



Troubleshooting and Fault Management Commands



Note

This document applies specifically to Cisco IOS Release 12.2T, up to and including 12.2(15)T. For command reference documentation updates, please see the [Cisco IOS Release 12.3 \(mainline\) Command Reference documents](#). Cisco IOS Release 12.3 contains all of the changes to commands implemented in the Cisco IOS Release 12.2T train.

This chapter describes the commands used to troubleshoot a routing device. To troubleshoot, you need to discover, isolate, and resolve the system problems. You can discover problems with the system monitoring commands, isolate problems with the system test commands (including **debug** commands), and resolve problems by reconfiguring your system with the suite of Cisco IOS software commands.

This chapter describes general fault management commands. For detailed troubleshooting procedures and a variety of scenarios, see the *Cisco IOS Internetwork Troubleshooting Guide* publication. For complete details on all **debug** commands, see the [Cisco IOS Debug Command Reference](#).

For troubleshooting tasks and examples, refer to the “Troubleshooting and Fault Management” chapter or the *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2*.

attach

To connect to a specific line card for the purpose of executing monitoring and maintenance commands on that line card only, use the **attach** command in privileged EXEC mode. To exit from the Cisco IOS software image on the line card and return to the Cisco IOS image on the GRP card, use the **exit** command.

attach *slot-number*

Syntax Description

<i>slot-number</i>	Slot number of the line card you want to connect to. Slot numbers range from 0 to 11 for the Cisco 12012 router and 0 to 7 for the Cisco 12008 router. If the slot number is omitted, you will be prompted for the slot number.
--------------------	---

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 GS	This command was introduced for the Cisco 12000 series.

Usage Guidelines

You must first use the **attach** privileged EXEC command to access the Cisco IOS software image on a line card before using line card-specific **show** EXEC commands. Alternatively, you can use the **execute-on** privileged EXEC command to execute a **show** command on a specific line card.

After you connect to the Cisco IOS image on the line card using the **attach** command, the prompt changes to LC-Slotx#, where *x* is the slot number of the line card.

The commands executed on the line card use the Cisco IOS image on that line card.

You can also use the **execute-on slot** privileged EXEC command to execute commands on one or all line cards.



Note

Do not execute the **config** EXEC command from the Cisco IOS software image on the line card.

Examples

In the following example, the user connects to the Cisco IOS image running on the line card in slot 9, gets a list of valid **show** commands, and returns the Cisco IOS image running on the GRP:

```
Router# attach 9
```

```
Entering Console for 4 Port Packet Over SONET OC-3c/STM-1 in Slot: 9
Type exit to end this session
```

```
Press RETURN to get started!
```

```
LC-Slot9# show ?
```

```

cef          Cisco Express Forwarding
clock       Display the system clock
context     Show context information about recent crash(s)
history     Display the session command history
hosts       IP domain-name, lookup style, nameservers, and host table
ipc         Interprocess communications commands
location    Display the system location
sessions    Information about Telnet connections
terminal    Display terminal configuration parameters
users       Display information about terminal lines
version     System hardware and software status
    
```

```

LC-Slot9# exit

Disconnecting from slot 9.
Connection Duration: 00:01:04
Router#
    
```



Note

Because not all statistics are maintained on the line cards, the output from some of the **show** commands might not be consistent.

Related Commands

Command	Description
attach shelf	Connects you to a specific (managed) shelf for the purpose of remotely executing commands on that shelf only.
execute-on slot	Executes commands remotely on a specific line card, or on all line cards simultaneously.

clear logging

To clear messages from the logging buffer, use the **clear logging** command in privileged EXEC mode.

clear logging

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	11.2	This command was introduced.

Examples In the following example, the logging buffer is cleared:

```
Router# clear logging

Clear logging buffer [confirm]
Router#
```

Related Commands	Command	Description
	logging buffered	Logs messages to an internal buffer.
	show logging	Displays the state of logging (syslog).

clear logging xml

To clear the contents of the XML system message logging (syslog) buffer, use the **clear logging xml** command in EXEC mode.

clear logging xml

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	12.2(15)T	This command was introduced.

Usage Guidelines This command clears the contents of the XML-formatted logging buffer, but does not clear the contents of the standard logging buffer. The system will prompt you to confirm the action before clearing the buffer.

Examples In the following example, the XML-specific buffer is cleared:

```
Router# clear logging xml
Clear XML logging buffer [confirm]?y
```

Related Commands	Command	Description
	logging buffered xml	Enables system message logging (syslog) to the XML-specific buffer in XML format.
	show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML-specific buffer.

diag

To perform field diagnostics on a line card, on the Gigabit Route Processor (GRP), on the Switch Fabric Cards (SFCs), and on the Clock Scheduler Card (CSC) in Cisco 12000 series Gigabit Switch Routers (GSRs), use the **diag** command in privileged EXEC mode. To disable field diagnostics on a line card, use the **no** form of this command.

diag *slot-number* [**halt** | **previous** | **post** | **verbose** [**wait**] | **wait**]

no diag *slot-number*

Syntax Description

<i>slot-number</i>	Slot number of the line card you want to test. Slot numbers range from 0 to 11 for the Cisco 12012 and 0 to 7 for the Cisco 12008 router. Slot numbers for the CSC are 16 and 17, and for the FSC are 18, 19, and 20.
halt	(Optional) Stops the field diagnostic testing on the line card.
previous	(Optional) Displays previous test results (if any) for the line card.
post	(Optional) Initiates an EPROM-based extended power-on self-test (EPOST) only. The EPOST test suite is not as comprehensive as the field diagnostics, and a pass/fail message is the only message displayed on the console.
verbose [wait]	(Optional) Enables the maximum status messages to be displayed on the console. By default, only the minimum status messages are displayed on the console. If you specify the optional wait keyword, the Cisco IOS software is not automatically reloaded on the line card after the test completes.
wait	(Optional) Stops the automatic reloading of the Cisco IOS software on the line card after the completion of the field diagnostic testing. If you use this keyword, you must use the microcode reload slot global configuration command, or manually remove and insert the line card (to power it up) in the slot so that the GRP will recognize the line card and download the Cisco IOS software image to the line card.

Defaults

No field diagnostics tests are performed on the line card.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 GS	This command was added to support the Cisco 12000 series GSR.

Usage Guidelines

The **diag** command must be executed from the GRP main console port.

Perform diagnostics on the CSC only if a redundant CSC is in the router.

Diagnostics will stop and ask you for confirmation before altering the router's configuration. For example, running diagnostics on a SFC or CSC will cause the fabric to go from full bandwidth to one-fourth bandwidth. Bandwidth is not affected by GRP or line card diagnostics.

The field diagnostic software image is bundled with the Cisco IOS software and is downloaded automatically from the GRP to the target line card prior to testing.

**Caution**

Performing field diagnostics on a line card stops all activity on the line card. Before the **diag EXEC** command begins running diagnostics, you are prompted to confirm the request to perform field diagnostics on the line card.

In normal mode, if a test fails, the title of the failed test is displayed on the console. However, not all tests that are performed are displayed. To view all the tests that are performed, use the **verbose** keyword.

After all diagnostic tests are completed on the line card, a PASSED or TEST FAILURE message is displayed. If the line card sends a PASSED message, the Cisco IOS software image on the line card is automatically reloaded unless the **wait** keyword is specified. If the line card sends a TEST FAILURE message, the Cisco IOS software image on the line card is not automatically reloaded.

If you want to reload the line card after it fails diagnostic testing, use the **microcode reload slot** global configuration command.

**Note**

When you stop the field diagnostic test, the line card remains down (that is, in an unbooted state). In most cases, you stopped the testing because you need to remove the line card or replace the line card. If that is not the case, and you want to bring the line card back up (that is, online), you must use the **microcode reload** global configuration command or power cycle the line card.

If the line card fails the test, the line card is defective and should be replaced. In future releases this might not be the case because DRAM and SDRAM SIMM modules might be field replaceable units. For example, if the DRAM test failed you might only need to replace the DRAM on the line card.

For more information, refer to the Cisco 12000 series installation and configuration guides.

Examples

In the following example, a user is shown the output when field diagnostics are performed on the line card in slot 3. After the line card passes all field diagnostic tests, the Cisco IOS software is automatically reloaded on the card. Before starting the diagnostic tests, you must confirm the request to perform these tests on the line card because all activity on the line card is halted. The total/indiv. timeout set to 600/220 sec. message indicates that 600 seconds are allowed to perform all field diagnostics tests, and that no single test should exceed 220 seconds to complete.

```
Router# diag 3

Running Diags will halt ALL activity on the requested slot. [confirm]
Router#
Launching a Field Diagnostic for slot 3
Running DIAG config check
RUNNING DIAG download to slot 3 (timeout set to 400 sec.)
sending cmd FDIAG-DO ALL to fdia in slot 3
(total/indiv. timeout set to 600/220 sec.)
Field Diagnostic ****PASSED**** for slot 3
```

```
Field Diag eeprom values: run 159 fial mode 0 (PASS) slot 3
  last test failed was 0, error code 0
sending SHUTDOWN FDIAG_QUIT to fdiag in slot 3
```

```
Board will reload
```

```
.
.
.
```

```
Router#
```

In the following example, a user is shown the output when field diagnostics are performed on the line card in slot 3 in verbose mode:

```
Router# diag 3 verbose
```

```
Running Diags will halt ALL activity on the requested slot. [confirm]
```

```
Router#
```

```
Launching a Field Diagnostic for slot 3
```

```
Running DIAG config check
```

```
RUNNING DIAG download to slot 3 (timeout set to 400 sec.)
```

```
sending cmd FDIAG-DO ALL to fdiag in slot 3
```

```
(total/indiv. timeout set to 600/220 sec.)
```

```
FDIAG_STAT_IN_PROGRESS: test #1 R5K Internal Cache
```

```
FDIAG_STAT_PASS test_num 1
```

```
FDIAG_STAT_IN_PROGRESS: test #2 Sunblock Ordering
```

```
FDIAG_STAT_PASS test_num 2
```

```
FDIAG_STAT_IN_PROGRESS: test #3 Dram Datapins
```

```
FDIAG_STAT_PASS test_num 3
```

```
.
.
.
```

```
Field Diags: FDIAG_STAT_DONE
```

```
Field Diagnostic ****PASSED**** for slot 3
```

```
Field Diag eeprom values: run 159 fial mode 0 (PASS) slot 3
```

```
  last test failed was 0, error code 0
```

```
sending SHUTDOWN FDIAG_QUIT to fdiag in slot 3
```

```
Board will reload
```

```
.
.
.
```

```
Router#
```

Related Commands

Command	Description
microcode reload	Reloads the Cisco IOS image on a line card on the Cisco 7000 series with RSP7000, Cisco 7500 series, or Cisco 12000 series routers after all microcode configuration commands have been entered.

exception core-file

To specify the name of the core dump file, use the **exception core-file** command in global configuration mode. To return to the default core filename, use the **no** form of this command.

exception core-file *file-name*

no exception core-file

Syntax Description

<i>file-name</i>	Name of the core dump file saved on the server.
------------------	---

Defaults

The core file is named *hostname-core*, where *hostname* is the name of the router.

Command Modes

Global configuration

Command History

Release	Modification
10.2	This command was introduced.

Usage Guidelines

If you use TFTP to dump the core file to a server, the router will only dump the first 16 MB of the core file. If the router’s memory is larger than 16 MB, the whole core file will not be copied to the server. Therefore, use rcp or FTP to dump the core file.



Caution

Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, File Transfer Protocol (FTP), or remote copy protocol (rcp) server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

Examples

In the following example, a user configures a router to use FTP to dump a core file named *dumpfile* to the FTP server at 172.17.92.2 when it crashes:

```
ip ftp username red
ip ftp password blue
exception protocol ftp
exception dump 172.17.92.2
exception core-file dumpfile
```

Related Commands	Command	Description
	exception dump	Causes the router to dump a core file to a particular server when the router crashes.
	exception memory	Causes the router to create a core dump and reboot when certain memory size parameters are violated.
	exception spurious-interrupt	Causes the router to create a core dump and reload after a specified number of spurious interrupts.
	exception protocol	Configures the protocol used for core dumps.
	ip ftp password	Specifies the password to be used for FTP connections.
	ip ftp username	Configures the username for FTP connections.

exception crashinfo file

To enable the creation of a diagnostic file at the time of unexpected system shutdowns, use the **exception crashinfo file** command in global configuration mode. To disable the creation of crashinfo files, use the **no** form of this command.

exception crashinfo file *device:filename*

no exception crashinfo file *device:filename*

Syntax Description

device:filename Specifies the flash device and file name to be used for storing the diagnostic information. The colon is required.

Defaults

Enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T, 12.2(11)	This command was introduced for the Cisco 3600 series only.
12.2(13)T	This command was implemented in 6400-NSP images.

Usage Guidelines

The “crashinfo” file saves information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). The switch writes the crash information to the console at the time of the failure, and the file is created the next time you boot the IOS image after the failure (instead of while the system is failing). The file name will be *filename_yyyyymmdd-hhmmss*, where y is year, m is month, d is date, h is hour, and s is seconds.

Examples

In the following example, a crashinfo file called “crashdata” will be created in the default flash memory device if a system crash occurs:

```
Router(config)# exception crashinfo file flash:crashinfo
```

Related Commands

Command	Description
exception crashinfo buffersize	Changes the size of the crashinfo buffer.

exception crashinfo buffersize

To change the size of the buffer used for crashinfo files, use the **exception crashinfo buffersize** command in global configuration mode. To revert to the default buffersize, use the **no** form of this command.

exception crashinfo buffersize *kilobytes*

no exception crashinfo buffersize *kilobytes*

Syntax Description	<i>kilobytes</i>	Sets the size of the buffersize to the specified value within the range of 32 to 100 kilobytes. The default is 32Kb.
---------------------------	------------------	--

Defaults	Crashinfo buffer is 32Kb.
-----------------	---------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(4)T, 12.2(11)	This command was introduced for the Cisco 3600 series only.
12.2(13)T	This command was implemented in 6400-NSP images.	

Usage Guidelines The crashinfo file saves information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). The switch writes the crash information to the console at the time of the failure, and the file is created the next time you boot the IOS image after the failure (instead of while the system is failing).

Examples In the following example, a the crashinfo buffer is set to 100Kb:

```
Router(config)# exception crashinfo buffersize 100
```

Related Commands	Command	Description
		exception crashinfo file

exception dump

To configure the router to dump a core file to a particular server when the router crashes, use the **exception dump** command in global configuration mode. To disable core dumps, use the **no** form of this command.

exception dump *ip-address*

no exception dump

Syntax Description

ip-address IP address of the server that stores the core dump file.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines



Caution

Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, File Transfer Protocol (FTP), or remote copy protocol (rcp) server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

If you use TFTP to dump the core file to a server, the router will only dump the first 16 MB of the core file. If the router's memory is larger than 16 MB, the whole core file will not be copied to the server. Therefore, use rcp or FTP to dump the core file.

The core dump is written to a file named *hostname-core* on your server, where *hostname* is the name of the router. You can change the name of the core file by configuring the **exception core-file** command.

This procedure can fail for certain types of system crashes. However, if successful, the core dump file will be the size of the memory available on the processor (for example, 16 MB for a CSC/4).

Examples

In the following example, a user configures a router to use FTP to dump a core file to the FTP server at 172.17.92.2 when it crashes:

```
ip ftp username red
ip ftp password blue
exception protocol ftp
exception dump 172.17.92.2
```

Related Commands	Command	Description
	exception core-file	Specifies the name of the core dump file.
	exception memory	Causes the router to create a core dump and reboot when certain memory size parameters are violated.
	exception spurious-interrupt	Causes the router to create a core dump and reload after a specified number of spurious interrupts.
	exception protocol	Configures the protocol used for core dumps.
	ip ftp password	Specifies the password to be used for FTP connections.
	ip ftp username	Configures the username for FTP connections.
	ip rcmd remote-username	Configures the remote username to be used when requesting a remote copy using rcp.

exception linecard

To enable storing of crash information for a line card and optionally specify the type and amount of information stored, use the **exception linecard** command in global configuration mode. To disable the storing of crash information for the line card, use the **no** form of this command.

```
exception linecard {all | slot slot-number} [corefile filename | main-memory size [k | m] |
queue-ram size [k | m] | rx-buffer size [k | m] | sqe-register-rx | sqe-register-tx | tx-buffer
size [k | m]]
```

```
no exception linecard
```

Syntax Description

all	Stores crash information for all line cards.
slot <i>slot-number</i>	Stores crash information for the line card in the specified slot. Slot numbers range from 0 to 11 for the Cisco 12012 and 0 to 7 for the Cisco 12008 router.
corefile <i>filename</i>	(Optional) Stores the crash information in the specified file in NVRAM. The default filename is <i>hostname-core-slot-number</i> (for example, <i>c12012-core-8</i>).
main-memory <i>size</i>	(Optional) Stores the crash information for the main memory on the line card and specifies the size of the crash information. Size of the memory to store is 0 to 268435456.
queue-ram <i>size</i>	(Optional) Stores the crash information for the queue RAM memory on the line card and specifies the size of the crash information. Size of the memory to store can be from 0 to 1048576.
rx-buffer <i>size</i>	(Optional) Stores the crash information for the receive and transmit buffer on the line card and specifies the size of the crash information. Size of the memory to store can be from 0 to 67108864.
tx-buffer <i>size</i>	
sqe-register-rx	(Optional) Stores crash information for the receive or transmit silicon queueing engine registers on the line card.
sqe-register-tx	
k	(Optional) The k option multiplies the specified <i>size</i> by 1K (1024), and the m option multiplies the specified <i>size</i> by 1M (1024*1024).
m	

Defaults

No crash information is stored for the line card.

If enabled with no options, the default is to store 256 MB of main memory.

Command Modes

Global configuration

Command History

Release	Modification
11.2 GS	This command was introduced.

Usage Guidelines

This command is currently supported only on Cisco 12000 series Gigabit Switch Routers (GSRs).

Use the **exception linecard** global configuration command only when directed by a technical support representative. Only enable options that the technical support representative requests you to enable. Technical support representatives need to be able to look at the crash information from the line card to troubleshoot serious problems on the line card. The crash information contains all the line card memory information including the main memory and transmit and receive buffer information.

**Caution**

Use caution when enabling the **exception linecard** global configuration command. Enabling all options could cause a large amount (150 to 250 MB) of crash information to be sent to the server.

