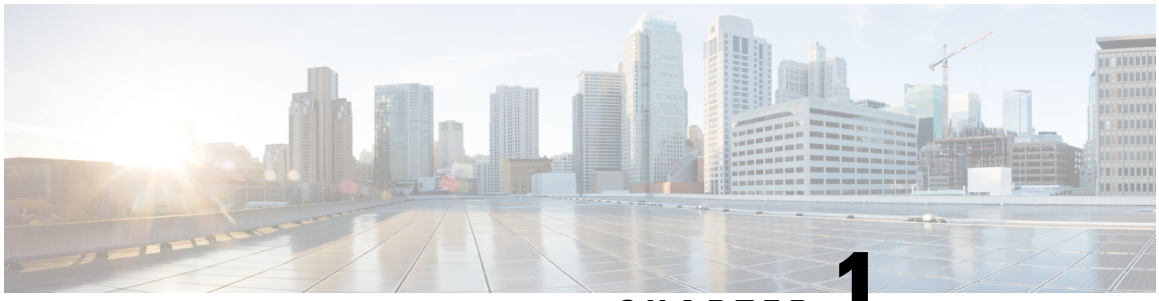
Basic System Management Configuration Guide, Cisco IOS XE 17 (Cisco ASR 920 Series)

First Published: 2019-11-14

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Performing Basic System Management

This module 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.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Performing Basic System Management

System Name

The system name, also called the hostname, is used to uniquely identify the system in your network. The system name is displayed at the CLI prompt. If no name is configured, the system default name is Router.

Command Aliases

Command aliases allow you to configure alternative syntax for commands. You may want to create aliases for commonly used or complex commands. For example, you could assign the alias **save config** to the **copy running-config startup-config** command to reduce the amount of typing you have to perform, or if your

users might find the **save config** command easier to remember. Use word substitutions or abbreviations to tailor the command syntax for you and your user community.

Remember that any aliases you configure will be effective only on your system, and that the original command syntax will appear in the configuration file.

Minor Services

Minor services are small servers that run on your routing device and are useful for basic system testing and for providing basic network functions. Minor services are useful for testing connections from another host on the network.

Cisco small servers are conceptually equivalent to daemons.

Small servers provided by Cisco IOS software-based devices include TCP, UDP, HTTP, Bootstrap Protocol (BOOTP), and Finger. For information about the HTTP server, see the "Using the Cisco Web Browser User Interface" chapter in the Cisco IOS Configuration Fundamentals Configuration Guide.

The TCP small server provides the following minor services:

- Chargen--Generates a stream of ASCII data. To test this service, issue the **telnet** *a.b.c.d* **chargen**command from a remote host.
- Daytime--Returns the system date and time if you have configured Network Time Protocol (NTP) or set the date and time manually. To test this service, issue the **telnet** *a.b.c.d* **daytime**command from a remote host.
- Discard--Discards whatever you type. To test this service, issue the **telnet** *a.b.c.d* **discard**command from a remote host.
- Echo--Echoes back whatever you type. To test this service, issue the **telnet** *a.b.c.d* **echo**command from a remote host.

The UDP small server provides the following minor services:

- Chargen--Discards the datagram that you send and responds with a 72-character string of ASCII characters terminated with a CR+LF (carriage return and line feed).
- Discard--Discards the datagram you send.
- Echo--Echoes the payload of the datagram that you send.

Minor services are disabled by default.

Caution Enabling minor services creates the potential for certain types of denial-of-service (DoS) attacks, such as the UDP diagnostic port attack. Therefore, any network device that has UDP, TCP, BOOTP, or Finger services should be protected by a firewall or have the minor services disabled. For information on preventing UDP diagnostic port attacks, see the white paper titled Defining Strategies to Protect Against UDP Diagnostic Port Denial of Service Attacks a vailable on Cisco.com.

BOOTP Server

You can enable or disable an async line Bootstrap Protocol (BOOTP) service on your routing device. This small server is enabled by default. Due to security considerations, this service should be disabled if you are not using it.

