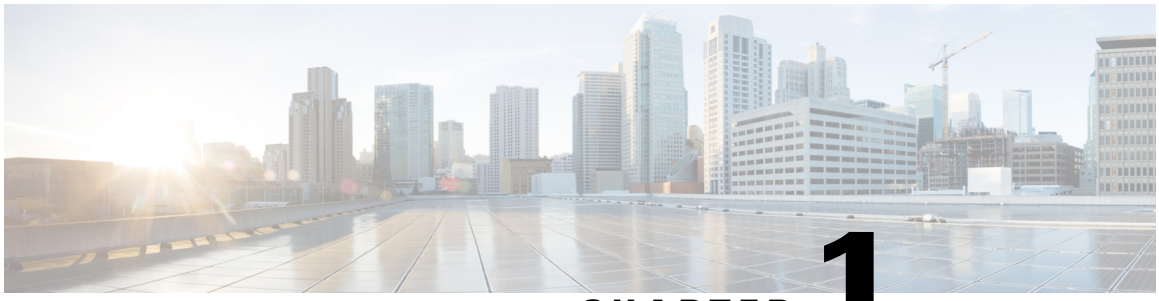
# Basic System Management Configuration Guide, Cisco IOS XE Fuji 16.8.x

**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

# Read Me First

### Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E (for Catalyst Switching) and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

### Feature Information

Use Cisco Feature Navigator to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

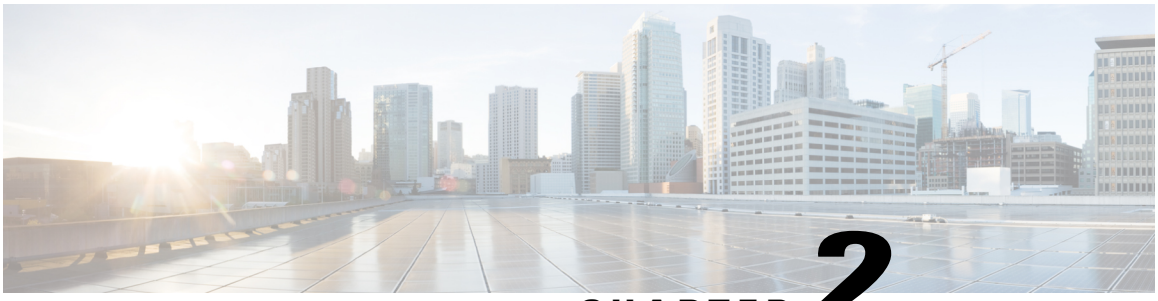
### Related References

- Cisco IOS Command References, All Releases

### Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.



CHAPTER 2

# 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* **charge**ncommand 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.

### SUMMARY STEPS

1. **hostname** *name*
2. **prompt** *string*
3. **alias** *mode alias-name alias-command-line*
4. **service tcp-small-servers**
5. **service udp-small-servers**
6. **no ip bootp server**
7. **ip finger**
8. **ip finger rfc-compliant**
9. **service hide-telnet-address**
10. **line** *line-number*
11. exit
12. **exit**
13. **busy-message** *hostname message*
14. **service exec-wait**
15. **service telnet-zero-idle**
16. **load-interval** *seconds*
17. **service nagle**
18. **scheduler interval** *milliseconds*
19. **scheduler allocate** [*network-microseconds process-microseconds*]
20. **scheduler process-watchdog** {**hang** | **normal** | **reload** | **terminate**}
21. **buffers** {**small** | **middle** | **big** | **verybig** | **large** | **huge** | *type number*} {**permanent** | **max-free** | **min-free** | **initial**} *number*
22. exit
23. **show aliases** [*mode*]
24. **show buffers**

### DETAILED STEPS

**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:<br>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 |

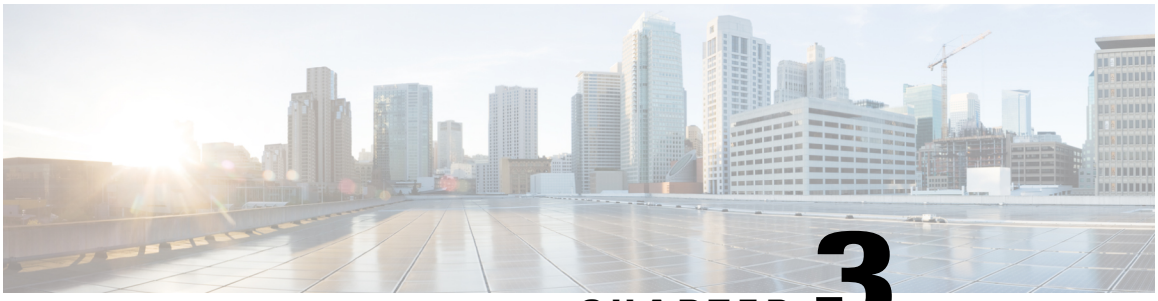
# Feature Information for Performing Basic System Management

