
| **ro** | (Optional) Specifies read-only access. Authorized management stations are only able to retrieve MIB objects. The default is **ro**. |
| **rw** | (Optional) Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects. The default is **ro**. |
| *number* | (Optional) Integer from 1 to 99 that specifies an access list of IP addresses that may use the community string to gain access to the SNMPv1 agent. |

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

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.

| | |
|---|---|
| *context-name* | Name of the context to be created or updated. This name serves as a label used to reference a record for this context. |
| *context-oid* | Object identifier to assign to the context. Specify this value in dotted decimal notation, with an optional text identifier; for example, 1.3.6.1.6.3.3.1.4.131.108.45.11.1(== initialContextId.131.108.45.11.1). |
| *view-name* | Name of a previously defined view. The view defines the objects available to the context. |

[**no**] **snmp-server host** *host community-string* [**envmon**] [**framerelay**] [**sdlc**] [**snmp**] [**tty**] [**x25**]

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.

| | |
|---|---|
| *host* | Name or Internet address of the host. |
| *community-string* | Password-like community string to send with the trap operation. |
| **envmon** | (Optional) Enables Cisco enterprise-specific environmental monitor traps to be sent to the trap receiver *host* when an environmental threshold has been exceeded. |
| **framerelay** | (Optional) Enables Frame Relay traps to be sent to the trap receiver *host*. |
| **sdlc** | (Optional) Enables SDLC traps to be sent to the trap receiver *host*. |
| **snmp** | (Optional) Enables the SNMP traps defined in RFC 1157. |

| | |
|---|---|
| **tty** | (Optional) Enables Cisco enterprise-specific traps when a TCP connection closes. |
| **x25** | (Optional) Enable X.25 event traps to be sent to *host*. |

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

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.

| | |
|---|---|
| *party-name* | 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. |

| | |
|---|---|
| *party-oid* | Object identifier to assign to the party. Specify this value in dotted decimal notation, with an optional text identifier; for example, 1.3.6.1.6.3.3.1.3.131.108.34.54.1 (= initialPartyId.131.108.34.54.1) |
| *protocol-address* | (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 *a.b.c.d port*. In future releases, additional protocols will be supported. This value is used to specify the destination of trap messages. |
| **packetsize** *size* | (Optional) Maximum size in bytes of a message that this party is able to receive. By default, the packet size set through the **snmp-server packetsize** command is used. |
| **local** \| **remote** | (Optional) Indicates that the party is local or remote. If neither **local** nor **remote** is specified, a default value of **local** is assumed. |
| **authentication** | (Optional) Indicates that the party uses an authentication protocol. If specified, either **md5** or **snmpv1** is required. |
| **md5** *key* | (Optional) Indicates that the party uses the Message Digest algorithm MD5 for message authentication. If **md5** is specified, you must also specify a 16-byte hexadecimal ASCII string representing the MD5 authentication key for the party. |
| **clock** *clock* | (Optional) Initial value of the authentication clock. |
| **lifetime** *lifetime* | (Optional) Lifetime, in seconds, that represents the upper bound on acceptable delivery delay for messages generated by the party. |

**snmpv1** *string* (Optional) Community string. The keyword **snmpv1** indicates that the party uses community-based authentication.

All messages sent to this party will be authenticated using the SNMPv1 community string specified by *string* instead of MD5.

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

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

*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, use 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.

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

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

**snmpv1** (Optional) Indicates that SNMP authentication traps will be sent to SNMPv1 management stations only. If no keyword is specified, trap message authentication is turned on by default. In this case, messages are sent to the host that is specified though the **snmp-server host** command and to any SNMP stations configured through access policies to receive trap messages.

**snmpv2** (Optional) Indicates that SNMP authentication traps will be sent to SNMPv2 management stations only. If no keyword is specified, trap message authentication is turned on by default. In this case, messages are sent to the host that is specified though the **snmp-server host** command and to any SNMP stations configured through access policies to receive trap messages.

**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.

**snmp-server userid** *user-id* [**view** *view-name*] [**ro** | **rw**]
[**password** *password*]
**no snmp-server userid** *user-id*

To create or update an SNMPv2 security context using the simplified security conventions method, use the **snmp-server userid** global configuration command. The **no** form of this command removes the specified security context.

| | |
|---|---|
| *user-id* | User ID name that identifies an approved SNMPv2 user. The user ID represents a set of security information for this user. This value can identify a particular user of the system or a background process. |
| **view** *view-name* | (Optional) View to be used for this security context. The argument *view-name* must be the name of a predefined view. For authenticated users, defaults to the predefined view *everything*. For users who are not authenticated, defaults to the predefined view *restricted*. |
| **ro** | (Optional) Specifies read-only access.This is the default for unauthenticated users. |
| **rw** | (Optional) Specifies read-write access. This is the default for authenticated users. |
| **password** *password* | (Optional) If specified, indicates that this is an authenticated user, and defines the password used to authenticate the user. The password must be at least eight characters long. |

**snmp-server view** *view-name oid-tree* {**included** | **excluded**}
**no snmp-server view** *view-name*

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.

| | |
|---|---|
| *view-name* | Label for the view record that you are updating or creating. The name is used to reference the record. |

| | |
|---|---|
| *oid-tree* | Object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as *1.3.6.2.4*, or a word, such as *system*. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4. |
| **included** \| **excluded** | Type of view. Either **included** or **excluded** is required. |

**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** [**always**] | **enable** | **slip** [**always**] [**access-lists**]}

To specify that the network or router must respond indicating whether the user may perform an action when the user attempts to perform the action, use the **tacacs-server authenticate** global configuration command.

| | |
|---|---|
| **connection** | Configures a required response when a user makes a TCP connection. |
| **always** | (Optional) Performs authentication even when a user is not logged in. This option only applies to the **connection** or **slip** keywords. |
| **enable** | Configures a required response when a user enters the **enable** command. |
| **slip** | Configures a required response when a user starts a SLIP or PPP session. |

**access-lists** (Optional) Requests and installs access lists. This option only applies to the **slip** keyword.

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

To enable an extended TACACS mode, use the **tacacs-server extended** global configuration command. Use the **no** form of this 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 key** [*key*]

Use the **tacacs-server key** command to set the authentication/encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon. To disable the key, use the **no** form of the command.

*key* The key used to set authentication and encryption. This key must match the key used on the TACACS+ daemon.

[**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** [**always**] | **enable** | **logout** [**always**] | **slip** [**always**]}

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.

| | |
|---|---|
| **connection** | Specifies that a message be transmitted when a user makes a TCP connection. |
| **always** | (Optional) Sends a message even when a user is not logged in. This option applies only to SLIP or PPP sessions and can be used with the **connection**, **logout**, or **slip** keywords. |
| **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. |
| **slip** | Specifies that a message be transmitted when a user starts a SLIP or PPP session. |

[**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 **no** form of this command restores the default.

| | |
|---|---|
| *retries* | Integer that specifies the retransmit count. The router software will try all servers, allowing each one to time out before increasing the *retries* 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** user EXEC or privileged 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** | (Optional) 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. |