Examples

In the following example, the user enables the storing of crash information for line card 8. By default, 256 MB of main memory is stored.

```
exception linecard slot 8
end
```

exception memory

To cause the router to create a core dump and reboot when certain memory size parameters are violated, use the **exception memory** command in global configuration mode. To disable the rebooting and core dump, use the **no** form of this command.

exception memory {*fragment size* | *minimum size*}

no exception memory {*fragment* | *minimum*}

Syntax Description	fragment <i>size</i>	The minimum contiguous block of memory in the free pool, in bytes.
	minimum <i>size</i>	The minimum size of the free memory pool, in bytes.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
		10.3

Usage Guidelines



Caution

Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, File Transfer Protocol (FTP), or remote copy protocol (rcp) server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

This command is useful to troubleshoot memory leaks.

The size is checked every 60 seconds. If you enter a size that is greater than the free memory, a core dump and router reload is generated after 60 seconds.

The **exception dump** command must be configured in order to generate a core dump file. If the **exception dump** command is not configured, the router reloads without generating a core dump.

Examples

In the following example, the user configures the router to monitor the free memory. If the amount of free memory falls below 250,000 bytes, the router will dump the core file and reload.

```
exception dump 131.108.92.2
exception core-file memory.overrun
exception memory minimum 250000
```

Related Commands	Command	Description
	exception core-file	Specifies the name of the core dump file.
	exception dump	Configures the router to dump a core file to a particular server when the router crashes.
	exception protocol	Configures the protocol used for core dumps.
	exception region-size	Specifies the size of the region for the exception-time memory pool.
	ip ftp password	Specifies the password to be used for FTP connections.
	ip ftp username	Configures the username for FTP connections.

exception protocol

To configure the protocol used for core dumps, use the **exception protocol** command in global configuration mode. To configure the router to use the default protocol, use the **no** form of this command.

exception protocol {ftp | rcp | tftp}

no exception protocol

Syntax Description

ftp	Uses File Transfer Protocol (FTP) for core dumps.
rcp	Uses remote copy protocol (rcp) for core dumps.
tftp	Uses TFTP for core dumps. This is the default.

Defaults

TFTP

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines



Caution

Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, File Transfer Protocol (FTP), or remote copy protocol (rcp) server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

If you use TFTP to dump the core file to a server, the router will only dump the first 16 MB of the core file. If the router's memory is larger than 16 MB, the whole core file will not be copied to the server. Therefore, use rcp or FTP to dump the core file.

Examples

In the following example, the user configures a router to use FTP to dump a core file to the FTP server at 172.17.92.2 when it crashes:

```
ip ftp username red
ip ftp password blue
exception protocol ftp
exception dump 172.17.92.2
```

Related Commands	Command	Description
	exception core-file	Specifies the name of the core dump file.
	exception dump	Causes the router to dump a core file to a particular server when the router crashes.
	exception memory	Causes the router to create a core dump and reboot when certain memory size parameters are violated.
	exception spurious-interrupt	Causes the router to create a core dump and reload after a specified number of spurious interrupts.
	ip ftp password	Specifies the password to be used for FTP connections.
	ip ftp username	Configures the username for FTP connections.

exception region-size

To specify the size of the region for the exception-time memory pool, use the **exception region-size** command in global configuration mode. To use the default region size, use the **no** form of this command.

exception region-size *size*

no exception region-size

Syntax Description	<i>size</i>	The size of the region for the exception-time memory pool.
---------------------------	-------------	--

Defaults	16,384 bytes
-----------------	--------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines



Caution

Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, File Transfer Protocol (FTP), or remote copy protocol (rcp) server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

The **exception region-size** command is used to define a small amount of memory to serve as a fallback pool when the processor memory pool is marked corrupt. The **exception memory** command must be used to allocate memory to perform a core dump.

Examples

In the following example, the region size is set at 1024:

```
Router# exception region-size 1024
```

Related Commands	Command	Description
	exception core-file	Specifies the name of the core dump file.
	exception dump	Configures the router to dump a core file to a particular server when the router crashes.
	exception memory	Causes the router to create a core dump and reboot when certain memory size parameters are violated.

Command	Description
exception protocol	Configures the protocol used for core dumps.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the username for FTP connections.

exception spurious-interrupt

To configure the router to create a core dump and reload after a specified number of spurious interrupts, use the **exception spurious-interrupt** command in global configuration mode. To disable the core dump and reload, use the **no** form of this command.

exception spurious-interrupt [*number*]

no exception spurious-interrupt

Syntax Description

<i>number</i>	(Optional) A number from 1 to 4294967295 that indicates the maximum number of spurious interrupts to include in the core dump before reloading.
---------------	---

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines



Caution

Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, File Transfer Protocol (FTP), or remote copy protocol (rcp) server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

If you use TFTP to dump the core dump file to a server, the router will only dump the first 16 MB of the file. If the router's memory is larger than 16 MB, the whole core file will not be copied to the server. Therefore, use rcp or FTP to dump the core file.

Examples

In the following example, the user configures a router to create a core dump with a limit of two spurious interrupts:

```
Router# exception spurious-interrupt 2
```

Related Commands	Command	Description
	exception core-file	Specifies the name of the core dump file.
	ip ftp password	Specifies the password to be used for FTP connections.
	ip ftp username	Configures the user name for FTP connections.

execute-on

To execute commands on a line card, use the **execute-on** command in privileged EXEC mode.

execute-on {*slot slot-number* | **all** | **master**} *command*

Syntax Description	
slot <i>slot-number</i>	Executes the command on the line card in the specified slot. Slot numbers can be chosen from the following ranges: <ul style="list-style-type: none"> • Cisco 12012 router: 0 to 11 • Cisco 12008 access server: 0 to 7 • Cisco AS5800 access server: 0 to 13
all	Executes the command on all line cards.
master	(AS5800 only) Executes the designated command on a Dial Shelf Controller (DSC). Do not use this option; it is used for technical support troubleshooting only.
<i>command</i>	Cisco IOS command to remotely execute on the line card.

Command Modes Privileged EXEC

Command History	Release	Modification
	11.2 GS	This command was introduced to support Cisco 12000 series Gigabit Switch Routers.
	11.3(2)AA	Support for this command was added to the Cisco AS5800 universal access server.

Usage Guidelines Use this command to execute a command on one or all line cards to monitor and maintain information on one or more line cards (for example, a line card in a specified slot on a dial shelf). This allows you to issue commands remotely; that is, to issue commands without needing to log in to the line card directly. The **all** form of the command allows you to issue commands to all the line cards without having to log in to each in turn.

Though this command does not have a **no** form, note that it is possible to use the **no** form of the remotely executed commands used in this command.



Tip

This command is useful when used with **show EXEC** commands (such as **show version**), because you can verify and troubleshoot the features found only on a specific line card. Please note, however, that because not all statistics are maintained on the line cards, the output from some of the **show** commands might not be consistent.

Cisco 12000 GSR Guidelines and Restrictions

You can use the **execute-on** privileged EXEC command only from Cisco IOS software running on the GRP card.

**Timesaver**

Though you can use the **attach** privileged EXEC command to execute commands on a specific line card, using the **execute-on slot** command saves you some steps. For example, first you must use the **attach** command to connect to the Cisco IOS software running on the line card. Next you must issue the **attach** command. Finally you must disconnect from the line card to return to the Cisco IOS software running on the GRP card. With the **execute-on slot** command, you can perform three steps with one command. In addition, the **execute-on all** command allows you to perform the same command on all line cards simultaneously.

Cisco AS5800 Guidelines and Restrictions

The purpose of the command is to conveniently enable certain commands to be remotely executed on the dial shelf cards from the router without connecting to each line card. This is the recommended procedure, because it avoids the possibility of adversely affecting a good configuration of a line card in the process. The **execute-on** command does not give access to every Cisco IOS command available on the Cisco AS5800 access server. In general, the purpose of the **execute-on** command is to provide access to statistical reports from line cards without directly connecting to the dial shelf line cards.

**Warning**

Do not use this command to change configurations on dial shelf cards, because such changes will not be reflected in the router shelf.

Using this command makes it possible to accumulate inputs for inclusion in the **show tech-support** command.

The **master** form of the command can run a designated command remotely on the router from the DSC card. However, using the console on the DSC is *not* recommended. It is used for technical support troubleshooting only.

The **show tech-support** command for each dial shelf card is bundled into the router shelf's **show tech-support** command via the **execute-on** facility.

The **execute-on** command also support interactive commands such as the following:

```
router: execute-on slave slot slot ping
```

The **execute-on** command has the same limitations and restrictions as a **vty telnet** client has; that is, it cannot reload DSC using the following command:

```
router: execute-on slave slot slot reload
```

You can use the **execute-on** command to enable remote execution of the commands included in the following partial list:

- **debug dsc clock**
- **show context**
- **show diag**
- **show environment**
- **show dsc clock**
- **show dsi**
- **show dsip**
- **show tech-support**

Examples

In the following example, the user executes the **show controllers** command on the line card in slot 4 of a Cisco 12000 series GSR:

```
Router# execute-on slot 4 show controllers
```

```
===== Line Card (Slot 4) =====
```

```
Interface POS0
Hardware is BFLC POS
lcpos_instance struct 6033A6E0
RX POS ASIC addr space 12000000
TX POS ASIC addr space 12000100
SUNI framer addr space 12000400
SUNI rsop intr status 00
CRC16 enabled, HDLC enc, int clock
no loop
```

```
Interface POS1
Hardware is BFLC POS
lcpos_instance struct 6033CEC0
RX POS ASIC addr space 12000000
TX POS ASIC addr space 12000100
SUNI framer addr space 12000600
SUNI rsop intr status 00
CRC32 enabled, HDLC enc, int clock
no loop
```

```
Interface POS2
Hardware is BFLC POS
lcpos_instance struct 6033F6A0
RX POS ASIC addr space 12000000
TX POS ASIC addr space 12000100
SUNI framer addr space 12000800
SUNI rsop intr status 00
CRC32 enabled, HDLC enc, int clock
no loop
```

```
Interface POS3
Hardware is BFLC POS
lcpos_instance struct 60341E80
RX POS ASIC addr space 12000000
TX POS ASIC addr space 12000100
SUNI framer addr space 12000A00
SUNI rsop intr status 00
CRC32 enabled, HDLC enc, ext clock
no loop
```

```
Router#
```

Related Commands

Command	Description
attach	Connects you to a specific line card for the purpose of executing commands using the Cisco IOS software image on that line card.

logging buffered

To enable system message logging to a local buffer and limit messages logged to the buffer based on severity, use the **logging buffered** command in global configuration mode. To cancel the use of the buffer, use the **no** form of this command. The **default** form of this command returns the buffer size to the default size.

logging buffered [*buffer-size* | *level*]

no logging buffered

default logging buffered

Syntax Description	
<i>buffer-size</i>	(Optional) Size of the buffer from 4096 to 4,294,967,295 bytes. The default size varies by platform.
<i>level</i>	(Optional) Limits the logging of messages to the buffer to a specified level. You can enter the level name or level number. See Table 55 for a list of the acceptable level name or level number keywords. The default logging level varies by platform, but is generally 7, meaning that messages at all levels (0-7) are logged to the buffer.

Defaults Varies by platform. For most platforms, logging to the buffer is disabled by default. When enabled, the default logging level is 7 (debugging).

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.
	11.1(17)T	The <i>level</i> argument was added.

Usage Guidelines This command copies logging messages to an internal buffer. The buffer is circular in nature, so newer messages overwrite older messages after the buffer is filled.

Specifying a level causes messages at that level and numerically lower levels to be logged in an internal buffer. See [Table 55](#) for a list of level arguments.

Do not make the buffer size too large because the router could run out of memory for other tasks. You can use the **show memory EXEC** command to view the free processor memory on the router; however, this is the maximum available and should not be approached. The **default logging buffered** command resets the buffer size to the default for the platform.

To display the messages that are logged in the buffer, use the **show logging** command. The first message displayed is the oldest message in the buffer.

The **show logging** command displays the addresses and levels associated with the current logging setup, and any other logging statistics.

Table 55 Error Message Logging Priorities and Corresponding Level Names/Numbers

Level Name	Level Number	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Examples

In the following example, the user enables standard system logging to the local syslog buffer:

```
Router(config)# logging buffered
```

Related Commands

Command	Description
clear logging	Clears messages from the logging buffer.
logging buffered xml	Enables system message logging (syslog) and sends XML-formatted logging messages to the XML-specific system buffer.
show logging	Displays the state of logging (syslog).

logging buffered xml

To enable system message logging (syslog) and send XML-formatted logging messages to the XML-specific system buffer, use the **logging buffered xml** command in global configuration mode. To disable the XML syslog buffer and return the size of the buffer to the default, use the **no** form of this command.

logging buffered xml [*xml-buffer-size*]

no logging buffered xml [*xml-buffer-size*]

Syntax Description

<i>xml-buffer-size</i>	(Optional) Size of the buffer, from 4,096 to 4,294,967,295 bytes (4 kilobytes to 2 gigabytes). The default size varies by platform. This value is ignored if entered as part of the no form of this command.
------------------------	---

Defaults

XML formatting of system logging messages is disabled.
 The default XML syslog buffer size is the same size as the standard syslog buffer.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Standard logging is enabled by default, but XML-formatted system message logging is disabled by default. If standard logging has been disabled on your system (using the **no logging on** command), standard logging must be reenabled using the **logging on** command before using the **logging buffered xml** command.

The **logging buffered xml** command copies logging messages to an internal XML buffer. The XML syslog buffer is separate from the standard syslog buffer (created using the **logging buffered** command).

The buffer is circular, so newer messages overwrite older messages as the buffer is filled.

The severity level for logged messages is determined by the setting of the **logging buffered** command. If the **logging buffered** command has not been used, the default severity level for that command is used. The default severity level varies by platform, but is generally level 7 (“debugging”), meaning that messages at all severity levels (0 through 7) are logged. For more information on severity levels, see the documentation of the **logging buffered** command.

Do not make the buffer size too large because the router could run out of memory for other tasks. You can use the **show memory EXEC** command to view the free processor memory on the router; however, this value is the maximum available and should not be approached.

To return the size of the XML logging buffer to the default, enter the **logging buffered xml** command again without a buffer size value.

To display the messages that are logged in the buffer, use the **show logging xml** command in EXEC mode. The first message displayed is the oldest message in the buffer.

Examples

In the following example, the user enables logging to the XML syslog buffer and sets the XML syslog buffer size to 14 kilobytes:

```
Router(config)# logging buffered xml 14336
```

Related Commands

Command	Description
clear logging xml	Clears all messages from the XML-specific system message logging (syslog) buffer.
logging on	Globally controls (enables or disables) system message logging.
logging buffered	Enables standard system message logging (syslog) to a local buffer and sets the severity level and buffer size for the logging buffer.
show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML-specific buffer.

logging console

To send system logging (syslog) messages to all available TTY lines and limit messages based on severity, use the **logging console** command in global configuration mode. To disable logging to the console terminal, use the **no** form of this command.

logging console [*severity-level*]

no logging console [*severity-level*]

Syntax Description

severity-level Limits the logging of messages displayed on the console terminal to the specified level and (numerically) lower levels. You can enter the level number or level name. See [Table 56](#) for a list of the level arguments.

Defaults

In general, the default is to log messages from level 0 (emergencies) to level 7 (debugging). However, the default level varies by platform.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **console** keyword indicates all available TTY lines. This can mean a console terminal attached to the router's TTY line, a dial-up modem connection, or a printer.

Specifying a level causes messages at that level and numerically lower levels to be sent to the console (TTY lines).

The **show logging EXEC** command displays the addresses and levels associated with the current logging setup, and any other logging statistics. See [Table 56](#).

Table 56 Error Message Logging Priorities and Corresponding Level Names/Numbers

Level Arguments	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

**Note**

The effect of the **log** keyword with the **IP access list** (extended) interface configuration command depends on the setting of the **logging console** command. The **log** keyword takes effect only if the logging console level is set to 6 or 7. If you change the default to a level lower than 6 and specify the **log** keyword with the **IP access list** (extended) command, no information is logged or displayed.

Examples

In the following example, the user changes the level of messages sent to the console terminal (TTY lines) to **alerts**, which means messages at levels 0 and 1 are sent:

```
Router(config)# logging console alerts
```

Related Commands

Command	Description
access-list (extended)	Defines an extended XNS access list.
logging facility	Configures the syslog facility in which error messages are sent.

logging console xml

To enable XML-formatted system message logging to the console connections, use the **logging console xml** command in global configuration mode. To disable all logging to the console connections, use the **no logging console xml** form of this command.

logging console xml [*severity-level*]

no logging console xml

Syntax Description

<i>severity-level</i>	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): <ul style="list-style-type: none"> { 0 emergencies }— System is unusable { 1 alerts }—Immediate action needed { 2 critical }—Critical conditions { 3 errors }—Error conditions { 4 warnings }—Warning conditions { 5 notifications }—Normal but significant conditions { 6 informational }—Informational messages { 7 debugging }— Debugging messages
-----------------------	--

Defaults

Logging to the console is enabled.
 XML-formatted logging to the console is disabled.
 The default severity level varies by platform, but is generally level 7 (messages at levels 0 through 7 are logged).

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

To return system logging messages to standard text (without XML formatting), issue the standard **logging console** command (without the **xml** keyword extension).

Examples

In the following example, the user enables XML-formatted system message logging to the console for messages at levels 0 through 4:

```
Router(config)# logging console xml 4
```

Related Commands	Command	Description
	show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML syslog buffer.

logging count

To enable the error log count capability, use the **logging count** command in global configuration mode. To disable the error log count capability, use the **no** form of this command.

logging count

no logging count

Syntax Description This command has no arguments or keywords.

Defaults This command is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.2(8)T	This command was introduced.

Usage Guidelines The **logging count** command counts every syslog message and time-stamps the occurrence of each message.

