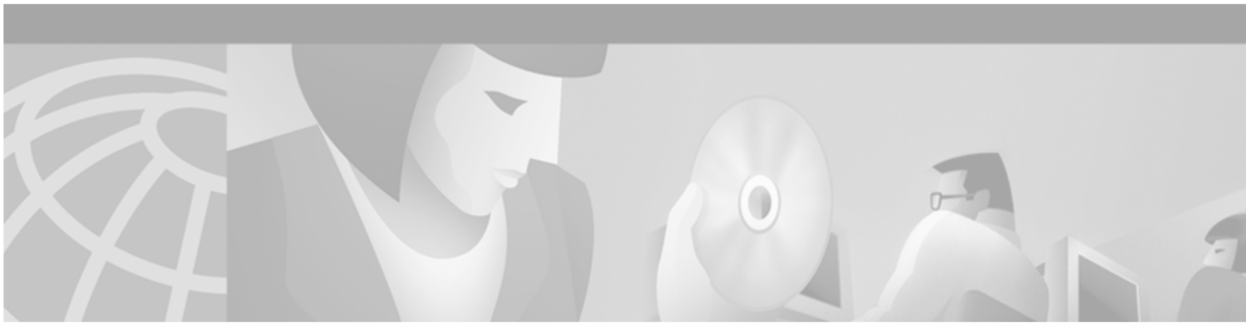

Basic System Management Commands

This chapter describes the commands used to perform basic system management tasks in Cisco IOS Release 12.1. Basic system management tasks include naming the router, enabling basic services, and configuring the Network Time Protocol (NTP).

For basic system management configuration tasks and examples, refer to the “Performing Basic System Management” chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.1*.

absolute

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

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

no absolute

Syntax Description

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end *time date*	(Optional) Absolute time and date that the associated **permit** or **deny** statement is no longer in effect.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

Defaults

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

Command Modes

Time-range configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.

Usage Guidelines

For Cisco IOS Release 12.1, IP and IPX extended access lists are the only functions that can use time ranges. For further information on using these functions, see the *Cisco IOS 12.1 IP and IP Routing* and the *Cisco IOS 12.1 AppleTalk and Novell IPX* publications.

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

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

Note All time specifications are taken as local time. To ensure that the time range entries take effect at the desired times, the system clock should be synchronized. Use NTP or the hardware calendar to synchronize the clock. For more information, refer to the "Performing Basic System Management" chapter of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Examples

The following example configures an access list named northeast, which references a time range named xyz. The access list and time range together permit traffic on Ethernet interface 0 starting at noon on January 1, 2001 and going forever.

```
time-range xyz
 absolute start 12:00 1 January 2001
!
ip access-list extended northeast
 permit ip any any time-range xyz
!
interface ethernet 0
 ip access-group northeast in
```

The following example permits UDP traffic until noon on December 31, 2000. After that time, UDP traffic is no longer allowed out Ethernet interface 0.

```
time-range abc
 absolute end 12:00 31 December 2000
!
ip access-list extended northeast
 permit udp any any time-range abc
!
interface ethernet 0
 ip access-group northeast out
```

The following example permits UDP traffic out Ethernet interface 0 on weekends only, from 8:00 a.m. on January 1, 1999 to 6:00 p.m. on December 31, 2001:

```
time-range test
 absolute start 8:00 1 January 1999 end 18:00 31 December 2001
 periodic weekends 00:00 to 23:59
!
ip access-list extended northeast
 permit udp any any time-range test
!
interface ethernet 0
 ip access-group northeast out
```

Related Commands

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

alias

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

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 104 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 Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

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

Table 104 shows the acceptable options for the *mode* argument in the **alias** global configuration command.

Table 104 mode Argument Options

Argument Options	Mode
configuration	Global configuration
controller	Controller configuration

Table 104 mode Argument Options (continued)

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

See the summary of command modes in the “Using the Command-Line Interface” chapter in the *Cisco IOS Configuration Fundamentals 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 **telnet 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**.

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

Examples

The following example creates the alias **fixmyrt** for the IP route198.92.116.16:

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

Related Commands

Command	Description
show aliases	Displays all alias commands.

buffers

To make adjustments to initial buffer pool settings and to the limits at which temporary buffers are created and destroyed, use the **buffers** global configuration command. 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 number	Interface type and interface number of the interface buffer pool. The type value cannot be **fddi**.
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. A maximum of 20,480 small buffers can be constructed in the 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.

Defaults

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 Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

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

Examples of Public Buffer Pool Tuning

The following example keeps at least 50 small buffers free in the system:

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

The following example increases the permanent buffer pool allocation for big buffers 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.

The following example increases the permanent Ethernet 0 interface buffer pool on a Cisco 4000 is 96 because the Ethernet 0 buffer pool is depleted:

```
buffers ethernet 0 permanent 96
```

Related Commands

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

buffers huge size

To dynamically resize all huge buffers to the value you specify, use the **buffers huge size** global configuration command. 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	Huge buffer size, in bytes.

Defaults

18024 bytes

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Examples

The following example resizes huge buffers to 20000 bytes:

```
buffers huge size 20000
```

Related Commands

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

calendar set

To set the system calendar, use one of the formats of 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 Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Some platforms have a calendar which is separate from the system clock. This calendar runs continuously, even if the router is powered off or rebooted. After you set the calendar, the system clock will be automatically set from the calendar when the system is restarted or when the **clock read-calendar** EXEC command is issued. The time specified in this command is relative to the configured time zone.

Examples

The following example manually sets the system calendar to 1:32 p.m. on July 23, 1997:

```
calendar set 13:32:00 23 July 1997
```

Related Commands

Command	Description
clock read-calendar	Manually reads the calendar into the system clock.
clock set	Manually set the system clock.
clock summer-time	Configures the system to automatically switch to summer time (daylight savings time).
clock timezone	Sets the time zone for display purposes.
clock update-calendar	Sets the calendar from the system clock.

clock calendar-valid

To configure a router as a time source for a network based on its calendar, use the **clock calendar-valid** global configuration command. Use the **no** form of this command to specify 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.

Defaults

The router is not configured as a time source.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Examples

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

```
clock calendar-valid
```

Related Commands

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

clock read-calendar

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

clock read-calendar

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Some platforms have a calendar which is separate from the system clock. This calendar runs continuously, even if the router is powered off or rebooted. When the router 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.

