CHAPTER 5

System Management Commands

This chapter describes the commands used to manage the router system and its performance on the network. In general, system or network management falls into the following categories. The commands that perform the tasks in these management categories are described in this chapter unless specified otherwise.

- Configuration Management

  The configuration of network devices determines the behavior of the network. To manage device configurations, you need to list and compare configuration files on running devices, store configuration files on network servers for shared access, and perform software installations and upgrades. (Configuration management commands required to perform these tasks are described in the chapter entitled "System Image, Microcode Image, and Configuration File Load Commands.")

  Other configuration management tasks include naming the router, setting router time services, configuring for synchronous logging of unsolicited messages and debug output, configuring a router for weighted fair queueing, and configuring SNMP support. Configuration management commands required to perform these tasks are described this chapter.

- Security Management

  To manage security on the network, you need to restrict access to the system. You can do so on several different levels:

  — Assign and encrypt passwords to restrict access to terminal lines, login connections, or privileged EXEC mode.

  — Establish one of three versions of Terminal Access Controller Access Control System (TACACS) protection for network servers that have shared access: TACACS, extended TACACS, or TACACS+, which is coupled with the Authentication, Authorization, and Accounting (AAA) model.

  — Restrict login connections to specific users with a username authentication system.

  — Control access on serial interfaces with Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP).

  — Create access lists to filter traffic to and from specific destinations. Subsequent chapters that describe the routing protocols in detail define access lists. This section provides general guidelines for creating access lists.

  — Create security labels for Internet Protocol (IP) datagrams using the Internet Protocol Security Option (IPSO), as described in the chapter entitled "IP Commands."

— Enable accounting for Internet Protocol (IP) access list violations and display the accounting data. For information on the IP accounting access-violations feature and commands, see the "Configuring IP" chapter of the *Router Products Configuration Guide* and the "IP Commands" chapter later in this publication.

Security management commands required to perform these tasks are described this chapter.

- Fault Management

  To manage network faults, you need to discover, isolate, and fix the problems. You can discover problems with the system's monitoring commands, isolate problems with the system's test commands, and resolve problems with other commands, including **debug**.

  This chapter describes general fault management commands. For detailed troubleshooting procedures and a variety of scenarios, see the *Troubleshooting Internetworking Systems* guide. For complete details on all **debug** commands, see the *Debug Command Reference* publication.

- System Performance Management

  To manage system performance, you need to monitor and determine response time, error rates, and availability. Once these factors are determined, you can perform load-balancing and modify system parameters to enhance performance. For example, priority queuing allows you to prioritize traffic order. You can configure fast and autonomous switching to improve network throughput, as described in the "Configuring Interfaces" chapter of the *Router Products Configuration Guide*.

  See the *Internetwork Design Guide* for additional information.

- Accounting Management

  Accounting management allows you to track both individual and group usage of network resources. You can then reallocate resources as needed. For example, you can change the system timers and configure TCP keepalives. See also the IP accounting feature in the "Configuring IP" chapter of the *Router Products Configuration Guide*. Additionally, the AAA/TACACS+ **aaa accounting** command allows you to set start-stop accounting for any or all of the listed functions for this command.

For system management configuration tasks and examples, refer to the chapter entitled "Managing the System" in the *Router Products Configuration Guide*.

Note One or more of the commands that previously appeared this chapter have been replaced by new commands. See the *Router Products Command Reference* publication for command information. The old commands continue to perform their normal function in the current release, but support for them will cease in future releases.

---

aaa accounting

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.

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

Syntax Description

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	The command level that should be accounted for. Valid entries are 0-15.
start-stop	Sends a start record accounting notice at the beginning of a process and a stop record 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.
tacacs+	Mandatory. Enables the TACACS-style accounting.

Default

AAA accounting is not enabled.

Command Mode

Global configuration

Usage Guideline

The **aaa accounting** command allows you to set start-stop accounting for any or all of the functions listed in "Syntax Description." For minimal accounting control, issue the **stop-only** keyword, which sends a stop record accounting notice at the end of the requested user process. For additional accounting control, you can issue the **start-stop** command, where TACACS+ sends a start accounting notice at the beginning of the requested process and a stop accounting notice at the end of the process. You can further control access and accounting by issuing the **wait-start** command, which ensures that the start notice is received by the TACACS+ server before granting the user's process request. Accounting is done only to the TACACS+ server.

Note This command, along with **aaa authorization**, replaces the **tacacs-server authenticate** command in previous versions of TACACS, and can be used only with AAA/TACACS+. This command can be used only with AAA TACACS+.

Examples

In the following example, accounting is set for outbound Telnet and rlogin, and both a start and stop accounting notice is sent to the TACACS+ server:

```
aaa accounting connection start-stop tacacs+
```

In the following example, accounting is set for privilege level 15 commands, with a wait-start restriction:

```
aaa accounting command 15 wait-start tacacs+
```

Related Commands

aaa authorization
aaa new-model

aaa authentication arap

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

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

Syntax Description

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	One of the keywords described in Table 5-1.

Default

If the **default** list is not set, only the local user database is checked. This version has the same effect as the following command:

```
aaa authentication arap default local
```

Command Mode

Global configuration

Usage Guideline

The list names and default that you set with the **aaa authentication arap** command are used with the **arap authentication** command. These lists can contain up to four authentication methods that are used when a user tries to log in with ARA.

Create a list by entering the **aaa authentication arap** *list-name method* command, where *list-name* is any character string used to name this list, such as *MIS-access*. The *method* argument identifies the list of methods the authentication algorithm tries in the given sequence. You can enter up to four methods, which are described in Table 5-1.

To create a default list that is used if no list is specified in the **arap authentication** command, use the **default** keyword followed by the methods you wish to be used in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails.

Use the **show running-config** command to view lists of authentication methods.

Table 5-1 AAA Authentication ARAP Method Descriptions

Keyword	Description
if-needed	Does not authenticate if the user has already been authenticated on a TTY line.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
tacacs+	Uses TACACS+ authentication.

Note This command cannot be used with TACACS or extended TACACS.

Examples

The following example creates a list called *MIS-access*, which first tries TACACS+ authentication and then none:

```
aaa authentication arap MIS-access tacacs+ none
```

The following example creates the same list, but sets it as the default list that is used for all ARA protocol authentications if no other list is specified:

```
aaa authentication arap default tacacs+ none
```

Related Commands

aaa authentication local-override
aaa new-model
arap authentication

aaa authentication enable default

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 this command to disable this authorization method.

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

Syntax Description

method At least one and up to four of the keywords described in Table 5-2.

Default

If the **default** list is not set, only the enable password is checked. This version has the same effect as the following command:

```
aaa authentication enable default enable
```

On the console, the enable password is used if it exists. If no password is set, the process will succeed anyway.

Command Mode

Global configuration

Usage Guideline

Use the **aaa authentication enable default** command to create a series of authentication methods that are used to determine if a user can access the privileged command level. You can specify up to four authentication methods. Method keywords are described in Table 5-2. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.

If a default authentication routine is not set for a function, the default is **none** and no authentication is performed. Use the **show running-config** command to view currently configured lists of authentication methods.

Table 5-2 AAA Authentication Enable Default Method Descriptions

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.
tacacs+	Uses TACACS+ authentication.

Note This command cannot be used with TACACS or extended TACACS.

Example

The following example creates an authentication list that first tries to contact a TACACS+ server. If no server can be found, then AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

```
aaa authentication enable default tacacs+ enable none
```

Related Commands

aaa authentication local-override
aaa authorization
aaa new-model
enable password

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 this command to disable the override.

aaa authentication local-override
no aaa authentication local-override

Syntax Description

This command has no arguments or keywords.

Default

Override is disabled.

Command Mode

Global configuration

Usage Guideline

This command is useful when you want to configure an override to the normal authentication process for certain personnel such as system administrators.

When this override is set, the user is always prompted for the username. The system then checks to see if the entered username corresponds to a local account. If the username does not correspond to one in the local database, login proceeds with the methods configured with other **aaa** commands (such as **aaa authentication login**). Note when using this command that `Username:` is fixed as the first prompt.

Example

The following example enables AAA authentication override:

```
aaa authentication local-override
```

Related Commands

aaa authentication arap
aaa authentication enable default
aaa authentication login
aaa authentication ppp
aaa new-model

aaa authentication login

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

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

Syntax Description

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 keywords described in Table 5-3.

Default

If the **default** list is not set, only the local user database is checked. This version has the same effect as the following command:

```
aaa authentication login default local
```

Note On the console, login will succeed without any authentication checks if **default** is not set.

Command Mode

Global configuration

Usage Guideline

The default and optional list names that you create with the **aaa authentication login** command are used with the **login authentication** command.

Create a list by entering the **aaa authentication** *list-name method* command, where *list-name* is any character string used to name this list, such as *MIS-access*. The *method* argument identifies the list of methods the authentication algorithm tries, in the given sequence. Method keywords are described in Table 5-3.

To create a default list that is used if no list is assigned to a line with the **login authentication** command, use the default argument followed by the methods you want in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication will succeed even if all methods return an error, specify **none** as the final method in the command line.

If authentication is not specifically set for a line, the default is to deny access—no authentication is performed. Use the **show running-config** command to view currently configured lists of authentication methods.

Table 5-3 AAA Authentication Login Method Descriptions

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
none	Uses no authentication.
tacacs+	Uses TACACS+ authentication.

Note This command cannot be used with TACACS or extended TACACS.

Examples

The following example creates an AAA authentication list called *MIS-access*. This authentication first tries to contact a TACACS+ server. If no server is found, TACACS+ returns an error and AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

```
aaa authentication login MIS-access tacacs+ enable none
```

The following example creates the same list, but sets it as the default list that is used for all login authentications if no other list is specified:

```
aaa authentication login default tacacs+ enable none
```

Related Commands

aaa authentication local-override
aaa new-model
login authentication

aaa authentication ppp

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

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

Syntax Description

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 keywords described in Table 5-4.

Default

If the **default** list is not set, only the local user database is checked. This version has the same effect as the following command:

```
aaa authentication ppp default local
```

Command Mode

Global configuration

Usage Guideline

The lists that you create with the **aaa authentication ppp** command are used with the **ppp authentication** command. These lists contain up to four authentication methods that are used when a user tries to log in to the serial interface.

Create a list by entering the **aaa authentication ppp** *list-name method* command, where *list-name* is any character string used to name this list, such as *MIS-access*. The *method* argument identifies the list of methods the authentication algorithm tries in the given sequence. You can enter up to four methods. Method keywords are described in Table 5-4.

The additional methods of authentication are only used if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to have authentication succeed even if all methods return an error.

If authentication is not specifically set for a function, the default is **none** and no authentication is performed. Use the **show running-config** command to view lists of authentication methods.

Table 5-4 AAA Authentication PPP Method Descriptions

Keyword	Description
if-needed	Does not authenticate if user has already been authenticated on a TTY line.
local	Uses the local username database for authentication.
none	Uses no authentication.
tacacs+	Uses TACACS+ authentication.

Note This command cannot be used with TACACS or extended TACACS.

Example

The following example creates an AAA authentication list called *MIS-access* for serial lines that use PPP. This authentication first tries to contact a TACACS+ server. If this action returns an error, the user is allowed access with no authentication.

```
aaa authentication MIS-access ppp tacacs+ none
```

Related Commands

aaa authentication local-override
aaa new-model
ppp authentication

aaa authorization

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 this command.

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

Syntax Description

network	Performs authorization for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARA protocol.
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	Table 5-5 lists the *methods* keywords.

Default

Authorization is disabled for all actions (equivalent to the keyword **none**).

Command Mode

Global configuration

Usage Guideline

Use the **aaa authorization** command to create a list of one and up to four authorization methods that can be used when a user accesses the specified function.

Note This command, along with **aaa accounting**, replaces the **tacacs-server** suite of commands in previous versions of TACACS.

The additional methods of authorization are only used if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to have authorization succeed even if all methods return an error.

Table 5-5 AAA Authorization Method Descriptions

Keyword	Description
tacacs+	Requests authorization information from the TACACS+ server.
if-authenticated	Allows the user to access the requested function if the user is authenticated.
none	No authorization is performed.
local	Uses the local database for authorization.

If authorization is not specifically set for a function, the default is **none** and no authorization is performed.

The authorization command causes a request packet containing a series of attribute value pairs to be sent to the TACACS daemon as part of the authorization process. The daemon can:

- accept the request as is
- make changes to the request
- refuse the request, and hence, refuse authorization

Table 5-6 describes attribute value pairs associated with the **aaa authorization** command. Registered users can find more information about TACACS+ and attribute pairs on Cisco Information Online.

Table 5-6 Attribute Value Pairs for Authorization

Attribute Value	Description
service=arap	Authorization for AppleTalk Remote Access is being requested.
service=shell	Authorization for EXEC startup and command authorization is being requested.
service=ppp	Authorization for PPP is being requested.
service=slip	Authorization for SLIP is being requested.
protocol=lcp	Authorization for LCP is being requested (lower layer of PPP).
protocol=ip	Used with service=slip and service=slip to indicate which protocol layer is being authorized.
protocol=ipx	Used with service=ppp to indicate which protocol layer is being authorized.
protocol=atalk	Used with service=ppp or service=arap to indicate which protocol layer is being authorized.
protocol=vines	Used with service=ppp for VINES over PPP.
protocol=unknown	Used for undefined or unsupported conditions.
cmd=*x*	Used with service=shell, if cmd=NULL, this is an authorization request to start an EXEC. If cmd is not NULL, this is a command authorization request and will contain the name of the command being authorized. For example, cmd=telnet.

Attribute Value	Description
cmd-arg=*x*	Used with service=shell. When performing command authorization, the name of the command is given by a cmd=*x* pair for each argument listed. For example, cmd-arg=archie.sura.net.
acl=*x*	Used with service=shell and service=arap. For ARA, this pair contains an access list number. For service=shell, this pair contains an access class number. For example, acl=2.
inacl=*x*	Used with service=ppp and protocol=ip. Contains an IP input access list for SLIP or PPP/IP. For example, inacl=2.
outacl=*x*	Used with service=ppp and protocol=ip. Contains an IP output access list for SLIP or PPP/IP. For example, outacl=4.
addr=*x*	Used with service=slip, service=ppp, and protocol=ip. Contains the IP address that the remote host should use when connecting via SLIP or PPP/IP. For example, addr=172.30.23.11.
routing=*x*	Used with service=slip, service=ppp, and protocol=ip. Equivalent in function to the /routing flag in SLIP and PPP commands. Can either be true or false. For example, routing=true.
timeout=*x*	Used with service=arap. The number of minutes before an ARA session disconnects. For example, timeout=60.
autocmd=*x*	Used with service=shell and cmd=NULL. Specifies an autocommand to be executed at EXEC startup. For example, autocmd=telnet foo.com.
noescape=*x*	Used with service=shell and cmd=NULL. Specifies a noescape option to the username configuration command. Can be either true or false. For example, noescape=true.
nohangup=*x*	Used with service=shell and cmd=NULL. Specifies a nohangup option to the username configuration command. Can be either true or false. For example. nohangup=false.
priv-lvl=*x*	Used with service=shell and cmd=NULL. Specifies the current privilege level for command authorization as a number from 0 to 15. For example, priv-lvl=15.
zonelist=*x*	Used with service=arap. Specifies an AppleTalk zonelist for ARA. For example, zonelist=5.
addr-pool=*x*	Used with service=ppp and protocol=ip. Specifies the name of a local pool from which to get the address of the remote host.

Examples

The following example specifies that TACACS+-style of authorization is used for all network-related requests. If this authorization method returns an error (if the TACACS+ server cannot be contacted), no authorization is performed and the request is successful.

```
aaa authorization network tacacs+ none
```

The following example specifies that TACACS+-style of authorization is run for level 15 commands. If this authorization method returns an error (if the TACACS+ server cannot be contacted), no authorization is performed and the request succeeds.

```
aaa authorization command 15 tacacs+ none
```

Related Commands

aaa accounting
aaa new-model

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 this command to disable this functionality.

aaa new-model
no aaa new-model

Syntax Description

This command has no arguments or keywords.

Default

AAA/TACACS+ is not enabled.

Command Mode

Global configuration

Usage Guideline

This command enables the AAA access control system and TACACS+. If you initialize this functionality and later decide to use TACACS or extended TACACS, issue the **no** version of this command and then enable the version of TACACS you want to use.

Example

The following example initializes AAA and TACACS+:

```
aaa new-model
```

Related Commands

aaa accounting
aaa authentication arap
aaa authentication enable default
aaa authentication local-override
aaa authentication login
aaa authentication ppp
aaa authorization

alias

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

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

Syntax Description

mode	Command mode of the original and alias commands. See Table 5-7 for a list of options for this argument.
alias-name	Command alias.
alias-command-line	Original command syntax.

Defaults

Default aliases are in EXEC mode as follows:

Command Alias	Original Command
h	**help**
lo	**logout**
p	**ping**
r	**resume**
s	**show**
w	**where**

Command Mode

Global configuration

Usage Guidelines

You can use simple words or abbreviations as aliases. The aliases in the Default section are predefined. They can be turned off using the **no alias** command.

Table 5-7 shows the acceptable options for the *mode* argument in the **alias** global configuration command.

Table 5-7 Mode Argument Options

Argument Options	Mode
configuration	Global configuration
controller	Controller configuration
exec	EXEC
hub	Hub configuration

Argument Options	Mode
interface	Interface configuration
ipx-router	IPX router configuration
line	Line configuration
map-class	Map class configuration
map-list	Map list configuration
route-map	Route map configuration
router	Router configuration

See the summary of command modes in the user interface chapter in the *Router Products Configuration Guide* for more information about command modes.

When you use online help, command aliases are indicated by an asterisk (*), as follows:

```
Router#lo?
*lo=logout  lock  login  logout
```

When you use online help, aliases that contain spaces (for example, *telnet device.cisco.com 25*) are displayed as follows:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#alias exec device-mail telnet device.cisco.com 25
Router(config)# end
Router# device-mail?
*device-mail="telnet device.cisco.com 25"
```

When you use online help, the alias is expanded and replaced with the original command, as shown in the following example with the *td* alias:

```
Router(config)#alias exec td trace device
Router(config)#^Z
Router#t?
*td="trace device"  telnet  terminal  test  tn3270
trace
```

To list only commands and omit aliases, begin your input line with a space. In the following example, the alias *td* is not shown, because there is a space before the **t?** command line.

```
Router# t?
telnet  terminal  test  tn3270  trace
```

As with commands, you can use online help to display the arguments and keywords that can follow a command alias. In the following example, the alias **td** is created to represent the command **telet device**. The **/debug** and **/line** switches can be added to **telnet device** to modify the command:

```
Router(config)# alias exec td telnet device
Router(config)# ^Z
Router#td ?
      /debug     Enable telnet debugging mode
      /line      Enable telnet line mode
      ...
      whois      Whois port
      <cr>

Router# telnet device
```

You must enter the complete syntax for the **alias** command. Partial syntax for aliases are not accepted. In the following example, the parser does not recognize the command *t* as indicating the alias *td*.

```
bones# t
% Ambiguous command:  "t"
```

Example

In the following example, the alias *fixmyrt* is created for the EXEC-mode command **clear ip route 198.92.116.16**.

```
alias exec fixmyrt clear ip route 198.92.116.16
```

Related Command

show aliases

arap authentication

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.

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

Caution If you use a *list-name* value that was not configured with the **aaa authentication arap** command, ARA protocol will be disabled on this line.

Syntax Description

default	Default list created with the **aaa authentication arap** command.
list-name	Indicated list created with the **aaa authentication arap** command.

Default

ARA protocol authentication uses the default set with **aaa authentication arap** command. If no default has been set, the local user database is checked.

Command Mode

Line configuration

Usage Guideline

This command is a per-line command that specifies the name of a list of AAA authentication methods to try at login. If no list is specified, the default list is used (whether or not it is specified in the command line). You create defaults and lists with the **aaa authentication arap** command. Entering the **no** version of **arap authentication** has the same effect as entering the command with the **default** argument.

Before issuing this command, create a list of authentication processes by using the **aaa authentication arap** global configuration command.

Example

The following example specifies that the TACACS+ authentication list called *MIS-access* is used on ARA line 7:

```
line 7
arap authentication MIS-access
```

Related Command

aaa authentication arap

buffers

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

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

Syntax Description

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.

Default

The default number of buffers in a pool is determined by the hardware configuration and can be displayed with the EXEC **show buffers** command.

Command Mode

Global configuration

Usage Guidelines

Normally you need not adjust these parameters; do so only after consulting with technical support personnel. Improper settings can adversely impact system performance.

You cannot configure FDDI buffers.

Examples of Public Buffer Pool Tuning

In the following example, the system will try to keep at least 50 small buffers free:

```
buffers small min-free 50
```

In the following example, the permanent buffer pool allocation for big buffers is increased to 200:

```
buffers big permanent 200
```

Example of Interface Buffer Pool Tuning

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

In the following example, the permanent Ethernet 0 interface buffer pool on a Cisco 4000 is increased to 96 because the Ethernet 0 buffer pool is depleted:

```
buffers ethernet 0 permanent 96
```

Related Commands

buffers huge size
show buffers

buffers huge size

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

buffers huge size *number*
no buffers huge size *number*

Syntax Description

number Size of huge buffers, in bytes.

Default

18024 bytes

Command Mode

Global configuration

Usage Guidelines

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

Example

In the following example, the system will resize huge buffers to 20000 bytes:

```
buffers huge size 20000
```

Related Commands

buffers
show buffers

calendar set

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

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

Syntax Description

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).

Command Mode

EXEC

Usage Guidelines

Once you set the Cisco 7000 calendar or the Cisco 4500 calendar, the system clock will be automatically set when the system is restarted or when the **clock read-calendar** EXEC command is issued. The calendar maintains its accuracy, even after a power failure or system reboot has occurred. The time specified in this command is relative to the configured time zone.

Example

In the following example, the system calendar is manually set to 1:32 p.m. on July 23, 1993:

```
calendar set 13:32:00 23 July 1993
```

Related Commands

clock read-calendar
clock set
clock summer-time
clock timezone
clock update-calendar

cdp enable

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

cdp enable
no cdp enable

Syntax Description

This command has no arguments or keywords.

Default

Enabled at the global level and on all supported interfaces.

Command Mode

Interface configuration

Usage Guidelines

CDP is enabled by default at the global level and on each interface in order to send or receive CDP information.

Note The **cdp enable**, **cdp timer**, and **cdp run** commands affect the operation of the IP on demand routing feature (that is, the **router odr** global configuration command). For more information on the **router odr** command, see the "IP Routing Protocols Commands" chapter in the *Network Protocols Command Reference, Part 1*.

Example

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

```
interface ethernet 0
cdp enable
```

Related Command

cdp run

cdp holdtime

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

cdp holdtime *seconds*
no cdp holdtime

Syntax Description

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

Default

180 seconds

Command Mode

Global configuration

Usage Guidelines

CDP packets are sent with time-to-live, or hold time, that is nonzero after an interface is enabled and a hold time of 0 immediately before an interface is idled down.

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

Example

In the following example, the CDP packets being sent from your device should be held by the receiving device for 60 seconds before being discarded. You might want to set the hold time lower than the default setting of 180 seconds if information about your device changes often and you want the receiving devices to purge this information more quickly.