Examples In the following example, syslog messages are logged to the system buffer and the logging count capability is enabled:

```
Router(config)# logging buffered notifications
Router(config)# logging count
Router(config)# end
Router# show logging count
```

Facility	Message Name	Sev	Occur	Last Time
SYS	BOOTTIME	6	1	00:00:12
SYS	RESTART	5	1	00:00:11
SYS	CONFIG_I	5	3	1d00h
SYS TOTAL			5	
LINEPROTO	UPDOWN	5	13	00:00:19
LINEPROTO TOTAL			13	
LINK	UPDOWN	3	1	00:00:18
LINK	CHANGED	5	12	00:00:09
LINK TOTAL			13	
SNMP	COLDSTART	5	1	00:00:11

■ logging count

SNMP TOTAL

Related Commands

Command	Description
show logging	Displays the state of system logging (syslog).

logging facility

To configure the syslog facility in which error messages are sent, use the **logging facility** command in global configuration mode. To revert to the default of **local7**, use the **no** form of this command.

logging facility *facility-type*

no logging facility

Syntax Description	<i>facility-type</i>	Syslog facility. See the Usage Guidelines section of this command reference entry for descriptions of acceptable keywords.
---------------------------	----------------------	--

Defaults	local7
-----------------	--------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines [Table 57](#) describes the acceptable keywords for the *facility-type* argument.

Table 57 logging facility facility-type Argument

Facility-type keyword	Description
auth	Authorization system
cron	Cron facility
daemon	System daemon
kern	Kernel
local0–7	Reserved for locally defined messages
lpr	Line printer system
mail	Mail system
news	USENET news
sys9	System use
sys10	System use
sys11	System use
sys12	System use
sys13	System use
sys14	System use
syslog	System log

Table 57 *logging facility facility-type Argument (continued)*

Facility-type keyword	Description
user	User process
uucp	UNIX-to-UNIX copy system

Examples

In the following example, the user configures the syslog facility to the kernel facility type:

```
logging facility kern
```

Related Commands

Command	Description
logging console	Limits messages logged to the console based on severity.

logging history

To limit syslog messages sent to the router’s history table and to an SNMP network management station based on severity, use the **logging history** command in global configuration mode. To return the logging of syslog messages to the default level, use the **no** form of this command with the previously configured severity level argument.

logging history [*severity-level-name* | *severity-level-number*]

no logging history [*severity-level-name* | *severity-level-number*]

Syntax Description		
<i>severity-level-name</i>	Name of the severity level. Specifies the lowest severity level for system error message logging. See the Usage Guidelines section of this command for available keywords.	
<i>severity-level-number</i>	Number of the severity level. Specifies the lowest severity level for system error message logging. See the Usage Guidelines section of this command for available keywords.	

Defaults Logging of error messages of severity levels 0 through 4 (emergency, alert, critical, error, and warning levels); in other words, “saving level warnings or higher”

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines The sending of syslog messages to an SNMP network management station (NMS) occurs when you enable syslog traps with the **snmp-server enable traps syslog** global configuration mode command. Because SNMP traps are potentially unreliable, at least one syslog message, the most recent message, is stored in a history table on the router. The history table, which contains table size, message status, and message text data, can be viewed using the **show logging history** command. The number of messages stored in the table is governed by the **logging history size** global configuration mode command. Severity levels are numbered 0 through 7, with 0 being the highest severity level and 7 being the lowest severity level (that is, the lower the number, the more critical the message). Specifying a *level* causes messages at that severity level and numerically lower levels to be stored in the router’s history table and sent to the SNMP network management station. For example, specifying the level **critical** causes messages as the critical (3), alert (2), and emergency (1) levels to be saved to the logging history table. [Table 58](#) provides a description of logging severity levels, listed from highest severity to lowest severity, and the arguments used in the **logging history** command syntax. Note that you can use the level name or the level number as the *level* argument in this command.

Table 58 Syslog Error Message Severity Levels

Severity Level Name	Severity Level Number	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Examples

In the following example, the system is initially configured to the default of saving severity level 4 or higher. The **logging history 1** command is used to configure the system to save only level 1 (alert) and level 0 (emergency) messages to the logging history table, and, by extension, to send only these levels in the SNMP notifications. The configuration is then confirmed using the **show logging history** command.

```
Router#show logging history
Syslog History Table:10 maximum table entries,
! The following line shows that system-error-message-logging is set to the
! default level of "warnings" (4).
saving level warnings or higher
23 messages ignored, 0 dropped, 0 recursion drops
1 table entries flushed
SNMP notifications not enabled
  entry number 2 : LINK-3-UPDOWN
    Interface FastEthernet0, changed state to up
    timestamp: 2766
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#logging history 1
Router(config)#snmp-server enable traps syslog
Router(config)#end
Router#
4w0d: %SYS-5-CONFIG_I: Configured from console by console
Router#show logging history
Syslog History Table:1 maximum table entries,
! The following line indicates that 'logging history level 1' (alerts) is configured.
saving level alerts or higher
18 messages ignored, 0 dropped, 0 recursion drops
1 table entries flushed
SNMP notifications enabled, 0 notifications sent
  entry number 2 : LINK-3-UPDOWN
    Interface FastEthernet0, changed state to up
    timestamp: 2766
Router#
```

Related Commands	Command	Description
	logging on	Controls (enables or disables) the logging of error messages.
	logging history size	Sets the maximum number of syslog messages that can be stored in the router's syslog history table.
	show logging	Displays the state of system logging (syslog) and contents of the local logging buffer.
	show logging history	Displays information about the system logging history table.
	snmp-server enable traps syslog	Controls (enables or disables) the sending of SYSLOG MIB notifications.
	snmp-server host	Specifies the recipient of an SNMP notification operation.

logging history size

To change the number of syslog messages stored in the router's history table, use the **logging history size** command in global configuration mode. To return the number of messages to the default value, use the **no** form of this command.

logging history size *number*

no logging history size

Syntax Description	<i>number</i>	Number from 1 to 500 that indicates the maximum number of messages stored in the history table.
---------------------------	---------------	---

Defaults	One message
-----------------	-------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines	When the history table is full (that is, it contains the maximum number of message entries specified with the logging history size command), the oldest message entry is deleted from the table to allow the new message entry to be stored.
-------------------------	---

Examples	In the following example, the user sets the number of messages stored in the history table to 20: <pre>logging history size 20</pre>
-----------------	---

Related Commands	Command	Description
	logging history	Limits syslog messages sent to the router's history table and the SNMP network management station based on severity.
	show logging	Displays the state of logging (syslog).

logging host

To log system messages and debug output to a remote host, use the **logging host** command in global configuration mode. To remove a specified logging host from the configuration, use the **no** form of this command.

logging host {*ip-address* | *host-name*} [**xml**]

no logging host {*ip-address* | *host-name*} [**xml**]

Syntax Description

<i>ip-address</i>	IP address of the host to be used as a syslog server.
<i>host-name</i>	Name of the host to be used as a syslog server.
xml	(Optional) Specifies that the logging output should be tagged using the Cisco defined XML tags. This applies to system logging messages only (not to debug command output).

Defaults

System logging messages are not sent to any remote host.

If this command is entered without the **xml** keyword, messages are sent in the standard format.

Command Modes

Global configuration

Command History

Release	Modification
10.0	The logging command was introduced.
12.0(14)S, 12.0(14)ST, 12.2(15)T	The logging host command replaced the logging command.
12.2(15)T	The xml keyword was added.

Usage Guidelines

System logging messages are also called system error messages.

Standard system message logging (syslog) is enabled by default. If logging has been disabled on your system (using the **no logging on** command), logging must be reenabled using the **logging on** command before using the **logging host** command.

The **logging host** command identifies a remote host (syslog server) to receive logging messages. By issuing this command more than once, you build a list of syslog servers that receive logging messages.

To specify the severity level for logging to all hosts, use the **logging trap** command.

You can specify that standard syslog messages are to be sent to one or more hosts while XML-formatted messages are to be sent to another host (or hosts) by repeating this command with the appropriate syntax.

If you enter the **logging host** {*ip-address* | *host-name*} command after entering the **logging host** {*ip-address* | *host-name*} **xml** command and you use the same IP address or host name in both commands, XML formatting is disabled for that host, and messages will be sent in the standard format. In other words, a standard **logging host** command will replace an XML **logging host** command, and vice versa, if the same host is specified.

**Note**

Any **no logging host** command (with or without the **xml** keyword) will disable all logging to the specified host.

Examples

In the following example, messages at severity levels 0 (emergencies) through 5 (notifications) are logged to a host at 209.165.202.169:

```
Router(config)# logging host 209.165.202.169
Router(config)# logging trap 5
```

Related Commands

Command	Description
logging on	Globally controls (enables or disables) system message logging.
logging trap	Limits messages sent to the syslog servers based on severity level.
show logging	Displays the state of system message logging, followed by the contents of the standard syslog buffer.
show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML syslog buffer.

logging linecard

To log messages to an internal buffer on a line card, use the **logging linecard** command in global configuration mode. To cancel the use of the internal buffer on the line cards, use the **no** form of this command.

logging linecard [*size* | *level*]

no logging linecard

Syntax Description	size	(Optional) Size of the buffer used for each line card. The range is from 4096 to 65,536 bytes. The default is 8 KB.
	level	(Optional) Limits the logging of messages displayed on the console terminal to a specified level. The message level can be one of the following: <ul style="list-style-type: none"> • alerts—Immediate action needed • critical—Critical conditions • debugging—Debugging messages • emergencies—System is unusable • errors—Error conditions • informational—Informational messages • notifications—Normal but significant conditions • warnings—Warning conditions

Defaults The Cisco IOS software logs messages to the internal buffer on the GRP card.

Command Modes Global configuration

Command History	Release	Modification
	11.2 GS	This command was added to support the Cisco 12000 series Gigabit Switch Routers.

Usage Guidelines Specifying a message level causes messages at that level and numerically lower levels to be stored in the internal buffer on the line cards.

[Table 59](#) lists the message levels and associated numerical level. For example, if you specify a message level of critical, all critical, alert, and emergency messages will be logged.

Table 59 *Message Levels*

Level Keyword	Level
emergencies	0
alerts	1
critical	2
errors	3
warnings	4
notifications	5
informational	6
debugging	7

To display the messages that are logged in the buffer, use the **show logging slot** EXEC command. The first message displayed is the oldest message in the buffer.

Do not make the buffer size too large because the router could run out of memory for other tasks. You can use the **show memory** EXEC command to view the free processor memory on the router; however, this is the maximum available and should not be approached.

Examples

The following example enables logging to an internal buffer on the line cards using the default buffer size and logging warning, error, critical, alert, and emergency messages:

```
logging linecard warnings
end
```

Related Commands

Command	Description
clear logging	Clears messages from the logging buffer.
show logging	Displays the state of logging (syslog).

logging monitor

To enable system message logging to the terminal lines (monitor connections) and limit these messages based on severity, use the **logging monitor** command in global configuration mode. To disable logging to terminal lines other than the console line, use the **no** form of this command.

logging monitor *severity-level*

no logging monitor

Syntax Description

<i>severity-level</i>	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): { 0 emergencies }— System is unusable { 1 alerts }—Immediate action needed { 2 critical }—Critical conditions { 3 errors }—Error conditions { 4 warnings }—Warning conditions { 5 notifications }—Normal but significant conditions { 6 informational }—Informational messages { 7 debugging }— Debugging messages
-----------------------	--

Defaults

debugging (severity-level 7)

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Specifying a *severity-level* causes messages only at that level and numerically lower levels to be displayed to the monitor (terminal lines).

Examples

In the following example, the user specifies that only messages of the levels **errors**, **critical**, **alerts**, and **emergencies** be logged to monitor connections:

```
Router(config)# logging monitor 3
```

Related Commands

Command	Description
logging monitor xml	Applies XML formatting to messages logged to the monitor connections.
terminal monitor	Displays debug command output and system error messages for the current terminal and session.

logging monitor xml

To enable XML-formatted system message logging to monitor connections, use the **logging console xml** command in global configuration mode. To disable all logging to the monitor connections, use the **no** form of this command.

logging monitor xml [*severity-level*]

no logging monitor xml

Syntax Description

<i>severity-level</i>	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): {0 emergencies }— System is unusable {1 alerts }—Immediate action needed {2 critical }—Critical conditions {3 errors }—Error conditions {4 warnings }—Warning conditions {5 notifications }—Normal but significant conditions {6 informational }—Informational messages {7 debugging }— Debugging messages
-----------------------	--

Defaults

Logging to monitor connections is enabled.
 XML-formatted logging to monitor connections is disabled.
 The default severity level varies by platform, but is generally level 7 (messages at levels 0 through 7 are logged).

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The **monitor** keyword specifies the TTY (TeleTYpe) line connections at all line ports. TTY lines (also called ports) communicate with peripheral devices such as terminals, modems, and serial printers. An example of a TTY connection is a PC with a terminal emulation program connected to the device using a dial-up modem, or a Telnet connection.

To return system logging messages to standard text (without XML formatting), issue the standard **logging monitor** command (without the **xml** keyword extension).

Examples

In the following example, the user enables XML-formatted system message logging to the console for messages at levels 0 through 4 and XML-formatted system message logging to TTY line connections at the default severity level:

```
Router(config)# logging console xml 4
Router(config)# logging monitor xml
```

Related Commands

Command	Description
logging monitor	Enables system message logging in standard (plain text) format to all monitor (TTY) connections.
show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML syslog buffer.

logging on

To enable logging of system messages, use the **logging on** command in global configuration mode. This command sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages. To disable the logging process, use the **no** form of this command.

logging on

no logging on

Syntax Description

This command has no arguments or keywords.

Defaults

The Cisco IOS software sends messages to the asynchronous logging process.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, terminal lines, or syslog server. System logging messages are also known as system error messages. You can turn logging on and off for these destinations individually using the **logging buffered**, **logging monitor**, and **logging** global configuration commands. However, if the **logging on** command is disabled, no messages will be sent to these destinations. Only the console will receive messages.

Additionally, the logging process logs messages to the console and the various destinations after the processes that generated them have completed. When the logging process is disabled, messages are displayed on the console as soon as they are produced, often appearing in the middle of command output.



Caution

Disabling the **logging on** command may substantially slow down the router. Any process generating debug or error messages will wait until the messages have been displayed on the console before continuing.

The **logging synchronous** line configuration command also affects the displaying of messages to the console. When the **logging synchronous** command is enabled, messages will appear only after the user types a carriage return.

Examples

The following example shows command output and message output when logging is enabled. The ping process finishes before any of the logging information is printed to the console (or any other destination).

```
Router(config)# logging on
Router(config)# end
```

```
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router# ping dirt

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.129, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
Router#
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
```

In the following example, logging is disabled. The message output is displayed as messages are generated, causing the debug messages to be interspersed with the message “Type escape sequence to abort.”

```
Router(config)# no logging on
Router(config)# end

%SYS-5-CONFIG_I: Configured from console by console
Router#
Router# ping dirt

IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sendingTyp
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1e
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending esc
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sendingape
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sendingse
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sendingquen
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1ce to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.129, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 152/152/156 ms
Router#
```

Related Commands

Command	Description
logging host	Logs messages to a syslog server host.
logging buffered	Logs messages to an internal buffer.
logging console	Logs messages to console connections.
logging monitor	Limits messages logged to the terminal lines (monitors) based on severity.
logging synchronous	Synchronizes unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty.

logging rate-limit

To limit the rate of messages logged per second, use the **logging rate-limit** command in global configuration mode. To disable the limit, use the **no** form of this command.

logging rate-limit { *number* | **all** | **console** } [**except** *severity*]

no logging rate-limit

Syntax Description		
<i>number</i>		Specifies rate of messages logged per second. The valid values are from 1 to 10000.
all		Sets the rate limit to all messages including the debug messages.
console		Sets the rate limit only to console messages.
except		(Optional) Excludes messages of this severity or higher.
<i>severity</i>		(Optional) Sets the logging severity level. The valid levels are from 0 to 7.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced.

Usage Guidelines The **logging rate-limit** command controls the output of messages from the system. Use this command if you want to avoid a flood of output messages. You can select the severity of the output messages and output rate by using the **logging rate-limit** command. You can use the **logging rate-limit** command anytime; it will not negatively impact the performance of your system and may improve the system performance by specifying the severities and rates of output messages.

You can use this command with or without the **logging synchronous** line configuration command. For example, if you want to see all severity 0, 1, and 2 messages, use the **no logging synchronous** command and specify **logging rate-limit 10 except 2**. By using the two commands together, you cause all messages of 0, 1, and 2 severity to print and limit the less severe ones (higher than 2) to only 10 per second.

Table 60 compares the error message logging numeric severity level with its equivalent word description.

Table 60 Error Message Logging Severity Level and Equivalent Word Descriptions

Numeric Severity Level	Equivalent Word	Description
0	emergencies	System unusable
1	alerts	Immediate action needed
2	critical	Critical conditions
3	errors	Error conditions
4	warnings	Warning conditions
5	notifications	Normal but significant condition
6	informational	Informational messages only
7	debugging	Debugging messages

For additional details about error message logging, see the “Troubleshooting the Router” chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2* .

Examples

In the following example, the **logging rate-limit** configuration mode command limits message output to 200 per second:

```
Router(config)# logging rate-limit 200
```

Related Commands

Command	Description
logging synchronous	Synchronizes unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty.

logging source-interface

To specify the source IP address of syslog packets, use the **logging source-interface** command in global configuration mode. To remove the source designation, use the **no** form of this command.

logging source-interface *interface-type interface-number*

no logging source-interface

Syntax Description		
	<i>interface-type</i>	Interface type.
	<i>interface-number</i>	Interface number.

Defaults No interface is specified.

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.

Normally, a syslog message contains the IP address of the interface it uses to leave the router. The **logging source-interface** command specifies that syslog packets contain the IP address of a particular interface, regardless of which interface the packet uses to exit the router.

Examples In the following example, the user specifies that the IP address for Ethernet interface 0 is the source IP address for all syslog messages:

```
logging source-interface ethernet 0
```

The following example specifies that the IP address for Ethernet interface 2/1 on a Cisco 7000 series router is the source IP address for all syslog messages:

```
logging source-interface ethernet 2/1
```

Related Commands	Command	Description
	logging	Logs messages to a syslog server host.

logging synchronous

To synchronize unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty, use the **logging synchronous** command in line configuration mode. To disable synchronization of unsolicited messages and debug output, use the **no** form of this command.

logging synchronous [*level severity-level* | **all**] [*limit number-of-buffers*]

no logging synchronous [*level severity-level* | **all**] [*limit number-of-buffers*]

Syntax Description

level <i>severity-level</i>	(Optional) Specifies the message severity level. Messages with a severity level equal to or higher than this value are printed asynchronously. Low numbers indicate greater severity and high numbers indicate lesser severity. The default value is 2.
all	(Optional) Specifies that all messages are printed asynchronously, regardless of the severity level.
limit <i>number-of-buffers</i>	(Optional) Specifies the number of buffers to be queued for the terminal after which new messages are dropped. The default value is 20.