Examples

The following example configures the system clock to set its date and time by the calendar setting:

```
clock read-calendar
```

Related Commands

Command	Description
calendar set	Sets the system calendar.
clock set	Manually set the system clock.
clock update-calendar	Sets the calendar from the system clock.
ntp update-calendar	Periodically updates the calendar from NTP.

clock set

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

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

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

Syntax Description

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

Command Modes

Privileged EXEC mode

Command History

Release	Modification
10.0	This command was introduced.

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 router 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.

Examples

The following example manually sets the system clock to 1:32 p.m. on July 23, 1997:

```
clock set 13:32:00 23 July 1997
```

Related Commands

Command	Description
calendar set	Sets the system calendar.
clock read-calendar	Manually reads the calendar into the system clock.
clock summer-time	Configures the system to automatically switch to summer time (daylight savings time).
clock timezone	Sets the time zone for display purposes.

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** global configuration command. Use the **no** form of this command to configure the Cisco IOS software not to automatically switch to summer time.

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

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

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

no clock summer-time

Syntax Description

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

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

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

The following example specifies that 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, 1997 at 02:00, and end on April 26, 1998 at 02:00, with the following example:

```
clock summer-time date 12 October 1997 2:00 26 April 1998 2:00
```

Related Commands

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

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-offset* [*minutes-offset*]

no clock timezone

Syntax Description

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

Defaults

UTC

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Table 105 lists common time zone acronyms used for the *zone* argument.

Table 105 Common Time Zone Acronyms

Acronym	Time Zone Name and UTC Offset
Europe	
GMT	Greenwich Mean Time, as UTC
BST	British Summer Time, as UTC +1 hour
IST	Irish Summer Time, as UTC +1 hour
WET	Western Europe Time, as UTC
WEST	Western Europe Summer Time, as UTC +1 hour
CET	Central Europe Time, as UTC +1
CEST	Central Europe Summer Time, as UTC +2
EET	Eastern Europe Time, as UTC +2
EEST	Eastern Europe Summer Time, as UTC +3
MSK	Moscow Time, as UTC +3
MSD	Moscow Summer Time, as UTC +4

Table 105 Common Time Zone Acronyms

Acronym	Time Zone Name and UTC Offset
US and Canada	
AST	Atlantic Standard Time, as UTC -4 hours
ADT	Atlantic Daylight Time, as UTC -3 hours
ET	Eastern Time, either as EST or EDT, depending on place and time of year
EST	Eastern Standard Time, as UTC -5 hours
EDT	Eastern Daylight Saving Time, as UTC -4 hours
CT	Central Time, either as CST or CDT, depending on place and time of year
CST	Central Standard Time, as UTC -6 hours
CDT	Central Daylight Saving Time, as UTC -5 hours
MT	Mountain Time, either as MST or MDT, depending on place and time of year
MST	Mountain Standard Time, as UTC -7 hours
MDT	Mountain Daylight Saving Time, as UTC -6 hours
PT	Pacific Time, either as PST or PDT, depending on place and time of year e.g. Los Angeles
PST	Pacific Standard Time, as UTC -8 hours
PDT	Pacific Daylight Saving Time, as UTC -7 hours
HST	Hawaiian Standard Time, as UTC -10 hours
AKST	Alaska Standard Time, as UTC -9 hours
AKDT	Alaska Standard Daylight Saving Time, as UTC -8 hours
Australia	
WST	Western Standard Time, as UTC +8 hours e.g. Perth
CST	Central Standard Time, as UTC +9.5 hours e.g. Darwin
EST	Eastern Standard/Summer Time, as UTC +10 hours (+11 hours during summer time) e.g. Canberra

Table 106 lists an alternative method for referring to time zones, in which single letters are used to refer to the time zone difference from UTC. Using this method, the letter Z is used to indicate the zero meridian, equivalent to UTC, and the letter J (Juliet) is used to refer to the local time zone. Using this method, the International Date Line is between time zones M and Y.

Table 106 Single Letter Time Zone Designators

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

Examples

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

```
clock timezone PST -8
```

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

```
clock timezone AT -3 30
```

Related Commands

Command	Description
calendar set	Sets the system calendar.
clock set	Manually set the system clock.
clock summer-time	Configures the system to automatically switch to summer time (daylight savings time).
show clock	Displays the system clock.

clock update-calendar

To set the 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 Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Some platforms have a calendar which is separate from the system clock. This calendar runs continuously, even if the router is powered off or rebooted.

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

Examples

The following example copies the current time from the system clock to the calendar:

```
clock update-calendar
```

Related Commands

Command	Description
clock read-calendar	Manually reads the calendar into the system clock.
ntp update-calendar	Periodically updates the calendar from NTP.

downward-compatible-config

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

downward-compatible-config *version*

no downward-compatible-config

Syntax Description

version	Cisco IOS Release number, not earlier than 10.2.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

In Cisco IOS Release 10.3, IP access lists changed format. Use this command to regenerate a configuration in a 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.

Examples

The following example generates a configuration file compatible with Cisco IOS Release 10.2:

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

Related Commands

Command	Description
access-list (extended)	Provides extended access lists that allow more detailed access lists.
access-list (standard)	Defines a standard XNS access list.

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.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

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*.

Examples

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

```
hostname sandbox
```

Related Commands

Command	Description
setup	Enables you to make major enhancements to your configurations, for example, adding a protocol suit, making major addressing scheme changes, or configuring newly installed interfaces.

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.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

By default, the BOOTP server is enabled.

The integrated Dynamic Host Configuration Protocol (DHCP) server was introduced in Cisco IOS Release 12.0(1)T. Because DHCP is interoperable with BOOTP, both of these services share the "well-known" UDP server port of 67 (per RFC 951, RFC 1534, and RFC 2131). If both the BOOTP server and DHCP server are disabled, and a helper address is not configured, "ICMP port unreachable" messages will be sent in response to incoming requests on port 67, and the original incoming packet will be discarded.

Examples

In the following example, BOOTP and DHCP services are disabled on the router:

```
Router(config)# no ip bootp server
Router(config)# no service dhcp
```

Related Commands

Command	Description
service dhcp	Enables the integrated Dynamic Host Configuration Protocol (DHCP) server and relay agent.

ip finger

To configure a system to accept Finger protocol requests (defined in RFC 742), use the **ip finger** global configuration command. To disable this service, use the **no** form of this command.

ip finger [**rfc-compliant**]

no ip finger

Syntax Description

rfc-compliant	(Optional) Configures the system to wait for "Return" or "/W" input when processing Finger requests. This keyword should not be used for those systems.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.1	The **rfc-compliant** keyword was introduced.