```
cdp holdtime 60
```

Related Commands

cdp timer
show cdp

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 run
no cdp run

Syntax Description

This command has no arguments or keywords.

Default

Enabled

Command Mode

Global configuration

Usage Guidelines

CDP is enabled on your router by default, which means the Cisco IOS software will receive CDP information. CDP also is enabled on supported interfaces by default. To disable CDP on an interface, use the **cdp enable** interface configuration command.

Note The **cdp enable**, **cdp timer**, and **cdp run** commands affect the operation of the IP on demand routing feature (that is, the **router odr** global configuration command). For more information on the **router odr** command, see the "IP Routing Protocols Commands" chapter in the *Network Protocols Command Reference, Part 1*.

Example

In the following example, CDP is disabled for the router:

```
no cdp run
```

Related Command

cdp enable

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.

cdp timer *seconds*
no cdp timer

Syntax Description

seconds	Specifies how often your router will send CDP updates.

Default

60 seconds

Command Mode

Global configuration

Usage Guidelines

The trade-off with sending more frequent transmissions is providing up-to-date information versus using bandwidth more often.

Example

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

```
cdp timer 80
```

Related Commands

cdp holdtime
show cdp

clear cdp counters

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

clear cdp counters

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC

Example

In the following example, the CDP counters have been cleared. The **show cdp traffic** output shows that all of the traffic counters have been reset to zero (0).

```
Router# clear cdp counters
Router# show cdp traffic

CDP counters:
        Packets output: 0, Input: 0
        Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
        No memory: 0, Invalid packet: 0, Fragmented: 0
```

Related Commands

clear cdp table
show cdp traffic

clear cdp table

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

clear cdp table

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC

Example

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

```
Router# clear cdp table

CDP-AD: Deleted table entry for neon.cisco.com, interface Ethernet0
CDP-AD: Deleted table entry for neon.cisco.com, interface Serial0
Router# show cdp neighbors


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

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

Related Commands

clear cdp counters
show cdp neighbors

clock calendar-valid

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

clock calendar-valid
no clock calendar-valid

Syntax Description

This command has no arguments or keywords.

Default

Neither the Cisco 7000 nor the Cisco 4500 are not configured as a time source.

Command Mode

Global configuration

Usage Guidelines

Use this command if no outside time source is available.

Example

In the following example, the Cisco 7000 is configured as the time source for a network based on its calendar:

```
clock calendar-valid
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

ntp master
vines time use-system †

clock read-calendar

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

clock read-calendar

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

When either the Cisco 7000 series or the Cisco 4500 calendar is rebooted, the calendar is automatically read into the system clock. However, you may use this command to manually read the calendar setting into the system clock. This command is useful if the **calendar set** command has been used to change the setting of the calendar.

Example

In the following example, the system clock is configured to set its date and time by the calendar setting:

```
clock read-calendar
```

Related Commands

calendar set
clock set
clock update-calendar
ntp update-calendar

clock set

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

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

Syntax Description

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).

Command Mode

EXEC

Usage Guidelines

Generally, if the system is synchronized by a valid outside timing mechanism, such as an NTP or VINES clock source, or if you have a Cisco 7000 with calendar capability, you do not need to set the system clock. Use this command if no other time sources are available. The time specified in this command is relative to the configured time zone.

Example

In the following example, the system clock is manually set to 1:32 p.m. on July 23, 1993:

```
clock set 13:32:00 23 July 1993
```

Related Commands

calendar set
clock read-calendar
clock summer-time
clock timezone

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.

clock summer-time *zone* **recurring** [*week day month hh:mm week day month hh:mm* [*offset*]]
clock summer-time *zone* **date** *date month year hh:mm date month year hh:mm* [*offset*]
clock summer-time *zone* **date** *month date year hh:mm month date year hh:mm* [*offset*]
no clock summer-time

Syntax Description

zone	Name of the time zone (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 summer time (default is 60).

Default

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

Command Mode

Global configuration

Usage Guidelines

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

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

Examples

In the following example, summer time starts on the first Sunday in April at 02:00 and ends on the last Sunday in October at 02:00:

```
clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October 2:00
```

If you live in a place where summer time does not follow the pattern in the first example, you could set it to start on October 12, 1993 at 02:00, and end on April 28, 1994 at 02:00, with the following example:

```
clock summer-time date 12 October 1993 2:00 28 April 1994 2:00
```

Related Commands

calendar set
clock timezone

clock timezone

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

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

Syntax Description

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.

Default

UTC

Command Mode

Global configuration

Usage Guidelines

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

Example

In the following example, the timezone is set to Pacific Standard Time and is offset 8 hours behind UTC:

```
clock timezone PST -8
```

Related Commands

calendar set
clock set
clock summer-time
show clock

clock update-calendar

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

clock update-calendar

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

If the system clock and calendar are not synchronized, and the system clock is more accurate, use this command to update the Cisco 7000 series or Cisco 4500 calendar to the correct date and time.

Example

In the following example, the current time is copied from the system clock to the Cisco 7000 calendar:

```
clock update-calendar
```

Related Commands

clock read-calendar
ntp update-calendar

custom-queue-list

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

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

Syntax Description

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

Default

No custom queue list is assigned.

Command Mode

Interface configuration

Usage Guidelines

Only one queue list can be assigned per interface. Use this command in place of the **priority-list** command (not in addition to it). Custom queuing allows a fairness not provided with priority queuing. With custom queuing, you can control the interfaces' available bandwidth when it is unable to accommodate the aggregate traffic enqueued. Associated with each output queue is a configurable byte count, which specifies how many bytes of data should be delivered from the current queue by the system before the system moves on to the next queue. When a particular queue is being processed, packets are sent until the number of bytes sent exceeds the queue byte count or until the queue is empty.

Use the **show queuing custom** and **show interface** commands to display the current status of the custom output queues.

Example

In the following example, custom queue list number 3 is assigned to serial interface 0:

```
interface serial 0
custom-queue-list 3
```

Related Commands

queue-list default
queue-list interface
queue-list protocol
queue-list queue byte-count
queue-list queue limit

downward-compatible-config

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

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

Syntax Description

version	Cisco IOS Release number, not earlier than 10.2.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

In Cisco IOS Release 10.3, the IP access list formats changed. Use this command to regenerate a configuration in the format prior to Release 10.3 if you are going to downgrade from a Release 10.3 or later to an earlier release. The earliest release this command accepts is 10.2.

When this command is configured, the router attempts to generate a configuration that is compatible with the specified version. Currently, this command affects only IP access lists.

Under some circumstances, the software might not be able to generate a fully backward-compatible configuration. In such a case, the software issues a warning message any time it writes a configuration that is not downward compatible.

Example

In the following example, the router will attempt to generate a configuration file compatible with Cisco IOS Release 10.2:

```
downward-compatible-config 10.2
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

access-list (extended)†
access-list (standard)†

enable

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

enable [*level*]

Syntax Description

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

Default

Level 15

Command Mode

EXEC

Usage Guidelines

The **enable** command is a privilege level 0 command. If you configure AAA authorization for a privilege level greater than 0, the **enable** command will not be included in the command set for the privilege level.

Example

In the following example, the user is logging on to privilege level 5 on the router:

```
enable 5
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

privilege level
disable †

enable last-resort

To specify what happens if the TACACS and extended 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.

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

Syntax Description

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

Default

Default action is to fail.

Command Mode

Global configuration

Usage Guideline

The secondary authentication is used only if the first attempt fails. The secondary authentication does not occur if the first authentication is only unsuccessful.

Note This command is not used in AAA/TACACS+, which takes the **aaa authentication** suite of commands instead.

Example

In the following example, if the TACACS servers do not respond to the **enable** command, the user can enable by entering the privileged level password:

```
enable last-resort password
```

Related Command

A dagger (†) indicates that the command is documented in another chapter.

enable †

enable password

To configure the enable password for a given level, use the **enable password** global configuration command. Use the **no** form of this command to remove the enable password for a given level.

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

Syntax Description

level	(Optional) Level for which the password applies. You can specify up to sixteen privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges. If this argument is not specified, the privilege level defaults to 15 (traditional enable privileges).
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	Password for the specified level or highest level if none is specified.

Default

No password is defined.

Command Mode

Global configuration

Usage Guidelines

Caution If neither the **enable password** command nor the **enable secret** command is configured, and if there is a line password configured for the console, the console line password will serve as the enable password for all VTY (Telnet and Secure Shell [SSH]) sessions.

Use this command with the **level** option to define a privilege level. Once the level and the password are specified, give the password to the users you want to have access at this level. Use the **privilege level (global)** configuration command to specify the commands that are accessible at the specified level.

You will not ordinarily enter an encryption type. Typically, you will only enter encryption type if you cut and paste a password that has already encrypted by the system back into this command.

Enable or disable password encryption with the **service password-encryption** command. If you enter a value for the encryption-type argument, but have not enabled encryption, the encryption type will be treated as part of the password.

An enable password can contain from 1 to 80 uppercase and lowercase alphanumeric characters, except that the first character cannot be a number. Some spaces are valid password characters; for example, "two words" is valid. Leading spaces are ignored, but trailing spaces are recognized. For example, " woolly" is interpreted as "woolly" (without the space). On the other hand, "woolly " is interpreted as "woolly " (with the space). To create an enable password containing a question mark (?), precede the question mark with keystrokes **Ctrl-V**. For example, to create the password "abc?123", you enter the letters abc followed by **Ctrl-V** followed by ? followed by the numbers 123. When the system prompts you to enter the enable password, you do not need to precede the question mark with the **Ctrl-V**. For example, you can simply enter abc?123 at the password prompt.

Example

In the following example, the password *pswd2* is enabled for privilege level 2:

```
enable password level 2 pswd2
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

disable †
enable †
privilege level (global)
service password-encryption
show privilege

enable secret

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.

enable secret *password*
no enable secret *password*

Syntax Description

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

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

Caution If neither the **enable password** command nor the **enable secret** command is configured, and if there is a line password configured for the console, the console line password will serve as the enable password for all VTY (Telnet and Secure Shell [SSH]) sessions.

The **enable secret** command is used in conjunction with the **enable password** command to provide an additional layer of security over the enable password. This process provides better security in two ways: first by enforcing the use of an additional password; second, by storing this second password using a non-reversible cryptographic function. This encryption method is especially useful in environments where the password crosses a network or is stored on a TFTP server.

If you use the same password for **enable password** and **enable secret**, you will receive an error message warning you that this practice is not recommended. The system will prompt you again for a password. You can reenter the password you use for enable password, and the system will accept it the second time. But if you do, you undermine the additional security that the **enable secret** command provides.

Note After you set a password using **enable secret**, a password set using the **enable password** command will no longer work unless enable secret is disabled or an older version of software is being used, such as when running an older rxboot image. Additionally, you cannot recover a lost password that has been encrypted by any method.

Examples

The following example specifies an enable secret password of gobbledegook:

```
enable secret gobbledegook
```

After specifying an enable secret password, users must enter this password to gain access. Any passwords set through enable password will no longer work.

```
Password: gobbledegook
```

Related Command

enable
enable password

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.

enable use-tacacs
no enable use-tacacs

Caution If you use the **enable use-tacacs** command, you must also use the **tacacs-server authenticate enable** command, or else you will be locked out of the router.

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

When you add this command to the configuration file, the EXEC **enable** command prompts for a new username and password pair. This pair is then passed to the TACACS server for authentication. If you are using extended TACACS, it also will pass any existing UNIX user identification code to the server.

Note This command initializes TACACS. Use the **tacacs server-extended** command to initialize extended TACACS, or use the **aaa new-model** command to initialize AAA/TACACS+.

Example

The following example sets TACACS verification on the privileged EXEC-level login sequence:

```
enable use-tacacs
tacacs-server authenticate enable
```

Related Command

tacacs-server authenticate enable

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.

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

Syntax Description

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 4096 inclusive. The congestive-discard threshold default is 64 messages.

Default

Fair queueing is enabled by default for physical interfaces whose bandwidth is less than or equal to 2.048 megabits per second (Mbps) and that do not use Link Access Procedure, Balanced (LAPB), X.25, PPP, or Synchronous Data Link Control (SDLC) encapsulations. (Fair queuing is not an option for these protocols.) However, if custom queueing or priority queueing is enabled for a qualifying link, it overrides fair queueing, effectively disabling it. Additionally, fair queuing is automatically disabled if you enable autonomous or SSE switching.

Fair queueing is disabled automatically on interfaces configured with the **ppp multlilink** command. If the **no ppp multilink** command is configured, you must enable fair queuing manually on the interface.

The congestive-discard threshold is 64 messages.

Command Mode

Interface configuration

Usage Guidelines

When enabled for an interface, weighted fair queueing provides traffic priority management that automatically sorts among individual traffic streams without requiring that you first define access lists. Enabling weighted fair queueing requires use of this command only.

Weighted fair queuing can manage duplex data streams, such as those between pairs of applications, and simplex data streams such as voice or video. From the perspective of weighted fair queueing, there are two categories of sessions: high-bandwidth sessions and low-bandwidth sessions. Low-bandwidth traffic has effective priority over high-bandwidth traffic, and high-bandwidth traffic shares the transmission service proportionally according to assigned weights.

When weighted fair queuing is enabled for an interface, new messages for high-bandwidth traffic streams are discarded after the configured or default congestive-messages threshold has been met. However, low-bandwidth conversations, which include control-message conversations, continue to enqueue data. As a result, the fair queue may occasionally contain more messages than its configured threshold number specifies.

Weighted fair queuing uses a traffic data stream discrimination registry service to determine which traffic stream a message belongs to. For each forwarding protocol, Table 5-8 shows the attributes of a message that are used to classify traffic into data streams.

Table 5-8 Weighted Fair Queuing Traffic Stream Discrimination Fields

Forwarder	Fields Used
AppleTalk	• Source net, node, socket • Destination net, node, socket • Type
CLNS	• Source NSAP • Destination NSAP
DECnet	• Source address • Destination address
Frame Relay switching	• DLCI value
DDN IP	• TOS • IP Protocol • Source IP address (if message is not fragmented) • Destination IP address (if message is not fragmented) • Source TCP/UDP port • Destination TCP/UDP port
Transparent bridging	• Unicast: Source MAC, Destination MAC • Ethertype SAP/SNAP multicast: Destination MAC address
Source-route bridging	• Unicast: Source MAC, Destination MAC • SAP/SNAP multicast: Destination MAC address
VINES	• Source Network/Host • Destination Network/Host • Level 2 Protocol
Apollo	• Source Network/Host/Socket • Destination Network/Host/Socket • Level 2 protocol
XNS	• Source/Destination Network/Host/Socket • Level 2 Protocol
Novell NetWare	• Source/Destination Network/Host/Socket • Level 2 Protocol
All others (default)	Value of pak -> linktype

It is important to note that IP precedence, congestion in Frame Relay switching, and discard eligibility flags affect the weights used for queuing.

IP precedence, which is set by the host, is a number in the range of 0 to 7. Data streams of precedence *number* are weighted so that they are given an effective bit rate of *number*+1 times as fast as a data stream of precedence 0, which is normal.

In Frame Relay switching, message flags for congestion (FECN and BECN) and discard eligible (DE) message flags cause the algorithm to select weights that effectively impose reduced queue priority, providing the application with "slow down" feedback and sorting traffic, giving the best service to applications within their Committed Information Rate.

Fair queueing is supported for all LAN and line (WAN) protocols except those that use LAPB, which are listed in "Default." Because tunnels are software interfaces that are themselves routed over physical interfaces, fair queueing is not supported for tunnels. If fair queueing is configured for an interface, the default of **no fair-queue** is applied for these links and tunnels on the interface and appears in the configuration script for them.

Note For Release 10.3 and earlier, if you used the **tx-queue-limit** command to set the transmit (tx-queue) limit available to an interface on an MCI or SCI card and you configured custom queuing or priority queuing for that interface, the configured transmit (tx-queue) limit was automatically overridden and set to 1. With this release, for weighted fair queuing, custom queuing, and priority queuing, the transmit (tx-queue) limit is derived from the bandwidth value set for the interface using the bandwidth command. Bandwidth value/ 512 rounded up yields the effective transmit (tx-queue) limit. However, the derived value only applies in the absence of a **tx-queue-limit** command; that is, a configured transmit (tx-queue) limit overrides this derivation.

Example

The following example enables use of weighted fair queuing on Serial 0, with a congestive discard threshold of 300. This means that messages will be discarded from the queuing system only when 300 or more messages have been queued and the message is in a data stream that has more than one message in the queue. The transmit queue limit is set to 1, based on the 384-kilobit (kb) line set by the bandwidth command:

```
interface serial 0
bandwidth 384
fair-queue 300
```

hostname

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

hostname *name*

Syntax Description

name	New host name for the network server.

Default

The factory-assigned default host name is *router.*

Command Mode

Global configuration

Usage Guidelines

The order of display at startup is banner message-of-the-day (MOTD), then login and password prompts, then EXEC banner.

Do not expect case to be preserved. Upper- and lowercase characters look the same to many internet software applications (often under the assumption that the application is doing you a favor). It may seem appropriate to capitalize a name the same way you might do in English, but conventions dictate that computer names appear all lowercase. For more information, refer to RFC 1178, *Choosing a Name for Your Computer.*

The name must also follow the rules for ARPANET host names. They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names must be 63 characters or fewer. For more information, refer to RFC 1035, *Domain Names—Implementation and Specification.*

Example

The following example changes the host name to *sandbox*:

```
hostname sandbox
```

ip bootp server

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

ip bootp server
no ip bootp server

Syntax Description

This command has no arguments or keywords.

Default

Enabled

Command Mode

Global configuration

Usage Guidelines

By default, the BOOTP server is enabled.

When you disable the BOOTP server, access to the BOOTP ports cause the Cisco IOS software to send an "ICMP port unreachable" message to the sender and discard the original incoming packet.

Note Unlike defaults for other commands, this command will display when you perform **show running config** to display current settings, whether or not you have changed the default using the **no ip boopt server** command.

Example

The following example disables the BOOTP service on the router:

```
no ip bootp server
```

load-interval

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

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

Syntax Description

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).

Default

300 seconds (or 5 minutes)

Command Mode

Interface configuration

Usage Guidelines

If you want load computations to be more reactive to short bursts of traffic, rather than averaged over five-minute periods, you can shorten the length of time over which load averages are computed.

If the load interval is set to thirty seconds, new data is used for load calculations over a thirty-second period. This data is used to compute load statistics, including input rate in bits and packets per second, output rate in bits and packets per second, load, and reliability.

Load data is gathered every five seconds on the router. This data is used for a weighted average calculation in which more-recent load data has more weight in the computation than older load data. If the load interval is set to thirty seconds, the average is computed for the last thirty seconds of load data.

The **load-interval** command allows you to change the default interval of five minutes to a shorter or longer period of time. If you change it to a shorter period of time, the input and output statistics that are displayed when you use the **show interface** command will be more current, and based on more instantaneous data, rather than reflecting a more average load over a longer period of time.

This command is often used for dial backup purposes, to increase or decrease the likelihood of a backup interface being implemented, but it can be used on any interface.

Example

In the following example, the default five-minute average is set it to a thirty-second average. A burst in traffic that would not trigger a dial backup for an interface configured with the default five-minute interval might trigger a dial backup for this interface that is set for a shorter, thirty-second interval.

```
interface serial 0
load-interval 30
```

Related Command

A dagger (†) indicates that the command is documented in another chapter.

show interfaces †

logging

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

logging *host*
no logging *host*

Syntax Description

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

Default

No messages are logged to a syslog server host.

Command Mode

Global configuration

Usage Guidelines

This command identifies a syslog server host to receive logging messages. By issuing this command more than once, you build a list of syslog servers that receive logging messages.

Example

The following example logs messages to a host named *johnson*:

```
logging johnson
```

Related Commands

logging trap
service timestamps

logging buffered

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

logging buffered [*size*]
no logging buffered

Syntax Description

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

Default

The router displays all messages to the console terminal.

Command Mode

Global configuration

Usage Guidelines

This command copies logging messages to an internal buffer instead of writing them to the console terminal. The buffer is circular in nature, so newer messages overwrite older messages after the buffer is filled.

To display the messages that are logged in the buffer, use the EXEC command **show logging**. The first message displayed is the oldest message in the buffer.

Do not make the buffer size too large because the router could run out of memory for other tasks. You can use the **show memory** EXEC command to view the free processor memory on the router; however, this is the maximum available and should not be approached.

Example

The following example illustrates how to enable logging to an internal buffer:

```
logging buffered
```

logging console

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

logging console *level*
no logging console

Syntax Description

level	Limits the logging of messages displayed on the console terminal to the named level. See Table 5-9 for a list of the *level* keywords.

Default

debugging

Command Mode

Global configuration

Usage Guidelines

Specifying a *level* causes messages at that level and numerically lower levels to be displayed at the console terminal.

The EXEC command **show logging** displays the addresses and levels associated with the current logging setup, as well as any other logging statistics.

Table 5-9 Error Message Logging Priorities

Level Name	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

The effect of the **log** keyword with the IP **access list (extended)** command depends on the setting of the **logging console** command. The **log** keyword takes effect only if the logging console level is set to 6 or 7. If you change the default to a level lower than 6 and specify the **log** keyword with the IP **access list (extended)** command, no information is logged or displayed.

