



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 in the “Cisco IOS System Management Commands” part 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:

- Customizing the Router Prompt
- Setting the Router Name
- Creating and Monitoring Command Aliases
- Accessing Services
- Enabling the Finger Protocol
- Hiding Telnet Addresses
- Setting Time and Calendar Services
- Setting Time and Calendar Services
- Delaying EXEC Startup
- Handling Idle Telnet Connection
- Setting the Interval for Load Data
- Limiting TCP Transactions
- Configuring Switching and Scheduling Priorities
- Modifying the System Buffer Size

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

Customizing 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, use either of the following commands in global configuration mode:

Command	Purpose
<code>prompt string</code>	Customizes the prompt.
<code>no service prompt config</code>	Removes the configuration prompt (config).

Setting the Router Name

One of the first basic commands 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`. To name the router, use the following command in global configuration mode:

Command	Purpose
<code>hostname name</code>	Sets the host name.

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

Creating and Monitoring 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:

- Creating a Command Alias
- Displaying Command Aliases

Creating a Command Alias

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

Command	Purpose
<code>alias mode alias-name alias-command-line</code>	Configures a command alias.

Displaying Command Aliases

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

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

Accessing Services

You can access TCP, UDP, and BOOTP services (sometimes called *minor services*) from hosts on the network. The TCP and UDP services are disabled by default. The BOOTP service is enabled by default.

To enable the TCP and UDP services or disable the BOOTP service, use any of the following commands in global configuration mode:

Command	Purpose
<code>service tcp-small-servers</code>	Accesses minor TCP services such as echo, chargen, discard, and daytime.
<code>service udp-small-servers</code>	Accesses minor UDP services such as echo, chargen, and discard.
<code>no ip bootp server</code>	Disables the BOOTP server.

Enabling 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, use the following command in global configuration mode:

Command	Purpose
<code>service finger</code>	Enables the Finger protocol requests.

Hiding Telnet Addresses

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

Command	Purpose
<code>service hide-telnet-address</code>	Hides addresses while establishing a Telnet session.

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.

Setting 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:

- Understanding Time Sources
- Configuring NTP
- Configuring SNTP
- Configuring VINES Time Service
- Configuring Time and Date Manually
- Monitoring Time and Calendar Services

Understanding Time Sources

Most Cisco routers have two clocks: a battery-powered system calendar in the hardware and a software system clock. These two clocks are managed separately.

The heart of the time service is the software-based 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 or rebooted, the system clock is set based on the time in the internal battery-powered system calendar. 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:

- access lists
- 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 typically 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 (for some specific platforms however, you can connect a GPS timesource device). 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, Cisco 1005, Cisco 1600, Cisco 1720, and Cisco 1750 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.

System Calendar (Hardware Clock)

Some routers contain a battery-powered hardware-based system calendar (hardware clock) that tracks the date and time across system restarts and power outages. The system calendar is always used to initialize the system clock (software clock) when the system is restarted.

The system calendar 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 system calendar can be updated periodically from NTP, compensating for the inherent drift in the calendar time.

Configuring NTP

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

- Configuring NTP Authentication
- Configuring NTP Associations
- Configuring NTP Broadcast Service
- Configuring NTP Access Restrictions

- Configuring the Source IP Address for NTP Packets
- Configuring the System as an Authoritative NTP Server
- Configuring NTP to Update the Calendar

Configuring NTP Authentication

If you want to authenticate the associations with other systems for security purposes, use the commands that follow. The first command enables the NTP authentication feature. The second command 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, use the following commands in global configuration mode:

	Command	Purpose
Step 1	<code>ntp authenticate</code>	Enables the NTP authentication feature.
Step 2	<code>ntp authentication-key number md5 value</code>	Defines the authentication keys.
Step 3	<code>ntp trusted-key key-number</code>	Defines trusted authentication keys.

Configuring 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, use one of the following commands in global configuration mode:

Command	Purpose
<code>ntp peer ip-address [normal-sync] [version number] [key keyid] [source interface] [prefer]</code>	Forms a peer association with another system.
<code>ntp server ip-address [version number] [key keyid] [source interface] [prefer]</code>	Forms a server association with another system.