Usage Guidelines

The Finger service allows remote users to view the output equivalent to the **show users** [**wide**] command.

When **ip finger** is configured, the router will respond to a **telnet** *a.b.c.d* **finger** command from a remote host by immediately displaying the output of the **show users** command and then closing the connection.

When the **ip finger rfc-compliant** command is configured, the router will wait for input before displaying anything (as required by RFC 1288). The remote user can then enter the Return key to display the output of the **show users** EXEC command, or enter **/W** to display the output of the **show users wide** EXEC command. After this information is displayed, the connection is closed.

Note As with all minor services, the Finger service should be disabled on your system if you do not have a need for it in your network.

Any network device that has UDP, TCP, BOOTP, or Finger services should be protected by a firewall or have the services disabled to protect against Denial of Service attacks.

Because of the potential for hung lines, the **rfc-compliant** form of this command should not be configured for devices with more than 20 simultaneous users.

Examples

The following example disables the Finger protocol:

```
Router(config)# no ip finger
```

ip telnet source-interface

To allow a user to select an address of an interface as the source address for Telnet connections, use the **ip telnet source-interface** global configuration command. Use the **no** form of this command to reset the source address to the default for each connection.

ip telnet source-interface *interface*

no ip telnet source-interface

Syntax Description

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

Defaults

The address of the closest interface to the destination as the source address. If the selected interface is *not* "up," the Cisco IOS software selects the address of the closest interface to the destination as the source address.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Use this command to set an interface's IP address as the source for all Telnet connections.

Examples

The following example makes the IP address for Ethernet interface 1 as the source address for Telnet connections:

```
ip telnet source-interface e 1
```

Related Commands

Command	Description
ip radius source-interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.

ip tftp source-interface

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

ip tftp source-interface *interface*

no ip tftp source-interface

Syntax Description

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

Defaults

The address of the closest interface to the destination as the source address. If the selected interface is not “up,” the Cisco IOS software selects the address of the closest interface to the destination as the source address.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Use this command to set an interface’s IP address as the source for all TFTP connections.

Examples

The following example makes the IP address for Ethernet interface 1 as the source address for TFTP connections:

```
ip tftp source-interface e 1
```

Related Commands

Command	Description
ip radius source-interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.

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 30, from 30 to 600 (30, 60, 90, 120, and so forth).

Defaults

300 seconds (or 5 minutes)

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

If you want load computations to be more reactive to short bursts of traffic, rather than averaged over 5-minute periods, you can shorten the length of time over which load averages are computed.

If the load interval is set to 30 seconds, new data is used for load calculations over a 30-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 5 seconds. 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 30 seconds, the average is computed for the last 30 seconds of load data.

The **load-interval** command allows you to change the default interval of 5 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.

Examples

In the following example, the default 5-minute average is set it to a 30-second average. A burst in traffic that would not trigger a dial backup for an interface configured with the default 5-minute interval might trigger a dial backup for this interface that is set for a shorter, 30-second interval.

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

Related Commands

Command	Description
show interfaces	Displays ALC information.

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.

Defaults

No access control (full access granted to all systems)

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

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.

Examples

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

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

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.

ntp authenticate

To enable Network Time Protocol (NTP) authentication, use the **ntp authenticate** 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 arguments or keywords.

Defaults

No authentication

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

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.

Examples

The following example configures the system 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

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp trusted-key	Authenticates the identity of a system to which NTP will synchronize.

ntp authentication-key

To define an authentication key for Network Time Protocol (NTP), use the **ntp authentication-key** 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 algorithm 5(MD5) algorithm. The key type **md5** is currently the only key type supported.
value	Key value (an arbitrary string of up to eight characters).

Defaults

No authentication key is defined for NTP.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

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.

Examples

The following example configures the system 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

Command	Description
ntp authenticate	Enables NTP authentication.
ntp peer	Configures the system clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the system clock to be synchronized by a time server.
ntp trusted-key	Authenticates the identity of a system to which NTP will synchronize.

ntp broadcast

To 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.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example configures Ethernet interface 0 to send NTP version 2 packets:

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

Related Commands

Command	Description
ntp broadcast client	Allows the system to receive NTP broadcast packets on an interface.
ntp broadcastdelay	Sets the estimated round-trip delay between the Cisco IOS software and an NTP broadcast server.

ntp broadcast client

To allow the system to receive Network Time Protocol (NTP) broadcast packets on an interface, use the **ntp broadcast client** interface configuration 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.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Examples

The following example synchronizes the Cisco IOS software to NTP packets broadcast on Ethernet interface 1:

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

Related Commands

Command	Description
ntp broadcast	Specifies that a specific interface should send NTP broadcast packets.
ntp broadcastdelay	Sets the estimated round-trip delay between the Cisco IOS software and an NTP broadcast server.

ntp broadcastdelay

To set the estimated round-trip delay between the Cisco IOS software and a Network Time Protocol (NTP) broadcast server, use the **ntp broadcastdelay** 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.

Defaults

3000 microseconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

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.

Examples

The following example sets the estimated round-trip delay between a router and the broadcast client to 5000 microseconds:

```
ntp broadcastdelay 5000
```

Related Commands

Command	Description
ntp broadcast	Specifies that a specific interface should send NTP broadcast packets.
ntp broadcast client	Allows the system to receive NTP broadcast packets on an interface.

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 to 32 seconds).

Defaults

17179869 2-32 seconds (4 milliseconds)

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

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.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command provides a simple method of access control.

Examples

The following example prevents Ethernet interface 0 from receiving NTP packets:

```
interface ethernet 0
 ntp disable
```

ntp master

To configure the Cisco IOS software as a Network Time Protocol (NTP) master clock to which peers synchronize themselves when an external NTP source is not available, use the **ntp master** 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 keeping time 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.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Because Cisco's 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.

Examples

The following example configures a router as an NTP master clock to which peers may synchronize:

```
ntp master 10
```

Related Commands

Command	Description
clock calendar-valid	Configures a router as a time source for a network based on its calendar.

ntp max-associations

To configure the maximum number of NTP peers and clients for the routing device, use the **ntp max-associations** command in global configuration mode. To return the maximum associations value to the default, use the **no** form of this command.

ntp max-associations *number*

no ntp max-associations

Syntax Description

number	Specifies the number of NTP associations. The range is 0 to 4294967295.