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 3

# Memory Threshold Notifications

The Memory Threshold Notifications feature allows you to reserve memory for critical notifications and to configure a router to issue notifications when available memory falls below a specified threshold.



## 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 Memory Threshold Notifications

The Memory Threshold Notifications feature provides two ways to mitigate low-memory conditions on a router: notifications can be sent to indicate that free memory has fallen below a configured threshold, and memory can be reserved to ensure that sufficient memory is available to issue critical notifications. To implement the Memory Threshold Notifications feature, you should understand the following concepts:

# Memory Threshold Notifications

The Memory Threshold Notifications feature allows you to reserve memory for critical notifications and to configure a router to issue notifications when available memory falls below a specified threshold.

# Memory Reservation

Memory reservation for critical operations ensures that management processes, such as event logging, continue to function even when router memory is exhausted.

# How to Define Memory Threshold Notifications

# Setting a Low Free Memory Threshold

Perform this task to set a low free memory threshold.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **memory free low-watermark** [**processor** *threshold*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **memory free low-watermark** [**processor** *threshold*<br><br>**Example:**<br><br>`Router(config)#` **memory free low-watermark processor 20000** | Specifies a threshold in kilobytes of free processor memory. To view acceptable values for the memory threshold, enter the following command:<br><br>• **memory free low-watermark processor ?** |

# Reserving Memory for Critical Notifications

When a router is overloaded by processes, the amount of available memory might fall to levels insufficient for it to issue critical notifications. Perform this task to reserve a region of memory to be used by the router for the issuing of critical notifications.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **memory reserve critical** *kilobytes*

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **memory reserve critical** *kilobytes*<br><br>**Example:**<br><br>`Router(config)#` **memory reserve critical 1000** | Reserves the specified amount of memory in kilobytes so that the router can issue critical notifications.<br><br>• The amount of memory reserved for critical notifications cannot exceed 25 percent of total available memory. |

# Configuration Examples for Memory Threshold Notifications

## Setting a Low Free Memory Threshold Examples

### Threshold for Free Processor Memory

The following example shows how to specify a threshold of 20000 KB of free processor memory before the router issues notifications:

```
Router(config)# memory free low-watermark processor 20000
```

If available free memory falls below the specified threshold, the router sends a notification message like this one:

```
000029: *Aug 12 22:31:19.559: %SYS-4-FREEMEMLOW: Free Memory has dropped below 20000k
Pool: Processor  Free: 66814056  freemem_lwm: 204800000
```

Once available free memory rises to above 5 percent of the threshold, the router sends a notification message like this one:

```
000032: *Aug 12 22:33:29.411: %SYS-5-FREEMEMRECOVER: Free Memory has recovered 20000k
Pool: Processor  Free: 66813960  freemem_lwm: 0
```

## Reserving Memory for Critical Notifications Example

The following example shows how to reserve 1000 KB of memory for critical notifications:

```
Router# memory reserved critical 1000
```

**Note** The amount of memory reserved for critical notifications cannot exceed 25 percent of total available memory.

# Additional References

For additional information related to the CPU Thresholding Notification feature, refer to the following references:

### Related Documents

| Related Topic | Document Title |
|---|---|
| SNMP traps | *Configuration Fundamentals Command Reference* |

### Standards

| Standards | Title |
|---|---|
| No new or modified standards are supported by this feature and support for existing standards has not been modified by this feature. | -- |

### MIBs

| MIBs | MIBs Link |
|---|---|
| CISCO-PROCESS-MIB | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFCs | Title |
|---|---|
| No new or modified RFCs are supported by this feature and support for existing RFCs has not been modified by this feature. | -- |