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

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

Configuring 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. Use one or more of the following commands in global configuration mode if you want to use NTP's broadcast feature:

Command	Purpose
<code>ntp broadcast [version number]</code>	Sends NTP broadcast packets.
<code>ntp broadcast client</code>	Receives NTP broadcast packets.
<code>ntp broadcastdelay microseconds</code>	Adjusts estimated delay.

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

Configuring NTP Access Restrictions

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

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

Creating 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, use the following command in global configuration mode:

Command	Purpose
<code>ntp access-group {query-only serve-only serve peer} access-list-number</code>	Creates an access group and applies a basic IP access list to it.

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).

Disabling 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 using the following command in interface configuration mode:

Command	Purpose
<code>ntp disable</code>	Disables NTP services on a specific interface.

Configuring 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. Use the following command in global configuration mode if you want to configure a specific interface from which the IP source address will be taken:

Command	Purpose
<code>ntp source interface</code>	Configures an interface from which the IP source address will be taken.

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.

Configuring the System as an Authoritative NTP Server

Use the following command 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:

Command	Purpose
<code>ntp master [stratum]</code>	Makes the system an authoritative NTP server.



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.

Configuring NTP to Update the Calendar

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

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

Command	Purpose
<code>ntp update-calendar</code>	Configures NTP to update the 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.

Configuring SNTP

SNTP is disabled by default. In order to enable SNTP on a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router, use one or both of the following commands in global configuration mode:

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

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.

Configuring VINES Time Service

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

Command	Purpose
<code>vines time use-system</code>	Distributes the system clock to other VINES systems.

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

Command	Purpose
<code>vines time set-system</code>	Receives VINES time service.

Configuring 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.

- Configuring the Time Zone
- Configuring Summer Time (Daylight Savings Time)

- Setting Time and Calendar Services

Configuring the Time Zone

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

Command	Purpose
<code>clock timezone zone hours-offset [minutes-offset]</code>	Sets the time zone. The <i>zone</i> argument is the name of the timezone (typically a standard acronym). The <i>hours-offset</i> argument is the number of hours the timezone is different from UTC. The <i>minutes-offset</i> argument is the number of minutes the timezone is different from UTC.



Tips

The *minutes-offset* argument of the **clock timezone** command is available for those cases where a local timezone is percentage of an hour different from Greenwich Mean Time/Coordinated Universal Time (UTC/GMT). For example, the timezone for some sections of Atlantic Canada (AST) is UTC -3.5. In this case, the necessary command would be **clock timezone AST -3 30**.

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

Configuring 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, use the following command in global configuration mode:

Command	Purpose
<code>clock summer-time zone recurring [week day month hh:mm week day month hh:mm [offset]]</code>	Configures summer time.

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 using one of the following commands in global configuration mode:

Command	Purpose
<code>clock summer-time zone date month date year hh:mm month date year hh:mm [offset]</code>	Configures summer time.
or	
<code>clock summer-time zone date date month year hh:mm date month year hh:mm [offset]</code>	

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

Setting the System Clock

Some routers have a separate hardware-based system calendar in addition to the software-based system clock. The system 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 system calendar capabilities:

Command	Purpose
<code>clock set hh:mm:ss date month year</code>	Sets the system clock. Performed in privileged EXEC mode.
or	
<code>clock set hh:mm:ss month date year</code>	

Using the System Calendar

Some routers have a separate hardware-based system calendar in addition to the software-based system clock. The system 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:

- Setting the Router Calendar
- Setting the Router as a Network Time Source
- Setting the Clock from the Calendar
- Setting the Calendar from the Clock

Setting the Router Calendar

The system 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 system calendar can be updated from the system clock instead.

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

Command	Purpose
<code>calendar set hh:mm:ss day month year</code>	Sets the system calendar.
or	
<code>calendar set hh:mm:ss month day year</code>	

Setting the Router as a Network Time Source

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

Command	Purpose
<code>clock calendar-valid</code>	Enables the router to act as a valid time source to which network peers can synchronize.

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

Setting the Clock from the Calendar

To set the system clock to the new system calendar setting, use the following command in EXEC mode:

Command	Purpose
<code>clock read-calendar</code>	Sets the system clock from the system calendar.