Defaults

100 maximum associations.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The router can be configured to define the the maximum number of NTP peer and client associations that the router will serve. The **ntp max-associations** command is used to set this limit.

This command is useful for ensuring that that the router isn't overwhelmed by huge numbers of NTP synchronization requests or, for an NTP master server, to allow large numbers of devices to sync to the router.

Examples

In the following example the router is configured so that it can act as an NTP server to over 100 clients:

```
Router(config)# ntp max-associations 200
```

Related Commands

Command	Description
show ntp associations	Shows all current NTP associations for the device.

ntp peer

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

ntp peer *ip-address* [**normal-sync**] [**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.
normal-sync	(Optional) Disables the rapid synchronization at startup.
version	(Optional) Defines the Network Time Protocol (NTP) version number.
number	(Optional) NTP version number (1 to 3).
key	(Optional) Defines the authentication key.
keyid	(Optional) Authentication key to use when sending packets to this peer.
source	(Optional) Names the interface.
interface	(Optional) Name of the interface from which to pick the IP source address.
prefer	(Optional) Makes this peer the preferred peer that provides synchronization.

Defaults

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 Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(14)T	The **normal-sync** keyword was added.

Usage Guidelines

Use this command if you want to allow this machine to synchronize with the peer, or vice versa. Using the **prefer** keyword reduces 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.

Examples

The following example configures a router to allow its system clock to be synchronized with the clock of the peer (or vice versa) at IP address 192.168.22.33 using NTP version 2. The source IP address is the address of Ethernet 0.

```
ntp peer 192.168.22.33 version 2 source ethernet 0
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp server	Allows the system clock to be synchronized by a time server.
ntp source	Uses a particular source address in NTP packets.

ntp server

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

ntp server *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]

no ntp server *ip-address*

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.

Defaults

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 Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

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 reduces 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.

Examples

The following example configures a router to allow its system clock to be synchronized with the clock of the peer at IP address 172.16.22.44 using NTP version 2:

```
ntp server 172.16.22.44 version 2
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp peer	Configures the system clock to synchronize a peer or to be synchronized by a peer.
ntp source	Uses a particular source address in NTP packets.

ntp source

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

ntp source *type number*

no ntp source

Syntax Description

type	Type of interface.
number	Number of the interface.

Defaults

Source address is determined by the outgoing interface.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

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.

Examples

The following example configures a router to use the IP address of Ethernet 0 as the source address of all outgoing NTP packets:

```
ntp source ethernet 0
```

Related Commands

Command	Description
ntp peer	Configures the system clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the system clock to be synchronized by a time server.

ntp trusted-key

To authenticate the identity of a system to which Network Time Protocol (NTP) will synchronize, use the **ntp trusted-key** 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.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

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.

Examples

The following example configures the system 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

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Defines an authentication key for NTP.

ntp update-calendar

To periodically update the system calendar from an NTP time-source, use the **ntp update-calendar** global configuration command. Use the **no** form of this command to disable the periodic updates.

ntp update-calendar

no ntp update-calendar

Syntax Description

This command has no arguments or keywords.

Defaults

The calendar is not updated.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Some platforms have a battery-powered system calendar in addition to the software based system clock. The system calendar runs continuously, even if the router is powered off or rebooted.

If the system clock is synchronized to an outside time source via NTP, it is a good idea to periodically update the system calendar with the time learned from NTP. Otherwise, the calendar will tend to gradually lose or gain time, and the clock and calendar may become out of sync with each other. The **ntp update-calendar** command will enable the system calendar to be periodically updated with the time specified by the NTP source. The calendar will be updated only if NTP has synchronized to an authoritative time server.

Many lower-end routers (for example, the Cisco 2500 series or the Cisco 2600 series) do not have system calendars, so this command is not available on those platforms.

To force a single update of the system calendar from the system clock, use the **clock update-calendar** command.

Examples

The following example configures the system to periodically update the calendar from the NTP time-source:

```
Router(config)# ntp update-calendar
```

Related Commands

Command	Description
clock read-calendar	Manually reads the calendar into the system clock.
clock update-calendar	Sets the calendar from the system clock.

periodic

To specify a recurring (weekly) time range for functions that support the time-range feature, use the **periodic** time-range configuration command. To remove the time limitation, use the **no** form of this command.

periodic *days-of-the-week hh:mm* **to** [*days-of-the-week*] *hh:mm*

no periodic *days-of-the-week hh:mm* **to** [*days-of-the-week*] *hh:mm*

Syntax Description

days-of-the-week	The first occurrence of this argument is the starting day or days that the associated time range is in effect. The second occurrence is the ending day or days the associated statement is in effect. This argument can be any single day or combinations of days: **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, **Sunday**. Other possible values are: **daily** — Monday through Sunday **weekdays** — Monday through Friday **weekend** — Saturday and Sunday If the ending days of the week are the same as the starting days of the week, they can be omitted.
hh:mm	The first occurrence of this argument is the starting *hours***:***minutes* that the associated time range is in effect. The second occurrence is the ending *hours***:***minutes* the associated statement is in effect. The *hours***:***minutes* are expressed in a 24-hour clock. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.

Defaults

No recurring time range is defined.

Command Modes

Time-range configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.

Usage Guidelines

Note For Cisco IOS Release 12.1, IP and IPX extended access lists are the only functions that can use time ranges. For further information on using these functions, see the *Cisco IOS 12.1 IP and IP Routing* and the *Cisco IOS 12.1 AppleTalk and Novell IPX* publications.

The **periodic** command is one way to specify when a time range is in effect. Another way is to specify an absolute time period with the **absolute** command. Use either of these commands after the **time-range** command, which specifies the name of the time range. Multiple **periodic** entries are allowed per **time-range** command.

If the end days-of-the-week are the same as the start, they can be omitted.

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

Note All time specifications are taken as local time. To ensure that the time range entries take effect at the desired times, you should synchronize the system clock, using NTP or the hardware calendar.

