

Performing Basic System Management

This chapter describes the basic tasks that you can perform to manage the general system features of the Cisco IOS software—those features that are generally not specific to a particular protocol.

For a complete description of the basic system management commands in this chapter, refer to the “Basic System Management Commands” chapter of the *Configuration Fundamentals Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

Basic System Management Task List

This chapter describes the basic system management tasks you can perform. Perform any of the tasks in the following sections:

- Customize the Router Prompt
- Set the Router Name
- Create and Monitor Command Aliases
- Enable Minor Services
- Enable the Finger Protocol
- Hide Telnet Addresses
- Generate a Downward-Compatible Configuration
- Set Time and Calendar Services
- Delay EXEC Startup
- Handle Idle Telnet Connection

Refer to the “Basic System Management Examples” section at the end of this chapter for examples.

Customize the Router Prompt

By default, the prompt consists of the router name followed by an angle bracket (>) for EXEC mode or a pound sign (#) for privileged EXEC mode. To customize your prompt, perform the following task in global configuration mode:

Task	Command
Customize the prompt.	prompt <i>string</i>
Remove the configuration prompt (config).	no service prompt config

Set the Router Name

One of the first basic tasks is to name your router. The name is considered the host name and is the name that is displayed by the system prompt. If no name is configured, the system default name is `Router`. You can name the router in global configuration mode as follows:

Task	Command
Set the host name.	<code>hostname name</code>

For an example of configuring a router name, see the section “System Configuration File Example” at the end of this chapter.

Create and Monitor Command Aliases

You can create aliases for commonly used or complex commands. Use word substitutions or abbreviations to tailor command syntax for you and your user community.

To create and display command aliases, perform the tasks in the following sections:

- Create a Command Alias
- Display Command Aliases

Create a Command Alias

To create a command alias, perform the following task in global configuration mode:

Task	Command
Configure a command alias.	<code>alias mode alias-name alias-command-line</code>

Display Command Aliases

To display alias names and the original command syntax, perform the following task in EXEC mode:

Task	Command
Show all command aliases and original command syntax, or specify the aliases in a particular command mode.	<code>show aliases [mode]</code>

Enable Minor Services

You can access minor TCP, UDP, and BOOTP services available from hosts on the network. These services are disabled by default.

To enable these services, perform the following tasks in global configuration mode:

Task	Command
Access minor TCP services such as echo, chargen, discard, and daytime.	<code>service tcp-small-servers</code>
Access minor UDP services such as echo, chargen, and discard.	<code>service udp-small-servers</code>
Access the BOOTP service.	<code>ip bootp server</code>

Enable the Finger Protocol

You can enable the Finger protocol so that people throughout the network can get a list of the users currently using the router. The information displayed includes the processes running on the system, the line number, connection name, idle time, and terminal location. To enable the Finger protocol, perform the following task in global configuration mode:

Task	Command
Enable the Finger protocol requests.	service finger

Hide Telnet Addresses

You can hide addresses while attempting to establish a Telnet session. To configure the router to suppress Telnet addresses, perform the following task in global configuration mode:

Task	Command
Hide addresses while establishing a Telnet session.	service hide-telnet-address

The hide feature suppresses the display of the address and 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.

Use the **busy-message** command with the **service hide-telnet-address** command to customize the information displayed during Telnet connection attempts. If the connection attempt is not successful, the router suppresses the address and displays the message specified with the **busy-message** command.

Generate a Downward-Compatible Configuration

In Cisco IOS Release 10.3, IP access lists changed format. If you decide to downgrade from Release 11.0 to Release 10.2, you can configure the software to regenerate a configuration in the format of Release 10.2, thereby saving time and making your IP access lists compatible with the software.

To have the software regenerate a configuration in the format prior to Release 10.3, perform the following task in global configuration mode:

Task	Command
Generate a backward-compatible configuration.	downward-compatible-config <i>version</i>

Set Time and Calendar Services

All Cisco routers provide an array of time-of-day services. These services allow the products to accurately keep track of the current time and date, to synchronize multiple products to the same time, and to provide time services to other systems. The following sections describe the time and calendar tasks:

- Understand Time Sources
- Configure NTP
- Configure Sntp

- Configure VINES Time Service
- Configure Time and Date Manually
- Monitor Time and Calendar Services

Understand Time Sources

The heart of the time service is the system clock. This clock runs from the moment the system starts up and keeps track of the current date and time. The system clock can be set from a number of sources and in turn can be used to distribute the current time through various mechanisms to other systems. When a router with a system calendar is initialized, the system clock is set based on the time in the internal battery-powered calendar; on other models, the system clock is set to midnight on March 1, 1993. The system clock can then be set from the following sources:

- Network Time Protocol (NTP)
- Simple Network Time Protocol (SNTP)
- VINES Time Service
- Manual configuration

The system clock can provide time to the following services:

- NTP
- VINES Time Service
- User **show** commands
- Logging and debugging messages

Note The system clock cannot provide time to the NTP or VINES Time Service if it was set using SNTP.