### 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 |

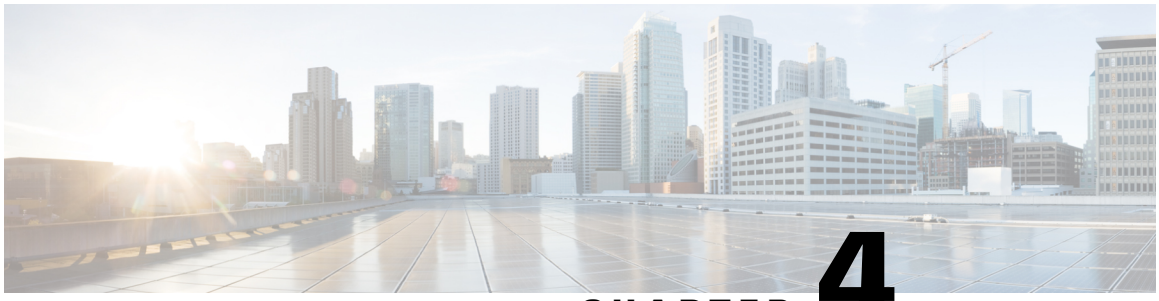
# Feature Information for Memory Threshold Notifications

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 Memory Threshold Notifications***

| Feature Name | Releases | Feature Information |
|---|---|---|
| Memory Threshold Notifications | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. |



CHAPTER 4

# NTPv4 MIB

The NTPv4 MIB feature introduces the Network Time Protocol Version 4 (NTPv4) MIB in Cisco software. It defines data objects that represent the current status of NTP entities. These data objects are accessed using the Simple Network Management Protocol (SNMP) and are used to monitor and manage local NTP entities.

This module describes the NTPv4 MIB.



# 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 the NTPv4 MIB

## NTPv4 MIB

The Network Time Protocol Version 4 (NTPv4) MIB feature, which is based on RFC 5907, defines data objects that represent the current status of NTP entities. These data objects are accessed using the Simple Network Management Protocol (SNMP) and are used to monitor and manage local NTP entities.

The data objects contain the following information about the NTP entities:

- Connectivity to the upstream NTP servers and to hardware reference clocks.
- Product
- Vendor
- Version

By using the information contained in the data objects, you can detect failures before the overall time synchronization of the network is impacted.

The following object groups that are addressed in RFC 5907 are supported in the NTPv4 MIB:

- ntpAssociation
- ntpEntInfo
- ntpEntStatus

The following object groups that are addressed in RFC 5907 are not supported in the NTPv4 MIB:

- ntpEntControl
- ntpEntNotifObjects

# How to Verify the NTPv4 MIB

No special configuration is needed for this feature. This feature is enabled by default.

# Verifying NTPv4 MIB

To verify information about the NTPv4 MIB, perform any or all of the following optional commands in any order.

### SUMMARY STEPS

1. **show ntp associations** [**detail**]
2. **show ntp status**
3. **show ntp info**
4. **show ntp packets**

### DETAILED STEPS

**Step 1** **show ntp associations** [**detail**]

**Example:**

```
Device> show ntp associations detail
```

(Optional) Displays detailed status of NTP associations.

**Step 2** **show ntp status**

**Example:**
```
Device> show ntp status
```

(Optional) Displays the status of NTP.

**Step 3** **show ntp info**

**Example:**
```
Device> show ntp info
```

(Optional) Displays information about NTP entities.

**Step 4** **show ntp packets**

**Example:**
```
Device> show ntp packets
```

(Optional) Displays information about NTP packets.