Defaults

This feature is turned off by default.

If you do not specify a severity level, the default value of 2 is assumed.

If you do not specify the maximum number of buffers to be queued, the default value of 20 is assumed.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When synchronous logging of unsolicited messages and debug output is turned on, unsolicited Cisco IOS software output is displayed on the console or printed after solicited Cisco IOS software output is displayed or printed. Unsolicited messages and debug output is displayed on the console after the prompt for user input is returned. To keep unsolicited messages and debug output from being interspersed with solicited software output and prompts. After the unsolicited messages are displayed, the console displays the user prompt again.

When specifying a severity level number, consider that for the logging system, low numbers indicate greater severity and high numbers indicate lesser severity.

When a message queue limit of a terminal line is reached, new messages are dropped from the line, although these messages might be displayed on other lines. If messages are dropped, the notice “%SYS-3-MSGLOST *number-of-messages* due to overflow” follows any messages that are displayed. This notice is displayed only on the terminal that lost the messages. It is not sent to any other lines, any logging servers, or the logging buffer.



Caution

By configuring abnormally large message queue limits and setting the terminal to “terminal monitor” on a terminal that is accessible to intruders, you expose yourself to “denial of service” attacks. An intruder could carry out the attack by putting the terminal in synchronous output mode, making a Telnet connection to a remote host, and leaving the connection idle. This could cause large numbers of messages to be generated and queued, and these messages would unlikely consume all available RAM. You should guard against this type of attack through proper configuration.

Examples

In the following example, line 4 is identified and synchronous logging for line 4 is enabled with a severity level of 6. Then another line, line 2, is identified and the synchronous logging for line 2 is enabled with a severity level of 7 and is specified with a maximum number of buffers to be 70,000.

```
line 4
logging synchronous level 6
line 2
logging synchronous level 7 limit 70000
```

Related Commands

Command	Description
line	Identifies a specific line for configuration and starts the line configuration command collection mode.
logging on	Controls logging of error messages and sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages.

logging trap

To limit messages logged to the syslog servers based on severity, use the **logging trap** command in global configuration mode. The command limits the logging of error messages sent to syslog servers to only those messages at the specified level. To disable logging to syslog servers, use the **no** form of this command.

logging trap *level*

no logging trap

Syntax Description

level Limits the logging of messages to the syslog servers to a specified level. You can enter the level number or level name. See the Usage Guidelines section for a list of acceptable *level* keywords.

Defaults

informational (level 6)

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **show logging EXEC** command displays the addresses and levels associated with the current logging setup. The command output also includes ancillary statistics.

Table 1 lists the syslog definitions that correspond to the debugging message levels. Additionally, four categories of messages are generated by the software, as follows:

- Error messages about software or hardware malfunctions at the LOG_ERR level.
- Output for the debug commands at the LOG_WARNING level.
- Interface up/down transitions and system restarts at the LOG_NOTICE level.
- Reload requests and low process stacks at the LOG_INFO level.

Use the **logging** and **logging trap** commands to send messages to a UNIX syslog server.

Table 61 logging trap Error Message Logging Priorities

Level Arguments	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING

Table 61 logging trap Error Message Logging Priorities (continued)

Level Arguments	Level	Description	Syslog Definition
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Examples

In the following example, the messages to a host named john is logged:

```
logging john
logging trap notifications
```

Related Commands

Command	Description
logging	Logs messages to a syslog server host.

ping

To diagnose basic network connectivity on AppleTalk, ATM, Connectionless Network Service (CLNS), DECnet, IP, Novell IPX, or source-route bridging (SRB) networks, use the **ping** command in user EXEC mode or privileged EXEC mode.

ping *[[protocol | tag | vrf] {host-name | system-address}]*

Syntax Description	
<i>protocol</i>	(Optional) Protocol keyword, one of appletalk , atm , clns , decnet , ipx , or srb . Note The ping atm interface atm , ping ip , ping ipv6 , and ping sna commands are documented separately.
tag	(Optional) Specifies a tag encapsulated IP (tag IP) ping.
vrf	(Optional) Specifies a ping over an MPLS VPN network.
<i>host-name</i>	Host name of the system to ping. If a <i>host-name</i> or <i>system-address</i> is not specified at the command line, it will be required in the ping system dialog.
<i>system-address</i>	Address of the system to ping. If a <i>host-name</i> or <i>system-address</i> is not specified at the command line, it will be required in the ping system dialog.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(7)T	The ping sna command was introduced.
	12.1(12c)E	The vrf keyword was added.
	12.2(2)T	Support for the IPv6 protocol was added.
	12.2(13)T	The atm protocol keyword was added. The following keywords were removed because the Apollo Domain, Banyan VINES, and XNS protocols are no longer supported in Cisco IOS software: <ul style="list-style-type: none"> • apollo • vines • xns

Usage Guidelines The **ping** command sends an echo request packet to an address, and then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning. For example, the **ping clns** command sends International Organization for Standardization (ISO) CLNS echo packets to test the reachability of a remote router over a connectionless Open System Interconnection (OSI) network.

If you enter the **ping** command without any other syntax (**ping**<cr>), the CLI will display a system dialog that prompts you for the additional syntax appropriate to the protocol you specify (See the “Examples” section).

To abnormally terminate a ping session, type the escape sequence—by default, **Ctrl-^ 6X**. You type the default by simultaneously pressing and releasing the **Ctrl**, **Shift**, and **6** keys and then pressing the **X** key.

Table 62 describes the test characters sent by the **ping** facility.

Table 62 ping Test Characters

Character	Description
!	Each exclamation point indicates receipt of a reply.
.	Each period indicates that the network server timed out while waiting for a reply.
U	A destination unreachable error protocol data unit (PDU) was received.
C	A congestion experienced packet was received.
I	User interrupted test.
?	Unknown packet type.
&	Packet lifetime exceeded.



Note

Not all protocols require hosts to support pings. For some protocols, the pings are Cisco-defined and can be answered only by another Cisco router.

The availability of protocol keywords depends on what protocols are enabled on your system.

Issuing the **ping** command in User EXEC mode will generally offer fewer syntax options than issuing the **ping** command in Privileged EXEC mode.

Examples

After you enter the **ping** command in privileged EXEC mode, the system prompts for one of the following keywords: **atm**, **clns**, **decnet**, **ip**, **ipv6**, **ipx**, or **srp**. The default protocol is IP.

If you enter a host name or address on the same line as the **ping** command, the default action is taken as appropriate for the protocol type of that name or address.

The following example is sample dialog from the **ping** command using default values. The specific dialog varies somewhat from protocol to protocol.

```
Router# ping

Protocol [ip]:
Target IP address: 192.168.7.27

Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/2/4 ms
```

Table 63 describes the relevant fields shown in the display.

Table 63 ping Field Descriptions for IP

Field	Description
Protocol [ip]:	Prompts for a supported protocol. Enter atm , clns , decnet , ip , ipv6 , ipx , or srp . Default: ip .
Target IP address:	Prompts for the IP address or host name of the destination node you plan to ping. If you have specified a supported protocol other than IP, enter an appropriate address for that protocol here. Default: none.
Repeat count [5]:	Number of ping packets that will be sent to the destination address. Default: 5.
Datagram size [100]:	Size of the ping packet (in bytes). Default: 100 bytes.
Timeout in seconds [2]:	Timeout interval. Default: 2 (seconds).
Extended commands [n]:	Specifies whether a series of additional commands appears.
Sweep range of sizes [n]:	Allows you to vary the sizes of the echo packets being sent. This capability is useful for determining the minimum sizes of the MTUs ¹ configured on the nodes along the path to the destination address. Packet fragmentation contributing to performance problems can then be reduced.
!!!!	Each exclamation point (!) indicates receipt of a reply. A period (.) indicates that the network server timed out while waiting for a reply. Other characters may appear in the ping output display, depending on the protocol type.
Success rate is 100 percent	Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.
round-trip min/avg/max = 1/2/4 ms	Round-trip travel time intervals for the protocol echo packets, including minimum/average/maximum (in milliseconds).

1. MTU = maximum transmission unit

The following example verifies connectivity to the neighboring ATM device for the ATM PVC with the virtual path identifier (VPI)/virtual channel identifier (VCI) value 0/16:

```
Router# ping

Protocol [ip]:atm
ATM Interface:atm1/0
VPI value [0]:
VCI value [1]:16
Loopback - End(0), Segment(1) [0]:1
Repeat Count [5]:
Timeout [2]:
Type escape sequence to abort.
Sending 5, 53-byte segment OAM echoes, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Table 64 describes the default ping fields shown in the display.

Table 64 ping Field Descriptions for ATM

Field	Description
Protocol [ip]:	Prompt for a supported protocol. Enter appletalk , atm , clns , ip , novell , apollo , vines , decnet , or xns . Default: ip .
ATM Interface:	Prompt for the ATM interface.
VPI value [0]:	Prompt for the virtual path identifier. Default: 0.
VCI value [1]:	Prompt for the virtual channel identifier. Default: 1.
Loopback - End(0), Segment(1) [0]:	Prompt to specify end loopback, which verifies end-to-end PVC integrity, or segment loopback, which verifies PVC integrity to the neighboring ATM device. Default: segment loopback.
Repeat Count [5]:	Number of ping packets that will be sent to the destination address. Default: 5.
Timeout [2]:	Timeout interval. Default: 2 (seconds).
!!!!	Each exclamation point (!) indicates receipt of a reply. A period (.) indicates that the network server timed out while waiting for a reply. Other characters may appear in the ping output display, depending on the protocol type.
Success rate is 100 percent	Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.
round-trip min/avg/max = 1/1/1 ms	Round-trip travel time intervals for the protocol echo packets, including minimum/average/maximum (in milliseconds).

Related Commands

Command	Description
ping atm interface atm	Tests the connectivity of a specific PVC.
ping ip	Tests network connectivity on IP networks.
ping ipv6	Tests the connection to a remote host on the network using IPv6.
ping sna	Tests network integrity and timing characteristics over an SNA Switching network.

ping ip

To test network connectivity on IP networks, use the **ping ip** command in privileged EXEC mode.

```
ping ip { host-name | system-address } [data [hex-data-pattern] | df-bit | repeat [repeat-count] | size [datagram-size] ] [source { source-address | source-interface } ] [timeout seconds] [validate]
```

Syntax Description

<i>host-name</i>	Host name of the system to ping.
<i>system-address</i>	Address of the system to ping.
data <i>hex-data-pattern</i>	(Optional) Specifies the data pattern. Range is from 0 to FFFF.
df-bit	(Optional) Enables the “do-not-fragment” bit in the IP header.
repeat <i>repeat-count</i>	(Optional) Specifies the number of pings sent. The range is from 1 to 2147483647. The default is 5.
size	(Optional) Specifies the datagram size. Datagram size is the number of bytes in each ping.
<i>datagram-size</i>	(Optional) Range is from 40 to 18024.
source	(Optional) Specifies the source address or source interface.
<i>source-address</i>	(Optional) IP address to use as the source in the ping packets.
<i>source-interface</i>	(Optional) Name of the interface from which the ping should be sent, and the Interface ID (slot/port/number). Interface name keywords include the following: <ul style="list-style-type: none"> • async (Asynchronous Interface) • bvi (Bridge-Group Virtual Interface) • ctunnel • dialer • ethernet • fastEthernet • lex • loopback • multilink (Multilink-group interface) • null • port-channel (Ethernet channel of interfaces) • tunnel • vif (PGM Multicast Host interface) • virtual-template • virtual-tokenring • xtagatm (Extended Tag ATM interface) <p>The availability of these keywords depends on your system hardware.</p>
timeout <i>seconds</i>	(Optional) Specifies the timeout interval in seconds. The default is 2 seconds. Range is from 0 to 3600.
validate	(Optional) Validates the reply data.

Command Modes Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.0	The data , df-bit , repeat , size , source , timeout , and validate keywords were added.

Usage Guidelines The **ping** command sends an echo request packet to an address, then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

To abnormally terminate a ping session, type the escape sequence—by default, **Ctrl-^ X**. You type the default by simultaneously pressing and releasing the **Ctrl**, **Shift**, and **6** keys, and then pressing the **X** key.

Table 65 describes the test characters that the ping facility sends.

Table 65 ping Test Characters

Character	Description
!	Each exclamation point indicates receipt of a reply.
.	Each period indicates that the network server timed out while waiting for a reply.
U	A destination unreachable error protocol data unit (PDU) was received.
C	A congestion experienced packet was received.
I	User interrupted test.
?	Unknown packet type.
&	Packet lifetime exceeded.



Note Not all protocols require hosts to support pings. For some protocols, the pings are Cisco-defined and are only answered by another Cisco router.

Examples After you enter the **ping** command in privileged mode, the system prompts for one of the following keywords: **apollo**, **appletalk**, **clns**, **decnet**, **ip**, **novell**, **vines**, or **xns**. The default protocol is IP.

If you enter a host name or address on the same line as the **ping** command, the default action is taken as appropriate for the protocol type of that name or address.

The optional **data**, **df-bit**, **repeat**, **size**, **source**, **timeout**, and **validate** keywords can be used to avoid extended **ping** command output. You can use as many of these keywords as you need, and you can use them in any order after the *host-name* or *system-address* arguments.

Although the precise dialog varies somewhat from protocol to protocol, all are similar to the ping session using default values shown in the following output:

```
Router# ping
Protocol [ip]:
Target IP address: 192.168.7.27
```

```
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/2/4 ms
```

Table 66 describes the default ping fields shown in the display.

Table 66 ping Field Descriptions

Field	Description
Protocol [ip]:	Prompts for a supported protocol. Enter appletalk , clns , ip , novell , apollo , vines , decnet , or xns . The default is IP.
Target IP address:	Prompts for the IP address or host name of the destination node you plan to ping. If you have specified a supported protocol other than IP, enter an appropriate address for that protocol here. The default is none.
Repeat count [5]:	Prompts for the number of ping packets that will be sent to the destination address. The default is 5 packets.
Datagram size [100]:	Prompts for the size of the ping packet (in bytes). The default is 100 bytes.
Timeout in seconds [2]:	Prompts for the timeout interval. The default is 2 seconds.
Extended commands [n]:	Specifies whether a series of additional commands appears.
Sweep range of sizes [n]:	Allows you to vary the sizes of the echo packets being sent. This capability is useful for determining the minimum sizes of the MTUs configured on the nodes along the path to the destination address. Packet fragmentation contributing to performance problems can then be reduced.
!!!!	Each exclamation point (!) indicates receipt of a reply. A period (.) indicates that the network server timed out while waiting for a reply. Other characters may appear in the ping output display, depending on the protocol type.
Success rate is 100 percent	Indicates the percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.
round-trip min/avg/max = 1/2/4 ms	Indicates the round-trip travel time intervals for the protocol echo packets, including minimum/average/maximum (in milliseconds).

Related Commands

Command	Description
ping ipv6	Tests the connection to a remote host on the network using IPv6.

service sequence-numbers

To enable visible sequence numbering of system logging messages, use the **service sequence-numbers** command in global configuration mode. To disable visible sequence numbering of logging messages, use the **no** form of this command.

service sequence-numbers

no service sequence-numbers

Syntax Description This command has no arguments or keywords.

Defaults Disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.0	This command was introduced.

Usage Guidelines Each system status messages logged in the system logging process have a sequence reference number applied. This command makes that number visible by displaying it with the message. The sequence number is displayed as the first part of the system status message. See the description of the **logging** commands for information on displaying logging messages.

Examples In the following example logging message sequence numbers are enabled:

```
.Mar 22 15:28:02 PST: %SYS-5-CONFIG_I: Configured from console by console
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# service sequence-numbers
Router(config)# end
Router#
000066: .Mar 22 15:35:57 PST: %SYS-5-CONFIG_I: Configured from console by console
```

Related Commands	Command	Description
	logging on	Enables system logging globally.
	service timestamps	Enables time-stamping of system logging messages or debugging messages.

service slave-log

To allow slave Versatile Interface Processor (VIP) cards to log important error messages to the console, use the **service slave-log** command in global configuration mode. To disable slave logging, use the **no** form of this command.

service slave-log

no service slave-log

Syntax Description This command has no arguments or keywords.

Defaults This command is enabled by default.

Command Modes Global configuration

Release	Modification
11.1	This command was introduced.

Usage Guidelines This command allows slave slots to log error messages of level 2 or higher (critical, alerts, and emergencies).

Examples In the following example, important messages from the slave cards to the console are logged:

```
service slave-log
```

In the following example sample output is illustrated when this command is enabled:

```
%IPC-5-SLAVELOG: VIP-SLOT2:
IPC-2-NOMEM: No memory available for IPC system initialization
```

The first line indicates which slot sent the message. The second line contains the error message.

service tcp-keepalives-in

To generate keepalive packets on idle incoming network connections (initiated by the remote host), use the **service tcp-keepalives-in** command in global configuration mode. To disable the keepalives, use the **no** form of this command.

service tcp-keepalives-in

no service tcp-keepalives-in

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Examples In the following example, keepalives on incoming TCP connections are generated:

```
service tcp-keepalives-in
```

Related Commands	Command	Description
	service tcp-keepalives-out	Generates keepalive packets on idle outgoing network connections (initiated by a user).

service tcp-keepalives-out

To generate keepalive packets on idle outgoing network connections (initiated by a user), use the **service tcp-keepalives-out** command in global configuration mode. To disable the keepalives, use the **no** form of this command.

service tcp-keepalives-out

no service tcp-keepalives-out

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

In the following example, keepalives on outgoing TCP connections are generated:

```
service tcp-keepalives-out
```

Related Commands

Command	Description
service tcp-keepalives-in	Generates keepalive packets on idle incoming network connections (initiated by the remote host).

service timestamps

To configure the system to time-stamp debugging or system logging messages, use one of the **service timestamps** commands in global configuration mode. To disable this service, use the **no** form of this command.

service timestamps { debug | log } uptime

service timestamps { debug | log } datetime [msec] [localtime] [show-timezone] [year]

no service timestamps [debug | log]

Syntax Description

debug	Indicates that the timestamp should be applied to debugging messages.
log	Indicates that the timestamp should be applied to system logging messages.
uptime	Time stamp with the time since the system was rebooted. The time stamp format for uptime is HHHH:MM:SS.
datetime	Time stamp with the date and time. The time stamp format for datetime is MMM DD HH:MM:SS.
msec	(Optional) Include milliseconds in the time stamp.
localtime	(Optional) Time stamp relative to the local time zone.
year	Include the year in the datetime format.
show-timezone	(Optional) Include the time zone name in the time stamp.

Defaults

No time-stamping.

If the **service timestamps** command is specified with no arguments or keywords, the default is **service timestamps debug uptime**.

The default for the **service timestamps type datetime** command is to format the time in Coordinated Universal Time (UTC), with no milliseconds and no time zone name.

The **no service timestamps** command by itself disables time stamps for both debug and log messages.

To set the local timezone, use the **clock timezone zone hours-offset** command in global configuration mode.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(15)T	The year keyword was added.

Usage Guidelines

Time stamps can be added to either debugging or logging messages independently. The **uptime** form of the command adds time stamps in the format HHHH:MM:SS, indicating the time since the system was rebooted. The **datetime** form of the command adds time stamps in the format MMM DD HH:MM:SS, indicating the date and time according to the system clock.

The timestamp will be preceded by an asterisk or period if the time is potentially inaccurate. [Table 67](#) describes the symbols that proceed the timestamp.

Table 67 *Timestamping Symbols for syslog Messages*

Symbol	Description	Example
(blank)	Time is authoritative: the software clock is in sync or has just been set manually	15:29:03.158 UTC Tue Feb 25 2003:
*	Time is not authoritative: the software clock has not been set, or is not in sync with configured Network Time Protocol (NTP) servers.	*15:29:03.158 UTC Tue Feb 25 2003:
.	Time is authoritative, but the Network Time Protocol (NTP) is not synchronized: the software clock was in sync, but has since lost contact with all configured NTP servers.	.15:29:03.158 UTC Tue Feb 25 2003:

Examples

In the following example, the user enables time stamps on debugging messages, showing the time since reboot:

```
service timestamps debug uptime
```

In the following example, the user enables time stamps on logging messages, showing the current time and date relative to the local time zone, with the time zone name included:

```
Router(config)#
! The following line shows timestamp with uptime.
1w0d: %SYS-5-CONFIG_I: Configured from console by console
Router(config)# service timestamps log datetime localtime show-timezone
Router(config)# end
Router#
! The following line shows timestamp with datetime.
.Mar 22 23:13:25 UTC: %SYS-5-CONFIG_I: Configured from console by console
```

The following example shows the change from UTC to local time:

```
Router#
.Mar 22 23:23:10 UTC: %SYS-5-CONFIG_I: Configured from console by console
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# clock timezone PST -8
Router(config)# end
Router#
.Mar 22 15:28:02 PST: %SYS-5-CONFIG_I: Configured from console by console
```

Related Commands

Command	Description
clock set	Manually sets the system clock.
ntp	Controls access to the system's NTP services.
service sequence-numbers	Stamps system logging messages with a sequence number.

show c2600 (2600)

To display information for troubleshooting the Cisco 2600 series router, use the **show c2600** command in EXEC mode.

show c2600

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	11.3 XA	This command was introduced.

Usage Guidelines The **show c2600** command provides complex troubleshooting information that pertains to the platform’s shared references rather than to a specific interface.

Examples In the following example, sample output is shown for the **show c2600** EXEC command. See [Table 68](#) for a description of the output display fields.

```
router# show c2600

C2600 Platform Information:
Interrupts:

Assigned Handlers...
Vect  Handler  # of Ints  Name
  00  801F224C  00000000  Xilinx bridge error interrupt
  01  801DE768  0D3EE155  MPC860 TIMER INTERRUPT
  02  801E94E0  0000119E  16552 Con/Aux Interrupt
  04  801F0D94  00000000  PA Network Management Int Handler
  05  801E6C34  00000000  Timebase Reference Interrupt
  06  801F0DE4  00002C1A  PA Network IO Int Handler
  07  801F0EA0  0000015D  MPC860 CPM INTERRUPT
  14  801F224C  00000000  Xilinx bridge error interrupt

IOS Priority Masks...
Level 00 = [ EF020000 ]
Level 01 = [ EC020000 ]
Level 02 = [ E8020000 ]
Level 03 = [ E0020000 ]
Level 04 = [ E0020000 ]
Level 05 = [ E0020000 ]
Level 06 = [ C0020000 ]
Level 07 = [ 00000000 ]

SIU_IRQ_MASK = FFFFFFFF  SIEN   = EF02xxxx  Current Level = 00
Spurious IRQs = 00000000  SIPEND = 0000xxxx

Interrupt Throttling:
```

```

Throttle Count = 00000000   Timer Count       = 00000000
Netint usec    = 00000000   Netint Mask usec = 000003E8
Active         =           0   Configured       =           0
Longest IRQ    = 00000000

IDMA Status:
Requests = 00000349   Drops           = 00000000
Complete = 00000349   Post Coalesce Frames = 00000349
Giant     = 00000000
Available Blocks = 256/256

ISP Status:
Version string burned in chip: "A986122997"
New version after next program operation: "B018020998"
ISP family type: "2096"
ISP chip ID: 0x0013
Device is programmable
    
```

Table 68 *show c2600 Field Descriptions*

Field	Description
Interrupts	Denotes that the next section describes the status of the interrupt services.
Assigned Handlers	Denotes a subsection of the Interrupt section that displays data about the interrupt handlers.
Vect	The processor vector number.
Handler	The execution address of the handler assigned to this vector.
# of Ints	The number of times this handler has been called.
Name	The name of the handler assigned to this vector.
IOS Priority Masks	Denotes the subsection of the Interrupt section that displays internal Cisco IOS priorities. Each item in this subsection indicates a Cisco IOS interrupt level and the bit mask used to mask out interrupt sources when that Cisco IOS level is being processed. Used exclusively for debugging.
SIU_IRQ_MASK	For engineering level debug only.
Spurious IRQs	For engineering level debug only.
Interrupt Throttling:	This subsection describes the behavior of the Interrupt Throttling mechanism on the platform.
Throttle Count	Number of times throttle has become active.
Timer Count	Number of times throttle has deactivated because the maximum masked out time for network interrupt level has been reached.
Netint usec	Maximum time network level is allowed to run (in microseconds).
Netint Mask usec	Maximum time network level interrupt is masked out to allow process level code to run (in microseconds).
Active	Indicates that the network level interrupt is masked or that the router is in interrupt throttle state.
Configured	Indicates that throttling is enabled or configured when set to 1.
Longest IRQ	Duration of longest network level interrupt (in microseconds).

Table 68 *show c2600 Field Descriptions (continued)*

Field	Description
IDMA Status	Monitors the activity of the Internal Direct Memory Access (IDMA) hardware and software. Used to coalesce packets (turn particalized packets into non particalized packets) for transfer to the process level switching mechanism.
Requests	Number of times the IDMA engine is asked to coalesce a packet.
Drops	Number of times the coalescing operation was aborted.
Complete	Number of times the operation was successful.
Post Coalesce Frames	Number of Frames completed post coalesce processing.
Giant	Number of packets too large to coalesce.
Available Blocks	Indicates the status of the request queue, in the format N/M where N is the number of empty slots in queue and M is the total number of slots; for example, 2/256 indicates that the queue has 256 entries and can accept two more requests before it is full.
ISP Status	Provides status of In-System-Programmable (ISP) hardware.
Version string burned in chip	Current version of ISP hardware.
New version after next program operation	Version of ISP hardware after next ISP programming operation.
ISP family type	Device family number of ISP hardware.
ISP chip ID	Internal ID of ISP hardware as designated by the chip manufacturer.
Device is programmable	“Yes” or “No.” Indicates if an ISP operation is possible on this board.

Related Commands

Command	Description
show context	Displays information stored in NVRAM when the router crashes.

show c7200 (7200)

To display information about the CPU and midplane for Cisco 7200 series routers, use the **show c7200** command in EXEC mode.

show c7200

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines You can use the output of this command to determine whether the hardware version level and upgrade is current. The information is generally useful for diagnostic tasks performed by technical support only.

Examples The following is sample output from the **show c7200** command:

```
Router# show c7200

C7200 Network IO Interrupt Throttling:
  throttle count=0, timer count=0
  active=0, configured=0
  netint usec=3999, netint mask usec=200

C7200 Midplane EEPROM:
  Hardware revision 1.2          Board revision A0
  Serial number      2863311530  Part number      170-43690-170
  Test history       0xAA         RMA number       170-170-170
  MAC=0060.3e28.ee00, MAC Size=1024
  EEPROM format version 1, Model=0x6
  EEPROM contents (hex):
    0x20: 01 06 01 02 AA AA AA AA AA AA AA AA 00 60 3E 28
    0x30: EE 00 04 00 AA AA AA AA AA AA AA 50 AA AA AA AA

C7200 CPU EEPROM:
  Hardware revision 2.0          Board revision A0
  Serial number      3509953     Part number      73-1536-02
  Test history       0x0         RMA number       00-00-00
  EEPROM format version 1
  EEPROM contents (hex):
    0x20: 01 15 02 00 00 35 8E C1 49 06 00 02 00 00 00 00
    0x30: 50 00 00 00 FF FF FF FF FF FF FF FF FF FF FF
```

show cls

To display the current status of all Cisco link services (CLS) sessions on the router, use the **show cls** command in EXEC mode.

show cls [brief]

Syntax Description	brief (Optional) Displays a brief version of the output.
---------------------------	---

Defaults Without the **brief** argument, displays complete output.

Command Modes EXEC

Command History	Release	Modification
	11.0	This command was introduced in a release prior to Cisco IOS Release 11.0.

Usage Guidelines The Cisco link service (CLS) is used as the interface between data link users (DLUs), such as DLSw, LAN Network Manager (LNM), downstream physical unit (DSPU), and SNASw, and their corresponding data link circuits (DLCs) such as Logic Link Control (LLC), VDLC, and Qualified Logic Link Control (QLLC). Each DLU registers a particular service access point (SAP) with CLS, and establishes circuits through CLS over the DLC.

The **show cls** command displays the SAP values associated with the DLU and the circuits established through CLS.

For further information about CLS, use the Release 12.2 *Cisco IOS Bridging and IBM Networking Configuration Guide*.

Examples The following is sample output from the **show cls** command:

```

IBD-4500B# show cls

DLU user:SNASW
  SSap:0x04  VDLC VDLC650
  DTE:1234.4000.0001 1234.4000.0002 04 04
  T1 timer:0  T2 timer:0  Inact timer:0
  max out:0  max in:0  retry count:10
  XID retry:10  XID timer:5000  I-Frame:0
  flow:0  DataIndQ:0  DataReqQ:0
DLU user:DLSWDLUPEER
DLU user:DLSWDLU
  Bridging  VDLC VDLC1000
  Bridging  VDLC VDLC650
    
```

The following is sample output from the **show cls brief** command:

```

IBD-4500B# show cls brief
    
```

```

DLU user:SNASw
  SSap:0x04  VDLC VDLC650
  DTE:1234.4000.0001 1234.4000.0002 04 04
DLU user:DLSWDLUPEER
DLU user:DLSWDLU
  Bridging  VDLC VDLC1000
  Bridging  VDLC VDLC650
    
```

The examples show two DLUs—SNASw and DLSw—active in the router. SNASw uses a SAP value of 0x04, and the associated DLC port is VDLC650. SNASw has a circuit established between MAC addresses 1234.4000.0001 and 1234.4000.0002 using source and destination SAPs 04 and 04. DLSw is a bridging protocol and uses VDLC1000 and VDLC650 ports. There are no circuits in place at this time.

In the output from the **show cls** command (without the **brief** argument), the values of timers and counters applicable to this circuit are displayed.

Related Commands

Command	Description
stun peer-name	Enables STUN for an IP address and uses Cisco Link Services (CLS) to access the Frame Relay network.

show context

To display information stored in NVRAM when an unexpected system reload (system exception) occurs, use the **show context** command in EXEC mode.

show context [**summary** | **all** | **slot** *slot-number* [*crash-index*] [**all**] [**debug**]]

Syntax Description

summary	Displays a summary of all the crashes recorded.
all	Displays all crashes for all the slots. When optionally used with the slot keyword, displays crash information for the specified slot.
slot <i>slot-number</i> [<i>crash-index</i>]	Displays information for a particular line card. Slot numbers range from 0 to 11 for the Cisco 12012 router and from 0 to 7 for the Cisco 12008. The index number allows you to look at previous crash contexts. Contexts from the last 24 line card crashes are saved on the GRP card. If the GRP reloads, the last 24 line card crash contexts are lost. For example, show context slot 3 2 shows the second most recent crash for line card in slot 3. Index numbers are displayed by the show context summary command.
debug	(Optional) Displays crash information as a hex record dump in addition to one of the options listed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
11.2 GS	The slot <i>slot-number</i> [<i>crash-index</i>] [all] [debug] syntax was added for Cisco 12000 series routers.

Usage Guidelines

The display from the **show context** command includes the following information:

- Reason for the system reboot
- Stack trace
- Software version
- The signal number, code, and router uptime information
- All the register contents at the time of the crash



Note

This command is intended primarily for use by Cisco technical support representatives for analyzing unexpected system reloads.

Output for this command will vary by platform. Context information is specific to processors and architectures. For example, context information for the Cisco 2600 series router differs from that for other router types because the Cisco 2600 runs with an M860 processor.

Examples

The following is sample output from the **show context** command following a system failure:

```
Router> show context

System was restarted by error - a Software forced crash, PC 0x60189354
GS Software (RSP-PV-M), Experimental Version 11.1(2033) [ganesh 111]
Compiled Mon 31-Mar-97 13:21 by ganesh
Image text-base: 0x60010900, data-base: 0x6073E000
Stack trace from system failure:
FP: 0x60AEA798, RA: 0x60189354
FP: 0x60AEA798, RA: 0x601853CC
FP: 0x60AEA7C0, RA: 0x6015E98C
FP: 0x60AEA7F8, RA: 0x6011AB3C
FP: 0x60AEA828, RA: 0x601706CC
FP: 0x60AEA878, RA: 0x60116340
FP: 0x60AEA890, RA: 0x6011632C
Fault History Buffer:
GS Software (RSP-PV-M), Experimental Version 11.1(2033) [ganesh 111]
Compiled Mon 31-Mar-97 13:21 by ganesh
Signal = 23, Code = 0x24, Uptime 00:04:19
$0 : 00000000, AT : 60930120, v0 : 00000032, v1 : 00000120
a0 : 60170110, a1 : 6097F22C, a2 : 00000000, a3 : 00000000
t0 : 60AE02A0, t1 : 8000FD80, t2 : 34008F00, t3 : FFFF00FF
t4 : 00000083, t5 : 3E840024, t6 : 00000000, t7 : 11010132
s0 : 00000006, s1 : 607A25F8, s2 : 00000001, s3 : 00000000
s4 : 00000000, s5 : 00000000, s6 : 00000000, s7 : 6097F755
t8 : 600FABBC, t9 : 00000000, k0 : 30408401, k1 : 30410000
gp : 608B9860, sp : 60AEA798, s8 : 00000000, ra : 601853CC
EPC : 60189354, SREG : 3400EF03, Cause : 00000024
Router>
```

The following is sample output from the **show context summary** command on a Cisco 12012 router. The **show context summary** command displays a summary of all the crashes recorded for each slot (line card).

```
Router# show context summary

CRASH INFO SUMMARY
  Slot 0 : 0 crashes
  Slot 1 : 0 crashes
  Slot 2 : 0 crashes
  Slot 3 : 0 crashes
  Slot 4 : 0 crashes
  Slot 5 : 0 crashes
  Slot 6 : 0 crashes
  Slot 7 : 2 crashes
    1 - crash at 18:06:41 UTC Tue Nov 5 1996
    2 - crash at 12:14:55 UTC Mon Nov 4 1996
  Slot 8 : 0 crashes
  Slot 9 : 0 crashes
  Slot 10: 0 crashes
  Slot 11: 0 crashes
Router#
```

The following is sample output from the **show context** command following an unexpected system reload on a Cisco 2600 series router. See [Table 69](#) for a description of the fields in this output.