Because DHCP is based on the BOOTP, both of these service share the well-known UDP server port 67 (per the Internet standards and RFCs). For more information about DHCP configuration in the Cisco IOS software, see the Cisco IOS IP Addressing Configuration Guide. For more information about BOOTP, see RFC 951. Interoperation between BOOTP and DHCP is defined in RFC 1534. DHCP is defined in RFC 2131.

Finger Protocol

The Finger protocol allows users throughout the network to get a list of the users currently using a particular routing device. The information displayed includes the processes running on the system, the line number, connection name, idle time, and terminal location. This information is provided through the Cisco IOS software **show users** EXEC command.

Hidden Telnet Addresses

You can hide addresses while attempting to establish a Telnet session. The hide feature suppresses the display of the address and continues to display all other messages that normally would be displayed during a connection attempt, such as detailed error messages if the connection fails.

EXEC Startup Delay

To delay the startup of the EXEC process on noisy lines until the line has been idle for 3 seconds, use the **service exec-wait** command in global configuration mode.

This command is useful on noisy modem lines or when a modem attached to the line is configured to ignore Microcom Networking Protocol (MNP) or V.42 negotiations, and when MNP or V.42 modems are 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 or password. This command is not useful on nonmodem lines or lines without some kind of login configured.

Idle Telnet Connections

Normally, data sent to noncurrent Telnet connections is accepted and discarded. When the **service telnet-zero-idle** command is enabled and a session is suspended (that is, some other connection is made active), 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 all messages sent by the host must 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.

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, depend 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.

Number of TCP Transactions

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

John Nagle's algorithm (RFC 896) helps alleviate the small-packet problem in TCP. The first character typed after the connection establishment is sent in a single packet, but TCP holds any additional characters that are typed until the receiver acknowledges the previous packet. Then the second, larger packet is sent, and the additional typed characters are saved until the acknowledgment comes back. The effect is to accumulate characters into larger chunks, and pace their transmission to the network at a rate matching the round-trip time of the given connection. This method is usually preferable for all TCP-based traffic.

By default, the Nagle algorithm is not enabled.

Switching and Scheduling Priorities

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

System Buffer Size

You can adjust the initial buffer pool settings and limits at which temporary buffers are created and destroyed.

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

- 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. Public buffer pools are labeled as small, middle, big, very big, large, 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.

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 outstanding buffers, the number of buffers in the free list, and the maximum number of buffers allowed in the free list.

How to Perform Basic System Management

Setting Basic System Parameters

To set basic system parameters perform the following steps. You can perform these steps based on the customization requirements of your system.

Procedure

Step 1 **hostname** *name*

Use the **hostname** *name* command to perform the basic system management task of assigning a name for your device.

Example:

```
Router(config)# hostname host1
```

Step 2 **prompt** *string*

or

no service prompt config

By default, the CLI prompt consists of the system name followed by an angle bracket (>) for user EXEC mode or a pound sign (#) for privileged EXEC mode. Use the the **prompt** *string* or the **no service prompt config** command to customize the CLI prompt for your system.

Example:

```
Router(config)# prompt Router123
```

or

Example:

```
Router(config)# no service prompt config
```

Step 3 **alias** *mode alias-name alias-command-line*

Use the **alias** *mode alias-name alias-command-line* command to create a command alias.

Example:

```
Router(config)# alias exec save config copy running-config startup-config
```

Step 4 **service tcp-small-servers**

Use the **service tcp-small-servers** command to enable minor TCP services such as chargen, daytime, discard, and echo.

Note The **no** form of the **service tcp-small-servers** command will appear in the configuration file when these basic services are disabled.

Example:

```
Router(config)# service tcp-small-servers
```

Step 5 **service udp-small-servers**

Use the **service udp-small-servers** command to enable minor UDP services such as chargen, daytime, discard, and echo.

Note The **no** form of the **service udp-small-servers** command will appear in the configuration file when these basic services are disabled.

Example:

```
Router(config)# service udp-small-servers
```

Step 6 **no ip bootp server**

Use the **no ip bootp server** command to disable the BOOTP server on your platform.

Example:

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

Step 7 **ip finger**

Use the **ip finger** command to enable a Cisco device to respond to Finger (port 79) requests. When the **ip finger** command 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.