The system clock keeps track of time internally based on Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT). You can configure information about the local time zone and summer time (daylight savings time) so that the time is displayed correctly relative to the local time zone.

The system clock keeps track of whether the time is “authoritative” or not (that is, whether it has been set by a time source considered to be authoritative). If it is not authoritative, the time will be available only for display purposes and will not be redistributed.

Network Time Protocol

The Network Time Protocol (NTP) is a protocol designed to time-synchronize a network of machines. NTP runs over UDP, which in turn runs over IP. NTP is documented in RFC 1305.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of one another.

NTP uses the concept of a “stratum” to describe how many NTP “hops” away a machine is from an authoritative time source. A “stratum 1” time server has a radio or atomic clock directly attached, a “stratum 2” time server receives its time via NTP from a “stratum 1” time server, and so on. A machine running NTP will automatically choose as its time source the machine with the lowest stratum number that it is configured to communicate with via NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP is careful to avoid synchronizing to a machine whose time may not be accurate. It avoids doing so in two ways. First of all, NTP will never synchronize to a machine that is not in turn synchronized itself. Secondly, NTP will compare the time reported by several machines, and will not synchronize to a machine whose time is significantly different than the others, even if its stratum is lower.

The communications between machines running NTP (known as “associations”) are usually statically configured; each machine is given the IP address of all machines with which it should form associations. Accurate timekeeping is made possible by exchanging NTP messages between each pair of machines with an association. However, in a local-area network (LAN) environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each machine can simply be configured to send or receive broadcast messages. However, the accuracy of timekeeping is marginally reduced because the information flow is one-way only.

The time kept on a machine is a critical resource, so we strongly recommend that you use the security features of NTP to avoid the accidental or malicious setting of incorrect time. Two mechanisms are available: an access list-based restriction scheme and an encrypted authentication mechanism.

Cisco’s implementation of NTP does not support stratum 1 service; in other words, it is not possible to connect to a radio or atomic clock. It is recommended that time service for your network be derived from the public NTP servers available in the IP Internet. If the network is isolated from the Internet, Cisco’s implementation of NTP allows a machine to be configured so that it acts as though it is synchronized via NTP, when in fact it has determined the time using other means. Other machines then synchronize to that machine via NTP.

When multiple sources of time (VINES, system calendar, manual configuration) are available, NTP is always considered to be more authoritative. NTP time overrides the time set by any other method.

A number of manufacturers include NTP software for their host systems, and a publicly available version for systems running UNIX and its various derivatives is also available. This software allows host systems to be time-synchronized as well.

Simple Network Time Protocol (SNTP)

Simple Network Time Protocol (SNTP) is a simplified, client-only version of NTP for use on Cisco 1003, Cisco 1004, and Cisco 1005 routers. SNTP 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. An SNTP client is more vulnerable to misbehaving servers than an NTP client and should only be used in situations where strong authentication is not required.

You can configure SNTP to request and accept packets from configured servers or to accept NTP broadcast packets from any source. When multiple sources are sending NTP packets, the server with the best stratum is selected. (See the “Network Time Protocol” section for a description of strata.) If multiple servers are at the same stratum, a configured server is preferred over a broadcast server. If

multiple servers pass both tests, the first one to send a time packet is selected. SNTP will only choose a new server if it stops receiving packets from the currently selected server, or if a better server (according to the above criteria) is discovered.

VINES Time Service

Time service is also available when Banyan VINES is configured. This protocol is a standard part of VINES. Cisco's implementation allows the VINES time service to be used in two ways. First, if the system has learned the time from some other source, it can act as a VINES time server and provide time to other machines running VINES. It also can use the VINES time service to set the system clock if no other form of time service is available.