Example

The following example changes the level of messages displayed to the console terminal to **alerts**, which means alerts and emergencies are displayed:

```
logging console alerts
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

logging facility
access-list (extended)†

logging facility

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

logging facility *facility-type*
no logging facility

Syntax Description

facility-type	Syslog facility. See Table 5-10 for the *facility-type* keywords.

Default

local7

Command Mode

Global configuration

Usage Guidelines

Table 5-10 describes the acceptable options for the *facility-type* keyword.

Table 5-10 Logging Facility Facility-Type Keywords

Keyword	Description
auth	Authorization system
cron	Cron facility
daemon	System daemon
kern	Kernel
local0–7	Reserved for locally defined messages
lpr	Line printer system
mail	Mail system
news	USENET news
sys9	System use
sys10	System use
sys11	System use
sys12	System use
sys13	System use
sys14	System use
syslog	System log
user	User process
uucp	UNIX-to-UNIX copy system

Example

The following example configures the syslog facility to *kernel*:

```
logging facility kern
```

Related Command

logging console

logging monitor

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

logging monitor *level*
no logging monitor

Syntax Description

level	One of the *level* keywords listed in Table 5-9.

Default

debugging

Command Mode

Global configuration

Usage Guidelines

Specifying a *level* causes messages at that level and numerically lower levels to be displayed to the monitor.

Example

The following example specifies that only messages of the levels **errors**, **critical**, **alerts**, and **emergencies** be displayed on terminals:

```
logging monitor errors
```

Related Command

A double dagger (††) indicates that the command is documented in the *Cisco Access Connection Guide*.

terminal monitor ††

logging on

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

logging on
no logging on

Syntax Description

This command has no arguments or keywords.

Default

The router logs messages to the console terminal.

Command Mode

Global configuration

Example

The following example shows how to direct error messages to the console terminal only:

```
no logging on
```

logging synchronous

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. Use the **no** form of this command to disable synchronization of unsolicited messages and debug output.

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

Syntax Description

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

Defaults

This feature is turned off by default.

If you do not specify a severity level, the default value of 2 is assumed.

If you do not specify the maximum number of buffers to be queued, the default value of 20 is assumed.

Command Mode

Line configuration

Usage Guidelines

When synchronous logging of unsolicited messages and **debug** output is turned on, unsolicited router output is displayed on the console or printed after solicited router output is displayed or printed. Unsolicited messages and **debug** output is displayed on the console after the prompt for user input is returned. This is to keep unsolicited messages and **debug** output from being interspersed with solicited router output and prompts. After the unsolicited messages are displayed, the console displays the user prompt again.

When specifying a severity level number, consider that for the logging system, low numbers indicate greater severity and high numbers indicate lesser severity.

When a terminal line's message-queue limit is reached, new messages are dropped from the line, although these messages might be displayed on other lines. If messages are dropped, the notice "%SYS-3-MSGLOST *number-of-messages* due to overflow" follows any messages that are displayed. This notice is displayed only on the terminal that lost the messages. It is not sent to any other lines, any logging servers, or the logging buffer.

Caution By configuring abnormally large message-queue limits and setting the terminal to "terminal monitor" on a terminal that is accessible to intruders, you expose yourself to "denial of service" attacks. An intruder could carry out the attack by putting the terminal in synchronous output mode, making a Telnet connection to a remote host, and leaving the connection idle. This could cause large numbers of messages to be generated and queued, and these messages would consume all available RAM. Although unlikely to occur, you should guard against this type of attack through proper configuration.

Example

The following example identifies line 4 and enables synchronous logging for line 4 with a severity level of 6. Then the example identifies another line, line 2, and enables synchronous logging for line 2 with a severity level of 7 and specifies a maximum number of buffers to be 70000:

```
line 4
logging synchronous level 6
line 2
logging synchronous level 7 limit 70000
```

Related Command

A dagger (†) indicates that the command is documented in another chapter.

line†

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.

logging trap *level*
no logging trap

Syntax Description

level	One of the *level* keywords listed in Table 5-9.

Default

informational

Command Mode

Global configuration

Usage Guidelines

The EXEC command **show logging** displays the addresses and levels associated with the current logging setup. The command output also includes ancillary statistics.

Table 5-9 lists the syslog definitions that correspond to the debugging message levels. Additionally, there are four categories of messages generated by the software, as follows:

- Error messages about software or hardware malfunctions at the LOG_ERR level.
- Output for the debug commands at the LOG_WARNING level.
- Interface up/down transitions and system restarts at the LOG_NOTICE level.
- Reload requests and low process stacks are at the LOG_INFO level.

Use the **logging** and **logging trap** commands to send messages to a UNIX syslog server.

Example

The following example logs messages to a host named *johnson*:

```
logging johnson
logging trap notifications
```

Related Command

logging

login authentication

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

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

Caution If you use a *list-name* value that was not configured with the **aaa authentication login** command, you will disable login on this line.

Syntax Description

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.

Default

Uses the default set with **aaa authentication login**.

Command Mode

Line configuration

Usage Guideline

This command is a per-line command used with AAA that specifies the name of a list of TACACS+ authentication methods to try at login. If no list is specified, the default list is used (whether or not it is specified in the command line). You create defaults and lists with the **aaa authentication login** command. Entering the **no** version of **login authentication** has the same effect as entering the command with the **default** argument.

Before issuing this command, create a list of authentication processes by using the global configuration **aaa authentication login** command.

Examples

The following example specifies that the default AAA authentication is to be used on line 4:

```
line 4
login authentication default
```

The following example specifies that the AAA authentication list called *MIS-access* is to be used on line 7:

```
line 7
login authentication MIS-access
```

Related Command

aaa authentication login

ntp access-group

To control access to the system's Network Time Protocol (NTP) services, use the **ntp access-group** global configuration command. To remove access control to the system's NTP services, use the **no** form of this command.

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

Syntax Description

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.

Default

No access control (full access granted to all systems)

Command Mode

Global configuration

Usage Guidelines

The access group options are scanned in the following order from least restrictive to most restrictive:

1. peer
2. serve
3. serve-only
4. query-only

Access is granted for the first match that is found. If no access groups are specified, all access is granted to all sources. If any access groups are specified, only the specified access is granted. This facility provides minimal security for the time services of the system. However, it can be circumvented by a determined programmer. If tighter security is desired, use the NTP authentication facility.

Example

In the following example, the system is configured to allow itself to be synchronized by a peer from access list 99. However, the system restricts access to allow only time requests from access list 42.

```
ntp access-group peer 99
ntp access-group serve-only 42
```

Related Command

A dagger (†) indicates that the command is documented in another chapter.

access-list †

ntp authenticate

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

ntp authenticate
no ntp authenticate

Syntax Description

This command has no keywords or arguments.

Default

No authentication

Command Mode

Global configuration

Usage Guidelines

Use this command if you want authentication. If this command is specified, the system will not synchronize to a system unless it carries one of the authentication keys specified in the **ntp trusted-key** command.

Example

The following example enables NTP authentication:

```
ntp authenticate
```

Related Commands

ntp authentication-key
ntp trusted-key

ntp authentication-key

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

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

Syntax Description

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

Default

No authentication key is defined for NTP.

Command Mode

Global configuration

Usage Guidelines

Use this command to define authentication keys for use with other NTP commands in order to provide a higher degree of security.

Note When this command is written to NVRAM, the key is encrypted so that it is not displayed when the configuration is viewed.

Example

The following example sets authentication key 10 to *aNiceKey*:

```
ntp authentication-key 10 md5 aNiceKey
```

Related Commands

ntp authenticate
ntp peer
ntp server
ntp trusted-key

ntp broadcast

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

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

Syntax Description

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

Default

Disabled

Command Mode

Interface configuration

Example

In the following example, Ethernet interface 0 is configured to send NTP version 2 packets:

```
interface ethernet 0
ntp broadcast version 2
```

Related Commands

ntp broadcast client
ntp broadcastdelay

ntp broadcast client

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

ntp broadcast client
no ntp broadcast client

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

Use this command to allow the system to listen to broadcast packets on an interface-by-interface basis.

Example

In the following example, the router synchronizes to NTP packets broadcasted on Ethernet interface 1:

```
interface ethernet 1
ntp broadcast client
```

Related Commands

ntp broadcast
ntp broadcastdelay

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.

ntp broadcastdelay *microseconds*
no ntp broadcastdelay

Syntax Description

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

Default

3000 microseconds

Command Mode

Global configuration

Usage Guidelines

Use this command when the router is configured as a broadcast client and the round-trip delay on the network is other than 3000 microseconds.

Example

In the following example, the estimated round-trip delay between the router and the broadcast client is set to 5000 microseconds:

```
ntp broadcastdelay 5000
```

Related Commands

ntp broadcast
ntp broadcast client

ntp clock-period

Caution Do not enter this command; it is documented for informational purposes only. The system automatically generates this command as Network Time Protocol (NTP) determines the clock error and compensates.

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

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

Syntax Description

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

Default

17179869 (4 milliseconds)

Command Mode

Global configuration

Usage Guidelines

If a **copy running-config startup-config** command is entered to save the configuration to NVRAM, this command will automatically be added to the configuration. It is a good idea to perform this task after NTP has been running for a week or so; this will help NTP synchronize more quickly if the system is restarted.

ntp disable

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

ntp disable
no ntp disable

Syntax Description

This command has no arguments or keywords.

Default

Enabled

Command Mode

Interface configuration

Usage Guidelines

This command provides a simple method of access control.

Example

In the following example, Ethernet interface 0 is prevented from receiving NTP packets:

```
interface ethernet 0
ntp disable
```

ntp master

To configure the router as a Network Time Protocol (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.

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

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

Syntax Description

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

Default

By default, the master clock function is disabled. When enabled, the default stratum is 8.

Command Mode

Global configuration

Usage Guidelines

Since our implementation of NTP does not support directly attached radio or atomic clocks, the router is normally synchronized, directly or indirectly, to an external system that has such a clock. In a network without Internet connectivity, such a time source may not be available. The **ntp master** command is used in such cases.

If the system has **ntp master** configured, and it cannot reach any clock with a lower stratum number, the system will claim to be synchronized at the configured stratum number, and other systems will be willing to synchronize to it via NTP.

Note The system clock must have been set from some source, including manually, before **ntp master** will have any effect. This protects against distributing erroneous time after the system is restarted.

Example

In the following example, the router is configured as an NTP master clock to which peers may synchronize:

```
ntp master 10
```

Related Command

clock calendar-valid

ntp peer

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.

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

Syntax Description

ip-address	IP address of the peer providing, or being provided, the clock synchronization.
version	(Optional) Defines the Network Time Protocol (NTP) version number.
number	(Optional) NTP version number (1 to 3).
key	(Optional) Defines the authentication key.
keyid	(Optional) Authentication key to use when sending packets to this peer.
source	(Optional) Names the interface.
interface	(Optional) Name of the interface from which to pick the IP source address.
prefer	(Optional) Makes this peer the preferred peer that provides synchronization.

Default

No peers are configured by default. If a peer is configured, the default NTP version number is 3, no authentication key is used, and the source IP address is taken from the outgoing interface.

Command Mode

Global configuration

Usage Guidelines

Use this command if you want to allow this machine to synchronize with the peer, or vice versa. Using the **prefer** keyword will reduce switching back and forth between peers.

If you are using the default version of 3 and NTP synchronization does not occur, try using NTP version number 2. Many NTP servers on the Internet run version 2.

Example

In the following example, the router is configured to allow its system clock to be synchronized with the clock of the peer (or vice versa) at IP address 131.108.22.33 using NTP version 2. The source IP address will be the address of Ethernet 0.

```
ntp peer 131.108.22.33 version 2 source ethernet 0
```

Related Commands

ntp authentication-key
ntp server
ntp source

ntp server

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.

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

Syntax Description

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.

Default

No peers are configured by default. If a peer is configured, the default NTP version number is 3, no authentication key is used, and the source IP address is taken from the outgoing interface.

Command Mode

Global configuration

Usage Guidelines

Use this command if you want to allow this machine to synchronize with the specified server. The server will not synchronize to this machine.

Using the **prefer** keyword will reduce switching back and forth between servers.

If you are using the default version of 3 and NTP synchronization does not occur, try using NTP version number 2. Many NTP servers on the Internet run version 2.

Example

In the following example, the router is configured to allow its system clock to be synchronized with the clock of the peer at IP address 128.108.22.44 using NTP version 2:

```
ntp server 128.108.22.44 version 2
```

Related Commands

ntp authentication-key
ntp peer
ntp source

ntp source

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

ntp source *interface*
no ntp source

Syntax Description

interface	Any valid system interface name.

Default

Source address is determined by the outgoing interface.

Command Mode

Global configuration

Usage Guidelines

Use this command when you want to use a particular source IP address for all NTP packets. The address is taken from the named interface. This command is useful if the address on an interface cannot be used as the destination for reply packets. If the **source** keyword is present on an **ntp server** or **ntp peer** command, that value overrides the global value.

Example

In the following example, the router is configured to use the IP address of Ethernet 0 as the source address of all outgoing NTP packets:

```
ntp source ethernet 0
```

Related Commands

ntp peer
ntp server

ntp trusted-key

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

ntp trusted-key *key-number*
no ntp trusted-key *key-number*

Syntax Description

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

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

If authentication is enabled, use this command to define one or more key numbers (corresponding to the keys defined with the**ntp authentication-key** command) that a peer NTP system must provide in its NTP packets, in order for this system to synchronize to it. This provides protection against accidentally synchronizing the system to a system that is not trusted, since the other system must know the correct authentication key.

Example

In the following example, the system is configured to synchronize only to systems providing authentication key 42 in its NTP packets:

```
ntp authenticate
ntp authentication-key 42 md5 aNiceKey
ntp trusted-key 42
```

Related Commands

ntp authenticate
ntp authentication-key

ntp update-calendar

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

ntp update-calendar
no ntp update-calendar

Syntax Description

This command has no arguments or keywords.

Default

The Cisco 7000 calendar is not updated.

Command Mode

Global configuration

Usage Guidelines

If a Cisco 7000 is synchronized to an outside time source via NTP, it is a good idea to periodically update the calendar with the time learned from NTP. Otherwise, the calendar will tend to gradually lose or gain time. The calendar will be updated only if NTP has synchronized to an authoritative time server.

Example

In the following example, the system is configured to periodically update the calendar from the system clock:

```
ntp update-calendar
```

Related Commands

clock read-calendar
clock update-calendar

ping (privileged)

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

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

Syntax Description

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.

Command Mode

Privileged EXEC

Usage Guidelines

The ping program sends an echo request packet to an address, then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

To abnormally terminate a ping session, type the escape sequence—by default, **Ctrl-^ X**. You type the default by simultaneously pressing and releasing the **Ctrl**, **Shift**, and **6** keys, and then pressing the **X** key.

Table 5-11 describes the test characters that the ping facility sends.

Table 5-11 Ping Test Characters

Char	Meaning
!	Each exclamation point indicates receipt of a reply.
.	Each period indicates the network server timed out while waiting for a reply.
U	A destination unreachable error PDU was received.
C	A congestion experienced packet was received.
I	User interrupted test.
?	Unknown packet type.
&	Packet lifetime exceeded.

Note Not all protocols require hosts to support pings. For some protocols, the pings are Cisco-defined and are only answered by another Cisco router.

Example

After you enter the **ping** command in privileged mode, the system prompts for one of the following keywords**: appletalk**, **clns**, **ip**, **novell**, **apollo**, **vines**, **decnet**, or **xns.** The default protocol is IP.

If you enter a host name or address on the same line as the **ping** command, the default action is taken as appropriate for the protocol type of that name or address.

While the precise dialog varies somewhat from protocol to protocol, all are similar to the ping session using default values shown in the following display.

```
Router# ping
Protocol [ip]:
Target IP address: 192.31.7.27
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.31.7.27, timeout is 2 seconds:
!!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/2/4 ms
```

Table 5-12 describes the default **ping** fields shown in the display.

Table 5-12 Ping Field Descriptions

Field	Description
Protocol [ip]:	Prompts for a supported protocol. Enter **appletalk**, **clns**, **ip**, **novell**, **apollo**, **vines**, **decnet**, or **xns**. Default: **ip**.
Target IP address:	Prompts for the IP address or host name of the destination node you plan to ping. If you have specified a supported protocol other than IP, enter an appropriate address for that protocol here. Default: none.
Repeat count [5]:	Number of ping packets that will be sent to the destination address. Default: 5.
Datagram size [100]:	Size of the ping packet (in bytes). Default: 100 bytes.
Timeout in seconds [2]:	Timeout interval. Default: 2 (seconds).
Extended commands [n]:	Specifies whether or not a series of additional commands appears. Many of the following displays and tables show and describe these commands.
Sweep range of sizes [n]:	Allows you to vary the sizes of the echo packets being sent. This capability is useful for determining the minimum sizes of the MTUs configured on the nodes along the path to the destination address. Packet fragmentation contributing to performance problems can then be reduced.
!!!!!	Each exclamation point (!) indicates receipt of a reply. A period (.) indicates the network server timed out while waiting for a reply. Other characters may appear in the ping output display, depending on the protocol type.
Success rate is 100 percent	Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.
round-trip min/avg/max = 1/2/4 ms	Round-trip travel time intervals for the protocol echo packets, including minimum/average/maximum (in milliseconds).

Related Command

ping (user)

ping (user)

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

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

Syntax Description

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.

Command Mode

EXEC

Usage Guidelines

The user-level ping feature provides a basic ping facility for users who do not have system privileges. This feature allows the router to perform the simple default ping functionality for a number of protocols. Only the nonverbose form of the **ping** command is supported for user-level pings.

If the system cannot map an address for a host name, it will return an "%Unrecognized host or address" error message.

To abnormally terminate a ping session, type the escape sequence—by default, **Ctrl-^ X**. You type the default by simultaneously pressing and releasing the **Ctrl**, **Shift**, and **6** keys and then pressing the **X** key.

Table 5-13 describes the test characters that the ping facility sends.

Table 5-13 Ping Test Characters

Char	Meaning
!	Each exclamation point indicates receipt of a reply.
.	Each period indicates the network server timed out while waiting for a reply.
U	A destination unreachable error PDU was received.
C	A congestion experienced packet was received.
I	User interrupted test.
?	Unknown packet type.
&	Packet lifetime exceeded.

Example

The following display shows sample ping output when you ping the IP host named *donald*:

```
Router> ping donald
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.31.7.27, timeout is 2 seconds:
!!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/3/4 ms
```

Related Command

ping (privileged)

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 this command to disable this authentication.

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

Caution If you use a *list-name* value that was not configured with the **aaa authentication ppp** command, you will disable PPP on this interface.

Syntax Description

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.

Default

PPP authentication is not enabled.

Command Mode

Interface configuration

Usage Guidelines

Once you have enabled CHAP or PAP, the local router requires a password from remote devices. If the remote device does not support CHAP or PAP, no traffic is passed to that device.

If you are using **autoselect** on a TTY line, you will probably want to use the **ppp authentication** command to turn on PPP authentication for the corresponding interface.

If you specify the **if-needed** option, PPP authentication is not required when the user has already provided authentication. This option is useful if you are using the **autoselect** command, but it cannot be used with AAA/TACACS+.

The *list-name* argument can be used only when AAA/TACACS+ is initialized and cannot be used with the **if-needed** argument.

Example

The following example enables CHAP on asynchronous interface 4, and uses the authentication list MIS-access:

```
interface async 4
encapsulation ppp
ppp authentication chap MIS-access
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

aaa authentication ppp
aaa new-model
autoselect †
encapsulation ppp
ppp use-tacacs
username

ppp use-tacacs

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

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

Note This command is not used in AAA/TACACS+ and has been replaced with the **aaa authentication ppp** command.

Syntax Description

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

Default

TACACS is not used for PPP authentication.

Command Mode

Interface configuration

Usage Guidelines

This is a per-interface command. Use this command only when you have set up an extended TACACS server. This command requires the new extended TACACS server.

When CHAP authentication is being used, the **ppp use-tacacs** command with the **single-line** option specifies that if a username and password are specified in the username, separated by an asterisk (*), then a standard tacacs login query is performed using that username and password. If the username does not contain an asterisk, then normal CHAP authentication is performed using TACACS.

This feature is useful when integrating TACACS with other authentication systems that require a clear-text version of the user's password. Such systems include one-time password systems, token card systems, kerberos, and others.

Caution Normal CHAP authentications prevent the clear-text password from being transmitted over the link. When you use the single-line option, passwords will cross the link in the clear.

If the username and password are contained in the CHAP password, then the CHAP secret is not used by the Cisco system. Because most PPP clients will require that a secret be specified, you can use any arbitrary string; the Cisco system will ignore it.

Examples

In the following example, asynchronous serial interface 1 is configured to use TACACS for CHAP authentication.

```
interface async 1
ppp authentication chap
ppp use-tacacs
```

In the following example, asynchronous serial interface 1 is configured to use TACACS for PAP authentication.

```
interface async 1
ppp authentication pap
ppp use-tacacs
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

ppp authentication†
ppp authentication†
tacacs-server extended
tacacs-server host

priority-group

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

priority-group *list*
no priority-group

Syntax Description

list	Priority list number assigned to the interface. An integer from 1 to 16.

Default

None

Command Mode

Interface configuration

Usage Guidelines

Only one list can be assigned per interface. Priority output queueing provides a mechanism to prioritize packets transmitted on an interface.

Use the **show queuing priority** and **show interface** commands to display the current status of the output queues.

Example

The following example causes packets on interface serial 0 to be classified by priority list 1:

```
interface serial 0
priority-group 1
```

Related Commands

priority-list
priority-list interface
priority-list queue-limit
priority-list stun

priority-list default

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

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

Syntax Description

list-number	Arbitrary integer between 1 and 16 that identifies the priority list selected by the user.
high | **medium** | **normal** | **low**	Priority queue level.

Default

The **normal** queue is assumed if you use the **no** form of the command.

Command Mode

Global configuration

Usage Guidelines

When using multiple rules, remember that the system reads the priority settings in order of appearance. When classifying a packet, the system searches the list of rules specified by **priority-list** commands for a matching protocol or interface type. When a match is found, the packet is assigned to the appropriate queue. The list is searched in the order it is specified, and the first matching rule terminates the search.

Example

The following example sets the priority queue for those packets that do not match any other rule in the priority list to a low priority:

```
priority-list 1 default low
```

Related Commands

priority-group
show queueing

priority-list interface

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

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

Syntax Description

list-number	Arbitrary integer between 1 and 16 that identifies the priority list selected by the user.
interface-type	Specifies the name of the interface.
interface-number	Number of the specified interface.
high | **medium** | **normal** | **low**	Priority queue level.

Default

No queuing priorities are established.

Command Mode

Global configuration

Usage Guidelines

When using multiple rules, remember that the system reads the priority settings in order of appearance. When classifying a packet, the system searches the list of rules specified by **priority-list** commands for a matching protocol or interface type. When a match is found, the packet is assigned to the appropriate queue. The list is searched in the order it is specified, and the first matching rule terminates the search.

Example

The following example sets any packet type entering on Ethernet interface 0 to a medium priority:

```
priority-list 3 interface ethernet 0 medium
```

Related Commands

priority-group
show queueing

priority-list protocol

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

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

Syntax Description

list-number	Arbitrary integer between 1 and 16 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, dlsw, ip**, **ipx**, **pad**, **rsrb**, **stun**, **vines**, **xns**, and **x25**.
high | **medium** | **normal** | **low**	Priority queue level.
queue-keyword keyword-value	Possible keywords are **fragments**, **gt**, **lt**, **list**, **tcp**, and **udp**. See Table 5-14.

Default

No queuing priorities are established.

Command Mode

Global configuration

Usage Guidelines

When using multiple rules, remember that the system reads the priority settings in order of appearance. When classifying a packet, the system searches the list of rules specified by **priority-list** commands for a matching protocol or interface type. When a match is found, the packet is assigned to the appropriate queue. The list is searched in the order it is specified, and the first matching rule terminates the search.

The **decnet_router-l1** keyword refers to the multicast address for all level-1 routers, which are intra-area routers, and the **decnet_router-l2** keyword refers to all level 2 routers, which are interarea routers.

The **dlsw**, **rsrb**, and **stun** keywords refer only to direct encapsulation.

Use Table 5-14, Table 5-15, and Table 5-16 to configure the queuing priorities for your system.

Table 5-14 Protocol Priority Queue Keywords and Values

Option	Description
fragments	Assigns the priority level defined to fragmented IP packets (for use with IP protocol only). More specifically, IP packets whose fragment offset field is nonzero are matched by this command. The initial fragment of a fragmented IP packet has a fragment offset of zero, so such packets are not matched by this command. Note: Packets with a nonzero fragment offset do not contain TCP or UDP headers, so other instances of this command that use the **tcp** or **udp** keyword will always fail to match such packets.
gt *byte-count*	Specifies a greater-than count. The priority level assigned goes into effect when a packet exceeds the value entered for the argument *byte-count*. The size of the packet must also include additional bytes due to MAC encapsulation on the outgoing interface.
lt *byte-count*	Specifies a less-than count. The priority level assigned goes into effect when a packet size is less than the value entered for *byte-count*. The size of the packet must also include additional bytes due to MAC encapsulation on the outgoing interface.
list *list-number*	Assigns traffic priorities according to a specified list when used with Appletalk, bridging, IP, IPX, VINES, or XNS. The *list-number* argument is the access list number as specified by the **access-list** global configuration command for the specified *protocol-name*. For example, if the protocol is AppleTalk, *list-number* should be a valid AppleTalk access list number.
tcp *port*	Assigns the priority level defined to TCP segments originating from or destined to a specified port (for use with the IP protocol only). Table 5-15 lists common TCP services and their port numbers.
udp *port*	Assigns the priority level defined to UDP packets originating from or destined to the specified port (for use with the IP protocol only). Table 5-16 lists common UDP services and their port numbers.

Table 5-15 Common TCP Services and Their Port Numbers

Service	Port
Telnet	23
SMTP	25

Table 5-16 Common UDP Services and Their Port Numbers

Service	Port
TFTP	69
NFS	2049
SNMP	161
RPC	111
DNS	53

Note The TCP and UDP ports listed in Table 5-15 and Table 5-16 include some of the more common port numbers. However, you can specify any port number to be prioritized; you are not limited to those listed.

Use the **no priority-list** global configuration command followed by the appropriate *list-number* argument and the **protocol** keyword to remove a priority list entry assigned by protocol type.

Examples

The following example assigns 1 as the arbitrary priority list number, specifies DECnet as the protocol type, and assigns a high-priority level to the DECnet packets transmitted on this interface:

```
priority-list 1 protocol decnet high
```

The following example assigns a medium-priority level to every DECnet packet with a size greater than 200 bytes:

```
priority-list 2 protocol decnet medium gt 200
```

The following example assigns a medium-priority level to every DECnet packet with a size less than 200 bytes:

```
priority-list 4 protocol decnet medium lt 200
```

The following example assigns a high-priority level to traffic that matches IP access list 10:

```
priority-list 1 protocol ip high list 10
```

The following example assigns a medium-priority level to Telnet packets:

```
priority-list 4 protocol ip medium tcp 23
```

The following example assigns a medium-priority level to UDP Domain Name service packets:

```
priority-list 4 protocol ip medium udp 53
```

The following example assigns a high-priority level to traffic that matches Ethernet type code access list 201:

```
priority-list 1 protocol bridge high list 201
```

The following example assigns a high-priority level to DLSw+ traffic with TCP encapsulation:

```
priority-list 1 protocol ip  high  tcp 2065
```

The following example assigns a high-priority level to DLSw+ traffic with Direct encapsulation:

```
priority-list 1 protocol dlsw high
```

Related Commands

priority-group
show queueing

priority-list queue-limit

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

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

Syntax Description

list-number	Arbitrary integer between 1 and 16 that identifies the priority list selected by the user.
high-limit medium-limit normal-limit low-limit	Priority queue maximum length. A value of 0 for any of the four arguments means that the queue can be of unlimited size for that particular queue.

Default

The default queue limit arguments are listed in Table 5-17.

Table 5-17 Priority Queue Packet Limits

Priority Queue Argument	Packet Limits
high-limit	20
medium-limit	40
normal-limit	60
low-limit	80

Command Mode

Global configuration

Usage Guidelines

If a priority queue overflows, excess packets are discarded and quench messages can be sent, if appropriate, for the protocol.

Example

The following example sets the maximum packets in the priority queue to 10:

```
priority-list 2 queue-limit 10 40 60 80
```

Related Commands

priority-group
show queueing

privilege level (global)

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.

privilege *mode* **level** *level command*
no privilege *mode* **level** *level command*

Syntax Description

mode	Configuration mode. See Table 5-7 in the description of the **alias** command 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.

Defaults

Level 15 is the level of access permitted by the **enable** password.

Level 1 is normal EXEC-mode user privileges.

Command Mode

Global configuration

Usage Guidelines

Table 5-7 in the description of the **alias** command shows the acceptable options for the *mode* argument in the **privilege level** global configuration command.

The password for the privilege level defined using the **privilege level** global configuration mode is configured using the **enable password**command.

Level 0 can be used to specify a more-limited subset of commands for specific users or lines. For example, you can allow user “guest” to only use the **show users** and **exit** commands.

If you set a command to a privilege level, all commands that have a syntax that is a subset of the syntax of that command will also be set to that level. For example, if you set the command **show ip route** to level 15, if you do not set **show** commands and **show ip** commands to a different level, they will also be at privilege level 15.

Example

In the following example, the **configure** command in global configuration mode is assigned a privilege level of 14. Only users who know the level 14 password will be able to use the **configure** command.

```
privilege exec level 14 configure
enable password level 14 pswd14
```

Related Commands

enable password
privilege level (line)

privilege level (line)

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.

privilege level *level*
no privilege level

Syntax Description

level	Privilege level to be associated with the specified line.

Defaults

Level 15 is the level of access permitted by the enable password.

Level 1 is normal EXEC-mode user privileges.

Command Mode

Line configuration

Usage Guidelines

The privilege level that is set using this command can be overridden by a user logging in to the line and enabling a different privilege level. The user can lower the privilege level by using the **disable** command. If they know the password to a higher privilege level, they can use that password to enable the higher privilege level.

Level 0 can be used to specify a more limited subset of commands for specific users or lines. For example, you can allow user "guest" to only use the **show users** and **exit** commands.

You might specify a high level of privilege for your console line if you are able to restrict who uses that line.

Example

In the following example, the auxiliary line is configured for privilege level 5. Anyone who is using the auxiliary line will have privilege level 5 by default.

```
line aux 0
privilege level 5
```

Related Commands

enable password
privilege level (line)

prompt

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.

prompt *string*
no prompt [*string*]

Syntax Description

string	Router prompt. It can consist of all printing characters and the escape sequences listed in Table 5-18 in the "Usage Guidelines" section.

Default

The default router prompt is either *Router* or the router name defined with the **hostname** global configuration command, followed by an angle bracket (>) for EXEC mode or a pound sign (#) for privileged EXEC mode.

Command Mode

Global configuration

Usage Guidelines

You can include escape sequences when specifying the router prompt. All escape sequences are preceded by a percent sign (%). Table 5-18 lists the valid escape sequences.

Table 5-18 Custom Router Prompt Escape Sequences

Escape Sequence	Interpretation
%h	Router's host name. This is either *Router* or the name defined with the **hostname** global configuration command.
%n	Physical terminal line (TTY) number of the EXEC user.
%p	Prompt character itself. It is either an angle bracket (>) for EXEC mode or a pound sign (#) for privileged EXEC mode.
%s	Space.
%t	Tab.
%%	Percent sign (%)

Specifying the command **prompt %h** has the same effect as issuing the **no prompt** command.

Examples

The following example changes the EXEC prompt to include the TTY number, followed by the router name and a space:

```
prompt TTY%n@%h%s%p
```

The following are examples of user and privileged EXEC prompts that result from the previous command:

```
TTY17@Router1 >
TTY17SRouter1 #
```

Related Command

hostname

queue-list default

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

queue-list *list-number* **default** *queue-number*
no queue-list *list-number* **default** *queue-number*

Syntax Description

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

Default

Queue number 1

Command Mode

Global configuration

Usage Guidelines

Queue number 0 is a system queue. It is emptied before any of the other queues are processed. The system enqueues high-priority packets, such as keepalives, to this queue.

When using multiple rules, remember that the system reads the **queue-list** commands in order of appearance. When classifying a packet, the system searches the list of rules specified by **queue-list** commands for a matching protocol or interface type. When a match is found, the packet is assigned to the appropriate queue. The list is searched in the order it is specified, and the first matching rule terminates the search.

Example

In the following example, the default queue for list 10 is set to queue number 2:

```
queue-list 10 default 2
```

Related Commands

custom-queue-list
show queueing

queue-list interface

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

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

Syntax Description

list-number	Number of the queue list. An integer from 1 to 16.
interface-type	Required argument that specifies the name of the interface.
interface-number	Number of the specified interface.
queue-number	Number of the queue. An integer from 1 to 16.

Default

No queuing priorities are established.

Command Mode

Global configuration

Usage Guidelines

When using multiple rules, remember that the system reads the **queue-list** commands in order of appearance. When classifying a packet, the system searches the list of rules specified by **queue-list** commands for a matching protocol or interface type. When a match is found, the packet is assigned to the appropriate queue. The list is searched in the order it is specified, and the first matching rule terminates the search.

Example

In the following example, queue list 4 established queuing priorities for packets entering on interface tunnel 3. The queue number assigned is 10.

```
queue-list 4 interface tunnel 3 10
```

Related Commands

custom-queue-list
show queueing

queue-list protocol

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

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

Syntax Description

list-number	Number of the queue list. An integer from 1 to 16.
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_routerl1**, **decnet_routerl2**, **dlsw**, **ip**, **ipx**, **pad**, **rsrb**, **stun**, **vines**, **xns**, and **x25**.
queue-number	Number of the queue. An integer from 1 to 16.
queue-keyword keyword-value	Possible keywords are **gt**, **lt**, **list**, **tcp**, and **udp**. See Table 5-14.

Default

No queuing priorities are established.

Command Mode

Global configuration

Usage Guidelines

When using multiple rules, remember that the system reads the **queue-list** commands in order of appearance. When classifying a packet, the system searches the list of rules specified by **queue-list** commands for a matching protocol or interface type. When a match is found, the packet is assigned to the appropriate queue. The list is searched in the order it is specified, and the first matching rule terminates the search.

The **decnet_router-l1** keyword refers to the multicast address for all level-1 routers, which are intra-area routers, and the **decnet_router-l2** keyword refers to all level 2 routers, which are interarea routers.

The **rsrb** keyword refers only to RSRB direct encapsulation.

Use Table 5-14, Table 5-15, and Table 5-16 from the **priority-list protocol** command to configure custom queuing for your system.

Examples

The following example assigns 1 as the custom queue list, specifies DECnet as the protocol type, and assigns 3 as a queue number to the packets transmitted on this interface:

```
queue-list 1 protocol decnet 3
```

The following example assigns DECnet packets with a size greater than 200 bytes to queue number 2:

```
queue-list 2 protocol decnet 2 gt 200
```

The following example assigns DECnet packets with a size less than 200 bytes to queue number 2:

```
queue-list 4 protocol decnet 2 lt 200
```

The following example assigns traffic that matches IP access list 10 to queue number 1:

```
queue-list 1 protocol ip 1 list 10
```

The following example assigns Telnet packets to queue number 2:

```
queue-list 4 protocol ip 2 tcp 23
```

The following example assigns UDP Domain Name service packets to queue number 2:

```
queue-list 4 protocol ip 2 udp 53
```

The following example assigns traffic that matches Ethernet type code access list 201 to queue number 1:

```
queue-list 1 protocol bridge 1 list 201
```

Related Commands

custom-queue-list
show queueing

queue-list queue byte-count

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

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

Syntax Description

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

Default

1500 bytes

Command Mode

Global configuration

Example

In the following example, queue list 9 establishes the byte-count as 1400 for queue number 10:

```
queue-list 9 queue 10 byte-count 1400
```

Related Commands

custom-queue-list
show queueing

queue-list queue limit

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

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

Syntax Description

list-number	Number of the queue list. An integer from 1 to 16.
queue-number	Number of the queue. An integer from 1 to 16.
limit-number	Maximum number of packets which can be enqueued at any time. Range is 0 to 32767 queue entries. A value of 0 means that the queue can be of unlimited size.

Default

20 entries

Command Mode

Global configuration

Example

In the following example, the queue length of queue 10 is increased to 40:

```
queue-list 5 queue 10 limit 40
```

Related Commands

custom-queue-list
show queueing

scheduler allocate

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

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

Syntax Description

interrupt-time	Integer (in microseconds) that limits the maximum number of microseconds to spend on fast switching within any one network interrupt context. The range is 400 to 60000 microseconds. The default is 4000 microseconds.
process-time	Integer (in microseconds) that guarantees the minimum number of microseconds to spend at the process level when network interrupts are disabled. The range is 100 to 4000. The default is 200 microseconds.

Default

Approximately 5 percent of the CPU is available for process tasks.

Command Mode

Global configuration

Usage Guidelines

This command applies to the Cisco 7200 series and Cisco 7500 series.

Caution Cisco recommends that you do not change the default values.

Example

The following example makes 20 percent of the CPU available for process tasks:

```
scheduler allocate 2000 500
```

Related Command

scheduler interval

scheduler interval

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

scheduler interval *milliseconds*
no scheduler interval

Syntax Description

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

Default

High-priority operations are allowed to use as much of the central processor as needed.

Command Mode

Global configuration

Usage Guidelines

The normal operation of the network server allows the switching operations to use as much of the central processor as is required. If the network is running unusually heavy loads that do not allow the processor the time to handle the routing protocols, give priority to the system process scheduler. High-priority operations are allowed to use as much of the central processor as needed.

On the Cisco 7200 series and Cisco 7500 series, use the **scheduler allocate** global configuration command.

Example

The following example changes the low-priority process schedule to an interval of 750 milliseconds:

```
scheduler interval 750
```

Related Command

scheduler allocate

service exec-wait

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

service exec-wait
no service exec-wait

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command delays startup of the EXEC until the line has been idle (no traffic seen) for 3 seconds. The default is to enable the line immediately on modem activation.

This command is useful on noisy modem lines or when a modem attached to the line is configured to ignore MNP or V.42 negotiations, and MNP or V.42 modems may be dialing in. In these cases, noise or MNP/V.42 packets may be interpreted as usernames and passwords, causing authentication failure before the user gets a chance to type a username/password. The command is not useful on non-modem lines or lines without some kind of login configured.

Example

The following example delays the startup of the EXEC:

```
service exec-wait
```

service finger

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

service finger
no service finger

Syntax Description

This command has no arguments or keywords.

Default

Enabled

Command Mode

Global configuration

Example

The following is an example of how to disable the Finger protocol:

```
no service finger
```

service hide-telnet-address

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

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

Syntax Description

This command has no arguments or keywords.

Default

Addresses are displayed.

Command Mode

Global configuration

Usage Guidelines

When you attempt to connect to a device, the router displays addresses and other messages (for example, Trying router1 (171.69.1.154, 2008)...). With the hide feature, the router suppresses the display of the address (for example, Trying router1 address #1...). The router continues to display all other messages that would normally display during a connection attempt, such as detailed error messages if the connection was not successful.

The hide feature improves the functionality of the busy-message feature. When you configure only the **busy-message** command, the normal messages generated during a connection attempt are not displayed; only the busy-message is displayed. When you use the hide and busy features together you can customize the information displayed during Telnet connection attempts. When you configure the **service hide-telnet-address** command and the **busy-message** command, the router suppresses the address and displays the message specified with the **busy-message** command if the connection attempt is not successful.

Example

The following example shows how to hide Telnet addresses:

```
service hide-telnet-address
```

Related Command

A dagger (†) indicates that the command is documented outside this chapter.

busy-message †

service nagle

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

service nagle
no service nagle

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

When using a standard TCP implementation to send keystrokes between machines, TCP tends to send one packet for each keystroke typed. On larger networks, many small packets use up bandwidth and contribute to congestion.

John Nagle's algorithm (RFC 896) helps alleviate the small-packet problem in TCP. In general, it works this way: The first character typed after connection establishment is sent in a single packet, but TCP holds any additional characters typed until the receiver acknowledges the previous packet. Then the second, larger packet is sent, and additional typed characters are saved until the acknowledgment comes back. The effect is to accumulate characters into larger chunks, and pace them out to the network at a rate matching the round-trip time of the given connection. This method is usually a good for all TCP-based traffic. However, do not use the **service nagle** command if you have XRemote users on X Window sessions.

Example

The following example enables the Nagle algorithm on the router:

```
service nagle
```

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.

service password-encryption
no service password-encryption

Syntax Description

This command has no arguments or keywords.

Default

No encryption

Command Mode

Global configuration

Usage Guidelines

The actual encryption process occurs when the current configuration is written or when a password is configured. Password encryption can be applied to both the privileged command password and to console and virtual terminal line access passwords.

When password encryption is enabled, the encrypted form of the passwords is displayed when a **show startup-config** command is entered.

Note It is not possible to recover a lost encrypted password.

Example

The following example causes password encryption to take place:

```
service password-encryption
```

service tcp-keepalives

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.

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

Syntax Description

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

Default

Disabled

Command Mode

Global configuration

Example

The following example generates keepalives on incoming TCP connections:

```
service tcp-keepalives in
```

service tcp-small-servers

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

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

Syntax Description

This command has no arguments or keywords.

Default

Enabled

Command Mode

Global configuration

Usage Guidelines

By default, the TCP servers for Echo, Discard, Chargen, and Daytime services are enabled.

When you disable the minor TCP/IP servers, access to the Echo, Discard, Chargen, and Daytime ports cause the Cisco IOS software to send a TCP RESET packet to the sender and discard the original incoming packet.

Note Unlike defaults for other commands, this command will display when you perform **show running config** to display current settings whether or not you have changed the default using the **no service tcp-small-servers** command.

Example

The following example enables minor TCP/IP services available from the network:

```
service tcp-small-servers
```

service telnet-zero-idle

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

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

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

Normally, data sent to noncurrent Telnet connections is accepted and discarded. When **service telnet-zero-idle** is enabled, if a session is suspended (that is, some other connection is made active or the EXEC is sitting in command mode), the TCP window is set to zero. This action prevents the remote host from sending any more data until the connection is resumed. Use this command when it is important that all messages sent by the host be seen by the users and the users are likely to use multiple sessions.

Do not use this command if your host will eventually time out and log out a TCP user whose window is zero.

Example

The following example sets the TCP window to zero when the Telnet connection is idle:

```
service telnet-zero-idle
```

Related Command

resume

service timestamps

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

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

Syntax Description

type	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 in the date and timestamp.
localtime	(Optional) Timestamp relative to the local time zone.
show-timezone	(Optional) Include the time zone name in the timestamp.

Default

No timestamping.

If **service timestamps** is specified with no arguments or keywords, default is **service timestamps debug uptime**.

The default for **service timestamps** *type* **datetime** is to format the time in UTC, with no milliseconds and no time zone name.

The command **no service timestamps** by itself disables timestamps for both debug and log messages.

Command Mode

Global configuration

Usage Guidelines

Timestamps can be added to either debugging or logging messages independently. The **uptime** form of the command adds timestamps in the format HHHH:MM:SS, indicating the time since the system was rebooted. The **datetime** form of the command adds timestamps in the format MMM DD HH:MM:SS, indicating the date and time according to the system clock. If the system clock has not been set, the date and time are preceded by an asterisk (*) to indicate that the date and time are probably not correct.

Examples

The following example enables timestamps on debugging messages, showing the time since reboot:

```
service timestamps debug uptime
```

The following example enables timestamps on logging messages, showing the current time and date relative to the local time zone, with the time zone name included:

```
service timestamps log datetime localtime show-timezone
```

Related Commands

clock set
debug (Refer to the *Debug Command Reference* publication.)
ntp

service udp-small-servers

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

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

Syntax Description

This command has no arguments or keywords.

Default

Enabled

Command Mode

Global configuration

Usage Guidelines

By default the UPD servers for Echo, Discard, and Chargen services are enabled.

When you disable the servers, access to Echo, Discard, and Chargen ports causes the Cisco IOS software to send an “ICMP port unreachable” message to the sender and discard the original incoming packet.

Note Unlike defaults for other commands, this command will display when you perform **show running config** to display current settings, whether or not you have changed the default using the **no service udp-small-servers** command.

Example

The following example disables minor UDP services on the router:

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

show aliases

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

show aliases [*mode*]

Syntax Description

mode	(Optional) Command mode. See Table 5-7 in the description of the **alias** command for acceptable options for the *mode* argument.

Command Mode

EXEC

Usage Guidelines

All of the modes listed in Table 5-7 have their own prompts, except for the null interface mode. For example, the prompt for interface configuration mode is *Router(config-if)*.

Sample Display

The following is sample output from the **show aliases exec** commands. The aliases configured for commands in EXEC mode are displayed.

```
Router# show aliases exec

Exec mode aliases:
  h                    help
  lo                   logout
  p                    ping
  r                    resume
  s                    show
  w                    where
```

Related Command

alias

show buffers

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

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

Syntax Description

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.

Command Mode

EXEC

Sample Displays

The following is sample output from the **show buffers** command with no arguments, showing all buffer pool information:

```
Router#show buffers
Buffer elements:
     398 in free list (500 max allowed)
     1266 hits, 0 misses, 0 created

Public buffer pools:
Small buffers, 104 bytes (total 50, permanent 50):
     50 in free list (20 min, 150 max allowed)
     551 hits, 0 misses, 0 trims, 0 created
Middle buffers, 600 bytes (total 25, permanent 25):
     25 in free list (10 min, 150 max allowed)
     39 hits, 0 misses, 0 trims, 0 created
Big buffers, 1524 bytes (total 50, permanent 50):
     49 in free list (5 min, 150 max allowed)
     27 hits, 0 misses, 0 trims, 0 created
VeryBig buffers, 4520 bytes (total 10, permanent 10):
     10 in free list (0 min, 100 max allowed)
     0 hits, 0 misses, 0 trims, 0 created
Large buffers, 5024 bytes (total 0, permanent 0):
     0 in free list (0 min, 10 max allowed)
     0 hits, 0 misses, 0 trims, 0 created
Huge buffers, 18024 bytes (total 0, permanent 0):
     0 in free list (0 min, 4 max allowed)
     0 hits, 0 misses, 0 trims, 0 created

Interface buffer pools:
Ethernet0 buffers, 1524 bytes (total 64, permanent 64):
     16 in free list (0 min, 64 max allowed)
     48 hits, 0 fallbacks
     16 max cache size, 16 in cache
Ethernet1 buffers, 1524 bytes (total 64, permanent 64):
     16 in free list (0 min, 64 max allowed)
```

```
     48 hits, 0 fallbacks
     16 max cache size, 16 in cache
Serial0 buffers, 1524 bytes (total 64, permanent 64):
     16 in free list (0 min, 64 max allowed)
     48 hits, 0 fallbacks
     16 max cache size, 16 in cache
Serial1 buffers, 1524 bytes (total 64, permanent 64):
     16 in free list (0 min, 64 max allowed)
     48 hits, 0 fallbacks
     16 max cache size, 16 in cache
TokenRing0 buffers, 4516 bytes (total 48, permanent 48):
     0 in free list (0 min, 48 max allowed)
     48 hits, 0 fallbacks
     16 max cache size, 16 in cache
TokenRing1 buffers, 4516 bytes (total 32, permanent 32):
     32 in free list (0 min, 48 max allowed)
     16 hits, 0 fallbacks