Setting the Calendar from the Clock

To update the system calendar with the new system clock setting, use the following command in EXEC mode:

Command	Purpose
<code>clock update-calendar</code>	Sets the system calendar from the system clock.

Monitoring Time and Calendar Services

To monitor clock, calendar, and NTP EXEC services, use any of the following commands in EXEC mode:

Command	Purpose
<code>show calendar</code>	Displays the current system calendar time.
<code>show clock [detail]</code>	Displays the current system clock time.
<code>show ntp associations [detail]</code>	Shows the status of NTP associations.
<code>show ntp status</code>	Shows the status of NTP.
<code>show sntp</code>	Displays information about SNTP (Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 only).

Configuring Time Ranges

Cisco IOS allows implementation of features based on what time of the day it is. The **time-range** command defines specific times of the day and week, which then can be referenced by a function, so that those time restrictions are imposed on the function itself.

In Cisco IOS Release 12.1, IP and IPX extended access lists are the only functions that can use time ranges. The time range allows the network administrator to define when the **permit** or **deny** statements in the access list are in effect. Prior to this feature, access list statements were always in effect once they were applied. Both named or numbered access lists can reference a time range.

Benefits of time ranges include the following:

- The network administrator has more control over permitting or denying a user access to resources. These resources could be an application (identified by an IP address/mask pair and a port number), policy routing, or an on-demand link (identified as interesting traffic to the dialer).
- Network administrators can set time-based security policy, including:
 - Perimeter security using the Cisco IOS Firewall feature set or access lists
 - Data confidentiality with Cisco Encryption Technology or IPSEC
- Policy-based routing and queuing functions are enhanced.
- When provider access rates vary by time of day, it is possible to automatically reroute traffic cost effectively.
- Service providers can dynamically change a Committed Access Rate (CAR) configuration to support the quality of service (QoS) Service Level Agreements (SLAs) that are negotiated for certain times of day.
- Network administrators can control logging messages. Access list entries can log traffic at certain times of the day, but not constantly. Therefore, administrators can simply deny access without having to analyze many logs generated during peak hours.

Defining a Time Range



Note

The time range relies on the router's system clock. For this feature to work the way you intend, you need a reliable clock source. It is recommended that you use Network Time Protocol (NTP) to synchronize the router clock.

To define a time range, use the following commands beginning in global configuration mode.

	Command	Purpose
Step 1	Router(config)# time-range <i>time-range-name</i>	Identifies the time-range by a meaningful name and enters time-range configuration mode.
Step 2	Router(config-time-range)# absolute [start <i>time date</i>] [end <i>time date</i>] or Router(config-time-range)# periodic <i>days-of-the-week</i> <i>hh:mm</i> to [<i>days-of-the-week</i>] <i>hh:mm</i>	Specifies when the function it will be applied to will be in effect. Use some combination of these commands; multiple periodic statements are allowed; only one absolute statement is allowed.

Repeat these tasks if you have multiple items you want in effect at different times. For example, repeat the steps to include multiple **permit** or **deny** statements in an access list in effect at different times. For further details on the above commands, see the corresponding chapter in the *Cisco IOS Configuration Fundamentals Command Reference*.

Referencing the Time Range

In order for a time range to be applied, you must reference it by name in a feature that can implement time ranges. To reference the time range, perform one of the following tasks:

- Creating an IP Extended Access List
 - Refer to the “Configuring IP Services” chapter in the *Cisco IOS 12.1 IP and IP Routing Configuration Guide* for instructions and further details.
- Creating an IPX Extended Access List
 - Refer to the “Configuring Novell IPX” chapter of the *Cisco IOS 12.1 Apple Talk and Novell IPX Configuration Guide* for instructions and further details.

Delaying 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, use the following command in global configuration mode:

Command	Purpose
<code>service exec-wait</code>	Delays startup of the EXEC.

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.

Handling 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, use the following command in global configuration mode:

Command	Purpose
<code>service telnet-zero-idle</code>	Sets the TCP window to zero when the Telnet connection is 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.

Setting the Interval for Load Data

You can change the period of time over which a set of data is used for computing load statistics. Decisions, such as dial backup decisions, are dependent on these statistics. If you decrease the load interval, the average statistics are computed over a shorter period of time and are more responsive to bursts of traffic.