Example:

```
Router(config)# ip finger
```

Step 8 **ip finger rfc-compliant**

Use the **ip finger rfc-compliant** command to configure the finger protocol to be compliant with RFC 1288. The **ip finger rfc-compliant** command should not be configured for devices with more than 20 simultaneous users. When the **ip finger rfc-compliant**command is configured, the router will wait for input before displaying any information. The remote user can then press the Return key to display the output of the **show users** command, or enter **/W** to display the output of the **show users wide** command. After this information is displayed, the connection is closed.

Example:

```
Router(config)# ip finger rfc-compliant
```

Step 9 **service hide-telnet-address**

Use the **service hide-telnet-address** command to configure the router to suppress Telnet addresses.

Example:

```
Router(config)# service hide-telnet-address
```

Step 10 **line** *line-number*

Use the line command to enter line configuration mode.

Example:

```
Router(config)# line 1
```

Step 11 exit

Use the **exit** command to exit line configuration mode and return to global configuration mode.

Example:

```
Router(config-line)# exit
```

Step 12 **exit**

Use the **exit** command to exit line configuration mode and return to global configuration mode.

Example:

```
Router(config-line)# exit
```

Step 13 **busy-message** *hostname message*

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 fails, the router suppresses the address and displays the message specified with the **busy-message** command.

Example:

```
Router(config)# busy-message host1 message1
```

Step 14 **service exec-wait**

Use the **service exec-wait**command to delay the startup of the EXEC process on noisy lines until the line has been idle for 3 seconds.

Example:

```
Router(config)# service exec-wait
```

Step 15 **service telnet-zero-idle**

Use the **service telnet-zero-idle** command to configure the Cisco IOS software to set the TCP window to zero (0) when the Telnet connection is idle.

Example:

```
Router(config)# service telnet-zero-idle
```

Step 16 **load-interval** *seconds*

Use the **load-interval** *seconds* command to change the length of time for which a set of data is used to compute load statistics.

Example:

```
Router(config)# load-interval 100
```

Step 17 **service nagle**

Use the **service nagle** command to enable the Nagle algorithm and thereby reduce the number of TCP transactions.

Example:

```
Router(config)# load-interval 100
```

Step 18 **scheduler interval** *milliseconds*

Use the **scheduler interval** *milliseconds* command to define the maximum amount of time that can elapse without running the lowest-priority system processes.

Example:

```
Router(config)# scheduler interval 100
```

Step 19 **scheduler allocate** [*network-microseconds process-microseconds*]

Use the **scheduler allocate** command 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 routers.

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

Example:

```
Router(config)# scheduler allocate 5000 200
```

Step 20 **scheduler process-watchdog** {**hang** | **normal** | **reload** | **terminate**}

Use the **scheduler process-watchdog** {**hang** | **normal** | **reload** | **terminate**} command to configure the characteristics for a looping process.

Example:

```
Router(config)# scheduler process-watchdog hang
```

Step 21 **buffers** {**small** | **middle** | **big** | **verybig** | **large** | **huge** | *type number*} {**permanent** | **max-free** | **min-free** | **initial**} *number*

Use the **buffers** {**small** | **middle** | **big** | **verybig** | **large** | **huge** | *type number*} {**permanent** | **max-free** | **min-free** | **initial**} *number* command to adjust the system buffer size.

Example:

```
Router(config)# buffers small permanent 10
```

Caution Cisco does not recommend that you adjust these parameters. Improper settings can adversely impact the system performance.

Step 22 exit

Use the **exit** command to exit global configuration mode and return to privileged EXEC mode.

Example:

```
Router(config)# exit
```

Step 23 **show aliases** [*mode*]

Use the **show aliases** [*mode*] command to display a list of command aliases currently configured on your system, and the original command syntax for those aliases.

Example:

```
Router# show aliases exec
```

Step 24 **show buffers**

Use the **show buffers**command to display buffer information. For more information about this command, see the Cisco IOS Configuration Fundamentals Command Reference.