```
router# show context

S/W Version: Cisco Internetwork Operating System Software
IOS (tm) c2600 Software (c2600-JS-M), Released Version 11.3(19980115:184921)
Copyright (c) 1986-1998 by cisco Systems, Inc.
Compiled Thu 15-Jan-98 13:49 by mmagno
Exception occurred at: 00:02:26 UTC Mon Mar 1 1993
```

show context

```

Exception type: Data TLB Miss (0x1200)
CPU Register Context:
PC = 0x80109964 MSR = 0x00009030 CR = 0x55FFFD35 LR = 0x80109958
CTR = 0x800154E4 XER = 0xC000BB6F DAR = 0x00000088 DSISR = 0x00000249
DEC = 0x7FFFDFCA TBU = 0x00000000 TBL = 0x15433FCF IMMR = 0x68010020
R0 = 0x80000000 R1 = 0x80E80BD0 R2 = 0x80000000 R3 = 0x00000000
R4 = 0x80E80BC0 R5 = 0x40800000 R6 = 0x00000001 R7 = 0x68010000
R8 = 0x00000000 R9 = 0x00000060 R10 = 0x00001030 R11 = 0xFFFFFFFF
R12 = 0x00007CE6 R13 = 0xFFF379E8 R14 = 0x80D50000 R15 = 0x00000000
R16 = 0x00000000 R17 = 0x00000000 R18 = 0x00000000 R19 = 0x00000000
R20 = 0x00000000 R21 = 0x00000001 R22 = 0x00000010 R23 = 0x00000000
R24 = 0x00000000 R25 = 0x80E91348 R26 = 0x01936010 R27 = 0x80E92A80
R28 = 0x00000001 R29 = 0x019BA920 R30 = 0x00000000 R31 = 0x00000018
Stack trace:
Frame 00: SP = 0x80E80BD0 PC = 0x80109958
Frame 01: SP = 0x80E80C28 PC = 0x8010A720
Frame 02: SP = 0x80E80C40 PC = 0x80271010
Frame 03: SP = 0x80E80C50 PC = 0x8025EE64
Frame 04: SP = 0x80DEE548 PC = 0x8026702C
Frame 05: SP = 0x80DEE558 PC = 0x8026702C
    
```

Table 69 show context Field Descriptions

Field	Description
S/W Version	Standard Cisco IOS version string as displayed.
Exception occurred at	Router real time when exception occurred. The router must have the clock time properly configured for this to be accurate.
Exception type	Technical reason for exception. For engineering analysis.
CPU Register Context	Technical processor state information. For engineering analysis.
Stack trace	Technical processor state information. For engineering analysis.

Related Commands

Command	Description
show processes	Displays information about the active processes.
show stacks	Monitors the stack usage of processes and interrupt routines.

show controllers (GRP image)

To display information that is specific to the hardware, use the **show controllers** command in privileged EXEC mode.

show controllers [**atm** *slot-number* | **clock** | **csar** [**register**] | **csc-fpga** | **dp83800** | **fab-clk** | **fia** [**register**] | **pos** [*slot-number*] [**details**] | **queues** [*slot-number*] | **sca** | **xbar**]

Syntax	Description
atm <i>slot-number</i>	(Optional) Displays the ATM controllers. Number is slot-number/port-number (for example, 4/0). Slot numbers range from 0 to 11 for the Cisco 12012 router and from 0 to 7 for the Cisco 12008 router.
clock	(Optional) Displays the clock card configuration.
csar [register]	(Optional) Displays the Cisco Cell Segmentation and Reassembly (CSAR) information. CSAR is the name of the chip on the card that handles traffic between the GRP and the switch fabric interface ASICs.
csc-fpga	(Optional) Displays the clock and scheduler card register information in the field programmable gate array (FPGA).
dp83800	(Optional) Displays the Ethernet information on the GRP card.
fab-clk	(Optional) Display the switch fabric clock register information. The switch fabric clock FPGA is a chip that monitors the incoming fabric clock generated by the switch fabric. This clock is needed by each card connecting to the switch fabric to properly communicate with it. Two switch fabric clocks arrive at each card; only one can be used. The FPGA monitors both clocks and selects which one to use if only one of them is running.
fia [register]	(Optional) Displays the fabric interface ASIC information and optionally displays the register information.
pos [<i>slot-number</i>] [details]	(Optional) Displays the POS framer state and optionally displays all the details for the interface. Number is slot-number/port-number (for example, 4/0). Slot numbers range from 0 to 11 for the Cisco 12012 router and from 0 to 7 for the Cisco 12008 router.
queues [<i>slot-number</i>]	(Optional) Displays the SDRAM buffer carve information and optionally displays the information for a specific line card. The SDRAM buffer carve information displayed is suggested carve information from the GRP card to the line card. Line cards might change the shown percentages based on SDRAM available. Slot numbers range from 0 to 11 for the Cisco 12012 router and from 0 to 7 for the Cisco 12008.
sca	(Optional) Displays the SCA register information. The SCA is an ASIC that arbitrates among the line cards requests to use the switch fabric.
xbar	(Optional) Displays the crossbar register information. The XBAR is an ASIC that switches the data as it passes through the switch fabric.

Command Modes Privileged EXEC

Command History

Release	Modification
11.2 GS	This command was added to support the Cisco 12000 series Internet Routers.

Usage Guidelines

This information provided by this command is intended for use only by technical support representatives in analyzing system failures in the field.

Examples

The following is sample output from the **show controllers pos** command for a Cisco 12012:

```
Router# show controllers pos 7/0

POS7/0
SECTION
  LOF = 2          LOS = 0          BIP(B1) = 5889
  Active Alarms: None
LINE
  AIS = 2          RDI = 2          FEBE = 146          BIP(B2) = 2106453
  Active Alarms: None
PATH
  AIS = 2          RDI = 4          FEBE = 63          BIP(B3) = 3216
  LOP = 0          PSE = 8          NSE = 3          NEWPTR = 2
  Active Alarms: None
APS
  COAPS = 3          PSBF = 2
  State: PSBF_state = False
  Rx(K1/K2): F0/15 Tx(K1/K2): 00/00
  S1S0 = 00, C2 = 64
PATH TRACE BUFFER : STABLE
  Remote hostname : GSR-C
  Remote interface: POS10/0
  Remote IP addr  : 10.201.101.2
  Remote Rx(K1/K2): F0/15 Tx(K1/K2): 00/00
Router#
```

Related Commands

Command	Description
clear controllers	Resets the T1 or E1 controller.
show controllers (line card image)	Displays information that is specific to the hardware on a line card.

show controllers (line card image)

To display information that is specific to the hardware on a line card, use the **attach** command in privileged EXEC mode to connect to the line card and then use the **show controllers** command in privileged EXEC mode or the **execute-on** command in privileged EXEC mode.

show controllers atm [[*port-number*] [**all** | **sar** | **summary**]]

show controllers fia [**register**]

**show controllers {frfab | tofab} {bma {microcode | ms-inst | register} | qelem
start-queue-element [end-queue-element] | qnum start-queue-number [end-queue-number] |
queues | statistics}**

show controllers io

show controllers l3

**show controllers pos {framers | queues | registers | rxsrpm port-number queue-start-address
[queue-length] | txsrpm port-number queue-start-address [queue-length]}**

Syntax Description

atm	Displays the ATM controller information.
<i>port-number</i>	(Optional) Displays request for the physical interface on the ATM card. The range of choices is from 0 to 3.
all	(Optional) Lists all details.
sar	(Optional) Lists SAR interactive command.
summary	(Optional) Lists SAR status summary.
fia	Displays the fabric interface ASIC information.
register	(Optional) Displays the register information.
frfab	(Optional) Displays the "from" (transmit) fabric information.
tofab	(Optional) Displays the "to" (receive) fabric information.
bma	For the frfab or tofab keywords, displays microcode, micro sequencer, or register information for the silicon queuing engine (SQE), also known as the buffer management ASIC (BMA).
microcode	Displays SQE information for the microcode bundled in the line card and currently running version.
mis-inst	Displays SQE information for the micro sequencer instruction.
register	Displays silicon queuing engine (SQE) information for the register.
qelem	For the frfab or tofab keywords, displays the SDRAM buffer pool queue element summary information.
<i>start-queue-element</i>	Specifies the start queue element number from 0 to 65535.
<i>end-queue-element</i>	(Optional) Specifies the end queue element number from 0 to 65535.
qnum	For the frfab or tofab keywords, displays the SDRAM buffer pool queue detail information.

show controllers (line card image)

<i>start-queue-number</i>	Specifies the start free queue number (from 0 to 127).
<i>end-queue-number</i>	(Optional) Specifies the end free queue number (from 0 to 127).
queues	For the frfab or tofab keywords, displays the SDRAM buffer pool information.
statistics	For the frfab or tofab keywords, displays the BMA counters.
io	Displays input/output registers.
l3	Displays Layer 3 ASIC information.
pos	Displays packet-over-sonic (POS) information for framer registers, framer queues, and ASIC registers.
framers	Displays the POS framer registers.
queues	Displays the POS framer queue information.
registers	Displays the ASIC registers.
rxsram	Displays the receive queue SRAM.
<i>port-number</i>	Specifies a port number (valid range is from 0 to 3).
<i>queue-start-address</i>	Specifies the queue SRAM logical starting address.
<i>queue-length</i>	(Optional) Specifies the queue SRAM length.
txsram	Displays the transmit queue SRAM.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 GS	This command was added to support the Cisco 12000 series Gigabit Switch Routers.

Usage Guidelines

This information displayed by this command is of use only to technical support representatives in analyzing unexpected system failures in the field. It is documented here in case you need to provide the displayed statistics to a technical support engineer.

Examples

Because you are executing this command on the line card, you must use the **execute-on** command to use the **show** command, or you must connect to the card using the **attach** command. All examples in this section use the **execute-on** command

The following is partial sample output from the **show controllers atm** command:

```
Router# execute-on slot 4 show controllers atm 0

TX SAR (Beta 1.0.0) is Operational;
RX SAR (Beta 1.0.0) is Operational;

Interface Configuration Mode:
    STS-12c

Active Maker Channels: total # 6
VCID  ChnnIID  Type  OutputInfo  InPkts  InOAMs  MacString
```

```

1  0888  UBR  0C010010      0      0  08882000AAAA030000000800
2  0988  VBR  04010020      0      0  09882000
3  8BC8  UBR  0C010030      0      0  8BC82000AAAA030000000800
4  0E08  UBR  0C010040      0      0  0E082000AAAA030000000800
10 1288  VBR  040100A0      0      0  12882000
11 8BE8  VBR  0C0100B0      0      0  8BE82000AAAA030000000800

```

```

SAR Total Counters:
total_tx_idle_cells 215267 total_tx_paks 0 total_tx_abort_paks 0
total_rx_paks 0 total_rx_drop_paks 0 total_rx_discard_cells 15

```

```

Switching Code Counters:
total_rx_crc_err_paks 0 total_rx_giant_paks 0
total_rx_abort_paks 0 total_rx_crc10_cells 0
total_rx_tmout_paks 0 total_rx_unknown_paks 0
total_rx_out_buf_paks 0 total_rx_unknown_vc_paks 0

```

```

BATMAN Asic Register Values:
hi_addr_reg 0x8000, lo_addr_reg 0x000C, boot_msk_addr 0x0780,
rmcell_msk_addr 0x0724, rmcnt_msk_addr 0x07C2, txbuf_msk_addr 0x070C,
.
.
.

```

```

CM622 SAR Boot Configuration:
txind_q_addr 0x14000 txcmd_q_addr 0x20000
.
.
.

```

```

SUNI-622 Framer Register Values:
Master Rst and Ident/Load Meters Reg (#0x0): 0x10
Master Configuration Reg (#0x1): 0x1F
Master Interrupt Status Reg (#0x2): 0x00
PISO Interrupt Reg (#0x3): 0x04
Master Auto Alarm Reg (#0x4): 0x03
Master Auto Alarm Reg (#0x5): 0x07
Parallel Output Port Reg (#0x6): 0x02
.
.
.
BERM Line BIP Threshold LSB Reg (#0x74): 0x00
BERM Line BIP Threshold MSB Reg (#0x75): 0x00
Router#

```

The following is partial sample output from the **show controllers** command:

```
Router# execute-on slot 6 show controllers
```

```

Interface POS0
Hardware is BFLC POS
lcpos_instance struct 60311B40
RX POS ASIC addr space 12000000
TX POS ASIC addr space 12000100
SUNI framer addr space 12000400
SUNI rsop intr status 00
CRC32 enabled, HDLC enc, int clock
no loop

```

```

Interface POS1
Hardware is BFLC POS
lcpos_instance struct 603142E0
RX POS ASIC addr space 12000000
TX POS ASIC addr space 12000100
SUNI framer addr space 12000600
SUNI rsop intr status 00
CRC32 enabled, HDLC enc, int clock

```

show controllers (line card image)

```
no loop
.
.
Router#
```

The following is partial sample output from the **show controllers pos framers** command:

```
Router# execute-on slot 6 show controllers pos framers
```

```
Framer 0, addr=0x12000400:
master reset          C0
master config         1F          rrate sts3c trate sts3c fixptr
master control        00
clock rcv cntrl      D0
RACP control          84
RACP gfc control      0F
TACP control status   04          hcsadd
RACP intr enable      04
RSOP cntrl intr enable 00
RSOP intr status      00
TPOP path sig lbl (c2) 13
SPTB control          04          tnull
SPTB status           00

Framer 1, addr=0x12000600:
master reset          C0
master config         1F          rrate sts3c trate sts3c fixptr
master control        00
clock rcv cntrl      D0
RACP control          84
RACP gfc control      0F
TACP control status   04          hcsadd
RACP intr enable      04
RSOP cntrl intr enable 00
RSOP intr status      00
TPOP path sig lbl (c2) 13
SPTB control          04          tnull
SPTB status           00

Framer 2, addr=0x12000800:
master reset          C0
master config         1F          rrate sts3c trate sts3c fixptr
master control        00
clock rcv cntrl      D0
RACP control          84
RACP gfc control      0F
TACP control status   04          hcsadd
RACP intr enable      04
RSOP cntrl intr enable 00
RSOP intr status      00
TPOP path sig lbl (c2) 13
SPTB control          04          tnull
SPTB status           00
.
.
Router#
```

The following is partial sample output from the **show controllers fia** command:

```
Router# execute-on slot 7 show controllers fia
```

```
===== Line Card (Slot 7) =====
```

Fabric configuration: Full bandwidth redundant
 Master Scheduler: Slot 17

From Fabric FIA Errors

```

-----
redund fifo parity 0          redund overflow 0          cell drops 0
crc32 lkup parity 0          cell parity 0          crc32 0
      0          1          2          3          4
-----
los 0          0          0          0          0
crc16 0          0          0          0          0
    
```

To Fabric FIA Errors

```

-----
sca not pres 0          req error 0          uni fifo overflow 0
grant parity 0          multi req 0          uni fifo undrflow 0
cntrl parity 0          uni req 0          crc32 lkup parity 0
multi fifo 0          empty dst req 0          handshake error 0
    
```

Related Commands

Command	Description
clear controllers	Resets the T1 or E1 controller.

show controllers logging

To display logging information about a Versatile Interface Processor (VIP) card, use the **show controllers logging** command in privileged EXEC mode.

show controllers vip *slot-number* logging

Syntax Description	vip <i>slot-number</i> VIP slot number.
---------------------------	--

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines	This command displays the state of syslog error and event logging, including host addresses, and whether console logging is enabled.
-------------------------	--

Examples	<p>The following is sample output from the show controllers logging command:</p> <pre>Router# show controllers vip 4 logging Syslog logging: enabled Console logging: disabled Monitor logging: level debugging, 266 messages logged. Trap logging: level informational, 266 messages logged. Logging to 192.180.2.238</pre>
-----------------	--

Table 70 describes the significant fields shown in the display.

Table 70 show controllers logging Field Descriptions

Field	Description
Syslog logging	When enabled, system logging messages are sent to a UNIX host that acts as a syslog server; that is, it captures and saves the messages.
Console logging	If enabled, states the level; otherwise, this field displays disabled.
Monitor logging	Minimum level of severity required for a log message to be sent to a monitor terminal (not the console).
Trap logging	Minimum level of severity required for a log message to be sent to a syslog server.

Related Commands	Command	Description
	show logging	Displays the state of logging (syslog).

show controllers tech-support

To display general information about a Versatile Interface Processor (VIP) card when reporting a problem, use the **show controllers tech-support** command in privileged EXEC mode.

show controllers vip *slot-number* tech-support

Syntax Description	vip <i>slot-number</i> VIP slot number.
---------------------------	--

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines Use this command to help collect general information about a VIP card when you are reporting a problem. This command displays the equivalent of the following **show** commands for the VIP card:

- **more system:running-config**
- **show buffers**
- **show controllers**
- **show interfaces**
- **show processes cpu**
- **show processes memory**
- **show stacks**
- **show version**

For a sample display of the **show controllers tech-support** command output, refer to these **show** commands.

Related Commands	Command	Description
	more system:running-config	Displays the running configuration.
	show buffers	Displays statistics for the buffer pools on the network server.
	show controllers	Displays information that is specific to the hardware.
	show interfaces	Uses the show interfaces EXEC command to display ALC information.
	show processes	Displays information about the active processes.
	show processes memory	Displays memory used.
	show stacks	Monitors the stack usage of processes and interrupt routines.

Command	Description
show tech-support	Displays general information about the router when reporting a problem.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show debugging

To display information about the types of debugging that are enabled for your router, use the **show debugging** command in privileged EXEC mode.

show debugging

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	11.1	This command was introduced.

Examples The following is sample output from the **show debugging** command. In this example, three types of CDP debugging are enabled.

```
Router# show debugging

CDP:
  CDP packet info debugging is on
  CDP events debugging is on
  CDP neighbor info debugging is on
```

Related Commands	Command	Description
	debug	Begin message logging for the specified debug command

show environment

To display temperature, voltage, and blower information on the Cisco 7000 series, Cisco 7200 series, Cisco 7500 series routers, Cisco AS5300 series Access Servers, and Cisco 12000 series Gigabit Switch Routers (GSRs), use the **show environment** command in privileged EXEC mode.

show environment [**alarms** | **all** | **fans** | **hardware** | **last** | **leds** | **power-supply** | **table** | **temperatures** | **voltages**]

Syntax Description	
alarms	(Optional) Displays the alarm contact information.
all	(Optional) Displays a detailed listing of all environmental monitor parameters (for example, the power supplies, temperature readings, voltage readings, and blower speeds). This is the default.
fans	(Optional) Displays blower and fan information.
hardware	(Optional) Displays hardware-specific information.
last	(Optional) Displays information on the last measurement made.
leds	(Optional) Displays the status of the MBus LEDs on the clock and scheduler cards and switch fabric cards.
power-supply	(Optional) Displays power supply voltage and current information. If applicable, displays the status of the Redundant Power Supply (RPS).
table	(Optional) Displays the temperature, voltage, and blower ranges and thresholds.
temperature	(Optional) Displays temperature information.
voltages	(Optional) Displays voltage information.

Defaults If no options are specified, the default is **all**.

Command Modes Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	11.2 GS	The alarms , fans , hardware , leds , power-supply , table temperature , and voltages keywords were added for Cisco 12000 series GSRs.
	11.3(6)AA	This command was expanded to monitor the RPS and board temperature for the Cisco AS5300 platform, Cisco 3600 Series routers, Cisco 7200 series routers, and the Cisco 12000 series routers.

Usage Guidelines The availability of keywords will depend on your system.

Once a minute a routine is run that gets environmental measurements from sensors and stores the output into a buffer. This buffer is displayed on the console when the **show environment** command is entered.

If a measurement exceeds desired margins, but has not exceeded fatal margins, a warning message is printed to the system console. The system software queries the sensors for measurements once a minute, but warnings for a given test point are printed at most once every hour for sensor readings in the warning range and once every 5 minutes for sensor readings in the critical range. If a measurement is out of line within these time segments, an automatic warning message appears on the console. As noted, you can query the environmental status with the **show environment** command at any time to determine whether a measurement is at the warning or critical tolerance.

If a shutdown occurs because of detection of fatal environmental margins, the last measured value from each sensor is stored in internal nonvolatile memory.

For environmental specifications, refer to the hardware installation and configuration publication for your individual chassis.

If the Cisco 12000 series exceeds environmental conditions, a message similar to the following is displayed on the console:

```
%GSR_ENV-2-WARNING: Slot 3 Hot Sensor Temperature exceeds 40 deg C;
Check cooling systems
```



Note

Blower temperatures that exceed environmental conditions do not generate a warning message.

You can also enable Simple Network Management Protocol (SNMP) notifications (traps or informs) to alert a network management system (NMS) when environmental thresholds are reached using the **snmp-server enable traps envmon** and **snmp-server host** global configuration commands.

Whenever Cisco IOS software detects a failure or recovery event from the DRPS unit, it sends an SNMP trap to the configured SNMP server. Unlike console messages, only one SNMP trap is sent when the failure event is first detected. Another trap is sent when the recovery is detected.

Cisco AS5300 DRPS software reuses the MIB attributes and traps defined in CISCO-ENVMON-MIB and CISCO-ACCESS-ENVMON-MIB. CISCO-ENVMON-MIB is supported by all Cisco routers with RPS units, and CISCO-ACCESS-ENVMON-MIB is supported by the Cisco 3600 series routers.

A power supply trap defined in CISCO-ENVMON-MIB is sent when a failure is detected and when a failure recovery occurs for the following events: input voltage fail, DC output voltage fail, thermal fail, and multiple failure events.

A fan failure trap defined in CISCO-ENVMON-MIB is sent when a fan failure or recovery event is detected by Cisco IOS software.

A temperature trap defined in CISCO-ACCESS-ENVMON-MIB is sent when a board overtemperature condition is detected by Cisco IOS software.

CISCO-ACCESS-ENVMON-MIB also defines an overvoltage trap. A similar trap is defined in CISCO-ENVMON-MIB, but it requires the `ciscoEnvMonVoltageStatusValue` in varbinds. This value indicates the current value of the voltage in the RPS. With Cisco AS5300 RPS units, the current voltage value is not sent to the motherboard.

CISCO-ENVMON-MIB is extended to add a new enumerated value, `internalRedundant(5)`, for MIB attribute `ciscoEnvMonSupplySource`. This is used to identify a RPS unit.

Examples

In the following example, the typical **show environment** display is shown when no warning conditions are in the system for the Cisco 7000 series and Cisco 7200 series routers. This information may vary slightly depending on the platform you are using. The date and time of the query are displayed, along with the data refresh information and a message indicating that there are no warning conditions.