0 failures (0 no memory)
```

Table 5-19 describes significant fields shown in the display.

Table 5-19 Show Buffers Field Descriptions

Field	Description
Buffer elements	Buffer elements are small structures used as placeholders for buffers in internal operating system queues. Buffer elements are used when a buffer may need to be on more than one queue.
Free list	Total number of the currently unallocated buffer elements.
Max allowed	Maximum number of buffers that are available for allocation.
Hits	Count of successful attempts to allocate a buffer when needed.
Misses	Count of buffer allocation attempts that resulted in growing the buffer pool to allocate a buffer.
Created	Count of new buffers created to satisfy buffer allocation attempts when the available buffers in the pool have already been allocated.
Public buffer pools	
Small buffers	Buffers that are 104 bytes long.
Middle buffers	Buffers that are 600 bytes long.
Big buffers	Buffers that are 1524 bytes long.
VeryBig buffers	Buffers that are 4520 bytes long.
Large buffers	Buffers that are 5024 bytes long.
Huge buffers	Buffers that are 18024 bytes long.
Total	Total number of this type of buffer.
Permanent	Number of these buffers that are permanent.
Free list	Number of available or unallocated buffers in that pool.
Min	Minimum number of free or unallocated buffers in the buffer pool
Max allowed	Maximum number of free or unallocated buffers in the buffer pool
Hits	Count of successful attempts to allocate a buffer when needed.
Misses	Count of buffer allocation attempts that resulted in growing the buffer pool in order to allocate a buffer.

Field	Description
Trims	Count of buffers released to the system because they were not being used. This field is displayed only for dynamic buffer pools, not interface buffer pools, which are static.
Created	Count of new buffers created in response to misses. This field is displayed only for dynamic buffer pools, not interface buffer pools, which are static.
Interface buffer pools	
Total	Total number of this type of buffer.
Permanent	Number of these buffers that are permanent.
Free list	Number of available or unallocated buffers in that pool.
Min	Minimum number of free or unallocated buffers in the buffer pool.
Max allowed	Maximum number of free or unallocated buffers in the buffer pool.
Hits	Count of successful attempts to allocate a buffer when needed.
Fall backs	Count of buffer allocation attempts that resulted in falling back to the public buffer pool that is the smallest pool at least as big as the interface buffer pool.
Max Cache Size	Maximum number of buffers from that interface's pool that can be in that interface buffer pool's cache. Each interface buffer pool has its own cache. These are not additional to the permanent buffers; they come from the interface's buffer pools. Some interfaces place all of their buffers from the interface pool into the cache. In this case, it is normal for the *free list* to display 0.
Failures	Total number of allocation requests that have failed because no buffer was available for allocation; the datagram was lost. Such failures normally occur at interrupt level.
(no memory)	Number of failures that occurred because no memory was available to create a new buffer.

The following is sample output from the **show buffers** command with an interface *type* and *number* :

```
Router#show buffers Ethernet 0
Ethernet0 buffers, 1524 bytes (total 64, permanent 64):
     16 in free list (0 min, 64 max allowed)
     48 hits, 0 fallbacks
     16 max cache size, 16 in cache
```

The following is sample output from the **show buffers** command when **alloc** is specified:

```
Router#show buffers alloc
Buffer elements:
     398 in free list (500 max allowed)
     1266 hits, 0 misses, 0 created

Public buffer pools:
Small buffers, 104 bytes (total 50, permanent 50):
     50 in free list (20 min, 150 max allowed)
     551 hits, 0 misses, 0 trims, 0 created
Middle buffers, 600 bytes (total 25, permanent 25):
     25 in free list (10 min, 150 max allowed)
     39 hits, 0 misses, 0 trims, 0 created
Big buffers, 1524 bytes (total 50, permanent 50):
     49 in free list (5 min, 150 max allowed)
     27 hits, 0 misses, 0 trims, 0 created
VeryBig buffers, 4520 bytes (total 10, permanent 10):
     10 in free list (0 min, 100 max allowed)
     0 hits, 0 misses, 0 trims, 0 created
```

```
Large buffers, 5024 bytes (total 0, permanent 0):
     0 in free list (0 min, 10 max allowed)
     0 hits, 0 misses, 0 trims, 0 created
Huge buffers, 18024 bytes (total 0, permanent 0):
     0 in free list (0 min, 4 max allowed)
     0 hits, 0 misses, 0 trims, 0 created

Interface buffer pools:
Ethernet0 buffers, 1524 bytes (total 64, permanent 64):
     16 in free list (0 min, 64 max allowed)
     48 hits, 0 fallbacks
     16 max cache size, 16 in cache
Ethernet1 buffers, 1524 bytes (total 64, permanent 64):
     16 in free list (0 min, 64 max allowed)
     48 hits, 0 fallbacks
     16 max cache size, 16 in cache
Serial0 buffers, 1524 bytes (total 64, permanent 64):
     16 in free list (0 min, 64 max allowed)
     48 hits, 0 fallbacks
     16 max cache size, 16 in cache
Serial1 buffers, 1524 bytes (total 64, permanent 64):
     16 in free list (0 min, 64 max allowed)
     48 hits, 0 fallbacks
     16 max cache size, 16 in cache
TokenRing0 buffers, 4516 bytes (total 48, permanent 48):
     0 in free list (0 min, 48 max allowed)
     48 hits, 0 fallbacks
     16 max cache size, 16 in cache
TokenRing1 buffers, 4516 bytes (total 32, permanent 32):
     32 in free list (0 min, 48 max allowed)
     16 hits, 0 fallbacks

0 failures (0 no memory)

Address  PakAddr  Data     Off Data  Pool  Ref Link Enc     Flags Output  Input
                  Area     set Size        Cnt Type Type    (Hex) Idb     Idb
-------------------------------------------------------------------------------
604B37A0 604B37C0 40004A38  62    60 Big     1   65    3        0 Et0
604C6DA0 604C6DC0 40007038  84     0 Ether   1    0    0        0
604C6F60 604C6F80 400076E4  84     0 Ether   1    0    0        0
604C7120 604C7140 40007D90  84     0 Ether   1    0    0        0
604C72E0 604C7300 4000843C  84     0 Ether   1    0    0        0
604C74A0 604C74C0 40008AE8  84     0 Ether   1    0    0        0
604C7660 604C7680 40009194  84     0 Ether   1    0    0        0
604C7820 604C7840 40009840  84     0 Ether   1    0    0        0
.
.
.
```

show calendar

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

show calendar

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

You can compare the time and date shown with this command with the time and date listed via the **show clock** command to verify that the calendar and system clock are in sync with each other. The time displayed is relative to the configured time zone.

Sample Display

In the following sample display, the hardware calendar indicates the timestamp of 12:13:44 p.m. on Friday, January 1, 1993:

```
Router# show calendar

12:13:44 PST Fri Jan 1 1993
```

Related Command

show clock

show cdp

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

show cdp

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC

Sample Display

The following is sample output from the **show cdp** command. Global CDP timer and hold-time parameters are set to the defaults of 60 and 180 seconds, respectively.

```
Router# show cdp

Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
```

Related Commands

cdp holdtime
cdp timer
show cdp entry
show cdp neighbors

show cdp entry

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

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

Syntax Description

*****	Shows all of the CDP neighbors.
entry-name	Name of neighbor about which you want information. You can enter an aserisk (*) at the end of an *entry-name*, such as `show cdp entry dev*`, which would show information about the neighbor, device.cisco.com.
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.

Command Mode

Privileged EXEC

Sample Displays

The following is sample output from the **show cdp** entry command with no limits. Information about the neighbor *device.cisco.com* is displayed, including device ID, address and protocol, platform, interface, hold time, and version.

```
Router# show cdp entry device.cisco.com

Device ID: device.cisco.com
Entry address(es):
  IP address: 198.92.68.18
  CLNS address: 490001.1111.1111.1111.00
  DECnet address: 10.1
Platform: AGS,  Capabilities: Router Trans-Bridge
Interface: Ethernet0,  Port ID (outgoing port): Ethernet0
Holdtime : 155 sec

Version :
GS Software (GS3), Experimental Version 10.2(10302) [asmith 161]
Copyright (c) 1986-1994 by cisco Systems, Inc.
Compiled Mon 07-Nov-94 14:34
```

The following is sample output from the **show cdp entry privilege** command. Only information about the protocols enabled on *neon-cisco.com* is displayed.

```
Router# show cdp entry device.cisco.com protocol

Protocol information for device.cisco.com :
  IP address: 198.92.68.18
  CLNS address: 490001.1111.1111.1111.00
  DECnet address: 10.1
```

The following is sample output from the **show cdp entry version** command. Only information about the version of software running on *device.cisco.com* is displayed.

```
Router# show cdp entry device.cisco.com version

Version information for device.cisco.com :
  GS Software (GS3), Experimental Version 10.2(10302) [asmith 161]
Copyright (c) 1986-1994 by cisco Systems, Inc.
Compiled Mon 07-Nov-94 14:34
```

Related Command

show cdp neighbors

show cdp interface

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

show cdp interface [*type number*]

Syntax Description

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

Command Mode

Privileged EXEC

Sample Displays

The following sample output form the **show cdp interface** command. Status information and information about CDP timer and hold time settings is displayed for all interfaces on which CDP is enabled.

```
Router# show cdp interface

Serial0 is up, line protocol is up, encapsulation is SMDS
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Ethernet0 is up, line protocol is up, encapsulation is ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

The following is sample output from the **show cdp interface** command with an interface specified. Status information and information about CDP timer and holdtime settings is displayed for Ethernet interface 0 only.

```
Router# show cdp interface ethernet 0

Ethernet0 is up, line protocol is up, encapsulation is ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

show cdp neighbors

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

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

Syntax Description

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.

Command Mode

Privileged EXEC

Sample Displays

The following is sample output from the **show cdp neighbors** command. Device ID, interface type and number, holdtime settings, capabilities, platform, and port ID information about the router's neighbors is displayed.

```
Router# show cdp neighbors

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

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
device.cisco.com      Eth 0          151         R T        AGS       Eth 0
device.cisco.com      Ser 0          165         R T        AGS       Ser 3
```

The following is sample output from the **show cdp neighbors detail** command. Additional detail is shown about the router's neighbors, including network address, enabled protocols, and software version:

```
Router# show cdp neighbors detail

Device ID: device.cisco.com
Entry address(es):
  IP address: 198.92.68.18
  CLNS address: 490001.1111.1111.1111.00
  DECnet address: 10.1
Platform: AGS,  Capabilities: Router Trans-Bridge
Interface: Ethernet0,  Port ID (outgoing port): Ethernet0
Holdtime : 143 sec

Version :
GS Software (GS3), Experimental Version 10.2(10302) [asmith 161]
Copyright (c) 1986-1994 by cisco Systems, Inc.
Compiled Mon 07-Nov-94 14:34
```

Related Command

show cdp entry

show cdp traffic

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

show cdp traffic

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC

Sample Display

The following is sample output from the **show cdp traffic** command.

```
Router# show cdp traffic

CDP counters :
        Packets output: 94, Input: 75
        Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
        No memory: 0, Invalid packet: 0, Fragmented: 0
```

In this example, traffic information is displayed including the numbers of packets sent, the number of packets received, header syntax, checksum errors, failed encapsulations, memory problems, and invalid and fragmented packets is displayed. Header syntax indicates the number of packets CDP receives with that have an invalid header format.

show clock

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

show clock [**detail**]

Syntax Description

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

Command Mode

EXEC

Usage Guidelines

The system clock keeps an "authoritative" flag that indicates whether or not the time is authoritative (believed to be accurate). If system clock has been set by a timing source (Cisco 7000 calendar, NTP, VINES, and so forth), the flag is set. If the time is not authoritative, it will be used only for display purposes. Until the clock is authoritative and the "authoritative" flag is set, the flag prevents the router from causing peers to synchronize to itself when the router time is invalid.

The symbol that precedes the **show clock** display indicates the following:

An asterisk (`*`) indicates not authoritative

A blank space indicates authoritative

A period (.) indicates authoritative, but NTP is not synchronized.

Sample Display

The following sample output shows that the current clock is authoritative and that the time source is NTP:

```
Router# show clock detail
15:29:03.158 PST Mon Mar 1 1993
Time source is NTP
Router#
```

Related Commands

clock set
show calendar

show context

Use the **show context** EXEC command to display information stored in NVRAM when the router crashes. This command only works on the Cisco 7000 series, Cisco 7200 series, and Cisco 7500 series platforms.

show context

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

The display from the **show context** command includes the following information:

- Reason for the system reboot
- Stack trace
- Software version
- The signal number, code, and router uptime information
- All the register contents at the time of the crash

This information is of use only to your technical support representative in analyzing crashes in the field. It is included here in case you need to read the displayed statistics to an engineer over the phone.

Sample Display

The following is sample output from the **show context** command following a system failure:

```
Router> show context

System was restarted by error - a Software forced crash, PC 0x60189354
GS Software (RSP-PV-M), Experimental Version 11.1(2033) [ganesh 111]
Compiled Mon 31-Mar-97 13:21 by ganesh
Image text-base: 0x60010900, data-base: 0x6073E000
Stack trace from system failure:
FP: 0x60AEA798, RA: 0x60189354
FP: 0x60AEA798, RA: 0x601853CC
FP: 0x60AEA7C0, RA: 0x6015E98C
FP: 0x60AEA7F8, RA: 0x6011AB3C
FP: 0x60AEA828, RA: 0x601706CC
FP: 0x60AEA878, RA: 0x60116340
FP: 0x60AEA890, RA: 0x6011632C
Fault History Buffer:
GS Software (RSP-PV-M), Experimental Version 11.1(2033) [ganesh 111]
Compiled Mon 31-Mar-97 13:21 by ganesh
Signal = 23, Code = 0x24, Uptime 00:04:19
$0 : 00000000, AT : 60930120, v0 : 00000032, v1 : 00000120
a0 : 60170110, a1 : 6097F22C, a2 : 00000000, a3 : 00000000
t0 : 60AE02A0, t1 : 8000FD80, t2 : 34008F00, t3 : FFFF00FF
t4 : 00000083, t5 : 3E840024, t6 : 00000000, t7 : 11010132
s0 : 00000006, s1 : 607A25F8, s2 : 00000001, s3 : 00000000
```

```
s4 : 00000000, s5 : 00000000, s6 : 00000000, s7 : 6097F755
t8 : 600FABBC, t9 : 00000000, k0 : 30408401, k1 : 30410000
gp : 608B9860, sp : 60AEA798, s8 : 00000000, ra : 601853CC
EPC : 60189354, SREG : 3400EF03, Cause : 00000024
```

Related Commands

show processes
show stacks

show environment

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

show environment

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

Once a minute a routine is run that gets environmental measurements from the CSC-ENVM card and stores the **show environment** output into a buffer. This buffer is displayed on the console when **show environment** is invoked.

If a measurement exceeds desired margins, but has not exceeded fatal margins, a warning message is printed to the system console. The system software queries the CSC-ENVM card for measurements once a minute, but warnings for a given testpoint are printed at most once every four hours. If a measurement is out of line within a four-hour period, an automatic warning message appears on the console. As noted, you can query the CSC-ENVM using the **show environment** command at any time to determine whether a measurement is at the warning tolerance.

Sample Displays

The following is sample output from the **show environment** command on the AGS+:

```
Router# show environment

Environmental controller firmware version 2.0
   Serial number is 00220846, calibrated on 2-14-92, by technician rma
   Internal temperature measured 34.3(C), shuts down at 43.0(C)
   Air flow appears good.
   +5 volt line measured at 5.061(V)
   +12 volt line measured at 12.120(V)
   -12 volt line measured at -11.936(V)
   -5 volt line measured at -4.986(V)
```

Table 5-20 describes significant fields shown in the display.

Table 5-20 Show Environment Field Descriptions for AGS+

Field	Description
Serial number is 00220846	Serial number of router.
calibrated on 2-14-92	Date on which these measurements were taken.
by technician rma	ID (initials in this case) of the technician taking the measurement.
Internal temperature measured 34.3 (C)	Internal temperature of the router (in celsius).

Field	Description
shuts down at 43.0(C)	Temperature (in celsius) at which the router is administratively shut down to prevent internal damage.
Air flow appears good.	Air flow is adequate for proper router operation.
+5 volt line at 5.061(V)	Voltage measurement of the +5 volt line.
+12 volt line measured at 12.120(V)	Voltage measurement of the +12 volt line.
–12 volt line measured at –11.936(V)	Voltage measurement of the –12 volt line.
–5 volt line measured at –4.986(V)	Voltage measurement of the –5 volt line.

The following is an example of a message that displays on the system console when a measurement has exceeded an acceptable margin:

```
Router#
ENVIRONMENTAL WARNING: Air flow appears marginal.
```

The following is an example of a message that displays on the system console when a measurement has exceeded an acceptable margin. In this example, the internal temperature reading is given:

```
Router#
ENVIRONMENTAL WARNING: Internal temperature measured 41.3(C)
```

The following is an example of a message that displays on the system console when a voltage measurement has exceeded an acceptable margin:

```
Router#
ENVIRONMENTAL WARNING:  +5 volt testpoint measured 5.310(V)
```

If the CSC-ENVM card on the AGS+ chassis detects that any of its voltage or temperature testpoints has exceeded maximum margins, it does the following in this order:

1. Saves the last measured values from each of the six testpoints to internal nonvolatile memory.
2. Interrupts the system software and causes a shutdown message to be printed on the system console.
3. Shuts off the power supply after a few milliseconds of delay.

The following is the message the system displays if voltage or temperature exceed maximum margins:

```
Router#
SHUTDOWN: air flow problem
```

For environmental specifications, refer to the *Hardware Installation and Maintenance* publication for your individual chassis.

The following example shows the typical **show environment** display on the Cisco 7000 when there are no warning conditions in the system. The date and time of the query are displayed, along with the data refresh information and a message indicating that there are no warning conditions.

```
Router> show environment
Environmental Statistics
  Environmental status as of 13:17:39 UTC Thu Oct 22 1992
  Data is 7 second(s) old, refresh in 53 second(s)

  All Environmental Measurements are within specifications
```

Table 5-21 describes the **show environment** display fields on the Cisco 7000.

Table 5-21 Show Environment Field Descriptions for Cisco 7000

Field	Description
Environmental status as of...	Current date and time.
Data age and refresh	Environmental measurements are output into a buffer every 60 seconds, unless other higher-priority processes are running.
WARNING	If environmental measurements are not within specification, warning messages are displayed.

show environment all

Use the **show environment all** EXEC command to display temperature and voltage information on the Cisco 7000 series and Cisco 7500 series console.

show environment all

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Displays

The following is sample output from the **show environment all** command on the Cisco 7000 when there are no warning conditions in the system:

```
7000> show environment all

Environmental Statistics
  Environmental status as of 13:17:39 UTC Thu Oct 22 1992
  Data is 11 second(s) old, refresh in 49 second(s)

  All Environmental Measurements are within specifications

  Lower Power Supply: 700W, ON     Upper Power Supply: Not Installed

  No Intermittent Powerfails

  +12 volt measured at  12.05(V)
   +5 volt measured at   4.92(V)
  -12 volt measured at -12.00(V)
  +24 volt measured at  23.80(V)

Airflow temperature measured at 30(C)
Inlet temperature measured at 25(C)
```

In the following example, there have been two intermittent power failures since the router was turned on, and the lower power supply is not functioning. The last intermittent power failure occurred on Sunday, October 25, 1992, at 11:07 p.m.

```
7000# show environment all

Environmental Statistics
  Environmental status as of 23:19:47 UTC Sun Oct 25 1992
  Data is 6 second(s) old, refresh in 54 second(s)

  WARNING: Lower Power Supply is NON-OPERATIONAL

  Lower Power Supply:700W, OFF     Upper Power Supply: 700W, ON

  Intermittent Powerfail(s): 2     Last on 23:07:05 UTC Sun Oct 25 1992

  +12 volts measured at  12.05(V)
   +5 volts measured at   4.96(V)
  -12 volts measured at -12.05(V)
  +24 volts measured at  23.80(V)
```

```
Airflow temperature measured at 38(C)
Inlet temperature measured at 25(C)
```

Table 5-22 describes the **show environment all** display fields.

Table 5-22 Show Environment All Field Descriptions for the Cisco 7000

Field	Description
Environmental status as of...	Date and time of last query.
Data age and refresh	Environmental measurements are output into a buffer every 60 seconds, unless other higher-priority processes are running.
WARNING	If environmental measurements are not within specification, warning messages are displayed.
`Lower Power Supply`	Type of power supply installed and its status (on or off).
`Upper Power Supply`	Type of power supply installed and its status (on or off).
`Intermittent Powerfails`	Number of power hits (not resulting in shutdown) since system was last booted.
`Voltage Specifications`	System voltage measurements.
`Airflow and Inlet temperature`	Temperature of air coming in and going out.

The following example shows typical output of the **show environment all** command on the Cisco 7010. The output shows the status of the single 600W power supply. The following example from a Cisco 7010 shows that a single 600W power supply is installed:

```
7010# show environment all

Environmental Statistics
  Environmental status as of Fri 11-5-1993 19:10:41
  Data is 31 second(s) old, refresh in 29 second(s)

 All Environmental Measurements are within specifications

  Power Supply: 600W AC

  No Intermittent Powerfails

  +12 volts measured at  12.00(V)
   +5 volts measured at   5.02(V)
  -12 volts measured at -12.05(V)
  +24 volts measured at  23.70(V)

  Airflow temperature measured at 35(C)
  Inlet   temperature measured at 26(C)
```

Table 5-23 describes the fields shown in the display.

Table 5-23 Show Environment Field Descriptions for the Cisco 7010

Field	Description
Environmental status as of...	Current date and time.

Field	Description
Data age and refresh	Environmental measurements are output into a buffer every 60 seconds, unless other higher-priority processes are running.
All Environmental Measurements are within specifications	All environment measurements are within specification. If they are not, warning messages are displayed.
Power Supply:	Type of power supply.
No Intermittent Powerfails	Indicates whether intermittent power failures are occurring.
+12 volts measured at 12.00(V)	Voltage measurement of the +12 volt line.
+5 volts measured at 5.02(V)	Voltage measurement of the +5 volt line.
–12 volts measured at –12.05(V)	Voltage measurement of the –12 volt line.
+24 volts measured at 23.70(V)	Voltage measurement of the +24 volt line.

The following is sample output from the **show environment all** command on the Cisco 7500 series router:

```
7500#show environment all

Arbiter type 1, backplane type 7513 (id 2)
Power supply #1 is 1200W AC (id 1), power supply #2 is removed (id 7)
Active fault conditions: none
Fan transfer point: 100%
Active trip points: Restart_Inhibit
15 of 15 soft shutdowns remaining before hard shutdown

                      1
              0123456789012
Dbus slots:   X     XX    X

card        inlet      hotpoint      exhaust
RSP(6)     35C/95F     47C/116F      40C/104F
RSP(7)     35C/95F     43C/109F      39C/102F

Shutdown temperature source is 'hotpoint' on RSP(6), requested RSP(6)

+12V measured at 12.31
+5V measured at 5.21
-12V measured at -12.07
+24V measured at 22.08
+2.5 reference is 2.49

PS1 +5V Current      measured at 59.61 A (capacity 200 A)
PS1 +12V Current     measured at 5.08 A (capacity 35 A)
PS1 -12V Current     measured at 0.42 A (capacity 3 A)
PS1 output is 378 W
```

Table 5-24 describes the fields shown in the display.

Table 5-24 Show Environment All Field Descriptions for the Cisco 7500

Field	Description
Arbiter type 1	Numbers indicating the arbiter type and backplane type.
Power supply	Number and type of power supply installed in the chassis.

Field	Description
Active fault conditions:	If any fault conditions exist (such as power supply failure, fan failure, and temperature too high), they are listed here.
Fan transfer point:	Software controlled fan speed. If the router is operating below its automatic restart temperature, the transfer point is reduced by 10 percent of the full range each minute. If the router is at or above its automatic restart temperature, the transfer point is increased in the same way.
Active trip points:	Temperature sensor is compared against the values displayed at the bottom of the **show environment table** command output.
15 of 15 soft shutdowns remaining	When the temperature increases above the "board shutdown" level, a soft shutdown occurs (that is, the cards are shut down, and the power supplies, fans, and CI continue to operate). When the system cools to the restart level, the system restarts. The system counts the number of times this occurs and keeps the up/down cycle from continuing forever. When the counter reaches zero, the system performs a hard shutdown, which requires a power cycle to recover. The soft shutdown counter is reset to its maximum value after the system has been up for 6 hours.
Dbus slots:	Indicates which chassis slots are occupied.
card, inlet, hotpoint, exhaust	Temperature measurements at the inlet, hotpoint, and exhaust areas of the card. The (6) and (7) indicate the slot numbers. Dual-RSP chassis can show two RSPs.
Shutdown temperature source	Indicates which of the three temperature sources is selected for comparison against the "shutdown" levels listed with the **show environment table** command.
Voltages (+12V, +5V, -12V, +24V, +2.5)	Voltages measured on the backplane.
Power supply current (PS1)	Current measured on the power supply.

show environment last

If a shutdown occurs due to detection of fatal environmental margins, the AGS+, Cisco 7000 series, or Cisco 7000 series router 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 last

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Displays

The following is sample output from the **show environment last** command on the AGS+:

```
Router# show environment last

Environmental controller firmware version 2.0
   Serial number is 3232, calibrated on 2-14-92, by technician rma
   Internal temperature measured 24.1(C), shuts down at 43.0(C)
   Air flow appears good.
   +5 volt line measured at 4.988(V)
   +12 volt line measured at 12.044(V)
   -12 volt line measured at -11.787(V)
   -5 volt line measured at -4.939(V)

LAST Environmental Shutdown Measurements:
   Internal temperature was 24.0(C)
   Air flow sensor was good
   +5 volt line was 4.990(V)
   +12 volt line was 9.900(V)*
   -12 volt line was -11.719(V)
   -5 volt line was -4.926(V)
```

As the display shows, the first block of data is equivalent to **show environment**, in that it displays the current measurements. The second block shows all the testpoint values at the time of the LAST environmental shutdown. An asterisk suffixes the testpoint that caused the failure. In this example, the +12 volt testpoint dropped to 9.900(V) to cause the shutdown.

The following example is for the Cisco 7000. The router retrieves the environmental statistics at the time of the last shutdown. In this example, the last shutdown was Tuesday, May 19, 1992 at 12:40p.m., so the environmental statistics at that time are displayed.