Example:

```
Router# show buffers
Buffer elements:
     1119 in free list (1119 max allowed)
     641606 hits, 0 misses, 619 created
Public buffer pools:
Small buffers, 104 bytes (total 50, permanent 50):
     48 in free list (20 min, 150 max allowed)
     2976557 hits, 0 misses, 0 trims, 0 created
     0 failures (0 no memory)
Middle buffers, 600 bytes (total 25, permanent 25, peak 37 @ 2w0d):
     25 in free list (10 min, 150 max allowed)
     445110 hits, 4 misses, 12 trims, 12 created
     0 failures (0 no memory)
Big buffers, 1536 bytes (total 50, permanent 50):
     50 in free list (5 min, 150 max allowed)
     58004 hits, 0 misses, 0 trims, 0 created
     0 failures (0 no memory)
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
     0 failures (0 no memory)
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
     0 failures (0 no memory)
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
     0 failures (0 no memory)
Interface buffer pools:
Syslog ED Pool buffers, 600 bytes (total 282, permanent 282):
     257 in free list (282 min, 282 max allowed)
     32 hits, 0 misses
IPC buffers, 4096 bytes (total 2, permanent 2):
     1 in free list (1 min, 8 max allowed)
     1 hits, 0 fallbacks, 0 trims, 0 created
     0 failures (0 no memory)
Header pools:
Header buffers, 0 bytes (total 511, permanent 256, peak 511 @ 2w0d):
     255 in free list (256 min, 1024 max allowed)
     171 hits, 85 misses, 0 trims, 255 created
     0 failures (0 no memory)
     256 max cache size, 256 in cache
     0 hits in cache, 0 misses in cache
Particle Clones:
     1024 clones, 0 hits, 0 misses
Public particle pools:
F/S buffers, 128 bytes (total 512, permanent 512):
     0 in free list (0 min, 512 max allowed)
     512 hits, 0 misses, 0 trims, 0 created
     0 failures (0 no memory)
     512 max cache size, 512 in cache
     0 hits in cache, 0 misses in cache
Normal buffers, 512 bytes (total 2048, permanent 2048):
     2048 in free list (1024 min, 4096 max allowed)
     0 hits, 0 misses, 0 trims, 0 created
     0 failures (0 no memory)
Private particle pools:
HQF buffers, 0 bytes (total 2000, permanent 2000):
     2000 in free list (500 min, 2000 max allowed)
     0 hits, 0 misses, 0 trims, 0 created
     0 failures (0 no memory)
Serial2/0 buffers, 512 bytes (total 256, permanent 256):
```

```
     0 in free list (0 min, 256 max allowed)
     256 hits, 0 fallbacks
     256 max cache size, 132 in cache
     124 hits in cache, 0 misses in cache
     10 buffer threshold, 0 threshold transitions
Serial2/1 buffers, 512 bytes (total 256, permanent 256):
     0 in free list (0 min, 256 max allowed)
     256 hits, 0 fallbacks
     256 max cache size, 132 in cache
     124 hits in cache, 0 misses in cache
     10 buffer threshold, 0 threshold transitions
```

Configuration Examples for Performing Basic System Management

There are no configuration examples for the Performing Basic System Management feature.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Network Management commands	*Cisco IOS Network Management Command Reference*
Cisco IOS fundamental configuration commands	*Cisco IOS Configuration Fundamentals Command Reference*
Cisco IOS fundamental configurations	*Cisco IOS Configuration Fundamentals Configuration Guide*
Preventing UDP diagnostic port attacks	Defining Strategies to Protect Against UDP Diagnostic Port Denial of Service Attacks
DHCP configuration	*Cisco IOS IP Addressing Configuration Guide*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 896	*Congestion Control in IP/TCP Internetworks*
RFC 951	*Algorithms for Synchronizing Network Clocks*
RFC 1288	*The Finger User Information Protocol*
RFC 1534	*Interoperation Between DHCP and BOOTP*
RFC 2131	*Dynamic Host Configuration Protocol*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