Calendar System

Some routers contain a battery-powered calendar system that tracks the date and time across system restarts and power outages. This calendar system is always used to initialize the system clock when the system is restarted. It can also be considered to be an authoritative source of time and be redistributed via NTP or VINES time service if no other source is available. Furthermore, if NTP is running, the calendar can be periodically updated from NTP, compensating for the inherent drift in the calendar time.

Configure NTP

NTP services are enabled on all interfaces by default. The optional tasks you can perform are documented in the following sections:

- Configure NTP Authentication
- Configure NTP Associations
- Configure NTP Broadcast Service
- Configure NTP Access Restrictions
- Configure the Source IP Address for NTP Packets
- Configure the System as an Authoritative NTP Server
- Configure NTP to Update the Calendar

Configure NTP Authentication

If you want to authenticate the associations with other systems for security purposes, perform the tasks that follow. The first task enables the NTP authentication feature. The second task defines each of the authentication keys. Each key has a key number, a type, and a value. Currently the only key type supported is **md5**. Third, a list of "trusted" authentication keys is defined. If a key is trusted, this system will be ready to synchronize to a system that uses this key in its NTP packets.

To configure NTP authentication, perform the following tasks in global configuration mode:

Task	Command
Step 1 Enable the NTP authentication feature.	ntp authenticate
Step 2 Define the authentication keys.	ntp authentication-key <i>number md5 value</i>
Step 3 Define trusted authentication keys.	ntp trusted-key <i>key-number</i>

Configure NTP Associations

An NTP association can be a peer association (meaning that this system is willing to either synchronize to the other system or to allow the other system to synchronize to it), or it can be a server association (meaning that only this system will synchronize to the other system, and not the other way around). If you want to form an NTP association with another system, perform one of the following tasks in global configuration mode:

Task	Command
Form a peer association with another system.	ntp peer <i>ip-address</i> [version <i>number</i>] [key <i>keyid</i>] [source <i>interface</i>] [prefer]
Form a server association with another system.	ntp server <i>ip-address</i> [version <i>number</i>] [key <i>keyid</i>] [source <i>interface</i>] [prefer]

Note that only one end of an association needs to be configured; the other system will automatically establish the association.

See the example entitled “Clock, Calendar, and NTP Configuration Examples” at the end of this chapter.

Configure NTP Broadcast Service

The system can either send broadcast packets or listen to them on an interface-by-interface basis. The estimated round-trip delay for broadcast packets can also be configured. Perform one or more of the following tasks in global configuration mode if you want to use NTP’s broadcast feature:

Task	Command
Send NTP broadcast packets.	ntp broadcast [version <i>number</i>]
Receive NTP broadcast packets.	ntp broadcast client
Adjust estimated delay.	ntp broadcastdelay <i>microseconds</i>

See the example entitled “Clock, Calendar, and NTP Configuration Examples” at the end of this chapter.

Configure NTP Access Restrictions

You can control NTP access on two levels by completing the tasks in the following sections:

- Create an Access Group and Assign a Basic IP Access List to It
- Disable NTP Services on a Specific Interface

Create an Access Group and Assign a Basic IP Access List to It

To control access to NTP services, you can create an NTP access group and apply a basic IP access list to it. To do so, perform the following task in global configuration mode:

Task	Command
Create an access group and apply a basic IP access list to it.	ntp access-group { query-only serve-only serve peer } <i>access-list-number</i>

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

- 1 Peer—Allows time requests and NTP control queries and allows the system to synchronize itself to a system whose address passes the access list criteria.
- 2 Serve—Allows time requests and NTP control queries, but does not allow the system to synchronize itself to a system whose address passes the access list criteria.
- 3 Serve-only—Allows only time requests from a system whose address passes the access list criteria.
- 4 Query-only—Allows only NTP control queries from a system whose address passes the access list criteria.

If the source IP address matches the access lists for more than one access type, the first type is granted. If no access groups are specified, all access types are granted to all systems. If any access groups are specified, only the specified access types will be granted.

For details on NTP control queries, see RFC 1305 (NTP version 3).

Disable NTP Services on a Specific Interface

NTP services are enabled on all interfaces by default. You can disable NTP packets from being received through an interface by performing the following task in interface configuration mode:

Task	Command
Disable NTP services on a specific interface.	ntp disable

Configure the Source IP Address for NTP Packets

When the system sends an NTP packet, the source IP address is normally set to the address of the interface through which the NTP packet is sent. Perform the following task in global configuration mode if you want to configure a specific interface from which the IP source address will be taken:

Task	Command
Configure an interface from which the IP source address will be taken.	ntp source <i>interface</i>

This interface will be used for the source address for all packets sent to all destinations. If a source address is to be used for a specific association, use the **source** parameter on the **ntp peer** or **ntp server** command shown earlier in this chapter.