```
Router> show environment
```

```
Environmental Statistics
  Environmental status as of 13:17:39 UTC Thu Jun 6 1996
  Data is 7 second(s) old, refresh in 53 second(s)

All Environmental Measurements are within specifications
```

Table 71 describes the significant fields shown in the display.

Table 71 show environment Field Descriptions

Field	Description
Environmental status as of...	Current date and time.
Data is..., refresh in...	Environmental measurements are output into a buffer every 60 seconds, unless other higher-priority processes are running.
Status message	If environmental measurements are not within specification, warning messages are displayed.

Cisco 7000 Series Routers

The following are examples of messages that display on the system console when a measurement has exceeded an acceptable margin:

```
ENVIRONMENTAL WARNING: Air flow appears marginal.
ENVIRONMENTAL WARNING: Internal temperature measured 41.3(C)
ENVIRONMENTAL WARNING: +5 volt testpoint measured 5.310(V)
```

The system displays the following message if voltage or temperature exceed maximum margins:

```
SHUTDOWN: air flow problem
```

In the following example, there have been two intermittent power failures since a router was turned on, and the lower power supply is not functioning. The last intermittent power failure occurred on Monday, June 10, 1996, at 11:07 p.m.

```
7000# show environment all

Environmental Statistics
  Environmental status as of 23:19:47 UTC Wed Jun 12 1996
  Data is 6 second(s) old, refresh in 54 second(s)

WARNING: Lower Power Supply is NON-OPERATIONAL

Lower Power Supply:700W, OFF      Upper Power Supply: 700W, ON

Intermittent Powerfail(s): 2      Last on 23:07:05 UTC Mon Jun 10 1996

+12 volts measured at 12.05(V)
+5 volts measured at 4.96(V)
-12 volts measured at -12.05(V)
+24 volts measured at 23.80(V)

Airflow temperature measured at 38(C)
Inlet temperature measured at 25(C)
```

Table 72 describes the significant fields shown in the display.

Table 72 *show environment all Field Descriptions for the Cisco 7000*

Field	Description
Environmental status as of...	Date and time of last query.
Data is..., refresh in...	Environmental measurements are output into a buffer every 60 seconds, unless other higher-priority processes are running.
WARNING:	If environmental measurements are not within specification, warning messages are displayed.
Lower Power Supply	Type of power supply installed and its status (On or Off).
Upper Power Supply	Type of power supply installed and its status (On or Off).
Intermittent Powerfail(s)	Number of power hits (not resulting in shutdown) since the system was last booted.
voltage specifications	System voltage measurements.
Airflow and inlet temperature	Temperature of air coming in and going out.

The following example is for the Cisco 7000 series router. The router retrieves the environmental statistics at the time of the last shutdown. In this example, the last shutdown was Friday, May 19, 1995, at 12:40 p.m., so the environmental statistics at that time are displayed.

```
Router# show environment last

Environmental Statistics
  Environmental status as of 14:47:00 UTC Sun May 21 1995
  Data is 6 second(s) old, refresh in 54 second(s)

  WARNING: Upper Power Supply is NON-OPERATIONAL

LAST Environmental Statistics
  Environmental status as of 12:40:00 UTC Fri May 19 1995
  Lower Power Supply: 700W, ON      Upper Power Supply: 700W, OFF

  No Intermittent Powerfails

  +12 volts measured at 12.05(V)
  +5 volts measured at 4.98(V)
  -12 volts measured at -12.00(V)
  +24 volts measured at 23.80(V)

  Airflow temperature measured at 30(C)
  Inlet temperature measured at 23(C)
```

Table 73 describes the significant fields shown in the display.

Table 73 *show environment last Field Descriptions for the Cisco 7000*

Field	Description
Environmental status as of...	Current date and time.
Data is..., refresh in...	Environmental measurements are output into a buffer every 60 seconds, unless other higher-priority processes are running.
WARNING:	If environmental measurements are not within specification, warning messages are displayed.

Table 73 show environment last Field Descriptions for the Cisco 7000 (continued)

Field	Description
LAST Environmental Statistics	Displays test point values at time of the last environmental shutdown.
Lower Power Supply: Upper Power Supply:	For the Cisco 7000 router, indicates the status of the two 700W power supplies. For the Cisco 7010 router, indicates the status of the single 600W power supply.

In the following example, shows sample output for the current environmental status in tables that list voltage and temperature parameters. There are three warning messages: one each about the lower power supply, the airflow temperature, and the inlet temperature. In this example, voltage parameters are shown to be in the normal range, airflow temperature is at a critical level, and inlet temperature is at the warning level.

Router> **show environment table**

```

Environmental Statistics
  Environmental status as of Mon 11-2-1992 17:43:36
  Data is 52 second(s) old, refresh in 8 second(s)

WARNING: Lower Power Supply is NON-OPERATIONAL
WARNING: Airflow temperature has reached CRITICAL level at 73(C)
WARNING: Inlet temperature has reached WARNING level at 41(C)

Voltage Parameters:

SENSE          CRITICAL          NORMAL          CRITICAL
-----|-----|-----|-----|
+12 (V)        10.20          12.05 (V)      13.80
+5 (V)         4.74           4.98 (V)       5.26
-12 (V)       -10.20         -12.05 (V)    -13.80
+24 (V)        20.00          24.00 (V)     28.00

Temperature Parameters:

SENSE  WARNING  NORMAL  WARNING  CRITICAL  SHUTDOWN
-----|-----|-----|-----|-----|
Airflow      10       60      70      73 (C)   88
Inlet        10       39      41 (C)  46       64
    
```

Table 74 describes the significant fields shown in the display.

Table 74 show environment Field Descriptions for the Cisco 7000 Series Router

Field	Description
SENSE (Voltage Parameters)	Voltage specification for a DC line.
SENSE (Temperature Parameters)	Air being measured. Inlet measures the air coming in, and Airflow measures the temperature of the air inside the chassis.
WARNING	System is approaching an out-of-tolerance condition.
NORMAL	All monitored conditions meet normal requirements.

Table 74 show environment Field Descriptions for the Cisco 7000 (continued)Series Router

Field	Description
CRITICAL	Out-of-tolerance condition exists.
SHUTDOWN	Processor has detected condition that could cause physical damage to the system.

Cisco 7200 Series Routers

The system displays the following message if the voltage or temperature enters the “Warning” range:

```
%ENVM-4-ENVWARN: Chassis outlet 3 measured at 55C/131F
```

The system displays the following message if the voltage or temperature enters the “Critical” range:

```
%ENVM-2-ENVCRIT: +3.45 V measured at +3.65 V
```

The system displays the following message if the voltage or temperature exceeds the maximum margins:

```
%ENVM-0-SHUTDOWN: Environmental Monitor initiated shutdown
```

The following message is sent to the console if a power supply has been inserted or removed from the system. This message relates only to systems that have two power supplies.

```
%ENVM-6-PSCHANGE: Power Supply 1 changed from ZyteK AC Power Supply to removed
```

The following message is sent to the console if a power supply has been powered on or off. In the case of the power supply being shut off, this message can be due to the user shutting off the power supply or to a failed power supply. This message relates only to systems that have two power supplies.

```
%ENVM-6-PSLEV: Power Supply 1 state changed from normal to shutdown
```

The following is sample output from the **show environment all** command on the Cisco 7200 series router when there is a voltage warning condition in the system:

```
7200# show environment all

Power Supplies:
    Power supply 1 is unknown. Unit is off.
    Power supply 2 is ZyteK AC Power Supply. Unit is on.

Temperature readings:
    chassis inlet    measured at 25C/77F
    chassis outlet 1 measured at 29C/84F
    chassis outlet 2 measured at 36C/96F
    chassis outlet 3 measured at 44C/111F

Voltage readings:
    +3.45 V measured at +3.83 V:Voltage in Warning range!
    +5.15 V measured at +5.09 V
    +12.15 measured at +12.42 V
    -11.95 measured at -12.10 V
```

Table 75 describes the significant fields shown in the display.

Table 75 show environment all Field Descriptions for the Cisco 7200 Series Router

Field	Description
Power Supplies:	Current condition of the power supplies including the type and whether the power supply is on or off.
Temperature readings:	Current measurements of the chassis temperature at the inlet and outlet locations.
Voltage readings:	Current measurement of the power supply test points.

The following example is for the Cisco 7200 series router. This example shows the measurements immediately before the last shutdown and the reason for the last shutdown (if appropriate).

```
7200# show environment last

chassis inlet      previously measured at 27C/80F
chassis outlet 1   previously measured at 31C/87F
chassis outlet 2   previously measured at 37C/98F
chassis outlet 3   previously measured at 45C/113F
+3.3 V            previously measured at 4.02
+5.0 V            previously measured at 4.92
+12.0 V           previously measured at 12.65
-12.0 V           previously measured at 11.71

last shutdown reason - power supply shutdown
```

Table 76 describes the significant fields shown in the display.

Table 76 show environment last Field Descriptions for the Cisco 7200 Series Router

Field	Description
chassis inlet	Temperature measurements at the inlet area of the chassis.
chassis outlet	Temperature measurements at the outlet areas of the chassis.
voltages	Power supply test point measurements.
last shutdown reason	Possible shutdown reasons are power supply shutdown, critical temperature, and critical voltage.

The following example is for the Cisco 7200 series router. This information lists the temperature and voltage shutdown thresholds for each sensor.

```
7200# show environment table

Sample Point      LowCritical    LowWarning    HighWarning    HighCritical
chassis inlet     40C/104F      50C/122F
chassis outlet 1  43C/109F      53C/127F
chassis outlet 2  75C/167F      75C/167F
chassis outlet 3  55C/131F      65C/149F
+3.45 V           +2.76         +3.10         +3.80          +4.14
+5.15 V           +4.10         +4.61         +5.67          +6.17
+12.15 V          +9.72         +10.91        +13.37         +14.60
-11.95 V          -8.37         -9.57         -14.34         -15.53
Shutdown system at 70C/158F
```

Table 77 describes the significant fields shown in the display.

Table 77 *show environment table Field Descriptions for the Cisco 7200 Series Router*

Field	Description
Sample Point	Area for which measurements are taken.
LowCritical	Level at which a critical message is issued for an out-of-tolerance voltage condition. The system continues to operate; however, the system is approaching shutdown.
LowWarning	Level at which a warning message is issued for an out-of-tolerance voltage condition. The system continues to operate, but operator action is recommended to bring the system back to a normal state.
HighWarning	Level at which a warning message is issued. The system continues to operate, but operator action is recommended to bring the system back to a normal state.
HighCritical	Level at which a critical message is issued. For the chassis, the router is shut down. For the power supply, the power supply is shut down.
Shutdown system at	The system is shut down if the specified temperature is met.

Cisco 7500 Series Router

The sample output for the Cisco 7500 series routers may vary depending on the specific model (for example, the Cisco 7513 router). The following is sample output from the **show environment all** command on the Cisco 7500 series router:

```
7500# show environment all

Arbiter type 1, backplane type 7513 (id 2)
Power supply #1 is 1200W AC (id 1), power supply #2 is removed (id 7)
Active fault conditions: none
Fan transfer point: 100%
Active trip points: Restart_Inhibit
15 of 15 soft shutdowns remaining before hard shutdown

          1
          0123456789012
Dbus slots:  X    XX    X

card      inlet      hotpoint      exhaust
RSP(6)    35C/95F      47C/116F      40C/104F
RSP(7)    35C/95F      43C/109F      39C/102F

Shutdown temperature source is 'hotpoint' on RSP(6), requested RSP(6)

+12V measured at 12.31
+5V measured at 5.21
-12V measured at -12.07
+24V measured at 22.08
+2.5 reference is 2.49

PS1 +5V Current      measured at 59.61 A (capacity 200 A)
PS1 +12V Current     measured at 5.08 A (capacity 35 A)
PS1 -12V Current     measured at 0.42 A (capacity 3 A)
PS1 output is 378 W
```

Table 78 describes the significant fields shown in the display.

Table 78 show environment all Field Descriptions for the Cisco 7500

Field	Description
Arbiter type 1	Numbers indicating the arbiter type and backplane type.
Power supply	Number and type of power supply installed in the chassis.
Active fault conditions:	Lists any fault conditions that exist (such as power supply failure, fan failure, and temperature too high).
Fan transfer point:	Software controlled fan speed. If the router is operating below its automatic restart temperature, the transfer point is reduced by 10 percent of the full range each minute. If the router is at or above its automatic restart temperature, the transfer point is increased in the same way.
Active trip points:	Compares temperature sensor against the values displayed at the bottom of the show environment table command output.
15 of 15 soft shutdowns remaining	When the temperature increases above the “board shutdown” level, a soft shutdown occurs (that is, the cards are shut down, and the power supplies, fans, and CI continue to operate). When the system cools to the restart level, the system restarts. The system counts the number of times this occurs and keeps the up/down cycle from continuing forever. When the counter reaches zero, the system performs a hard shutdown, which requires a power cycle to recover. The soft shutdown counter is reset to its maximum value after the system has been up for 6 hours.
Dbus slots:	Indicates which chassis slots are occupied.
card, inlet, hotpoint, exhaust	Temperature measurements at the inlet, hotpoint, and exhaust areas of the card. The (6) and (7) indicate the slot numbers. Dual-Route/Switch Processor (RSP) chassis can show two RSPs.
Shutdown temperature source	Indicates which of the three temperature sources is selected for comparison against the “shutdown” levels listed with the show environment table command.
Voltages (+12V, +5V, -12V, +24V, +2.5)	Voltages measured on the backplane.
PS1	Current measured on the power supply.

The following example is for the Cisco 7500 series router. This example shows the measurements immediately before the last shutdown.

```
7500# show environment last

RSP(4) Inlet      previously measured at 37C/98F
RSP(4) Hotpoint  previously measured at 46C/114F
RSP(4) Exhaust   previously measured at 52C/125F
+12 Voltage      previously measured at 12.26
+5 Voltage       previously measured at 5.17
-12 Voltage      previously measured at -12.03
+24 Voltage      previously measured at 23.78
```

Table 79 describes the significant fields shown in the display.

Table 79 *show environment last Field Descriptions for the Cisco 7500 Series Router*

Field	Description
RSP(4) Inlet, Hotpoint, Exhaust	Temperature measurements at the inlet, hotpoint, and exhaust areas of the card.
Voltages	Voltages measured on the backplane.

The following example is for the Cisco 7500 series router. This information lists the temperature and voltage thresholds for each sensor. These thresholds indicate when error messages occur. There are two level of messages: warning and critical.

7500# **show environment table**

```

Sample Point      LowCritical    LowWarning    HighWarning    HighCritical
RSP(4) Inlet
RSP(4) Hotpoint
RSP(4) Exhaust
+12 Voltage      10.90         11.61         12.82         13.38
+5 Voltage       4.61          4.94          5.46          5.70
-12 Voltage      -10.15        -10.76        -13.25        -13.86
+24 Voltage      20.38         21.51         26.42         27.65
2.5 Reference
Shutdown boards at      70C/158F
Shutdown power supplies at 76C/168F
Restart after shutdown below 40C/104F
    
```

Table 80 describes the significant fields shown in the display.

Table 80 *show environment table Field Descriptions for the Cisco 7500 Series Router*

Field	Description
Sample Point	Area for which measurements are taken.
LowCritical	Level at which a critical message is issued for an out-of-tolerance voltage condition. The system continues to operate; however, the system is approaching shutdown.
LowWarning	Level at which a warning message is issued for an out-of-tolerance voltage condition. The system continues to operate, but operator action is recommended to bring the system back to a normal state.
HighWarning	Level at which a warning message is issued. The system continues to operate, but operator action is recommended to bring the system back to a normal state.
HighCritical	Level at which a critical message is issued. For the chassis, the router is shut down. For the power supply, the power supply is shut down.
Shutdown boards at	The card is shut down if the specified temperature is met.
Shutdown power supplies at	The system is shut down if the specified temperature is met.
Restart after shutdown	The system will restart when the specified temperature is met.

Cisco AS5300 Series Access Servers

In the following example, how keywords and options are limited according to the physical characteristics of the system is shown:

```
as5300# show environment ?
all      All environmental monitor parameters
last     Last environmental monitor parameters
table    Temperature and voltage ranges
|        Output modifiers
<cr>

as5300# show environment table

%This option not available on this platform
```

Cisco 12000 Series GSR

The following examples are for the Cisco 12000 series GSRs.

The following is sample output from the **show environment** command for a Cisco 12012 router. Slots 0 through 11 are the line cards, slots 16 and 17 are the clock and scheduler cards, slots 18 through 20 are the switch fabric cards, slots 24 through 26 are the power supplies, and slots 28 and 29 are the blowers. An “NA” in the table means that no values were returned. In some cases it is because the equipment is not supported for that environmental parameter (for example, the power supply and blowers in slots 24, 26, 28, and 29 do not have a 3V power supply, so an NA is displayed).