Here are some typical settings for your convenience:

If you want:	Configure this:
Monday through Friday, 8:00 a.m. to 6:00 p.m. only	**periodic weekday 8:00 to 18:00**
Every day of the week, from 8:00 a.m. to 6:00 p.m. only	**periodic daily 8:00 to 18:00**
Every minute from Monday 8:00 a.m. to Friday 8:00 p.m.	**periodic monday 8:00 to friday 20:00**
All weekend, from Saturday morning through Sunday night	**periodic weekend 00:00 to 23:59**
Saturdays and Sundays, from noon to midnight.	**periodic weekend 12:00 to 23:59**

Examples

The following example denies HTTP traffic on Monday through Friday between the hours of 8:00 a.m. and 6:00 p.m.:

```
time-range no-http
 periodic weekdays 8:00 to 18:00
!
ip access-list extended strict
 deny tcp any any eq http time-range no-http
!
interface ethernet 0
 ip access-group strict in
```

The following example permits Telnet traffic on Mondays, Tuesdays, and Fridays between the hours of 9:00 a.m. and 5:00 p.m.:

```
time-range testing
 periodic Monday Tuesday Friday 9:00 to 17:00
!
ip access-list extended legal
 permit tcp any any eq telnet time-range testing
!
interface ethernet 0
 ip access-group legal in
```

Related Commands

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

process-max-time

To configure the amount of time after which a process should voluntarily yield to another process, use the **process-max-time** command in global configuration mode. To reset this value to the system default, use the **no** form of this command.

process-max-time *milliseconds*

no process-max-time [*milliseconds*]

Syntax Description

milliseconds	Maximum duration (in milliseconds) that a process can run before suspension. The range is from 20-200 milliseconds.

Defaults

Default maximum process time is 200 milliseconds.

Command Modes

Global configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

Lowering the maximum time a process can run is useful in some circumstances to ensure equitable division of CPU time among different tasks.

Only use this command if recommended to do so by the Cisco Technical Assistance Center (TAC).

Examples

The following example limits the time to 100 milliseconds that a process can run without suspending:

```
process-max-time 100
```

prompt

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

prompt *string*

no prompt [*string*]

Syntax Description

string	Prompt. It can consist of all printing characters and the escape sequences listed in Table 107.

Defaults

The default prompt is either `Router` or the 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 Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

You can include escape sequences when specifying the prompt. All escape sequences are preceded by a percent sign (%). Table 107 lists the valid escape sequences.

Table 107 Custom Prompt Escape Sequences

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

Issuing the **prompt %h** command 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 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 Commands

Command	Description
hostname	Specifies or modifies the host name for the network server.

scheduler allocate

To guarantee CPU time for processes, use the **scheduler allocate** global configuration command on the Cisco 7200 series and Cisco 7500 series routers. 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.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

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.

Examples

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

```
scheduler allocate 2000 500
```

Related Commands

Command	Description
scheduler interval	Controls the maximum amount of time that can elapse without running system processes.

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.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

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.

Examples

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

```
scheduler interval 750
```

Related Commands

Command	Description
scheduler allocate	Guarantees CPU time for processes.

service decimal-tty

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

service decimal-tty

no service decimal-tty

Syntax Description

This command has no arguments or keywords.

Defaults

Decimal numbers are displayed.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example displays decimal rather than octal line numbers:

```
service decimal-tty
```

service exec-wait

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

service exec-wait

no service exec-wait

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

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.

Examples

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. Use the **no** form of this command to remove this service.

service finger

no service finger

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example disables 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.

Defaults

Addresses are displayed.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

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.

Examples

The following example hides Telnet addresses:

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

Related Commands

Command	Description
busy-message	Creates a “host failed” message that displays when a connection fails.

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 the algorithm.

service nagle

no service nagle

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

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.

Examples

The following example enables the Nagle algorithm:

```
service nagle
```

service prompt config

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

service prompt config

no service prompt config

Syntax Description

This command has no arguments or keywords.

Defaults

The configuration mode prompts (*hostname*(config)#) appear in all configuration modes.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Examples

In the following example, the **no service prompt config** command prevents the configuration prompt from being displayed. The prompt is still displayed in EXEC mode. When the **service prompt config** command is entered, the configuration mode prompt reappears.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no service prompt config
hostname bob
end
bob# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
service prompt config
bob(config)# hostname Router
Router(config)# end
Router#
```

Related Commands

Command	Description
hostname	Specifies or modifies the host name for the network server.
prompt	Customizes the prompt.

service tcp-small-servers

To access minor TCP/IP services available from hosts on the network, use the **service tcp-small-servers** global configuration 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.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

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

When the minor TCP/IP servers are disabled, 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.

Examples

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 service.

service telnet-zero-idle

no service telnet-zero-idle

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

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.

Examples

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

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

Related Commands

Command	Description
resume	Switches to another open Telnet, rlogin, LAT, or PAD session.

service udp-small-servers

To access minor User Datagram Protocol (UDP) services available from hosts on the network, use the **service udp-small-servers** global configuration 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.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

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

When the servers are disabled, 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.

Any network device that has UDP and TCP diagnostic services should be protected by a firewall or have the services disabled. UDP and TCP services are disabled using the **no service udp-small-servers** and **no service tcp-small-servers** global cofiguration commands.

Examples

The following example enables minor UDP services on the router:

```
Router(config)# 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 104 in the description of the **alias** command for acceptable options for the *mode* argument.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

All of the modes listed in Table 102 have their own prompts, except for the null interface mode. For example, the prompt for interface configuration mode is Router(config-if*)*.

Examples

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 Commands

Command	Description
alias	Creates a command alias.

show buffers

To display statistics for the buffer pools on the network server, use the **show buffers** EXEC command.

show buffers [**address** ***hex-addr*** | [**all** | **assigned** | **failures** | **free** | **old** [**dump** | **header** | **packet**]]
| **input-interface** ***interface-type identifier*** | **pool** ***pool-name***]

Syntax Description

address	(Optional) Displays buffers at a specified address.
hex-addr	Address, in hexadecimal notation, of the buffer to display.
all	(Optional) Displays all buffers.
assigned	(Optional) Displays the buffers in use.
failures	(Optional) Displays buffer allocation failures.
free	(Optional) Displays the buffers available for use.
old	(Optional) Displays buffers older than one minute.
dump	(Optional) Shows the buffer header and all data in the display.
header	(Optional) Shows the buffer header only in the display.
packet	(Optional) Shows the buffer header and packet data in the display.
input-interface	(Optional) Displays interface pool information. If the specified *interface-type* has its own buffer pool, displays information for that pool.
interface-type	Value of *interface-type* can be **ethernet**, **fastethernet**, **loopback**, **serial**, or **null**.
identifier	Identifier of the interface specified in *interface-type*.
pool	(Optional) Displays buffers in a specified buffer pool.
pool-name	Specifies the name of a buffer pool to use.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The peak field in the output of the **show buffers** command shows the maximum number of buffers created (highest total) and the time when that peak occurred relative to when you issued the **show buffers** command. Formats include weeks, days, hours, minutes, and seconds. Not all systems report a peak value, which means this field may not display in output.