To change the length of time for which a set of data is used to compute load statistics, use the following command in interface configuration mode:

Command	Purpose
<code>load-interval seconds</code>	Sets the length of time for which data is used for load calculations.

Limiting TCP Transactions

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

John Nagle's algorithm (RFC 896) helps alleviate the small-packet problem in TCP. 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 good for all TCP-based traffic. However, do not enable the Nagle slow packet avoidance algorithm if you have XRemote users on X Window sessions.

By default, the Nagle algorithm is not enabled. To enable the Nagle algorithm and thereby reduce TCP transactions, use the following command in global configuration mode:

Command	Purpose
<code>service nagle</code>	Enables the Nagle slow packet avoidance algorithm.

Configuring Switching and Scheduling Priorities

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, you might need to give priority to the system process scheduler. To do so, use the following command in global configuration mode:

Command	Purpose
<code>scheduler interval milliseconds</code>	Defines the maximum amount of time that can elapse without running the lowest-priority system processes.

To change the amount of time that the CPU spends on fast switching and process level operations on the Cisco 7200 series and Cisco 7500 series, use the following command in global configuration mode:

Command	Purpose
<code>scheduler allocate network-microseconds process-microseconds</code>	For the Cisco 7200 series and Cisco 7500 series, changes the default time the CPU spends on process tasks and fast switching.



Caution Cisco recommends that you do not change the default values of the **scheduler allocate** command.

To configure the characteristics for a looping process, use the following command in global configuration mode:

Command	Purpose
<code>scheduler process-watchdog {hang normal reload terminate}</code>	Configures an action for a looping process.

Modifying the System Buffer Size

You can adjust initial buffer pool settings and the limits at which temporary buffers are created and destroyed. To do so, use either of the following commands in global configuration mode:

Command	Purpose
<code>buffers {small middle big verybig large huge type number} {permanent max-free min-free initial} number</code>	Adjusts the system buffer sizes.
<code>buffers huge size number</code>	Dynamically resizes all huge buffers to the value that you supply.



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

During normal system operation, there are two sets of buffer pools: public and interface.

- The buffers in the public pools grow and shrink based upon demand. Some public pools are temporary and are created and destroyed as needed. Other public pools are permanently allocated and cannot be destroyed. The public buffer pools are small, middle, big, large, very big, and huge.
- Interface pools are static—that is, they are all permanent. One interface pool exists for each interface. For example, a Cisco 4000 1E 4T configuration has one Ethernet buffer pool and four serial buffer pools. In the **buffers** command, the *type* and *number* arguments allow the user to tune the interface pools.

See the section “Buffer Modification Examples” at the end of this chapter.

The server has one pool of queueing elements and six public pools of packet buffers of different sizes. For each pool, the server keeps count of the number of buffers outstanding, the number of buffers in the free list, and the maximum number of buffers allowed in the free list. To display statistics about the buffer pool on the system, use any of the following commands in EXEC mode:

Command	Purpose
<code>show buffers</code>	Displays all public pool information.
<code>show buffers address <i>hex-addr</i></code>	Displays buffer information for an address.
<code>show buffers all [dump header packet]</code>	Displays all public and interface pool information.
<code>show buffers assigned [dump header packet]</code>	Displays a listing of all buffers in use.
<code>show buffers failures [dump header packet]</code>	Displays buffer allocation failures
<code>show buffers free [dump header packet]</code>	Displays buffers available for use
<code>show buffers old [dump header packet]</code>	Displays buffers older than one minute.
<code>show buffers input-interface <i>interface-type identifier</i></code>	Displays buffer information for an input interface.
<code>show buffers pool <i>pool name</i></code>	Displays all interface pool information.

Basic System Management Examples

The following sections provide system management examples:

- System Configuration File Example
- Clock, Calendar, and NTP Configuration Examples
- Buffer Modification 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 system 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
```

Buffer Modification Examples

The following example instructs the system to keep at least 50 small buffers free:

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

The following example instructs the system to keep no more than 200 medium buffers free:

```
buffers middle max-free 200
```

The following example instructs the system to create one large temporary extra buffer, just after a reload:

```
buffers large initial 1
```

The following example instructs the system to create one permanent huge buffer:

```
buffers huge permanent 1
```