# Configuration Examples for NTPv4 MIB

## Example: Verifying the NTP4 MIB

### Sample Output for the show ntp associations Command

```
Device> show ntp associations detail

172.31.32.2 configured, ipv4, our_master, sane, valid, stratum 1
ref ID .LOCL., time D2352248.2337CCB8 (06:12:24.137 IST Tue Oct 4 2011)
our mode active, peer mode passive, our poll intvl 16, peer poll intvl 16
root delay 0.00 msec, root disp 0.00, reach 377, sync dist 16.05
delay 0.00 msec, offset 0.0000 msec, dispersion 8.01, jitter 0.5 msec
precision 2**7, version 4
assoc ID 1, assoc name 192.0.2.1,
assoc in packets 60, assoc out packets 60, assoc error packets 0
org time D2352248.2337CCB8 (06:12:24.137 IST Tue Oct 4 2011)
rec time 00000000.00000000 (00:00:00.000 IST Mon Jan 1 1900)
xmt time D2352248.2337CCB8 (06:12:24.137 IST Tue Oct 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 =     7.81    8.05    8.29    8.53    8.77    9.01    9.25    9.49
minpoll = 4, maxpoll = 4

192.168.13.33 configured, ipv6, insane, invalid, unsynced, stratum 16
ref ID .INIT., time 00000000.00000000 (00:00:00.000 IST Mon Jan 1 1900)
our mode client, peer mode unspec, our poll intvl 1024, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 0, sync dist 15951.96
delay 0.00 msec, offset 0.0000 msec, dispersion 15937.50,  jitter 1000.45 msec
precision 2**7, version 4
assoc ID 2, assoc name myserver
assoc in packets 0, assoc out packets 0, assoc error packets 0
org time D2351E93.2235F124 (05:56:35.133 IST Tue Oct 4 2011)
rec time 00000000.00000000 (00:00:00.000 IST Mon Jan 1 1900)
xmt time 00000000.00000000 (00:00:00.000 IST 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
```

### Sample Output for the show ntp status Command

```
Device> show ntp status

Clock is synchronized, stratum 2, reference assoc id 1, reference is 192.0.2.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**7
reference time is D2352258.243DDF14 (06:12:40.141 IST Tue Oct 4 2011)
clock offset is 0.0000 msec, root delay is 0.00 msec, time resolution 1000 (1 msec),
root dispersion is 15.91 msec, peer dispersion is 8.01 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 16, last update was 6 sec ago.
system uptime (00:00:00.000) UTC,
system time is D2352258.243DDF14 (06:12:40.141 IST Tue Oct 4 2011)
leap time is D2352258.243DDF14 (24:00:00.000 IST Tue Dec 31 2011)
leap direction is 1
```

### Sample Output for the show ntp info Command

```
Device> show ntp info

Ntp Software Name: Example
NtP Software Version: ntp-1.1
Ntp Software Vendor: Example
Ntp System Type: Example_System
```