Configure the System as an Authoritative NTP Server

Perform the following task in global configuration mode if you want the system to be an authoritative NTP server, even if the system is not synchronized to an outside time source:

Task	Command
Make the system an authoritative NTP server.	ntp master [<i>stratum</i>]



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

For an example of configuring an authoritative NTP server, see the section “Clock, Calendar, and NTP Configuration Examples” at the end of this chapter.

Configure NTP to Update the Calendar

On systems which have calendars, you can configure NTP to periodically update the calendar.

Perform the following task in global configuration mode if the system is synchronized to an outside time source via NTP and you want the calendar to be synchronized periodically to NTP time:

Task	Command
Configure NTP to update the calendar.	ntp update-calendar

For an example of configuring NTP to update the calendar, see the section “Clock, Calendar, and NTP Configuration Examples” at the end of this chapter.

Configure SNTP

SNTP is disabled by default. In order to enable SNTP on a Cisco 1003, Cisco 1004, or Cisco 1005 router, perform one or both of the following tasks in global configuration mode:

Task	Command
Configure SNTP to request NTP packets from an NTP server.	sntp server { <i>address hostname</i> } [version number]
Configure SNTP to accept NTP packets from any NTP broadcast server.	sntp broadcast client

Enter the **sntp server** command once for each NTP server. The NTP servers must be configured to respond to the SNTP messages from the router.

If you enter both the **sntp server** command and the **sntp broadcast client** command, the router will accept time from a broadcast server but prefers time from a configured server, assuming the strata are equal.

To display information about SNTP, use the **show sntp EXEC** command.

Configure VINES Time Service

Perform the following task in global configuration mode if you want to distribute the system clock to other VINES systems:

Task	Command
Distribute the system clock to other VINES systems.	vines time use-system

To receive VINES time service to control the system clock, perform the following task in global configuration mode:

Task	Command
Receive VINES time service.	vines time set-system

Configure Time and Date Manually

If no other source of time is available, you can manually configure the current time and date after the system is restarted. The time will remain accurate until the next system restart. We recommend that you use manual configuration only as a last resort.

To set up time services, complete the tasks in the following sections as needed. If you have an outside source to which the router can synchronize, you do not need to manually set the system clock.

- Configure the Time Zone
- Configure Summer Time (Daylight Savings Time)
- Set the System Clock
- Set the System Calendar

Configure the Time Zone

Complete the following task in global configuration mode to manually configure the time zone used by the Cisco IOS software:

Task	Command
Set the time zone.	clock timezone <i>zone hours [minutes]</i>

For an example of configuring the time zone, see the section “Clock, Calendar, and NTP Configuration Examples” at the end of this chapter.

Configure Summer Time (Daylight Savings Time)

To configure summer time (daylight savings time) in areas where it starts and ends on a particular day of the week each year, perform the following task in global configuration mode:

Task	Command
Configure summer time.	clock summer-time <i>zone recurring [week day month hh:mm week day month hh:mm [offset]]</i>

If summer time in your area does not follow this pattern, you can configure the exact date and time of the next summer time events by performing one of the following tasks in global configuration mode:

Task	Command
Configure summer time.	clock summer-time <i>zone date month date year hh:mm month date year hh:mm [offset]</i>
	or
	clock summer-time <i>zone date date month year hh:mm date month year hh:mm [offset]</i>

For an example of configuring summer time, see the section “Clock, Calendar, and NTP Configuration Examples” at the end of this chapter.

Set the System Clock

If you have an outside source on the network that provides time services (such as an NTP server or VINES time service), you do not need to manually set the system clock.

However, if you do not have any time service source, complete one of the following tasks in EXEC mode to set the system clock:

Task	Command
Set the system clock.	clock set <i>hh:mm:ss date month year</i>
	or
	clock set <i>hh:mm:ss month date year</i>

Set the System Calendar

Some routers have a separate system calendar in addition to the system clock. The calendar can set the system time and control the system clock, as well as enable the router to act as a time service for the network.