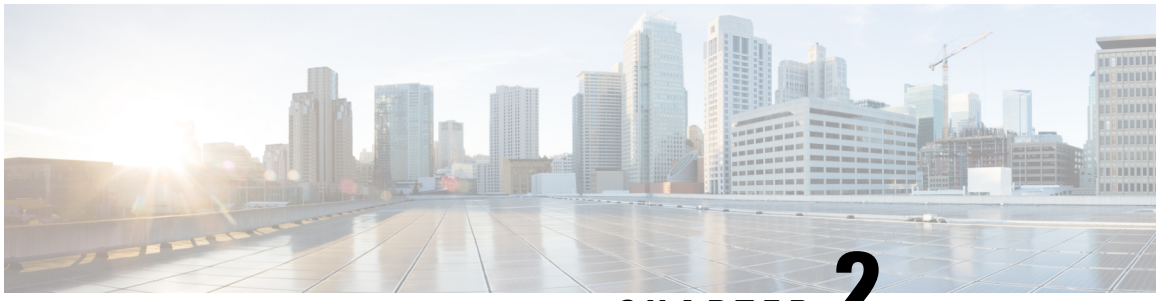
Feature Information for Performing Basic System Management

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Performing Basic System Management

Feature Name	Releases	Feature Information
Performing Basic System Management		This module describes the basic tasks to manage the general system features of the Cisco IOS software.



CHAPTER 2

Network Time Protocol

Network Time Protocol (NTP) is a protocol designed to time-synchronize a network of machines. NTP runs on User Datagram Protocol (UDP), which in turn runs on IP. NTP Version 3 is documented in RFC 1305.

This module describes how to configure Network Time Protocol on Cisco devices.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Network Time Protocol

The Network Time Protocol (NTP) package contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. NTP versions 4.2.4p7 and earlier are vulnerable.

The vulnerability is due to an error in handling of certain malformed messages. An unauthenticated, remote attacker could send a malicious NTP packet with a spoofed source IP address to a vulnerable host. The host that processes the packet sends a response packet back to the transmitter. This action could start a loop of messages between the two hosts that could cause both the hosts to consume excessive CPU resources, use up the disk space by writing messages to log files, and consume the network bandwidth. All of these could cause a DoS condition on the affected hosts.

For more information, see the Network Time Protocol Package Remote Message Loop Denial of Service Vulnerability web page.

Cisco software releases that support NTPv4 are not affected. All other versions of Cisco software are affected.

To display whether a device is configured with NTP, use the **show running-config | include ntp** command. If the output returns any of the following commands, then that device is vulnerable to the attack:

- **ntp broadcast client**
- **ntp master**
- **ntp multicast client**
- **ntp peer**
- **ntp server**

For more information on understanding Cisco software releases, see the White Paper: Cisco IOS and NX-OS Software Reference Guide.

There are no workarounds for this vulnerability other than disabling NTP on the device. Only packets destined for any configured IP address on the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.

Depending on your release, your feature will process NTP mode 7 packets and will display the message "NTP: Receive: dropping message: Received NTP private mode 7 packet " if debugs for NTP are enabled. Configure the **ntp allow mode private** command to process NTP mode 7 packets. This command is disabled by default.

Note NTP peer authentication is not a workaround and is a vulnerable configuration.

NTP services are disabled on all interfaces by default.

Networking devices running NTP can be configured to operate in a variety of association modes when synchronizing time with reference time sources. A networking device can obtain time information on a network in two ways: by polling host servers and by listening to NTP broadcasts.

Information About Network Time Protocol

Network Time Protocol

Network Time Protocol (NTP) is a protocol designed to time-synchronize a network of machines. NTP runs on User Datagram Protocol (UDP), which in turn runs on IP. NTP Version 3 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 the accuracy of 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 an authoritative time source (such as a radio or atomic clock, or a Global Positioning System (GPS) time source) directly attached, a stratum 2 time server receives its time via NTP from a stratum 1 time server, and so on.

NTP has two ways to avoid synchronizing to a machine whose time may not be accurate. NTP will never synchronize to a machine that is not in turn synchronized. NTP will compare the time reported by several machines, and will not synchronize to a machine whose time is significantly different from others, even if its stratum is lower. This strategy effectively builds a self-organizing tree of NTP servers.

The Cisco implementation of NTP does not support stratum 1 service; that is, you cannot connect to a radio or atomic clock (for some specific platforms, however, you can connect to a GPS time-source device). Cisco recommends that the 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, the Cisco 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 can then synchronize to that machine via NTP.