Examples

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)
```

The following is sample output from the **show buffers** command with no arguments, showing onlybuffer pool information for Huge buffers. This output shows a highest total of five Huge buffers created five days and 18 hours before the command was issued.

```
Router> show buffers
```

```
Huge buffers, 18024 bytes (total 5, permanent 0, peak 5 @ 5d18h):
     4 in free list (3 min, 104 max allowed)
     0 hits, 1 misses, 101 trims, 106 created
     0 failures (0 no memory)
```

The following is sample output from the **show buffers** command with no arguments, showing only buffer pool information for Huge buffers. This output shows a highest total of 184 Huge buffers created one hour, one minute, and 15 seconds before the command was issued.

```
Router> show buffers

Huge buffers, 65280 bytes (total 4, permanent 2, peak 184 @ 01:01:15):
     4 in free list (0 min, 4 max allowed)
     32521 hits, 143636 misses, 14668 trims, 14670 created
     143554 failures (0 no memory)
```

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

Table 108 describes significant fields shown in the display.

Table 108 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.

Table 108 show buffers Field Descriptions (continued)

Field	Description
peak	Maximum number of buffers created (highest total) and the time when that peak occurred. Formats include weeks, days, hours, minutes, and seconds. Not all systems report a peak value, which means this field may not display in output.
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.
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.
fallbacks	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 the pool of that interface that can be in the buffer pool's cache of that interface. Each interface buffer pool has its own cache. These are not additional to the permanent buffers; they come from the buffer pools of the interface. 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.

show calendar

To display the calendar hardware setting, use the **show calendar** EXEC command:

show calendar

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Some platforms have a calendar which is separate from the system clock. This calendar runs continuously, even if the router is powered off or rebooted.

You can compare the time and date shown with this command with the time and date listed via the **show clock** 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.

Examples

In the following sample display, the hardware calendar indicates the timestamp of 12:13:44 p.m. on Friday, July 19, 1996:

```
Router# show calendar

12:13:44 PST Fri Jul 19 1996
```

Related Commands

Command	Description
show clock	Displays the system clock.

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, system calendar, and so forth) and the current summer-time setting (if any).

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The system clock keeps an “authoritative” flag that indicates whether the time is authoritative (believed to be accurate). If the system clock has been set by a timing source (system 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 peers from synchronizing to the system clock.

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

Symbol	Description
*	Time is not authoritative.
(blank)	Time is authoritative.
.	Time is authoritative, but NTP is not synchronized.

Note In general, NTP synchronization takes approximately 15-20 minutes.

Examples

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

```
Router# show clock detail

15:29:03.158 PST Mon Mar 3 1999
Time source is NTP
```

The following example shows the current clock is authoritative, but NTP is not yet synchronized:

```
Router# show clock

.16:42:35.597 UTC Wed Nov 1 1999
```

Related Commands

Command	Description
clock set	Manually sets the system clock.
show calendar	Displays the calendar hardware setting.

show idb

To display information about the status of interface descriptor blocks (IDBs), use the **show idb** command in privileged EXEC mode.

show idb

Syntax Description

This command has nor arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1	This command was introduced.

Examples

The following is sample output from the **show idb** command:

```
Router# show idb

Maximum number of IDBs 4096

42 SW IDBs allocated (2440 bytes each)

40 HW IDBs allocated (5760 bytes each)
HWIDB#1   1   SRP0/0 (HW IFINDEX, SRP)
HWIDB#2   2   POS1/0 (HW IFINDEX, SONET, Serial)
HWIDB#3   7   FastEthernet3/0 (HW IFINDEX, Ether)
HWIDB#4   8   FastEthernet3/1 (HW IFINDEX, Ether)
HWIDB#5   9   FastEthernet3/2 (HW IFINDEX, Ether)
HWIDB#6   10  FastEthernet3/3 (HW IFINDEX, Ether)
HWIDB#7   11  FastEthernet3/4 (HW IFINDEX, Ether)
HWIDB#8   12  FastEthernet3/5 (HW IFINDEX, Ether)
HWIDB#9   13  FastEthernet3/6 (HW IFINDEX, Ether)
HWIDB#10  14  FastEthernet3/7 (HW IFINDEX, Ether)
HWIDB#11  15  POS4/0 (HW IFINDEX, SONET, Serial)
HWIDB#12  16  POS4/1 (HW IFINDEX, SONET, Serial)
HWIDB#13  17  POS4/2 (HW IFINDEX, SONET, Serial)
HWIDB#14  18  POS4/3 (HW IFINDEX, SONET, Serial)
HWIDB#15  19  GigabitEthernet6/0 (HW IFINDEX, Ether)
HWIDB#16  21  POS10/0 (HW IFINDEX, SONET, Serial)
HWIDB#17  22  POS11/0 (HW IFINDEX, SONET, Serial)
HWIDB#18  23  Loopback0 (HW IFINDEX)
HWIDB#19  24  Loopback1 (HW IFINDEX)
HWIDB#20  25  Tunnel100 (HW IFINDEX)
HWIDB#21  26  Tunnel909 (HW IFINDEX)
HWIDB#22  27  Ethernet0 (HW IFINDEX, Ether)
```

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 Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

Detailed descriptions of the information displayed by this command can be found in the NTP specification (RFC 1305).

The following is sample output from the **show ntp associations** command:

```
Router# show ntp associations

     address         ref clock     st  when  poll  reach  delay  offset    disp
 ~172.31.32.2      172.31.32.1       5    29  1024  377     4.2   -8.59     1.6
+~192.168.13.33    192.168.1.111     3    69   128  377     4.1    3.48     2.3
*~192.168.13.57    192.168.1.111     3    32   128  377     7.9   11.18     3.6
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

Table 109 describes significant fields shown in the display.