### Sample Output for the show ntp packets Command

```
Device> show ntp packets

Ntp In packets: 100
Ntp Out packets: 110
Ntp bad version packets: 4
Ntp protocol error packets: 0
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Master Command List, All Releases |
| Basic System Management commands | Basic System Management Command Reference |
| Basic System Management configuration tasks | “Setting Time and Calendar Services” module in the *Basic System Management Configuration Guide* |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| RFC 5907 | *Definitions of Managed Objects for Network Time Protocol Version 4 (NTPv4)* |

### MIBs

| MIB | MIBs Link |
|---|---|
| NTPv4-MIB | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### 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 |

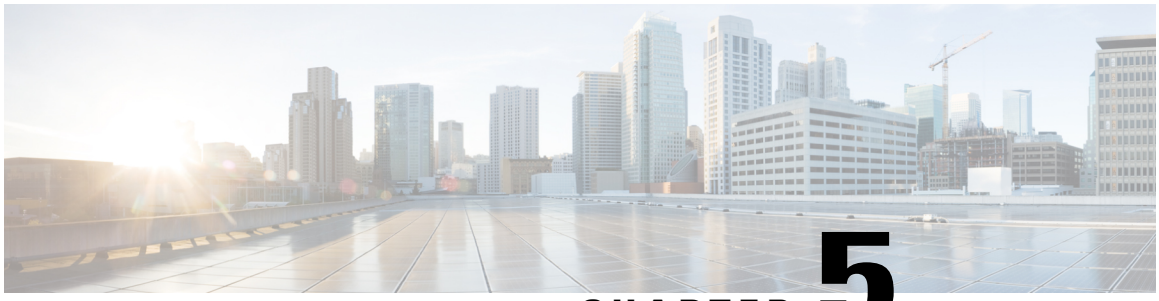
# Feature Information for the NTPv4 MIB

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 3: Feature Information for the NTPv4 MIB*

| Feature Name | Releases | Feature Information |
|---|---|---|
| NTPv4 MIB | | The NTPv4 MIB feature introduces the Network Time Protocol Version 4 (NTPv4) MIB in Cisco software. It defines data objects that represent the current status of NTP entities. These data objects are accessed using the Simple Network Management Protocol (SNMP) and are used to monitor and manage local NTP entities. |



CHAPTER 5

# Simple Network Time Protocol

Simple Network Time Protocol (SNTP) is a simplified version of Network Time Protocol(NTP). This module describes how to configure Simple 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 Simple Network Time Protocol

- Simple Network Time Protocol (SNTP) and Network Time Protocol (NTP) cannot coexist on the same machine as they use the same port. This means that these two services cannot be configured on the system at the same time.
- Support for IPv6 addresses is available only if the image supports IPv6 addressing.

# Information About Simple Network Time Protocol

## Simple Network Time Protocol

Simple Network Time Protocol (SNTP) is a simplified, client-only version of NTP. SNTP can receive only 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 servers that have unexpected behavior than an NTP client, and should be used only 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 on page 3 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 choose a new server only if it stops receiving packets from the currently selected server, or if a better server (according to the criteria described) is discovered.

# How to Configure Simple Network Time Protocol

## Configuring Simple Network Time Protocol (SNTP) Authentication

Simple Network Time Protocol (SNTP) is a simplified version of Network Time Protocol (SNTP). This module describes how to configure SNTP on Cisco devices.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sntp authenticate**
4. **sntp authentication-key** *number* **md5** *key*
5. **sntp trusted-key** *key-number* [**-** *end-key*]
6. **sntp server** *ip-address* **key** *key-id*
7. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable** | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device> enable` | • Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **sntp authenticate**<br>**Example:**<br>`Device(config)# sntp authenticate` | Enables the SNTP Authentication feature. |
| **Step 4** | **sntp authentication-key** *number* **md5** *key*<br>**Example:**<br>`Device(config)# sntp authentication-key 1 md5 key1` | Defines authentication keys.<br>• Each key has a key number, a type, and a value.<br>• Repeat this step to define additional authentication keys. |
| **Step 5** | **sntp trusted-key** *key-number* [**-** *end-key*]<br>**Example:**<br>`Device(config)# sntp trusted-key 1 - 3` | Defines trusted authentication keys.<br>• If a key is trusted, this device will be ready to synchronize to a system that uses this key in its SNTP packets. |
| **Step 6** | **sntp server** *ip-address* **key** *key-id*<br>**Example:**<br>`Device(config)# sntp server 172.16.22.44 key 2` | Allows the software clock to be synchronized by an SNTP time server. |
| **Step 7** | **end**<br>**Example:**<br>`Device(config)# end` | Exits global configuration mode and returns to privileged EXEC mode. |

# Verifying and Troubleshooting Simple Network Time Protocol

To verify and troubleshoot Simple Network Time Protocol configuration, use the following commands.

•

### SUMMARY STEPS

1. **enable**
2. **debug sntp packets** [**detail**]
3. **debug sntp select**
4. **show sntp**

### DETAILED STEPS

**Step 1** **enable**

**Example:**
```
Device> enable
```
Enables privileged EXEC mode.

- Enter your password if prompted.

**Step 2** **debug sntp packets** [**detail**]

**Example:**
```
Device> debug sntp packets
```
Displays the NTP packet sent and received along with the SNTP packet fields.

**Step 3** **debug sntp select**

**Example:**
```
Device> debug sntp select
```
Displays the SNTP server selection for IPv4 and IPv6 servers.

**Step 4** **show sntp**

**Example:**
```
Device# show sntp

SNTP server     Stratum   Version    Last Receive
172.168.10.1      16        1        never
Broadcast client mode is enabled.
Multicast client 224.0.1.1 is enabled.
```
Displays information about SNTP available in Cisco devices.

# Configuration Examples for Simple Network Time Protocol

## Example: Configuring Simple Network Time Protocol

```
clock timezone PST -8
clock summer-time PDT recurring
sntp update-calendar
```

```
sntp server 192.168.13.57
sntp server 192.168.11.58
interface Ethernet 0/0
 sntp broadcast
```

# Additional References for Simple 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* |
| 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 the SNTP

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 4: Feature Information for the SNTPv4***

| Feature Name | Releases | Feature Information |
|---|---|---|
| Simple Network Time Protocol | | Simple Network Time Protocol (SNTP) is a simplified version of Network Time Protocol(NTP). This module describes how to configure Simple Network Time Protocol on Cisco devices.<br><br>The following commands were introduced or modified: **sntp server**, **sntp authenticate**, **sntp authentication-key**, **sntp multicast**, **sntp trusted-key**. |