A number of manufacturers include NTP software for their host systems and a publicly available version for systems running UNIX. This software also allows UNIX-derivative servers to acquire the time directly from an atomic clock, which would subsequently propagate time information along to Cisco routers.

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 through exchange of NTP messages between each pair of machines with an association.

However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each machine can 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 Cisco strongly recommends 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.

When multiple sources of time (Virtual Integrated Network System (VINES), hardware clock, manual configuration) are available, NTP is always considered to be more authoritative. NTP time overrides the time set by any other method.

NTP services are disabled on all interfaces by default.

For more information about NTP, see the following sections:

Poll-Based NTP Associations

Networking devices running NTP can be configured to operate in variety of association modes when synchronizing time with reference time sources. A networking device can obtain time information on a network in two ways—by polling host servers and by listening to NTP broadcasts. This section focuses on the poll-based association modes. Broadcast-based NTP associations are discussed in the *Broadcast-Based NTP Associations* section.

The following are the two most commonly used poll-based association modes:

- Client mode
- Symmetric active mode

The client and the symmetric active modes should be used when NTP is required to provide a high level of time accuracy and reliability.

When a networking device is operating in the client mode, it polls its assigned time-serving hosts for the current time. The networking device will then pick a host from among all the polled time servers to synchronize with. Because the relationship that is established in this case is a client-host relationship, the host will not capture or use any time information sent by the local client device. This mode is most suited for file-server and workstation clients that are not required to provide any form of time synchronization to other local clients. Use the **ntp server** command to individually specify the time server that you want your networking device to consider synchronizing with and to set your networking device to operate in the client mode.

When a networking device is operating in the symmetric active mode, it polls its assigned time-serving hosts for the current time and it responds to polls by its hosts. Because this is a peer-to-peer relationship, the host will also retain time-related information of the local networking device that it is communicating with. This mode should be used when a number of mutually redundant servers are interconnected via diverse network paths. Most stratum 1 and stratum 2 servers on the Internet adopt this form of network setup. Use the **ntp peer** command to individually specify the time serving hosts that you want your networking device to consider synchronizing with and to set your networking device to operate in the symmetric active mode.

The specific mode that you should set for each of your networking devices depends primarily on the role that you want them to assume as a timekeeping device (server or client) and the device's proximity to a stratum 1 timekeeping server.

A networking device engages in polling when it is operating as a client or a host in the client mode or when it is acting as a peer in the symmetric active mode. Although polling does not usually place a burden on memory and CPU resources such as bandwidth, an exceedingly large number of ongoing and simultaneous polls on a system can seriously impact the performance of a system or slow the performance of a given network. To avoid having an excessive number of ongoing polls on a network, you should limit the number of direct, peer-to-peer or client-to-server associations. Instead, you should consider using NTP broadcasts to propagate time information within a localized network.

Broadcast-Based NTP Associations

Broadcast-based NTP associations should be used when time accuracy and reliability requirements are modest and if your network is localized and has more than 20 clients. Broadcast-based NTP associations are also recommended for use on networks that have limited bandwidth, system memory, or CPU resources.

A networking device operating in the broadcast client mode does not engage in any polling. Instead, it listens for NTP broadcast packets that are transmitted by broadcast time servers. Consequently, time accuracy can be marginally reduced because time information flows only one way.

Use the **ntp broadcast client** command to set your networking device to listen for NTP broadcast packets propagated through a network. For broadcast client mode to work, the broadcast server and its clients must be located on the same subnet. You must enable the time server that transmits NTP broadcast packets on the interface of the given device by using the **ntp broadcast** command.

NTP Access Group

The access list-based restriction scheme allows you to grant or deny certain access privileges to an entire network, a subnet within a network, or a host within a subnet. To define an NTP access group, use the **ntp access-group** command in global configuration mode.

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

1. **ipv4**—Configures IPv4 access lists.
2. **ipv6**—Configures IPv6 access lists.

3. **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.
4. **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.
5. **serve-only**—Allows only time requests from a system whose address passes the access list criteria.
6. **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 access. If no access groups are specified, all access types are granted access to all systems. If any access groups are specified, only the specified access types will be granted access.