You can complete the tasks in the following sections to enable the calendar capabilities:

- Set the Router Calendar
- Set the Router as a Network Time Source
- Set the System Clock from the Calendar
- Set the Calendar from the System Clock

Set the Router Calendar

The calendar maintains time separately from the system clock. It continues to run when the system is restarted or power is turned off. Typically, it only needs to be manually set once, when the system is first installed. If time is available from an external source using NTP, the calendar can be updated from the system clock instead.

If you do not have an external time source, perform the following task in EXEC mode to set the system calendar:

Task	Command
Set the calendar.	calendar set <i>hh:mm:ss day month year</i>
	or
	calendar set <i>hh:mm:ss month day year</i>

Set the Router as a Network Time Source

Although the system clock is always initialized from the calendar when the system is restarted, by default it is not considered to be authoritative and so will not be redistributed with NTP or VINES Time Service. To make the calendar be authoritative, complete the following task in global configuration mode:

Task	Command
Enable the router to act as a valid time source to which network peers can synchronize.	clock calendar-valid

For an example of making the calendar authoritative, see the section “Clock, Calendar, and NTP Configuration Examples” at the end of this chapter.

Set the System Clock from the Calendar

To set the system clock to the new calendar setting, perform the following task in EXEC mode:

Task	Command
Set the system clock from the calendar.	clock read-calendar

Set the Calendar from the System Clock

To update the calendar with the new clock setting, perform the following task in EXEC mode:

Task	Command
Set the calendar from the system clock.	clock update-calendar

Monitor Time and Calendar Services

To monitor clock, calendar, and NTP EXEC services, complete the following tasks in EXEC mode:

Task	Command
Display the current calendar time.	show calendar
Display the current system clock time.	show clock [detail]
Show the status of NTP associations.	show ntp associations [detail]
Show the status of NTP.	show ntp status
Display information about SNTP (Cisco 1003, Cisco 1004, and Cisco 1005 only).	show sntp

Delay EXEC Startup

You can delay the startup of the EXEC on noisy lines until the line has been idle for 3 seconds. To do so, perform the following task in global configuration mode:

Task	Command
Delay startup of the EXEC.	service exec-wait

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 might be interpreted as usernames and passwords, causing authentication failure before the user can type a username/password. The command is not useful on nonmodem lines or lines without some kind of login configured.

Handle Idle Telnet Connection

You can configure the Cisco IOS software to set the TCP window to zero (0) when the Telnet connection is idle. To do so, perform the following task in global configuration mode:

Task	Command
Set the TCP window to zero when the Telnet connection is idle.	service telnet-zero-idle

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.

Basic System Management Examples

The following sections provide system management examples:

- System Configuration File Example
- Clock, Calendar, and NTP Configuration Examples

System Configuration File Example

The following is an example of a typical system configuration file:

```

! Define line password
line 0 4
  password secret
  login
!
! Define privileged-level password
enable-password Secret Word
!
! Define a system hostname
hostname TIP
! Specify a configuration file to load at system startup
boot host host1-config 192.168.1.111
boot host host2-config 192.168.1.111
! Specify the system image to boot at startup
boot system sys1-system 192.168.13.111
boot system sys2-system 192.168.1.111
boot system rom
!
! Enable SNMP
snmp-server community red
snmp-server enable traps snmp authentication
snmp-server host 192.168.1.27 public
snmp-server host 192.168.1.111 public
snmp-server host 192.168.2.63 public
!
! Define TACACS server hosts
tacacs-server host 192.168.1.27
tacacs-server host 192.168.13.33
tacacs-server host 192.168.1.33
!

```

```
! Define a message-of-the-day banner
banner motd ^C
The Information Place welcomes you

Please call 1-800-555-2222 for a login account, or enter
your password at the prompt.
^C
```

Clock, Calendar, and NTP Configuration Examples

In the following example, a router with a system calendar has server associations with two other systems, transmits broadcast NTP packets, periodically updates the calendar, and redistributes time into VINES:

```
clock timezone PST -8
clock summer-time PDT recurring
ntp update-calendar
ntp server 192.168.13.57
ntp server 192.168.11.58
interface Ethernet 0/0
 ntp broadcast
vines time use-system
```

In the following example, a router with a calendar has no outside time source, so it uses the calendar as an authoritative time source and distributes the time via NTP broadcast packets.

```
clock timezone MET 2
clock calendar-valid
ntp master
interface fddi 0/0
 ntp broadcast
```