```
Router# show environment last

Environmental Statistics
  Environmental status as of 14:47:00 UTC Thu May 21 1992
  Data is 6 second(s) old, refresh in 54 second(s)

  WARNING: Upper Power Supply is NON-OPERATIONAL

LAST Environmental Statistics
  Environmental status as of 12:40:00 UTC Tues May 19 1992
```

```
Lower Power Supply: 700W, ON     Upper Power Supply: 700W, OFF

No Intermittent Powerfails

+12 volts measured at  12.05(V)
 +5 volts measured at   4.98(V)
-12 volts measured at -12.00(V)
+24 volts measured at  23.80(V)

Airflow temperature measured at 30(C)
Inlet   temperature measured at 23(C)
```

Table 5-25 describes the **show environment last** display fields.

Table 5-25 Show Environment Last Field Descriptions for the Cisco 7000

Field	Description
Environmental status as of...	Current date and time.
Data age and refresh	Environmental measurements are output into a buffer every 60 seconds, unless other higher-priority processes are running.
WARNING	If environmental measurements are not within specification, warning messages are displayed.
`LAST`	Displays test point values at time of the last environmental shutdown.
`Lower Power Supply/Upper Power Supply Power Supply:`	For the Cisco 7000, indicates the status of the two 700W power supplies. For the Cisco 7010, indicates the status of the single 600W power supply.

The following example is for the Cisco 7500 series router. This example shows the measurements immediately before the last shutdown.

```
7500#show environment last
 RSP(4) Inlet       previously measured at 37C/98F
 RSP(4) Hotpoint    previously measured at 46C/114F
 RSP(4) Exhaust     previously measured at 52C/125F
 +12 Voltage        previously measured at 12.26
 +5 Voltage         previously measured at 5.17
 -12 Voltage        previously measured at -12.03
 +24 Voltage        previously measured at 23.78
```

Table 5-26 describes the fields shown in the display

Table 5-26 Show Environment Last Field Descriptions for the Cisco 7500

Field	Description
RSP(4) Inlet, Hotpoint, Exhaust	Temperature measurements at the inlet, hotpoint, and exhaust areas of the card.
Voltages	Voltages measured on the backplane.

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 and Cisco 7500 series.

show environment table

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Display

The following sample output for the Cisco 7000 shows the current environmental status in tables that list voltage and temperature parameters. There are three warning messages; one each about the lower power supply, the airflow temperature, and the inlet temperature. In this example, voltage parameters are shown to be in the normal range, airflow temperature is at a critical level, and inlet temperature is at the warning level.

```
Router> show environment table
Environmental Statistics
  Environmental status as of Mon 11-2-1992 17:43:36
  Data is 52 second(s) old, refresh in 8 second(s)

  WARNING: Lower Power Supply is NON-OPERATIONAL
  WARNING: Airflow temperature has reached CRITICAL level at 73(C)
  WARNING: Inlet temperature has reached WARNING level at 41(C)

Voltage Parameters:

 SENSE        CRITICAL                NORMAL                CRITICAL
-------|--------------------|-----------------------|--------------------

+12(V)                    10.20      12.05(V)      13.80
 +5(V)                     4.74       4.98(V)       5.26
-12(V)                   -10.20     -12.05(V)     -13.80
+24(V)                    20.00      24.00(V)      28.00

Temperature Parameters:

 SENSE     WARNING      NORMAL      WARNING      CRITICAL      SHUTDOWN
-------|-------------|------------|-------------|--------------|--------------

Airflow            10           60           70    73(C)   88

Inlet              10           39    41(C)  46           64
```

Table 5-27 describes the **show environment table** display fields.

Table 5-27 Show Environment Table Field Descriptions for the Cisco 7000

Field	Description
SENSE (Voltage Parameters)	Voltage specification for DC line.

Field	Description
SENSE (Temperature Parameters)	Air being measured. Inlet measures the air coming in, and Airflow measures the temperature of the air inside the chassis.
NORMAL	All monitored conditions meet normal requirements.
WARNING	System is approaching an out-of-tolerance condition.
CRITICAL	Out-of-tolerance condition exists.
PROCESSOR SHUTDOWN	Processor has detected condition that could cause physical damage to the system.

The following example is for the Cisco 7500 series router. This information lists the temperature and voltage thresholds for each sensor. These thresholds indicate when error messages occur. There are two level of messages: warning and critical.

```
7500#show env table
Sample Point      LowCritical    LowWarning     HighWarning    HighCritical
RSP(4) Inlet                                    44C/111F       50C/122F
RSP(4) Hotpoint                                 54C/129F       60C/140F
RSP(4) Exhaust
+12 Voltage       10.90          11.61          12.82          13.38
+5 Voltage        4.61           4.94           5.46           5.70
-12 Voltage       -10.15         -10.76         -13.25         -13.86
+24 Voltage       20.38          21.51          26.42          27.65
2.5 Reference                    2.43           2.51
Shutdown boards at           70C/158F
Shutdown power supplies at   76C/168F
Restart after shutdown below 40C/104F
```

Table 5-28 describes the fields shown in the display.

Table 5-28 Show Environment Table Field Descriptions for the Cisco 7500

Field	Description
Sample Point	Area for which measurements are taken.
LowCritical	Level at which a critical message is issued for an out-of-tolerance voltage condition. The system continues to operate; however, the system is approaching shutdown.
LowWarning	Level at which a warning message is issued for an out-of-tolerance voltage condition. The system continues to operate, but operator action is recommended to bring the system back to a normal state.
HighWarning	Level at which a warning message is issued. The system continues to operate, but operator action is recommended to bring the system back to a normal state.
HighCritical	Level at which a critical message is issued. For the chassis, the router is shut down. For the power supply, the power supply is shut down.
Shutdown boards at	The card is shut down if the specified temperature is met.
Shutdown power supplies at	The system is shut down if the specified temperature is met.
Restart after shutdown	The system will restart when the specified temperature is met.

show logging

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

show logging

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.

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Display

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

```
Router# show logging

Syslog logging: enabled
     Console logging: disabled
     Monitor logging: level debugging, 266 messages logged.
     Trap logging: level informational, 266 messages logged.
     Logging to 131.108.2.238

SNMP logging: disabled, retransmission after 30 seconds
    0 messages logged
```

Table 5-29 describes significant fields shown in the display.

Table 5-29 Show Logging Field Descriptions

Field	Description
Syslog logging	When enabled, system logging messages are sent to a UNIX host that acts as a syslog server; that is, it captures and saves the messages.
Console logging	If enabled, states the level; otherwise, this field displays disabled.
Monitor logging	Minimum level of severity required for a log message to be sent to a monitor terminal (not the console).
Trap logging	Minimum level of severity required for a log message to be sent to a syslog server.
SNMP logging	Shows whether SNMP logging is enabled and the number of messages logged, and the retransmission interval.

show memory

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

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

Syntax Description

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.

summary (Optional) Displays a summary of memory usage including the size and number of blocks allocated for each address of the system call that allocated the block.

Command Mode

EXEC

Usage Guidelines

The **show memory** command displays information about memory available after the system image decompresses and loads.

Sample Displays

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

```
Router# show memory

              Head   Total(b)    Used(b)    Free(b)  Lowest(b) Largest(b)
Processor    B0EE38    5181896    2210036    2971860    2692456    2845368

          Processor memory
Address   Bytes Prev.    Next     Ref  PrevF   NextF   Alloc PC  What
B0EE38     1056 0        B0F280     1                  18F132    List Elements
B0F280     2656 B0EE38   B0FD08     1                  18F132    List Headers
B0FD08     2520 B0F280   B10708     1                  141384    TTY data
B10708     2000 B0FD08   B10F00     1                  14353C    TTY Input Buf
B10F00      512 B10708   B11128     1                  14356C    TTY Output Buf
B11128     2000 B10F00   B11920     1                  1A110E    Interrupt Stack
B11920       44 B11128   B11974     1                  970DE8    *Init*
B11974     1056 B11920   B11DBC     1                  18F132    messages
B11DBC       84 B11974   B11E38     1                  19ABCE    Watched Boolean
B11E38       84 B11DBC   B11EB4     1                  19ABCE    Watched Boolean
B11EB4       84 B11E38   B11F30     1                  19ABCE    Watched Boolean
B11F30       84 B11EB4   B11FAC     1                  19ABCE    Watched Boolean
Router#
```

The following is sample output from the **show memory free** command:

```
Router# show memory free
              Head   Total(b)    Used(b)    Free(b)  Lowest(b) Largest(b)
Processor    B0EE38    5181896    2210076    2971820    2692456    2845368
```

```
          Processor memory
Address  Bytes Prev.    Next     Ref  PrevF   NextF   Alloc PC  What
             24    Free list 1
CEB844       32 CEB7A4   CEB88C     0  0       0       96B894    SSE Manager
             52    Free list 2
             72    Free list 3
             76    Free list 4
             80    Free list 5
D35ED4       80 D35E30   D35F4C     0  0       D27AE8  96B894    SSE Manager
D27AE8       80 D27A48   D27B60     0  D35ED4  0       22585E    SSE Manager
             88    Free list 6
            100    Free list 7
D0A8F4      100 D0A8B0   D0A980     0  0       0       2258DA    SSE Manager
            104    Free list 8
B59EF0      108 B59E8C   B59F84     0  0       0       2258DA    (fragment)
```

The display of **show memory free** contains the same types of information as the **show memory** display, except that only free memory is displayed, and the information is displayed in order for each free list.

The first section of the display includes summary statistics about the activities of the system memory allocator. Table 5-30 describes significant fields shown in the first section of the display.

Table 5-30 Show Memory Field Descriptions—First Section

Field	Description
Head	Hexadecimal address of the head of the memory allocation chain.
Total (b)	Sum of used bytes plus free bytes.
Used (b)	Amount of memory in use.
Free (b)	Amount of memory not in use.
Lowest(b)	Smallest amount of free memory since last boot.
Largest (b)	Size of largest available free block.

The second section of the display is a block-by-block listing of memory use. Table 5-31 describes significant fields shown in the second section of the display.

Table 5-31 Characteristics of Each Block of Memory—Second Section

Field	Description
Address	Hexadecimal address of block.
Bytes	Size of block in bytes.
Prev.	Address of previous block (should match Address on previous line).
Next	Address of next block (should match address on next line).
Ref	Reference count for that memory block, indicating how many different processes are using that block of memory.
PrevF	Address of previous free block (if free).
NextF	Address of next free block (if free).
Alloc PC	Address of the system call that allocated the block.
What	Name of process that owns the block, or “(fragment)” if the block is a fragment, or “(coalesced)” if the block was coalesced from adjacent free blocks.

The **show memory io** command displays the free IO memory blocks. On the Cisco 4000, this command quickly shows how much unused IO memory is available.

The following is sample output from the **show memory io** command:

```
Router# show memory io

Address   Bytes Prev.   Next     Ref  PrevF   NextF   Alloc PC  What
6132DA0   59264 6132664 6141520  0    0      600DDEC  3FCF0     *Packet Buffer*
600DDEC     500 600DA4C 600DFE0  0   6132DA0 600FE68 0
600FE68     376 600FAC8 600FFE0  0   600DDEC 6011D54 0
6011D54     652 60119B4 6011FEO  0   600FE68 6013D54 0
614FCA0     832 614F564 614FFE0  0   601FD54 6177640 0
6177640 2657056 6172E90 0        0   614FCA0 0       0
Total: 2723244
```

The **show memory sram** command displays the free SRAM memory blocks. For the Cisco 4000, this command supports the high-speed static RAM memory pool to make it easier to debug or diagnose problems with allocation or freeing of such memory.

The following is sample output from the **show memory sram** command:

```
Router# show memory sram

Address   Bytes Prev.   Next     Ref  PrevF   NextF   Alloc PC  What
7AE0      38178 72F0    0        0    0       0       0
Total     38178
```

The **show memory** command on the Cisco 4000 includes information about SRAM memory and IO memory, and appears as follows:

```
Router# show memory

              Head   Total(b)    Used(b)    Free(b)  Lowest(b) Largest(b)
Processor    49C724   28719324    1510864   27208460   26511644   15513908
      I/O   6000000    4194304    1297088    2897216    2869248    2896812
     SRAM      1000      65536      63400       2136       2136       2136

Address   Bytes Prev.   Next     Ref  PrevF   NextF   Alloc PC  What
1000       2032 0       17F0       1                   3E73E     *Init*
17F0       2032 1000    1FE0       1                   3E73E     *Init*
1FE0        544 17F0    2200       1                   3276A     *Init*
2200         52 1FE0    2234       1                   31D68     *Init*
2234         52 2200    2268       1                   31DAA     *Init*
2268         52 2234    229C       1                   31DF2     *Init*
72F0       2032 6E5C    7AE0       1                   3E73E     Init
7AE0      38178 72F0    0          0    0      0       0
Router#
```

The **show memory summary** command displays a summary of all memory pools as well as memory usage per Alloc PC (address of the system call that allocated the block).

The following is a partial sample output from the **show memory summary** command. This command shows the size, blocks, and bytes allocated. Bytes equal the size multiplied by the blocks. For a description of the other fields, see Table 5-30 and Table 5-31.

```
router# show memory summary
              Head   Total(b)    Used(b)    Free(b)  Lowest(b) Largest(b)
Processor    B0EE38    5181896    2210216    2971680    2692456    2845368

          Processor memory
Alloc PC        Size     Blocks      Bytes    What
0x2AB2           192          1        192    IDB: Serial Info
```

```
0x70EC            92          2        184    Init
0xC916           128         50       6400    RIF Cache
0x76ADE         4500          1       4500    XDI data
0x76E84         4464          1       4464    XDI data
0x76EAC          692          1        692    XDI data
0x77764          408          1        408    Init
0x77776          116          1        116    Init
0x777A2          408          1        408    Init
0x777B2          116          1        116    Init
0xA4600           24          3         72    List
0xD9B5C           52          1         52    SSE Manager
.......................
0x0                0       3413    2072576    Pool Summary
0x0                0         28    2971680    Pool Summary (Free Blocks)
0x0               40       3441     137640    Pool Summary(All Block Headers)
0x0                0       3413    2072576    Memory Summary
0x0                0         28    2971680    Memory Summary (Free Blocks)
```

Related Command

show processes memory

show ntp associations

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

show ntp associations [**detail**]

Syntax Description

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

Command Mode

EXEC

Sample Displays

Detailed descriptions of the information displayed by this command can be found in the NTP specification (RFC 1305).

The following is sample output from the **show ntp associations** command:

```
Router# show ntp associations
     address         ref clock     st  when  poll reach  delay  offset    disp
 ~160.89.32.2      160.89.32.1       5    29  1024  377     4.2   -8.59     1.6
+~131.108.13.33    131.108.1.111     3    69   128  377     4.1    3.48     2.3
*~131.108.13.57    131.108.1.111     3    32   128  377     7.9   11.18     3.6
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
Router#
```

Table 5-32 describes significant fields shown in the display.

Table 5-32 Show NTP Associations Field Descriptions

Field	Description
address	Address of peer.
ref clock	Address of peer's reference clock.
st	Peer's stratum.
when	Time since last NTP packet received from peer.
poll	Polling interval (seconds).
reach	Peer reachability (bit string, in octal).
delay	Round-trip delay to peer (milliseconds).
offset	Relative time of peer’s clock to local clock (milliseconds).
disp	Dispersion
The first character of the line can be one or more of the following:	
*	Synchronized to this peer.
#	Almost synchronized to this peer.
+	Peer selected for possible synchronization.
-	Peer is a candidate for selection.
~	Peer is statically configured.

The following is sample output of the **show ntp associations detail** command:

```
Router# show ntp associations detail
160.89.32.2 configured, insane, invalid, stratum 5
ref ID 160.89.32.1, time AFE252C1.6DBDDFF2 (00:12:01.428 PDT Mon Jul 5 1993)
our mode active, peer mode active, our poll intvl 1024, peer poll intvl 64
root delay 137.77 msec, root disp 142.75, reach 376, sync dist 215.363
delay 4.23 msec, offset -8.587 msec, dispersion 1.62
precision 2**19, version 3
org time AFE252E2.3AC0E887 (00:12:34.229 PDT Mon Jul 5 1993)
rcv time AFE252E2.3D7E464D (00:12:34.240 PDT Mon Jul 5 1993)
xmt time AFE25301.6F83E753 (00:13:05.435 PDT Mon Jul 5 1993)
filtdelay =     4.23    4.14    2.41    5.95    2.37    2.33    4.26    4.33
filtoffset =   -8.59   -8.82   -9.91   -8.42  -10.51  -10.77  -10.13  -10.11
filterror =     0.50    1.48    2.46    3.43    4.41    5.39    6.36    7.34

131.108.13.33 configured, selected, sane, valid, stratum 3
ref ID 131.108.1.111, time AFE24F0E.14283000 (23:56:14.078 PDT Sun Jul 4 1993)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 83.72 msec, root disp 217.77, reach 377, sync dist 264.633
delay 4.07 msec, offset 3.483 msec, dispersion 2.33
precision 2**6, version 3
org time AFE252B9.713E9000 (00:11:53.442 PDT Mon Jul 5 1993)
rcv time AFE252B9.7124E14A (00:11:53.441 PDT Mon Jul 5 1993)
xmt time AFE252B9.6F625195 (00:11:53.435 PDT Mon Jul 5 1993)
filtdelay =     6.47    4.07    3.94    3.86    7.31    7.20    9.52    8.71
filtoffset =    3.63    3.48    3.06    2.82    4.51    4.57    4.28    4.59
filterror =     0.00    1.95    3.91    4.88    5.84    6.82    7.80    8.77

131.108.13.57 configured, our_master, sane, valid, stratum 3
ref ID 131.108.1.111, time AFE252DC.1F2B3000 (00:12:28.121 PDT Mon Jul 5 1993)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 125.50 msec, root disp 115.80, reach 377, sync dist 186.157
delay 7.86 msec, offset 11.176 msec, dispersion 3.62
precision 2**6, version 2
org time AFE252DE.77C29000 (00:12:30.467 PDT Mon Jul 5 1993)
rcv time AFE252DE.7B2AE40B (00:12:30.481 PDT Mon Jul 5 1993)
xmt time AFE252DE.6E6D12E4 (00:12:30.431 PDT Mon Jul 5 1993)
filtdelay =    49.21    7.86    8.18    8.80    4.30    4.24    7.58    6.42
filtoffset =   11.30   11.18   11.13   11.28    8.91    9.09    9.27    9.57
filterror =     0.00    1.95    3.91    4.88    5.78    6.76    7.74    8.71
```

Table 5-33 describes significant fields shown in the display.

Table 5-33 Show NTP Associations Detail Field Descriptions

Field	Descriptions
configured	Peer was statically configured.
dynamic	Peer was dynamically discovered.
our_master	Local machine is synchronized to this peer.
selected	Peer is selected for possible synchronization.
candidate	Peer is a candidate for selection.
sane	Peer passes basic sanity checks.
insane	Peer fails basic sanity checks.
valid	Peer time is believed to be valid.
invalid	Peer time is believed to be invalid.
leap_add	Peer is signaling that a leap second will be added.

Field	Descriptions
leap-sub	Peer is signaling that a leap second will be subtracted.
unsynced	Peer is not synchronized to any other machine.
ref ID	Address of machine peer is synchronized to.
time	Last timestamp peer received from its master.
our mode	Our mode relative to peer (active / passive / client / server / bdcast / bdcast client).
peer mode	Peer's mode relative to us.
our poll ivl	Our poll interval to peer.
peer poll ivl	Peer's poll interval to us.
root delay	Delay along path to root (ultimate stratum 1 time source).
root disp	Dispersion of path to root.
reach	Peer reachability (bit string in octal).
sync dist	Peer synchronization distance.
delay	Round trip delay to peer.
offset	Offset of peer clock relative to our clock.
dispersion	Dispersion of peer clock.
precision	Precision of peer clock in Hz.
version	NTP version number that peer is using.
org time	Originate time stamp.
rcv time	Receive time stamp.
xmt time	Transmit time stamp.
filtdelay	Round trip delay in milliseconds of each sample.
filtoffset	Clock offset in milliseconds of each sample.
filterror	Approximate error of each sample.

show ntp status

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

show ntp status

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Display

The following is sample output from the **show ntp status** command:

```
Router# show ntp status

Clock is synchronized, stratum 4, reference is 131.108.13.57
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**19
reference time is AFE2525E.70597B34 (00:10:22.438 PDT Mon Jul 5 1993)
clock offset is 7.33 msec, root delay is 133.36 msec
root dispersion is 126.28 msec, peer dispersion is 5.98 msec
```

Table 5-34 shows the significant fields in the display.

Table 5-34 Show NTP Status Field Descriptions

Field	Description
synchronized	System is synchronized to an NTP peer.
unsynchronized	System is not synchronized to any NTP peer.
stratum	NTP stratum of this system.
reference	Address of peer we are synchronized to.
nominal freq	Nominal frequency of system hardware clock.
actual freq	Measured frequency of system hardware clock.
precision	Precision of this system's clock (in Hz).
reference time	Reference timestamp.
clock offset	Offset of our clock to synchronized peer.
root delay	Total delay along path to root clock.
root dispersion	Dispersion of root path.
peer dispersion	Dispersion of synchronized peer.

show privilege

To display your current level of privilege, use the **show privilege** EXEC command.

show privilege

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Display

The following is sample output from the **show privilege** command. The current privilege level is 15.