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

The encrypted NTP authentication scheme should be used when a reliable form of access control is required. Unlike the access list-based restriction scheme that is based on IP addresses, the encrypted authentication scheme uses authentication keys and an authentication process to determine if NTP synchronization packets sent by designated peers or servers on a local network are deemed as trusted before the time information that they carry along with them is accepted.

The authentication process begins from the moment an NTP packet is created. Cryptographic checksum keys are generated using the message digest algorithm 5 (MD5) and are embedded into the NTP synchronization packet that is sent to a receiving client. Once a packet is received by a client, its cryptographic checksum key is decrypted and checked against a list of trusted keys. If the packet contains a matching authentication key, the time-stamp information that is contained within the packet is accepted by the receiving client. NTP synchronization packets that do not contain a matching authenticator key are ignored.

Note In large networks, where many trusted keys must be configured, the Range of Trusted Key Configuration feature enables configuring multiple keys simultaneously.

It is important to note that the encryption and decryption processes used in NTP authentication can be very CPU-intensive and can seriously degrade the accuracy of the time that is propagated within a network. If your network setup permits a more comprehensive model of access control, you should consider the use of the access list-based form of control.

After NTP authentication is properly configured, your networking device will synchronize with and provide synchronization only to trusted time sources.

NTP Services on a Specific Interface

Network Time Protocol (NTP) services are disabled on all interfaces by default. NTP is enabled globally when any NTP commands are entered. You can selectively prevent NTP packets from being received through a specific interface by using the **ntp disable** command in interface configuration mode.

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 **ntp source** *interface* command in global configuration mode to configure a specific 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** keyword in the **ntp peer** or **ntp server** command.

System as an Authoritative NTP Server

Use the **ntp master** 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.

Note Use the **ntp master** command with 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.

How to Configure Network Time Protocol

Configuring NTP

Configuring Poll-Based NTP Associations

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ntp peer** *ip-address* [**normal-sync**] [**version** *number*] [**key** *key-id*] [**prefer**] **Example:** `Device(config)# ntp peer 192.168.10.1 normal-sync version 2 prefer`	Forms a peer association with another system.
Step 4	**ntp server** *ip-address* [**version** *number*] [**key** *key-id*] [**prefer**] **Example:** `Device(config)# ntp server 192.168.10.1 version 2 prefer`	Forms a server association with another system.

	Command or Action	Purpose
Step 5	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring Broadcast-Based NTP Associations

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0`	Configures an interface and enters interface configuration mode.
Step 4	**ntp broadcast version** *number* **Example:** `Device(config-if)# ntp broadcast version 2`	Configures the specified interface to send NTP broadcast packets.
Step 5	**ntp broadcast client** **Example:** `Device(config-if)# ntp broadcast client`	Configures the specified interface to receive NTP broadcast packets.
Step 6	**ntp broadcastdelay** *microseconds* **Example:** `Device(config-if)# ntp broadcastdelay 100`	Adjusts the estimated round-trip delay for NTP broadcasts.
Step 7	**end** **Example:**	Exits interface configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-if)# end`	

Configuring an External Reference Clock

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**line aux** *line-number* **Example:** `Device(config)# line aux 0`	Enters line configuration mode for the auxiliary port 0.
Step 4	**end** **Example:** `Device(config-line)# end`	Exits line configuration mode and returns to privileged EXEC mode.
Step 5	**show ntp associations** **Example:** `Device# show ntp associations`	Displays the status of NTP associations, including the status of the GPS reference clock.
Step 6	**show ntp status** **Example:** `Device# show ntp status`	Displays the status of NTP.
Step 7	**debug ntp refclock** **Example:** `Device# debug ntp refclock`	Allows advanced monitoring of reference clock activities for the purposes of debugging.