Table 109 show ntp associations Field Descriptions

Field	Description
(leading characters in display lines)	The first characters in a display line can be one or more of the following characters: * —Synchronized to this peer # —Almost synchronized to this peer + —Peer selected for possible synchronization - —Peer is a candidate for selection ~ —Peer is statically configured
address	Address of peer.
ref clock	Address of peer's reference clock.
st	Peer’s stratum.
when	Time since last NTP packet received from peer.

Table 109 show ntp associations Field Descriptions (continued)

Field	Description
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 following is sample output of the **show ntp associations detail** command:

```
Router# show ntp associations detail

172.31.32.2 configured, insane, invalid, stratum 5
ref ID 172.31.32.1, time AFE252C1.6DBDDFF2 (00:12:01.428 PDT Mon Jul 5 1993)
our mode active, peer mode active, our poll intvl 1024, peer poll intvl 64
root delay 137.77 msec, root disp 142.75, reach 376, sync dist 215.363
delay 4.23 msec, offset -8.587 msec, dispersion 1.62
precision 2**19, version 3
org time AFE252E2.3AC0E887 (00:12:34.229 PDT Mon Jul 5 1993)
rcv time AFE252E2.3D7E464D (00:12:34.240 PDT Mon Jul 5 1993)
xmt time AFE25301.6F83E753 (00:13:05.435 PDT Mon Jul 5 1993)
filtdelay =     4.23    4.14    2.41    5.95    2.37    2.33    4.26    4.33
filtoffset =   -8.59   -8.82   -9.91   -8.42  -10.51  -10.77  -10.13  -10.11
filterror =     0.50    1.48    2.46    3.43    4.41    5.39    6.36    7.34

192.168.13.33 configured, selected, sane, valid, stratum 3
ref ID 192.168.1.111, time AFE24F0E.14283000 (23:56:14.078 PDT Sun Jul 4 1993)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 83.72 msec, root disp 217.77, reach 377, sync dist 264.633
delay 4.07 msec, offset 3.483 msec, dispersion 2.33
precision 2**6, version 3
org time AFE252B9.713E9000 (00:11:53.442 PDT Mon Jul 5 1993)
rcv time AFE252B9.7124E14A (00:11:53.441 PDT Mon Jul 5 1993)
xmt time AFE252B9.6F625195 (00:11:53.435 PDT Mon Jul 5 1993)
filtdelay =     6.47    4.07    3.94    3.86    7.31    7.20    9.52    8.71
filtoffset =    3.63    3.48    3.06    2.82    4.51    4.57    4.28    4.59
filterror =     0.00    1.95    3.91    4.88    5.84    6.82    7.80    8.77

192.168.13.57 configured, our_master, sane, valid, stratum 3
ref ID 192.168.1.111, time AFE252DC.1F2B3000 (00:12:28.121 PDT Mon Jul 5 1993)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 125.50 msec, root disp 115.80, reach 377, sync dist 186.157
delay 7.86 msec, offset 11.176 msec, dispersion 3.62
precision 2**6, version 2
org time AFE252DE.77C29000 (00:12:30.467 PDT Mon Jul 5 1993)
rcv time AFE252DE.7B2AE40B (00:12:30.481 PDT Mon Jul 5 1993)
xmt time AFE252DE.6E6D12E4 (00:12:30.431 PDT Mon Jul 5 1993)
filtdelay =    49.21    7.86    8.18    8.80    4.30    4.24    7.58    6.42
filtoffset =   11.30   11.18   11.13   11.28    8.91    9.09    9.27    9.57
filterror =     0.00    1.95    3.91    4.88    5.78    6.76    7.74    8.71
```

Table 110 describes significant fields shown in the display.

Table 110 show ntp associations detail Field Descriptions

Field	Descriptions
configured	Peer was statically configured.
dynamic	Peer was dynamically discovered.
our_master	Local machine is synchronized to this peer.
selected	Peer is selected for possible synchronization.
candidate	Peer is a candidate for selection.
sane	Peer passes basic sanity checks.
insane	Peer fails basic sanity checks.
valid	Peer time is believed to be valid.
invalid	Peer time is believed to be invalid.
leap_add	Peer is signalling that a leap second will be added.
leap-sub	Peer is signalling that a leap second will be subtracted.
unsynced	Peer is not synchronized to any other machine.
ref ID	Address of machine peer is synchronized to.
time	Last time stamp peer received from its master.
our mode	Our mode relative to peer (active / passive / client / server / bdcast / bdcast client).
peer mode	Peer's mode relative to us.
our poll intvl	Our poll interval to peer.
peer poll intvl	Peer's poll interval to us.
root delay	Delay along path to root (ultimate stratum 1 time source).
root disp	Dispersion of path to root.
reach	Peer reachability (bit string in octal).
sync dist	Peer synchronization distance.
delay	Round trip delay to peer.
offset	Offset of peer clock relative to our clock.
dispersion	Dispersion of peer clock.
precision	Precision of peer clock in 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.

Related Commands

Command	Description
show ntp status	Shows the status of NTP.

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 Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show ntp status** command:

```
Router# show ntp status

Clock is synchronized, stratum 4, reference is 192.168.13.57
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**19
reference time is AFE2525E.70597B34 (00:10:22.438 PDT Mon Jul 5 1993)
clock offset is 7.33 msec, root delay is 133.36 msec
root dispersion is 126.28 msec, peer dispersion is 5.98 msec
```

Table 111 shows the significant fields in the display.

Table 111 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 the clock of this system (in Hz).
reference time	Reference time stamp.
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.

Related Commands

Command	Description
show ntp associations	Shows the status of NTP associations.

show registry

To show the function registry information, use the **show registry** EXEC command.

show registry [*registry-name* [*registry-num*] [**brief**]] [**brief** | **statistics**]

Syntax Description

registry-name	Name of the registry to examine.
registry-num	Number of the registry to examine.
brief	Displays limited functions and services information.
statistics	Displays function registry statistics.

Defaults

Brief

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.