```
Router# show privilege

Current privilege level is 15
```

Related Command

enable password level

show processes

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

show processes [**cpu**]

Syntax Description

cpu (Optional) Displays detailed CPU utilization statistics.

Command Mode

EXEC

Sample Displays

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

```
Router# show processes
Glenfarclas#show process
CPU utilization for five seconds: 21%/0%; one minute: 2%; five minutes: 2%
PID QTy      PC Runtime (ms)   Invoked   uSecs     Stacks    TTY  Process
  1 Mwe  2FEA4E         1808       464    3896     1796/3000   0  IP-EIGRP Router
  2 Lst  11682          10236      109   93908     1828/2000   0  Check heaps
  3 Mst  3AE9C              0      280       0     1768/2000   0  Timers
  4 Lwe  74AD2              0       12       0     1492/2000   0  ARP Input
  5.ME   912E4              0        2       0     1892/2000   0  IPC Zone Manager
  6.ME   91264              0        1       0     1936/2000   0  IPC Realm Manager
  7.ME   91066              0       30       0     1784/2000   0  IPC Seat Manager
  8.ME  133368              0        1       0     1928/2000   0  CXBus hot stall
  9.ME  1462EE              0        1       0     1940/2000   0 Microcode load
 10 Msi 127538              4       76      52     1608/2000   0 Env Mon
 11.ME  160CF4              0        1       0     1932/2000   0 MIP Mailbox
 12 Mwe 125D7C              4      280      14     1588/2000   0 SMT input
 13 Lwe AFD0E               0        1       0     1772/2000   0 Probe Input
 14 Mwe AF662               0        1       0     1784/2000   0 RARP Input
 15 Hwe A1F9A             228      549     415     3240/4000   0 IP Input
 16 Msa C86A0               0      114       0     1864/2000   0 TCP Timer
 17 Lwe CA700               0        1       0     1756/2000   0 TCP Protocols
 18.ME  CCE7C               0        1       0     1940/2000   0 TCP Listener
 19 Mwe AC49E               0        1       0     1592/2000   0 BOOTP Server
 20 Mwe 10CD84             24       77     311     1652/2000   0 CDP Protocol
 21 Mwe 27BF82              0        2       0     1776/2000   0 ATMSIG Input
```

The following is sample output from the **show processes cpu** command:

```
Router# show processes cpu

CPU utilization for five seconds: 5%/2%; one minute: 3%; five minutes: 2%
  PID  Runtime (ms)    Invoked   uSecs   5Sec  1Min  5Min  TTY Process
    1          1736         58   29931     0%    0%    0%  Check heaps
    2            68        585     116  1.00% 1.00%    0%  IP Input
    3             0        744       0     0%    0%    0%  TCP Timer
    4             0          2       0     0%    0%    0%  TCP Protocols
    5             0          1       0     0%    0%    0%  BOOTP Server
    6            16        130     123     0%    0%    0%  ARP Input
    7             0          1       0     0%    0%    0%  Probe Input
    8             0          7       0     0%    0%    0%  MOP Protocols
    9             0          2       0     0%    0%    0%  Timers
   10           692         64   10812     0%    0%    0%  Net Background
   11             0          5       0     0%    0%    0%  Logger
```

```
 12             0         38       0     0%    0%    0%  BGP Open
 13             0          1       0     0%    0%    0%  Net Input
 14           540       3466     155     0%    0%    0%  TTY Background
 15             0          1       0     0%    0%    0%  BGP I/O
 16          5100       1367    3730     0%    0%    0%  IGRP Router
 17            88       4232      20  0.20% 1.00%    0%  BGP Router
 18           152      14650      10     0%    0%    0%  BGP Scanner
 19           224         99    2262     0%    0% 1.00%  Exec
```

Table 5-35 describes significant fields shown in the two displays.

Table 5-35 Show Processes Field Descriptions

Field	Description
CPU utilization for five seconds	CPU utilization for the last 5 seconds. The second number indicates the percent of CPU time spent at the interrupt level.
one minute	CPU utilization for the last minute.
five minutes	CPU utilization for the last 5 minutes.
PID	Process ID.
Q	Process queue priority. Possible values: H (high), M (medium), L (low).
Ty	Scheduler test. Possible values: * (currently running), E (waiting for an event), S (ready to run, voluntarily relinquished processor), rd (ready to run, wakeup conditions have occurred), we (waiting for an event), sa (sleeping until an absolute time), si (sleeping for a time interval), sp (sleeping for a time interval (alternate call), st (sleeping until a timer expires), hg (hung; the process will never execute again), xx (dead. The process has terminated, but not yet been deleted.).
PC	Current program counter.
Runtime (ms)	CPU time the process has used, in milliseconds.
Invoked	Number of times the process has been invoked.
uSecs	Microseconds of CPU time for each process invocation.
Stacks	Low water mark/Total stack space available, shown in bytes.
TTY	Terminal that controls the process.
Process	Name of process.
5Sec	CPU utilization by task, in last 5 seconds.
1Min	CPU utilization by task in last minute.
5Min	CPU utilization by task in last 5 minutes.

Note Because the network server has a 4-millisecond clock resolution, run times are considered reliable only after a large number of invocations or a reasonable, measured run time.

show processes memory

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

show processes memory

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Display

The following is sample output from the **show processes memory** command:

```
Router# show processes memory

Total: 5611448, Used: 2307548, Free: 3303900
 PID  TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
   0    0     199592       1236    1907220          0          0 *Init*
   0    0        400      76928        400          0          0 *Sched*
   0    0    5431176    3340052     140760     349780          0 *Dead*
   1    0        256        256       1724          0          0 Load Meter
   2    0        264          0       5032          0          0 Exec
   3    0          0          0       2724          0          0 Check heaps
   4    0      97932          0       2852      32760          0 Pool Manager
   5    0        256        256       2724          0          0 Timers
   6    0         92          0       2816          0          0 CXBus hot stall
   7    0          0          0       2724          0          0 IPC Zone Manager
   8    0          0          0       2724          0          0 IPC Realm Manager
   9    0          0          0       2724          0          0 IPC Seat Manager
  10    0        892        476       3256          0          0 ARP Input
  11    0         92          0       2816          0          0 SERIAL A'detect
  12    0        216          0       2940          0          0 Microcode Loader
  13    0          0          0       2724          0          0 RFSS watchdog
  14    0   15659136   15658584       3276          0          0 Env Mon
...
  77    0        116          0       2844          0          0 IPX-EIGRP Hello
                                    2307224 Total
```

Table 5-36 describes significant fields shown in the display.

Table 5-36 Show Processes Memory Field Descriptions

Field	Description
Total	Total amount of memory held.
Used	Total amount of used memory.
Free	Total amount of free memory.
PID	Process ID.
TTY	Terminal that controls the process.
Allocated	Bytes of memory allocated by the process.
Freed	Bytes of memory freed by the process, regardless of who originally allocated it.

Table 5-36 Show Processes Memory Field Descriptions (Continued)

Field	Description
Holding	Amount of memory currently allocated to the process.
Getbuffs	Number of times the process has requested a packet buffer.
Retbuffs	Number of times the process has relinguished a packet buffer.
Process	Process name.
Init	System initialization.
Sched	The scheduler.
Dead	Processes as a group that are now dead.
Total	Total amount of memory held by all processes.

show protocols

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

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

show protocols

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Display

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

```
Router# show protocols

Global values:
  Internet Protocol routing is enabled
  DECNET routing is enabled
  XNS routing is enabled
  Appletalk routing is enabled
  X.25 routing is enabled
Ethernet 0 is up, line protocol is up
  Internet address is 131.108.1.1, subnet mask is 255.255.255.0
  Decnet cost is 5
  XNS address is 2001.AA00.0400.06CC
  AppleTalk address is 4.129, zone Twilight
Serial 0 is up, line protocol is up
  Internet address is 192.31.7.49, subnet mask is 255.255.255.240
Ethernet 1 is up, line protocol is up
  Internet address is 131.108.2.1, subnet mask is 255.255.255.0
  Decnet cost is 5
  XNS address is 2002.AA00.0400.06CC
  AppleTalk address is 254.132, zone Twilight
Serial 1 is down, line protocol is down
  Internet address is 192.31.7.177, subnet mask is 255.255.255.240
  AppleTalk address is 999.1, zone Magnolia Estates
```

For more information on the parameters or protocols shown in this sample output, see the *Router Products Configuration Guide* publication.

show queueing

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

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

Syntax Description

custom (Optional) Shows status of custom queue lists.

priority (Optional) Shows status of priority lists.

Command Mode

Privileged EXEC

Usage Guidelines

If no keyword is entered, this command show the status of both custom and priority queue lists.

Sample Displays

The following is sample output from the **show queueing custom** EXEC command:

```
Router# show queueing custom
Current custom queue configuration:

List   Queue  Args
3      10     default
3      3      interface Tunnel3
3      3      protocol ip
3      3      byte-count 444 limit 3
```

The following is sample output from the **show queueing** command. On interface Serial0, there are two active conversations. Weighted fair queueing will ensure that both of these IP data streams—both using TCP—receive equal bandwidth on the interface while they have messages in the pipeline, even though there is more FTP data in the queue than rcp data.

```
Router# show queueing
Current fair queue configuration:
Interface Serial0

  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Output queue: 18/64/30 (size/threshold/drops)
     Conversations 2/8 (active/max active)
     Reserved Conversations 0/0 (allocated/max allocated)

  (depth/weight/discards) 3/4096/30
  Conversation 117, linktype: ip, length: 556, flags: 0x280
  source: 171.69.128.115, destination: 171.69.58.89, id: 0x1069, ttl: 59,
  TOS: 0 prot: 6, source port 514, destination port 1022

  (depth/weight/discards) 14/4096/0
  Conversation 155, linktype: ip, length: 1504, flags: 0x280
  source: 171.69.128.115, destination: 171.69.58.89, id: 0x104D, ttl: 59,
  TOS: 0 prot: 6, source port 20, destination port 1554
```

Related Commands

custom-queue-list
priority-group
priority-list interface
priority-list queue-limit
queue-list default
queue-list interface
queue-list protocol
queue-list queue byte-count
queue-list queue limit

show snmp

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

show snmp

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

This command provides counter information for RFC 1213 SNMP operations. It also displays the chassis ID string defined with the **snmp-server chassis-id** command.

Sample Display

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

```
Router# show snmp
Chassis: SN#TS02K229
167 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    167 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    167 Get-next PDUs
    0 Set-request PDUs
167 SNMP packets output
    0 Too big errors (Maximum packet size 484)
    0 No such name errors
    0 Bad values errors
    0 General errors
    167 Get-response PDUs
    0 SNMP trap PDUs
```

Related Command

snmp-server chassis-id

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.

show stacks

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Display

The following is sample output from the **show stacks** command following a system failure:

```
Router# show stacks

Minimum process stacks:
Free/Size  Name
 652/1000  Router Init
 726/1000  Init
 744/1000  BGP Open
 686/1200  Virtual Exec

Interrupt level stacks:
Level    Called Free/Size  Name
  1           0 1000/1000  env-flash
  3         738  900/1000  Multiport Communications Interfaces
  5         178  970/1000  Console UART
System was restarted by bus error at PC 0xAD1F4, address 0xD0D0D1A
GS Software (GS3), Version 9.1(0.16), BETA TEST SOFTWARE
Compiled Tue 11-Aug-92 13:27 by jthomas
Stack trace from system failure:
FP: 0x29C158, RA: 0xACFD4
FP: 0x29C184, RA: 0xAD20C
FP: 0x29C1B0, RA: 0xACFD4
FP: 0x29C1DC, RA: 0xAD304
FP: 0x29C1F8, RA: 0xAF774
FP: 0x29C214, RA: 0xAF83E
FP: 0x29C228, RA: 0x3E0CA
FP: 0x29C244, RA: 0x3BD3C
```

show tech-support

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

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

Syntax Description

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

Default

Display output without page breaks and remove passwords and other security information.

Command Mode

Privileged EXEC

Usage Guidelines

Use this command to help collect general information about the router when you are reporting a problem. This command displays the equivalent of the following show commands:

- **show version**
- **show running-config**
- **show controllers**
- **show stacks**
- **show interfaces**
- **show buffers**
- **show processes memory**
- **show processes cpu**

For a sample display of the output of the **show tech-support** command, refer to these show commands.

Related Commands

A dagger (†) indicates that the command is documented outside this chapter.

show buffers
show controllers †
show interfaces †
show processes cpu
show processes memory
show running-config †
show stacks
show version †

snmp-server access-policy

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

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

Syntax Description

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.
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.
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.
privileges	Bit mask representing the access privileges that govern the management operations that the source party can ask the destination party to perform.

Command Mode

Global configuration

Usage Guidelines

An access policy defines the management operations the destination party can perform in relation to resources defined by the specified context when requested by the source party. A destination party performs management operations that are requested by a source party. A source party sends communications to a destination party requesting the destination party to perform management operations. A context identifies object resources accessible to a party.

Access policies are defined on the router for communications from the manager to the agent; in this case, the agent is the destination party and the manager is the source party. Access policies can also be defined on the router for Response message and trap message communication from the agent to the manager; in this case, the manager is the destination party and the agent is the source party.

The *privileges* argument specifies the types of SNMP operations that are allowed between the two parties. There are seven types of SNMP operations.You specify the privileges as a bit mask representing the access privileges that govern the management operations that the source party can ask the destination party to perform. In other words, the bit mask identifies the commands that the source party can send to the destination party.

You 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

To remove an access-policy entry, all three arguments specified as command arguments must match exactly the values of the entry to be deleted. A difference of one value constitutes a different access policy.

The first **snmp-server** command that you enter enables both versions of SNMP.

Examples

The following example configures an access policy providing the manager with read-only access to the agent:

```
snmp-server access-policy agt1 mgr1 ctx1 0x23
```

The following example configures an access policy providing the manager with read-write access to the agent:

```
snmp-server access-policy agt2 mgr2 ctx2 43
```

The following example configures an access policy that allows responses and SNMP v.2 traps to be sent from the agent to a management station:

```
snmp-server access-policy mgr1 agt1 ctx1 132
```

The following example removes the access policy configured for the destination party named *agt1*, the source party named *mgr1*, and with a context named *ctx1*.

```
no snmp-server access-policy agt1 mgr1 ctx1
```

Related Commands

snmp-server context
snmp-server party

snmp-server chassis-id

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

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

Syntax Description

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

Default

On hardware platforms where the serial number can be machine read, the default is the serial number. For example, an AGS+ does not have a default value; a Cisco 7000 has a default value of its serial number.

Command Mode

Global configuration

Usage Guidelines

The Cisco MIB provides a chassis MIB variable that enables the SNMP manager to gather data on system card descriptions, chassis type, chassis hardware version, chassis ID string, software version of ROM monitor, software version of system image in ROM, bytes of processor RAM installed, bytes of NVRAM installed, bytes of NVRAM in use, current configuration register setting, and the value of the configuration register at the next reload. The following installed card information is provided: type of card, serial number, hardware version, software version, and chassis slot number.

The chassis ID message can be seen with **show snmp** command.

Example

In the following example, the chassis serial number specified is 1234456:

```
snmp-server chassis-id 1234456
```

Related Command

show snmp

snmp-server community

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

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

Syntax Description

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

Default

By default, an SNMP community string permits read-only access.

Command Mode

Global configuration

Usage Guidelines

For the previous version of this command, the *string* argument was optional. The *string* argument is now required. However, to prevent errors and provide backward-compatibility, if the string option is omitted, a default value of public is assumed.

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

The first **snmp-server** command that you enter enables both versions of SNMP.

Examples

The following example assigns the string *comaccess* to SNMPv1 allowing read-only access and specifies that IP access list 4 can use the community string:

```
snmp-server community comaccess ro 4
```

The following example disables both versions of SNMP:

```
no snmp-server
```

Related Command

snmp-server party

snmp-server contact

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

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

Syntax Description

text	String that describes the system contact information.

Default

No syscontact string is set.

Command Mode

Global configuration

Example

The following is an example of a syscontact string:

```
snmp-server contact Dial System Operator at beeper # 27345
```

snmp-server context

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

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

Syntax Description

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.

Command Mode

Global configuration

Usage Guidelines

A context record identifies object resources accessible to a party. A context record is one of the components that make up an access policy. Therefore, you must configure a context record before you can create an access policy that includes the context. Context records and party records further codify MIB views.

To remove a context entry, specify only the name of the context. The name identifies the context to be deleted.

The first **snmp-server** command that you enter enables both versions of SNMP.

Example

The following example shows how to create a context that includes all objects in the MIB-II subtree using a previously defined view named *mib2*:

```
snmp-server context mycontext initialContextid.131.108.24.56.3 mib2
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

snmp-server view
write memory †
write terminal †

snmp-server enable

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

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

Syntax Description

traps	Enables all traps.
trap-type	(Optional) Type of trap to enable. If no type is specified, all traps are sent (including **envmon** and **repeater**). It can be one of the following values: • **bgp**—send Border Gateway Protocol (BGP) state change traps. • **frame-relay**—send Frame Relay traps. • **isdn**—send ISDN traps. • **envmon**—send Cisco enterprise-specific environmental monitor traps when an environmental threshold is exceeded. When **envmon** is selected, you can specify a *trap-option*.,
trap-option	(Optional) When **envmon** is used, you can enable a specific environmental trap type, or accept all trap types from the environmental monitor system. If no option is specified, all environmental types are enabled. It can be one or more of the following values: **voltage**, **shutdown**, **supply, fan**, and **temperature**.

Defaults

No traps are enabled.

If you enter this command with no keywords, the default is to enable all trap types.

Command Mode

Global configuration

Usage Guidelines

Use the **snmp-server enable** command to specify which SNMP traps the router sends, and use the **snmp-server host** command to specify which host or hosts receive SNMP traps.

You must issue a separate **snmp-server enable** command for each trap type, including **envmon**.

Examples

The following example enables the router to send Frame Relay and environmental monitor traps.

```
snmp-server enable trap frame-relay
snmp-server enable trap envmon temperature
```

Related Commands

A dagger (†) indicates that the command is documented outside this chapter.

snmp trap illegal-address†
snmp-server host

snmp-server host

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

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

Syntax Description

host	Name or Internet address of the host.
community-string	Password-like community string to send with the trap operation.
trap-type	(Optional) Type of trap to be sent to the trap receiver *host*. If no type is specified, all traps are sent. It can be one or more of the following values: • **bgp**—Send Border Gateway Protocol (BGP) state change traps. • **config**—Send configuration traps. • **envmon**—Send Cisco enterprise-specific environmental monitor traps when an environmental threshold is exceeded. • **frame-relay**—Send Frame Relay traps. • **isdn**—Send ISDN traps. • **llc2**—Send Logical Link Control, type 2 (LLC2) traps. • **rsrb**—Send remote source route bridging (RSRB) traps. • **sdlc**—Send Synchronous Data Link Control (SDLC) traps. • **sdllc**—Send SDLLC traps. • **snmp**—Send SNMP traps defined in RFC 1157. • **stun**—Send serial tunnel (STUN) traps. • **tty**—Send Cisco enterprise-specific traps when a TCP connection closes. • **x25**—Send X.25 event traps.

Defaults

No traps are sent.

If you enter this command with no keywords, the default is to send all trap types.

Command Mode

Global configuration

Usage Guidelines

The **snmp-server host** command specifies which host or hosts should receive SNMP traps. You need to issue the **snmp-server host** command once for each host acting as a trap recipient.

When multiple **snmp-server host** commands are given for the same host, the community string in the last command is used, and in general, the trap types set in the last command will be used to filter the SNMP trap messages sent to that host.

To control which traps are sent by the router, use the **snmp-server enable** command.

Whether a trap-type option is available depends on the router type and Cisco IOS software features supported on the router. For example, **envmon** is available only if the environmental monitor is part of the system.

Examples

The following example sends the SNMP traps defined in RFC 1157 to the host specified by the name cisco.com. The community string is defined as the string *comaccess*.

```
snmp-server host cisco.com comaccess snmp
```

The following example sends the SNMP and Cisco environmental monitor enterprise-specific traps to address 172.30.2.160:

```
snmp-server host 172.30.2.160 snmp envmon
```

Related Commands

snmp-server enable
snmp-server trap-timeout

snmp-server location

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

snmp-server location *text*
no snmp-server location

Syntax Description

text	String that describes the system location information.

Default

No system location string is set.

Command Mode

Global configuration

Example

The following example illustrates a system location string:

```
snmp-server location Building 3/Room 214
```

snmp-server packetsize

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

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

Syntax Description

byte-count	Integer byte count from 484 to 8192.

Default

484 bytes

Command Mode

Global configuration

Example

The following example establishes a packet filtering of a maximum size of 1024 bytes:

```
snmp-server packetsize 1024
```

snmp-server party

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

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

Syntax Description

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. All messages sent to this party will be authenticated using the SNMP v2 MD5 authentication method with the key specified by *key.*
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 SNMP v1community string specified by *string* instead of MD5.

Defaults

If neither **local** nor **remote** is specified to indicate the location of the party, the party is assumed to be local.

If you do not specify a packet size, the packet size set through the **snmp-server packetsize** command is used.

Command Mode

Global configuration

Usage Guidelines

You define parties to identify managers and agents. An SNMP v2 party identity is unique; it includes the logical network location of the party, characterized by the transport protocol domain and transport addressing information, and, optionally, an authentication method and its arguments.The authentication protocol reliably identifies the origin of all messages sent by the party. The authentication protocol also ensures the integrity of the messages; in other words, it ensures that the message received is the message that was sent.

Specifying **md5** as the authentication method implies that this party record pertains to an SNMPv2 party.

Specifying **snmpv1** as the authentication method implies that this party record pertains to an SNMPv1 party. Instead of using the **snmp-server community** command, you can use the **snmp-server party** command with the **snmpv1** keyword to define an SNMP v.1 party to be used to communicate with an SNMP v.1 management station.

If authentication is not specified, the party record pertains to an SNMPv2 party, and no authentication will be performed for messages sent to this party.

To remove a party record, specify only the name of the party. The name identifies the party to be deleted.

The first **snmp-server** command that you enter enables both versions of SNMP.

Examples

The following example configures a remote unauthenticated party:

```
snmp-server party mgr1 initialPartyId.131.108.45.32.3 udp 131.108.45.76 162
```

The following example configures a local MD5-authenticated party with a large maximum packet size. You enter this command as a single line:

```
snmp-server party agt1 initialPartyId.131.108.45.32.4 packetsize 1500 local
 authentication md5 23de457623900ac3ef568fcb236589 lifetime 400
```

The following example configures an SNMP v.1 proxy party for the community *public*:

```
snmp-server party proxyv1 initialPartyId.131.108.45.32.100 authentication snmpv1 public
```

The following example removes the party named *mgr1*:

```
no snmp-server party mgr1
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

snmp-server community
write memory †
write terminal †

snmp-server queue-length

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

snmp-server queue-length *length*

Syntax Description

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

Default

10 events

Command Mode

Global configuration

Usage Guidelines

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.

Example

The following example establishes a message queue that traps four events before it must be emptied:

```
snmp-server queue-length 4
```

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** form of this command prevents an SNMP system-shutdown request (from an SNMP manager) from resetting the Cisco agent.

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

Syntax Description

This command has no arguments or keywords.

Default

This command is not included in the configuration file.

Command Mode

Global configuration

Example

The following example illustrates how to include the SNMP message reload feature in the device configuration:

```
snmp-server system-shutdown
```

snmp-server tftp-server-list

To limit the TFTP servers used via SNMP-controlled TFTP operations (saving and loading configuration files) to the servers specified in an access list, use the **snmp-server tftp-server-list** global configuration command. To disable this feature, use the **no** form of this command.

snmp-server tftp-server-list *number*
no snmp-server tftp-server-list

Syntax Description

number	Standard IP access list number from 1 to 99.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.2.

Example

The following example limits the TFTP servers that can be used for configuration file copies via SNMP to the servers in access list 44.