Configuring NTP Authentication

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ntp authenticate** **Example:** `Device(config)# ntp authenticate`	Enables the NTP Authentication feature.
Step 4	**ntp authentication-key** *number* **md5** *key* **Example:**	Defines authentication keys. • Each key has a key number, a type, and a value.
Step 5	**ntp authentication-key** *number* **md5** *key* **Example:**	Defines authentication keys. • Each key has a key number, a type, and a value.
Step 6	**ntp authentication-key** *number* **md5** *key* **Example:**	Defines authentication keys. • Each key has a key number, a type, and a value.
Step 7	**ntp trusted-key** *key-number* [**-** *end-key*] **Example:** `Device(config)# ntp trusted-key 1 - 3`	Defines trusted authentication keys. • If a key is trusted, this device will be ready to synchronize to a system that uses this key in its NTP packets.
Step 8	**ntp server** *ip-address* **key** *key-id* **Example:** `Device(config)# ntp server 172.16.22.44 key 2`	Allows the software clock to be synchronized by an NTP time server.
Step 9	**end** **Example:**	Exits global configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config)# end`	

Verifying Network Time Protocol

Procedure

Step 1 **show clock** [**detail**]

This command displays the current software clock time. The following is sample output from this command.

Example:

```
Device# show clock detail

*18:38:21.655 UTC Tue Jan 4 2011
Time source is hardware calendar
```

Step 2 **show ntp associations detail**

This command displays the status of NTP associations. The following is sample output from this command.

Example:

```
Device# show ntp associations detail

192.168.10.1 configured, insane, invalid, unsynced, stratum 16
ref ID .INIT., time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
our mode active, peer mode unspec, our poll intvl 64, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 0, sync dist 15940.56
delay 0.00 msec, offset 0.0000 msec, dispersion 15937.50
precision 2**24, version 4
org time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
rec time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
xmt time D0CDE881.9A6A9005 (18:42:09.603 UTC Tue Jan 4 2011)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =  16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0
minpoll = 6, maxpoll = 10
192.168.45.1 configured, insane, invalid, unsynced, stratum 16
ref ID .INIT., time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
our mode client, peer mode unspec, our poll intvl 64, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 0, sync dist 16003.08
delay 0.00 msec, offset 0.0000 msec, dispersion 16000.00
precision 2**24, version 4
org time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
rec time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
xmt time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =  16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0
minpoll = 6, maxpoll = 10
```

Step 3 **show ntp status**

This command displays the status of NTP. The following is sample output from this command.

Example:

```
Device# show ntp status

Clock is synchronized, stratum 8, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**10
reference time is D25AF07C.4B439650 (15:26:04.294 PDT Tue Oct 21 2011)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 2.31 msec, peer dispersion is 1.20 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 16, last update was 10 sec ago.
```

Configuration Examples for Network Time Protocol

Example: Configuring Network Time Protocol

In the following example, a device with a hardware clock that has server associations with two other systems sends broadcast NTP packets, periodically updates the hardware clock, and redistributes time into VINES:

```
clock timezone PST -8
clock summer-time PDT recurring

ntp server 192.168.13.57
ntp server 192.168.11.58
interface GigabitEthernet 0/0
 ntp broadcast
vines time use-system
```

In the following example, a device with a hardware clock has no outside time source, so it uses the hardware clock as an authoritative time source and distributes the time via NTP broadcast packets:

```
clock timezone MET 2
clock calendar-valid
ntp master
interface vlan 3
 ntp broadcast
```

Additional References for Network Time Protocol

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Basic System Management commands	Basic System Management Command Reference
NTP4 in IPv6	*Cisco IOS Basic System Management Guide*

Related Topic	Document Title
IP extended access lists	*Cisco IOS IP Addressing Configuration Guide*
IPX extended access lists	*Novell IPX Configuration Guide*
NTP package vulnerability	*Network Time Protocol Package Remote Message Loop Denial of Service Vulnerability*
Cisco IOS and NX-OS software releases	*'White Paper: Cisco IOS and NX-OS Software Reference Guide*

Standards and RFCs

Standard/RFCs	Title
RFC 1305	*Network Time Protocol (Version 3) Specification, Implementation and Analysis*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Network Time Protocol

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for Network Time Protocol

Feature Name	Releases	Feature Information
Network Time Protocol		NTP is a protocol designed to time-synchronize a network of machines. NTP runs on UDP, which in turn runs on IP. NTP is documented in RFC 1305.