Examples

The following example is sample output of the **show registry** command using the brief argument:

```
Switch# show registry atm 3/0/0 brief
Registry objects: 1799  bytes: 213412

--
Registry 23: ATM Registry
  Service 23/0:
  Service 23/1:
  Service 23/2:
  Service 23/3:
  Service 23/4:
  Service 23/5:
  Service 23/6:
  Service 23/7:
  Service 23/8:
  Service 23/9:
  Service 23/10:
  Service 23/11:
  Service 23/12:
  Service 23/13:
  Service 23/14:

--
RegistrY 25: ATM routing Registry
  Service 25/0:
```

show sntp

To show information about the Simple Network Time Protocol (SNTP), use the **show sntp** EXEC command on a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router.

show sntp

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Examples

The following is sample output from the **show sntp** command:

```
Router# show sntp

SNTP server     Stratum   Version    Last Receive
171.69.118.9       5         3        00:01:02
172.21.28.34       4         3        00:00:36    Synced  Bcast

Broadcast client mode is enabled.
```

Table 112 describes the fields show in this display.

Table 112 show sntp Field Descriptions

Field	Description
SNTP server	Address of the configured or broadcast NTP server.
Stratum	NTP stratum of the server. The stratum indicates how far away from an authoritative time source the server is.
Version	NTP version of the server.
Last Receive	Time since the last NTP packet was received from the server.
Synced	Indicates the server chosen for synchronization.
Bcast	Indicates a broadcast server.

Related Commands

Command	Description
sntp broadcast client	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use the SNTP to accept NTP traffic from any broadcast server.
sntp server	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use the SNTP to request and accept NTP traffic from a time server.

sntp broadcast client

To use the Simple Network Time Protocol (SNTP) to accept Network Time Protocol (NTP) traffic from any broadcast server, use the **sntp broadcast client** global configuration command to configure a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router. The **no** form of the command prevents the router from accepting broadcast traffic.

sntp broadcast client

no sntp broadcast client

Syntax Description

This command has no arguments or keywords.

Defaults

The router does not accept SNTP traffic from broadcast servers.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

SNTP is a compact, client-only version of the NTP. SNMP can only receive the time from NTP servers; it cannot be used to provide time services to other systems.

SNTP typically provides time within 100 milliseconds of the accurate time, but it does not provide the complex filtering and statistical mechanisms of NTP. In addition, SNTP does not authenticate traffic, although you can configure extended access lists to provide some protection.

You must configure the router with either this command or the **sntp server** command in order enable SNTP.

Examples

The following example enables the router to accept broadcast NTP packets and shows sample **show sntp** command output:

```
Router(config)# sntp broadcast client
Router(config)# end
Router#
%SYS-5-CONFIG: Configured from console by console
Router# show sntp

SNTP server     Stratum   Version    Last Receive
172.21.28.34       4         3        00:00:36    Synced  Bcast

Broadcast client mode is enabled.
```

Related Commands

Command	Description
show sntp	Displays information about the SNTP on a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router.
sntp server	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use the SNTP to request and accept NTP traffic from a time server.

sntp server

To configure a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, Cisco 1750, or Cisco 800 router to use the Simple Network Time Protocol (SNTP) to request and accept Network Time Protocol (NTP) traffic from a stratum 1 time server, use the **sntp server** global configuration command. The **no** form of the command removes a server from the list of NTP servers.

sntp server {*address* | *hostname*} [**version** *number*]

no sntp server {*address* | *hostname*}

Syntax Description

address	IP address of the time server.
hostname	Host name of the time server.
version *number*	(Optional) Version of NTP to use. The default is 1.

Defaults

The router does not accept SNTP traffic from a time server.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

SNTP is a compact, client-only version of the NTP. SNMP can only receive the time from NTP servers; it cannot be used to provide time services to other systems.

SNTP typically provides time within 100 milliseconds of the accurate time, but it does not provide the complex filtering and statistical mechanisms of NTP. In addition, SNTP does not authenticate traffic, although you can configure extended access lists to provide some protection.

Enter this command once for each NTP server.

You must configure the router with either this command or the **sntp broadcast client** command in order enable SNTP.

SNTP time servers should operate only at the root (stratum 1) of the subnet, and then only in configurations where no other source of synchronization other than a reliable radio or modem time service is available. A stratum 2 server cannot be used as an SNTP time server. The use of SNTP rather than NTP in primary servers should be carefully considered.

Examples

The following example enables the router to request and accept NTP packets from the server at 172.21.118.9 and shows sample **show sntp** command output:

```
Router(config)# sntp server 172.21.118.9
Router(config)# end
Router#
%SYS-5-CONFIG: Configured from console by console
Router# show sntp

SNTP server     Stratum   Version    Last Receive
172.21.118.9       5         3        00:01:02    Synced
```

Related Commands

Command	Description
show sntp	Shows information about the SNTP on a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router.
sntp broadcast client	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use the SNTP to accept NTP traffic from any broadcast server.

time-range

To enable time-range configuration mode and define time ranges for functions (such as extended access lists), use the **time-range** global configuration command. To remove the time limitation, use the **no** form of this command.

time-range *time-range-name*

no time-range *time-range-name*

Syntax Description

time-range-name	Desired name for the time range. The name cannot contain a space or quotation mark, and must begin with a letter.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.

Usage Guidelines

The **time-range** entries are identified by a name, which is referred to by one or more other configuration commands. Multiple time ranges can occur in a single access list or other feature.

After the **time-range** command, use the **periodic** command, the **absolute** command, or some combination of them to define when the feature is in effect. Multiple **periodic** commands are allowed in a time range; only one **absolute** command is allowed.

Note For Cisco IOS Release 12.1, IP and IPX extended access lists are the only functions that can use time-ranges. For further information on using these functions, see the *Cisco IOS 12.1 IP and IP Routing* and the *Cisco IOS 12.1 AppleTalk and Novell IPX* publications.

Note To avoid confusion, use different names for time ranges and named access lists.

Examples

The following example denies HTTP traffic on Monday through Friday between the hours of 8:00 a.m. and 6:00 p.m. The example allows UDP traffic on Saturday and Sunday from noon to midnight only.

```
time-range no-http
 periodic weekdays 8:00 to 18:00
!
time-range udp-yes
 periodic weekend 12:00 to 24:00
!
ip access-list extended strict
 deny tcp any any eq http time-range no-http
 permit udp any any time-range udp-yes
!
interface ethernet 0
 ip access-group strict in
```

Related Commands

Command	Description
absolute	Specifies an absolute start and end time for a time range.
ip access-list	Defines an IP access list by name.
periodic	Specifies a recurring (weekly) start and end time for a time range.
permit (IP)	Sets conditions under which a packet passes a named IP access list.