```
snmp-server tftp-server-list 44
```

snmp-server trap-authentication

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

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

Syntax Description

snmpv1	(Optional) Indicates that SNMP authentication traps will be sent to SNMPv1 management stations only.
snmpv2	(Optional) Indicates that SNMP authentication traps will be sent to SNMPv2 management stations only.

Defaults

Specifying the **snmp-server trap-authentication** command without a keyword turns on trap message authentication. 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.

Command Mode

Global configuration

Usage Guidelines

Specify the **snmpv1** or **snmpv2** keyword to indicate the type of management stations to send the trap messages to.

This command enables the router as an agent to send a trap message when it receives an SNMPv1 packet with an incorrect community string or an SNMPv2 packet with an incorrect MD5 authentication key.

The SNMP specification requires that a trap message be generated for each packet with an incorrect community string or authentication key; however, because this action can result in a security breach, the router (as an agent) by default does not send a trap message when it receives an incorrect community string or authentication key.

The community string or key is checked before any access list that may be set, so it is possible to get spurious trap messages. In other words, if you have issued an **snmp-server community** command with a specified access list, you might receive messages that come from someone that is not on the access list; in this case, an authentication trap is issued.The only workarounds are to disable trap authentication or to configure an access list on a router between the SNMP agent and the SNMP manager to prevent packets from getting to the SNMP agent.

To turn off all message authentication traps, use the **no snmp-server trap-authentication** without a keyword. To turn off message authentication traps only for SNMPv1 stations or only for SNMPv2 stations, give the negative form of the command with the appropriate keyword.

The first **snmp-server** command that you enter enables both versions of SNMP.

Example

The following example illustrates how to enter the command that establishes trap message authentication:

```
snmp-server trap-authentication
```

Related Command

snmp-server host

snmp-server trap-source

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

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

Syntax Description

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

Default

No interface is specified.

Command Mode

Global configuration

Usage Guidelines

When an SNMP trap is sent from a Cisco SNMP server, it has a trap address of whatever interface it happened to go out of at that time. Use this command if you want to use the trap address to trace particular needs.

Examples

The following example specifies that the IP address for interface Ethernet 0 is the source for all traps on the router:

```
snmp-server trap-source ethernet 0
```

The following example specifies that the IP address for interface Ethernet 2/1 on a Cisco 7000 is the source for all traps on the router:

```
snmp-server trap-source ethernet 2/1
```

snmp-server trap-timeout

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

snmp-server trap-timeout *seconds*

Syntax Description

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

Default

30 seconds

Command Mode

Global configuration

Usage Guidelines

Before the router tries to send a trap, it looks for a route to the destination address. If there is no known route, the trap is saved in a retransmission queue. The **server trap-timeout** command determines the number of seconds between retransmission attempts.

Example

The following example sets an interval of 20 seconds to try resending trap messages on the retransmission queue:

```
snmp-server trap-timeout 20
```

Related Command

snmp-server host

snmp-server view

To create or update a view entry, use the **snmp-server view** global configuration command. To remove the specified SNMP server view entry, use the **no** form of this command.

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

Syntax Description

view-name	Label for the view record that you are updating or creating. The name is used to reference the record.
oid-tree	Object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as *1.3.6.2.4*, or a word, such as *system*. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
included | **excluded**	Type of view. You must specify either **included** or **excluded**.

Command Mode

Global configuration

Usage Guidelines

Other SNMP commands require a view as an argument. You use this command to create a view to be used as arguments for other commands that create records including a view.

Two standard predefined views can be used when a view is required, instead of defining a view. One is *everything*, which indicates that the user can see all objects. The other is *restricted*, which indicates that the user can see three groups: system, snmpStats, and snmpParties. The predefined views are described in RFC 1447.

The first **snmp-server** command that you enter enables both versions of SNMP.

Examples

The following example creates a view that includes all objects in the MIB-II subtree:

```
snmp-server view mib2 mib-2 included
```

The following example creates a view that includes all objects in the MIB-II system group and all objects in the Cisco enterprise MIB:

```
snmp-server phred system included
snmp-server view phred cisco included
```

The following example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group:

```
snmp-server view agon system included
snmp-server view agon system.7 excluded
snmp-server view agon ifEntry.*.1 included
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

snmp-server context
write memory †
write terminal †

snmp trap link-status

To enable SNMP link trap generation, use the **snmp trap link-status** command. To disable SNMP link traps, use the **no** form of this command.

snmp trap link-status
no snmp trap link-status

Syntax Description:

This command has no arguments or keywords.

Default

SNMP link traps are sent when an interface goes up or down.

Command Mode

Interface Configuration

Usage Guidelines

By default, SNMP link traps are sent when an interface goes up or down. For interfaces expected to go up and down during normal usage, such as ISDN interfaces, the output generated by these traps may not be useful. The **no** form of this command disables these traps.

Example

This example disables the sending of SNMP link traps related to the ISDN BRI 0 interface. This will stop all SNMP %LINK-UPDOWN messages from being sent for this interface.

```
interface bri 0
 no snmp trap link-status
```

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.

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

Syntax Description

count	Integer that sets the number of attempts.

Default

Three attempts

Command Mode

Global configuration

Example

The following example changes the login attempt to just one try:

```
tacacs-server attempts 1
```

tacacs-server authenticate

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

tacacs-server authenticate {**connection** [**always**] | **enable** | **slip** [**always**] [**access-lists**]}

Syntax Description

connection	Configures a required response when a user makes a TCP connection.
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.
always	(Optional) Performs authentication even when a user is not logged in. This option only applies to the **connection** or **slip** keywords.
access-lists	(Optional) Requests and installs access lists. This option only applies to the **slip** keyword.

Command Mode

Global configuration

Usage Guidelines

Enter one of the keywords to specify the action (when a user makes a TCP connection, for example).

Note Before you use the **tacacs-server authenticate** command, you must enable the **tacacs-server extended** command.

Note This command is not used in AAA/TACACS+ and has been replaced by the **aaa authorization** command.

Example

The following example configures TACACS logins that authenticate user TCP connections:

```
tacacs-server authenticate connect
```

Related Command

enable secret

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.

tacacs-server extended
no tacacs-server extended

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

Note This command initializes extended TACACS. To initialize AAA/TACACS+, use the **aaa new-model** command.

Example

The following example enables extended TACACS mode:

```
tacacs-server extended
```

tacacs-server host

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.

tacacs-server host *name*
no tacacs-server host *name*

Syntax Description

name	Name or IP address of the host.

Default

No TACACS host is specified.

Command Mode

Global configuration

Example

The following example specifies a TACACS host named SCACAT:

```
tacacs-server host SCACAT
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

login tacacs †
ppp †
slip †

tacacs-server 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.

tacacs-server key *key*
no tacacs-server key [*key*]

Syntax Description

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

Command Mode

Global Configuration

Usage Guidelines

After enabling AAA with the **aaa new-model** command, you must set the authentication and encryption key using the **tacas-server key** command.

The key entered must match the key used on the TACACS+ daemon. All leading spaces are ignored, spaces within and at the end of the key are not. If you use spaces in your key, do not enclose the key in double quotes unless the quotes themselves are part of the key.

Example

The following example illustrates how to set the authentication and encryption key to ‘dare to go’:

```
tacacs-server key dare to go
```

Related Commands

aaa new-model

tacacs-server last-resort

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 tacacs-server last-resort** command restores the system to the default behavior.

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

Syntax Description

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.

Default

If, when running the TACACS server, the TACACS server does not respond, the default action is to deny the request.

Command Mode

Global configuration

Usage Guidelines

Use the **tacacs-server last-resort** command to be sure that login can occur; for example, when a systems administrator needs to log in to troubleshoot TACACS servers that might be down.

Note This command is not used in AAA/TACACS+.

Example

The following example forces successful login:

```
tacacs-server last-resort succeed
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

enable password
login (EXEC) †

tacacs-server notify

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.

tacacs-server notify {**connection** [**always**] | **enable** | **logout** [**always**] | **slip** [**always**]}

Syntax Description

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.

Default

No message is transmitted to the TACACS server.

Command Mode

Global configuration

Usage Guidelines

The terminal user 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).

Note This command is not used in AAA/TACACS+ and has been replaced by the **aaa accounting** suite of commands.

Example

The following example sets up notification of the TACACS server when a user logs out:

```
tacacs-server notify logout
```

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 optional-passwords
no tacacs-server optional-passwords

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

When the user types in the login name, the login request is transmitted with the name and a zero-length password. If accepted, the login procedure completes. If the TACACS server refuses this request, the server software prompts for a password and tries again when the user supplies a password. The TACACS server must support authentication for users without passwords to make use of this feature. This feature supports all TACACS requests—login, SLIP, enable, and so on.

Note This command is not used by AAA/TACACS+.

Example

The following example configures the first login to not require TACACS verification:

```
tacacs-server optional-passwords
```

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 timeout before increasing the retransmit count. The **no** form of this command restores the default.

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

Syntax Description

retries	Integer that specifies the retransmit count.

Default

Two retries

Command Mode

Global configuration

Example

The following example specifies a retransmit counter value of five times:

```
tacacs-server retransmit 5
```

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.

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

Syntax Description

seconds	Integer that specifies the timeout interval in seconds.

Default

5 seconds

Command Mode

Global configuration

Example

The following example changes the interval timer to 10 seconds:

```
tacacs-server timeout 10
```

test flash

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

test flash

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Example

The following example illustrates how to begin the interface test:

```
test flash
```

test interfaces

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

test interfaces

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

The **test interfaces** EXEC command is intended for the factory checkout of network interfaces. It is not intended for diagnosing problems with an operational router. The **test interfaces** output does not report correct results if the router is attached to a "live" network. For each network interface that has an IP address that can be tested in loopback (MCI and ciscoBus Ethernet and all serial interfaces), the **test interfaces** command sends a series of ICMP echoes. Error counters are examined to determine the operational status of the interface.

Example

The following example illustrates how to begin the interface test:

```
test interfaces
```

test memory

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

test memory

Caution The memory test overwrites memory. If you use the **test memory** command, you will need to rewrite nonvolatile memory. For example, if you test Multibus memory, which is the memory used by the CSC-R 4-Mbps Token Ring interfaces, you will need to reload the system before the network interfaces will operate properly. The **test memory** command is intended primarily for use by Cisco personnel.

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

Example

The following example illustrates how to begin the memory test:

```
test memory
```

trace (privileged)

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

trace [*protocol*] [*destination*]

Syntax Description

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.

Default

The *protocol* argument is based on the router's examination of the format of *destination*. For example, if the router finds a *destination* argument in IP format, the *protocol* value defaults to **ip**.

Command Mode

Privileged EXEC

Usage Guidelines

The **trace** command works by taking advantage of the error messages generated by routers when a datagram exceeds its time-to-live (TTL) value.

The **trace** command starts by sending probe datagrams with a TTL value of one. This causes the first router to discard the probe datagram and send back an error message. The **trace** command sends several probes at each TTL level and displays the round-trip time for each.

The **trace** command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A "time exceeded" error message indicates that an intermediate router has seen and discarded the probe. A "destination unreachable" error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, **trace** prints an asterisk (*).

The **trace** command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with the escape sequence. By default, to invoke the escape sequence, type **Ctrl-^ X**—by simultaneously pressing and releasing the **Ctrl**, **Shift**, and **6** keys, and then pressing the **X** key.

To use nondefault parameters and invoke an extended **trace** test, enter the command without a *destination* argument. You will be stepped through a dialog to select the desired parameters.

Common Trace Problems

Due to bugs in the IP implementation of various hosts and routers, the IP **trace** command may behave in odd ways.

Not all destinations will respond correctly to a probe message by sending back an "ICMP port unreachable" message. A long sequence of TTL levels with only asterisks, terminating only when the maximum TTL has been reached, may indicate this problem.

There is a known problem with the way some hosts handle an "ICMP TTL exceeded" message. Some hosts generate an "ICMP" message but they reuse the TTL of the incoming packet. Since this is zero, the ICMP packets do not make it back. When you trace the path to such a host, you may see a set of TTL values with asterisks (*). Eventually the TTL gets high enough that the *ICMP* message can get back. For example, if the host is six hops away, **trace** will time out on responses 6 through 11.

Sample Display Showing Trace IP Routes

The following display shows sample IP **trace** output when a destination host name has been specified:

```
Router# trace ABA.NYC.mil

Type escape sequence to abort.
Tracing the route to ABA.NYC.mil (26.0.0.73)
  1 DEBRIS.CISCO.COM (131.108.1.6) 1000 msec 8 msec 4 msec
  2 BARRNET-GW.CISCO.COM (131.108.16.2) 8 msec 8 msec 8 msec
  3 EXTERNAL-A-GATEWAY.STANFORD.EDU (192.42.110.225) 8 msec 4 msec 4 msec
  4 BB2.SU.BARRNET.NET (131.119.254.6) 8 msec 8 msec 8 msec
  5 SU.ARC.BARRNET.NET (131.119.3.8) 12 msec 12 msec 8 msec
  6 MOFFETT-FLD-MB.in.MIL (192.52.195.1) 216 msec 120 msec 132 msec
  7 ABA.NYC.mil (26.0.0.73) 412 msec 628 msec 664 msec
```

Table 5-37 describes the fields shown in the display.

Table 5-37 Trace Field Descriptions

Field	Description
1	Indicates the sequence number of the router in the path to the host.
DEBRIS.CISCO.COM	Host name of this router.
131.108.1.6	Internet address of this router.
1000 msec 8 msec 4 msec	Round-trip time for each of the three probes that are sent.

Sample Display Showing Extended IP Trace Dialog

The following display shows a sample **trace** session involving the extended dialog of the **trace** command.

```
Router# trace

Protocol [ip]:
Target IP address: mit.edu
Source address:
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to MIT.EDU (18.72.2.1)
```

```
 1 ICM-DC-2-V1.ICP.NET (192.108.209.17) 72 msec 72 msec 88 msec
 2 ICM-FIX-E-H0-T3.ICP.NET (192.157.65.122) 80 msec 128 msec 80 msec
 3 192.203.229.246 540 msec 88 msec 84 msec
 4 T3-2.WASHINGTON-DC-CNSS58.T3.ANS.NET (140.222.58.3) 84 msec 116 msec 88 msec
 5 T3-3.WASHINGTON-DC-CNSS56.T3.ANS.NET (140.222.56.4) 80 msec 132 msec 88 msec
 6 T3-0.NEW-YORK-CNSS32.T3.ANS.NET (140.222.32.1) 92 msec 132 msec 88 msec
 7 T3-0.HARTFORD-CNSS48.T3.ANS.NET (140.222.48.1) 88 msec 88 msec 88 msec
 8 T3-0.HARTFORD-CNSS49.T3.ANS.NET (140.222.49.1) 96 msec 104 msec 96 msec
 9 T3-0.ENSS134.T3.ANS.NET (140.222.134.1) 92 msec 128 msec 92 msec
10 W91-CISCO-EXTERNAL-FDDI.MIT.EDU (192.233.33.1) 92 msec 92 msec 112 msec
11 E40-RTR-FDDI.MIT.EDU (18.168.0.2) 92 msec 120 msec 96 msec
12 MIT.EDU (18.72.2.1) 96 msec 92 msec 96 msec
```

Table 5-38 describes the fields that are unique to the extended trace sequence, as shown in the display.

Table 5-38 Trace Field Descriptions

Field	Description
Target IP address	You must enter a host name or an IP address. There is no default.
Source address	One of the interface addresses of the router to use as a source address for the probes. The router will normally pick what it feels is the best source address to use.
Numeric display	The default is to have both a symbolic and numeric display; however, you can suppress the symbolic display.
Timeout in seconds	The number of seconds to wait for a response to a probe packet. The default is 3 seconds.
Probe count	The number of probes to be sent at each TTL level. The default count is 3.
Minimum Time to Live [1]	The TTL value for the first probes. The default is 1, but it can be set to a higher value to suppress the display of known hops.
Maximum Time to Live [30]	The largest TTL value that can be used. The default is 30. The **trace** command terminates when the destination is reached or when this value is reached.
Port Number	The destination port used by the UDP probe messages. The default is 33434.
Loose, Strict, Record, Timestamp, Verbose	IP header options. You can specify any combination. The **trace** command issues prompts for the required fields. Note that **trace** will place the requested options in each probe; however, there is no guarantee that all routers (or end nodes) will process the options.
Loose	Allows you to specify a list of nodes that must be traversed when going to the destination.
Strict	Allows you to specify a list of nodes that must be the only nodes traversed when going to the destination.
Record	Allows you to specify the number of hops to leave room for.
Timestamp	Allows you to specify the number of time stamps to leave room for.
Verbose	If you select any option, the verbose mode is automatically selected and **trace** prints the contents of the option field in any incoming packets. You can prevent verbose mode by selecting it again, toggling its current setting.

Table 5-39 describes the characters that can appear in **trace** output.

Table 5-39 IP Trace Text Characters

Char	Description
nn msec	For each node, the round-trip time in milliseconds for the specified number of probes.
*	The probe timed out.
?	Unknown packet type.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.
U	Port unreachable.

Related Command

trace (user)

trace (user)

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

trace [*protocol*] [*destination*]

Syntax Description

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.

Default

The *protocol* argument is based on the router's examination of the format of the *destination* argument. For example, if the router finds a *destination* in IP format, the *protocol* defaults to **ip**.

Command Mode

EXEC

Usage Guidelines

The **trace** command works by taking advantage of the error messages generated by routers when a datagram exceeds its time-to-live (TTL) value.

The **trace** command starts by sending probe datagrams with a TTL value of one. This causes the first router to discard the probe datagram and send back an error message. The **trace** command sends several probes at each TTL level and displays the round-trip time for each.

The **trace** command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A "time exceeded" error message indicates that an intermediate router has seen and discarded the probe. A "destination unreachable" error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, **trace** prints an asterisk (*).

The **trace** command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with the escape sequence. By default, to invoke the escape sequence, type **Ctrl-^ X** by simultaneously pressing and releasing the **Ctrl**, **Shift**, and **6** keys, and then pressing the **X** key.

Common Trace Problems

Due to bugs in the IP implementation of various hosts and routers, the IP **trace** command may behave in odd ways.

Not all destinations will respond correctly to a probe message by sending back an "ICMP port unreachable" message. A long sequence of TTL levels with only asterisks, terminating only when the maximum TTL has been reached, may indicate this problem.

There is a known problem with the way some hosts handle an "ICMP TTL exceeded" message. Some hosts generate an *ICMP* message but they reuse the TTL of the incoming packet. Since this is zero, the ICMP packets do not make it back. When you trace the path to such a host, you may see a set of TTL values with asterisks (*). Eventually the TTL gets high enough that the "ICMP" message can get back. For example, if the host is six hops away, **trace** will time out on responses 6 through 11.

Sample Display Showing Trace IP Routes

The following display shows sample IP **trace** output when a destination host name has been specified:

```
Router# trace ip ABA.NYC.mil

Type escape sequence to abort.
Tracing the route to ABA.NYC.mil (26.0.0.73)
  1 DEBRIS.CISCO.COM (131.108.1.6) 1000 msec 8 msec 4 msec
  2 BARRNET-GW.CISCO.COM (131.108.16.2) 8 msec 8 msec 8 msec
  3 EXTERNAL-A-GATEWAY.STANFORD.EDU (192.42.110.225) 8 msec 4 msec 4 msec
  4 BB2.SU.BARRNET.NET (131.119.254.6) 8 msec 8 msec 8 msec
  5 SU.ARC.BARRNET.NET (131.119.3.8) 12 msec 12 msec 8 msec
  6 MOFFETT-FLD-MB.in.MIL (192.52.195.1) 216 msec 120 msec 132 msec
  7 ABA.NYC.mil (26.0.0.73) 412 msec 628 msec 664 msec
```

Table 5-40 describes the fields shown in the display.

Table 5-40 Trace Field Descriptions

Field	Description
1	Indicates the sequence number of the router in the path to the host.
DEBRIS.CISCO.COM	Host name of this router.
131.108.1.61	Internet address of this router.
1000 msec 8 msec 4 msec	Round-trip time for each of the three probes that are sent.

Table 5-41 describes the characters that can appear in **trace** output.

Table 5-41 IP Trace Text Characters

Char	Description
nn msec	For each node, the round-trip time in milliseconds for the specified number of probes.
*	The probe timed out.
?	Unknown packet type.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.

Related Command

trace (privileged)

username

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

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

Syntax Description

name	Host name, server name, user ID, or command name. The *name* argument can only be one word. White spaces and quotation marks are not allowed.
nopassword	(Optional) 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 communication server from disconnecting the user after an automatic command (set up with the **autocommand** keyword) has completed. Instead, the user gets another login prompt.
privilege	(Optional) Sets the privilege level for the user.
level	(Optional) Number between 0 and 15 that specifies the privilege level for the user.

Default

None

Command Mode

Global configuration

Usage Guidelines

The **username** command provides username/password authentication for login purposes only. (Note that it does not provide username/password authentication for enable mode when the **enable use-tacacs** command is also used.)

Multiple **username** commands can be used to specify options for a single user.

Add a **username** entry for each remote system that the local router communicates with and requires authentication from. The remote device must have a **username** entry for the local router. This entry must have the same password as the local router's entry for that remote device.

This command can be useful for defining usernames that get special treatment, for example, an "info" username that does not require a password, but connects the user to a general purpose information service.

The **username** command is also required as part of the configuration for the Challenge Handshake Authentication Protocol (CHAP). For each remote system that the local router communicates with from which it requires authentication, add a **username** entry.

Note To enable the local router to respond to remote CHAP challenges, one **username** *name* entry must be the same as the **hostname** *name* entry that has already been assigned to your router.

If there is no *secret* specified and **debug serial-interface** is enabled, an error is displayed when a link is established and the CHAP challenge is not implemented. Debugging information on CHAP is available using the **debug serial-interface** and **debug serial-packet** commands. For more information about **debug** commands, refer to the *Debug Command Reference* publication.

Examples

To implement a service similar to the UNIX **who** command, which can be entered at the login prompt and lists the current users of the router, the **username** command takes the following form:

```
username who nopassword nohangup autocommand show users
```

To implement an information service that does not require a password to be used, the command takes the following form:

```
username info nopassword noescape autocommand telnet nic.ddn.mil
```

To implement an ID that will work even if the TACACS servers all break, the command takes the following form:

```
username superuser password superpassword
```

The following example configuration enables CHAP on interface serial 0. It also defines a password for the local server, Adam, and a remote server, Eve.

```
hostname Adam
interface serial 0
encapsulation ppp
ppp authentication chap
username Adam password oursystem
username Eve password theirsystem
```

When you look at your configuration file, the passwords will be encrypted and the display will look similar to the following:

```
hostname Adam
interface serial 0
encapsulation ppp
ppp authentication chap
username Adam password 7 1514040356
username Eve password 7 121F0A18
```

Related Command

hostname