```
Router# show environment

Slot # 3V      5V      MBUS 5V Hot Sensor      Inlet Sensor
      (mv)     (mv)     (mv)     (deg C)         (deg C)
0     3300    4992    5040    42.0            37.0
2     3296    4976    5136    40.0            33.0
4     3280    4992    5120    38.5            31.5
7     3280    4984    5136    42.0            32.0
9     3292    4968    5160    39.5            31.5
11    3288    4992    5152    40.0            30.5
16    3308    NA      5056    42.5            38.0
17    3292    NA      5056    40.5            36.5
18    3304    NA      5176    36.5            35.0
19    3300    NA      5184    37.5            33.5
20    3304    NA      5168    36.5            34.0
24    NA     5536    5120    NA              31.5
26    NA     5544    5128    NA              31.5
28    NA     NA      5128    NA              NA
29    NA     NA      5104    NA              NA

Slot # 48V     AMP_48
      (Volt)   (Amp)
24    46      12
26    46      19

Slot # Fan 0   Fan 1   Fan 2
      (RPM)   (RPM)   (RPM)
28    2160   2190   2160
29    2130   2190   2070
Router#
```

Table 81 describes the significant fields shown and lists the equipment supported by each environmental parameter. “NA” indicates that the reading could not be obtained, so the command should be again.

Table 81 show environment Field Descriptions for the Cisco 12000 Series Routers

Field	Description
Slot #	Slot number of the equipment. On the Cisco 12012 router, slots 0 through 11 are the line cards, slots 16 and 17 are the clock and scheduler cards, slots 18 through 20 are the switch fabric cards, slots 24 through 27 are the power supplies, and slots 28 and 29 are the blowers.
3V (mv)	Measures the 3v power supply on the card. The 3v power supply is on the line cards, GRP card, clock and scheduler cards, and switch fabric cards.
5V (mv)	Measures the 5v power supply on the card. The 5v power supply is on the line cards, GRP card, and power supplies.
MBUS 5V (mv)	Measures the 5v MBus on the card. The 5v MBus is on all equipment.
Hot Sensor (deg C)	Measures the temperature at the hot sensor on the card. The hot sensor is on the line cards, GRP card, clock and scheduler cards, switch fabric cards, and blowers.
Inlet Sensor (deg C)	Measures the current inlet temperature on the card. The inlet sensor is on the line cards, GRP card, clock and scheduler cards, switch fabric cards, and power supplies.
48V (Volt)	Measures the DC power supplies.
AMP_48 (Amp)	Measures the AC power supplies.
Fan 0, Fan 1, Fan 2	Measures the fan speed in rotations per minute.

The following is sample output from the **show environment all** command for the Cisco 12008 router. Slots 0 through 7 are the line cards, slots 16 and 17 are the clock scheduler cards (the clock scheduler cards control the fans), slots 18 through 20 are the switch fabric cards, and slots 24 and 26 are the power supplies. The Cisco 12008 router does not support slots 25, 27, 28, and 29. An “NA” in the table means that no values were returned. In some cases it is because the equipment is not supported for that environmental parameter (for example, the power supplies in slots 24 and 26 do not have a hot sensor, so an NA is displayed).

```
Router# show environment all

Slot # Hot Sensor      Inlet Sensor
      (deg C)         (deg C)
2      31.0            22.0
5      33.5            26.5
16     25.5            21.5
18     22.0            21.0
19     22.5            21.0
24     NA              29.5
26     NA              24.5

Slot # 3V      5V      MBUS 5V
      (mv)    (mv)    (mv)
2      3292    5008    5136
5      3292    5000    5128
16     3272    NA      5128
18     3300    NA      5128
19     3316    NA      5128

Slot # 5V      MBUS 5V 48V      AMP_48
      (mv)    (mv)    (Volt)  (Amp)
```

show environment

```
24      0      5096    3      0
26     5544    5144    47     3
```

```
Slot #  Fan Information
16      Voltage 16V Speed slow: Main Fans Ok Power Supply fans Ok
```

```
Alarm Indicators
No alarms
```

```
Slot #  Card Specific Leds
16      Mbus OK SFCs Failed
18      Mbus OK
19      Mbus OK
24      Input Failed
26      Input Ok
```

The following is sample output from the **show environment table** command for a Cisco 12012 router. The **show environment table** command lists the warning, critical, and shutdown limits on your system and includes the GRP card and line cards (slots 0 to 15), clock and scheduler cards (slots 16 and 17), switch fabric cards (slots 18 to 20), and blowers.

```
Router# show environment table
```

```
Hot Sensor Temperature Limits (deg C):
Warning Critical Shutdown
GRP/GLC (Slots 0-15)    40     46     57
CSC   (Slots 16-17)    46     51     65
SFC   (Slots 18-20)    41     46     60
```

```
Inlet Sensor Temperature Limits (deg C):
Warning Critical Shutdown
GRP/GLC (Slots 0-15)    35     40     52
CSC   (Slots 16-17)    40     45     59
SFC   (Slots 18-20)    37     42     54
```

```
3V Ranges (mv):
Warning          Critical          Shutdown
Below  Above    Below  Above    Below  Above
GRP/GLC (Slots 0-15)  3200  3400    3100  3500    3050  3550
CSC   (Slots 16-17)  3200  3400    3100  3500    3050  3550
SFC   (Slots 18-20)  3200  3400    3100  3500    3050  3550
```

```
5V Ranges (mv):
Warning          Critical          Shutdown
Below  Above    Below  Above    Below  Above
GRP/GLC (Slots 0-15)  4850  5150    4750  5250    4680  5320
```

```
MBUS_5V Ranges (mv):
Warning          Critical          Shutdown
Below  Above    Below  Above    Below  Above
GRP/GLC (Slots 0-15)  5000  5250    4900  5350    4750  5450
CSC   (Slots 16-17)  4820  5150    4720  5250    4750  5450
SFC   (Slots 17-20)  5000  5250    4900  5350    4750  5450
```

```
Blower Operational Range (RPM):
```

```
Top Blower:
Warning          Critical
Below           Below
Fan 0           1000          750
Fan 1           1000          750
Fan 2           1000          750
```

```

Bottom Blower:
                Warning   Critical
                Below     Below
Fan 0           1000      750
Fan 1           1000      750
Fan 2           1000      750
    
```

The following is sample output from the **show environment leds** command for a Cisco 12012 router. The **show environment leds** command lists the status of the MBus LEDs on the clock, scheduler, and the switch fabric cards.

```

Router# show environment leds

16 leds Mbus OK
18 leds Mbus OK
19 leds Mbus OK
20 leds Mbus OK
    
```

Related Commands

Command	Description
snmp-server enable traps envmon	Controls (enables or disables) environmental monitoring SNMP notifications.
snmp-server host	Specifies how SNMP notifications should be sent (as traps or informs), the version of SNMP to use, the security level of the notifications (for SNMPv3), and the recipient (host) of the notifications.

show gsr

To display hardware information on the Cisco 12000 series Gigabit Switch Routers (GSRs), use the **show gsr** command in EXEC mode.

show gsr [chassis-info [details]]

Syntax Description	chassis-info	(Optional) Displays backplane NVRAM information.
	details	(Optional) In addition to the information displayed, this option includes hexadecimal output of the backplane NVRAM information.

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	11.2 GS	This command was added to support the Cisco 12000 series GSRs.

Usage Guidelines Use this command to determine the type of hardware installed in your Cisco 12000 series GSR router.

Examples The following is sample output from the **show gsr** command for a Cisco 12012 router. This command shows the type and state of the card installed in the slot.

```
Router# show gsr

Slot 0 type = Route Processor
      state = IOS Running MASTER
Slot 7 type = 1 Port Packet Over SONET OC-12c/STM-4c
      state = Card Powered
Slot 16 type = Clock Scheduler Card
      state = Card Powered PRIMARY CLOCK
```

The following is sample output from the **show gsr chassis-info** command for a Cisco 12012 router:

```
Router# show gsr chassis-info

Backplane NVRAM [version 0x20] Contents -
Chassis: type 12012 Fab Ver: 1
      Chassis S/N: ZQ24CS3WT86MGVHL
PCA: 800-3015-1 rev: A0 dev: 257 HW ver: 1.0
      Backplane S/N: A109EXPR75FUNYJK
MAC Addr: base 0000.EAB2.34FF block size: 1024
RMA Number: 0x5F-0x2D-0x44 code: 0x01 hist: 0x1A
```

show gt64010 (7200)

To display all GT64010 internal registers and interrupt status on the Cisco 7200 series routers, use the **show gt64010** command in EXEC mode.

show gt64010

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines This command displays information about the CPU interface, DRAM/device address space, device parameters, direct memory access (DMA) channels, timers and counters, and protocol control information (PCI) internal registers. The information is generally useful for diagnostic tasks performed by technical support only.

Examples The following is a partial sample output for the **show gt64010** command:

```
Router# show gt64010

GT64010 Channel 0 DMA:
dma_list=0x6088C3EC, dma_ring=0x4B018480, dma_entries=256
dma_free=0x6088CECC, dma_reqt=0x6088CECC, dma_done=0x6088CECC
thread=0x6088CEAC, thread_end=0x6088CEAC
backup_thread=0x0, backup_thread_end=0x0
dma_working=0, dma_complete=6231, post_coalesce_frames=6231
exhausted_dma_entries=0, post_coalesce_callback=6231

GT64010 Register Dump: Registers at 0xB4000000

CPU Interface:
cpu_interface_conf : 0x80030000 (b/s 0x00000380)
addr_decode_err   : 0xFFFFFFFF (b/s 0xFFFFFFFF)
Processor Address Space :
ras10_low         : 0x00000000 (b/s 0x00000000)
ras10_high        : 0x07000000 (b/s 0x00000007)
ras32_low         : 0x08000000 (b/s 0x00000008)
ras32_high        : 0x0F000000 (b/s 0x0000000F)
cs20_low          : 0xD0000000 (b/s 0x000000D0)
cs20_high         : 0x74000000 (b/s 0x00000074)
cs3_boot_low      : 0xF8000000 (b/s 0x000000F8)
cs3_boot_high     : 0x7E000000 (b/s 0x0000007E)
pci_io_low        : 0x00080000 (b/s 0x00000800)
pci_io_high       : 0x00000000 (b/s 0x00000000)
pci_mem_low       : 0x00020000 (b/s 0x00000200)
pci_mem_high      : 0x7F000000 (b/s 0x0000007F)
internal_spc_decode : 0xA0000000 (b/s 0x000000A0)
```

```
■ show gt64010 (7200)
```

```
bus_err_low      : 0x00000000 (b/s 0x00000000)  
bus_err_high     : 0x00000000 (b/s 0x00000000)  
.  
.  
.
```

show logging

To display the state of system logging (syslog) and the contents of the standard syslog (system error message) buffer, use the **show logging** command in privileged EXEC mode.

show logging [*slot slot-number* | **summary**]

Syntax Description	slot <i>slot-number</i>	(Optional) Displays information in the syslog history table for a specific line card. Slot numbers range from 0 to 11 for the Cisco 12012 Internet router and 0 to 7 for the Cisco 12008 Internet router.
	summary	(Optional) Displays counts of messages by type for each line card.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	11.2 GS	The slot and summary keywords were added for the Cisco 12000 family.
	12.2(8)T	Command output was expanded to show the status of the logging count facility (“Count and timestamp logging messages”).
	12.2(15)T	Command output was expanded to show the status of XML syslog formatting.

Usage Guidelines This command displays the state of syslog error and event logging, including host addresses, and which logging destinations (console, monitor, buffer, or host) logging is enabled. This command also displays Simple Network Management Protocol (SNMP) logging configuration parameters and protocol activity.

This command will also display the contents of the standard system logging buffer, if logging to the buffer is enabled. Logging to the buffer is enabled or disabled using the **[no] logging buffered** command. The number of system error and debugging messages in the system logging buffer is determined by the configured size of the syslog buffer. This size of the syslog buffer is also set using the **logging buffered** command.

To enable and set the format for syslog message timestamping, use the **service timestamps log** command.

If debugging is enabled (using any **debug** command), and the logging buffer is configured to include level 7 (debugging) messages, debug output will be included in the system log. Debugging output is not formatted like system error messages, and will not be preceded by the percent symbol (%).

Examples The following is sample output from the **show logging** command. In this example, buffer logging is disabled, so no syslog messages are displayed with this command.

```
Router# show logging
```

```
Syslog logging: enabled (0 messages dropped, 1 messages rate-limited, 0 flushes)
  Console logging: level debugging, 31 messages logged, xml disabled
  Monitor logging: level debugging, 0 messages logged, xml disabled
  Buffer logging: disabled, xml disabled
  Logging Exception size (4096 bytes)
  Count and timestamp logging messages: enabled
  Trap logging: level informational, 35 message lines logged
```

Table 82 describes the significant fields shown in the display.

Table 82 show logging Field Descriptions

Field	Description
Syslog logging	Shows general state of system logging (enabled or disabled), and status of logged messages (number of messages dropped, rate-limited, or flushed).
Console logging	Logging to the console port. Shows “disabled” or, if enabled, the severity level limit and number of messages logged. Enabled using the logging console command.
Monitor logging	Logging to the monitor (all TTY lines). Shows “disabled” or, if enabled, the severity level limit and number of messages logged. Enabled using the logging monitor command.
Buffer logging	Logging to the standard syslog buffer. Shows “disabled” or, if enabled, the severity level limit and number of messages logged. Enabled using the logging buffered command.
Trap logging	Logging to a remote host (syslog host). Shows “disabled” or, if enabled, the severity level limit and number of messages logged. (The word “trap” means a trigger in the system software for sending error messages to a remote host.) Prior to Cisco IOS release 12.2(15)T, trap logging was enabled using the logging <host-name> command. Now enabled using the logging host command. The severity level limit is set using the logging trap command.
SNMP logging	Displays whether SNMP logging is enabled, the number of messages logged, and the retransmission interval. If not shown on your platform, use the show logging history command.

The following example includes syslog messages from the system buffer, with timestamping :

```
Router> show logging

Syslog logging:enabled (2 messages dropped, 0 flushes, 0 overruns)
  Console logging:disabled
  Monitor logging:level debugging, 0 messages logged
  Buffer logging:level debugging, 4104 messages logged
  Trap logging:level debugging, 4119 message lines logged
    Logging to 216.231.111.14, 4119 message lines logged
Log Buffer (262144 bytes):

Jul 11 12:17:49 EDT:%BGP-4-MAXPFX:No. of prefix received from 209.165.200.225 (afi 0)
reaches 24, max 24
! THE FOLLOWING LINE IS A DEBUG MESSAGE FROM NTP.
```

```

! NOTE THAT IT IS NOT PRECEDED BY THE % SYMBOL.
Jul 11 12:17:48 EDT: NTP: Maxslew = 213866
Jul 11 15:15:41 EDT:%SYS-5-CONFIG:Configured from tftp://host.com/addc5505-rsm.nyiix
.Jul 11 15:30:28 EDT:%BGP-5-ADJCHANGE:neighbor 209.165.200.226 Up
.Jul 11 15:31:34 EDT:%BGP-3-MAXPFEXCEED:No. of prefix received from
209.165.200.226 (afi 0):16444 exceed limit 375
.Jul 11 15:31:34 EDT:%BGP-5-ADJCHANGE:neighbor 209.165.200.226 Down BGP
Notification sent
.Jul 11 15:31:34 EDT:%BGP-3-NOTIFICATION:sent to neighbor 209.165.200.226 3/1 (update
malformed) 0 bytes
. . .
    
```

The software clock keeps an “authoritative” flag that indicates whether the time is authoritative (believed to be accurate). If the software clock has been set by a timing source (for example, via NTP), the flag is set. If the time is not authoritative, it will be used only for display purposes. Until the clock is authoritative and the “authoritative” flag is set, the flag prevents peers from synchronizing to the software clock.

Table 83 describes the symbols that proceed the timestamp.

Table 83 *Timestamping Symbols for syslog Messages*

Symbol	Description	Example
*	Time is not authoritative: the software clock is not in sync or has never been set.	*15:29:03.158 UTC Tue Feb 25 2003:
(blank)	Time is authoritative: the software clock is in sync or has just been set manually	15:29:03.158 UTC Tue Feb 25 2003:
.	Time is authoritative, but NTP is not synchronized: the software clock was in sync, but has since lost contact with all configured NTP servers	.15:29:03.158 UTC Tue Feb 25 2003:

The following is sample output from the **show logging summary** command for a Cisco 12012 router. A number in the column indicates that the syslog contains that many messages for the line card. For example, line card in slot 9 has 1 error message, 4 warning messages, and 47 notification messages.



Note

For similar log counting on other platforms, use the **show logging count** command.

```
Router# show logging summary
```

```

+-----+-----+-----+-----+-----+-----+-----+-----+
| SLOT | EMERG | ALERT | CRIT  | ERROR | WARNING | NOTICE | INFO  | DEBUG |
+-----+-----+-----+-----+-----+-----+-----+-----+
| * 0* |       |       |       |       |       |       |       |       |
| 1   |       |       |       |       |       |       |       |       |
| 2   |       |       |       | 1     | 4     | 45    |       |       |
| 3   |       |       |       |       |       |       |       |       |
| 4   |       |       |       | 5     | 4     | 54    |       |       |
| 5   |       |       |       |       |       |       |       |       |
| 6   |       |       |       |       |       |       |       |       |
| 7   |       |       |       | 17    | 4     | 48    |       |       |
| 8   |       |       |       |       |       |       |       |       |
| 9   |       |       |       | 1     | 4     | 47    |       |       |
| 10  |       |       |       |       |       |       |       |       |
| 11  |       |       |       | 12    | 4     | 65    |       |       |
    
```

```
+-----+-----+-----+-----+-----+-----+-----+-----+
Router#
```

Table 84 describes the logging level fields shown in the display.

Table 84 *show logging summary Field Descriptions*

Field	Description
SLOT	Indicates the slot number of the line card. An asterisk next to the slot number indicates the GRP card whose error message counts are not displayed. For information on the GRP card, use the show logging command.
EMERG	Indicates that the system is unusable.
ALERT	Indicates that immediate action is needed.
CRIT	Indicates a critical condition.
ERROR	Indicates an error condition.
WARNING	Indicates a warning condition.
NOTICE	Indicates a normal but significant condition.
INFO	Indicates an informational message only.
DEBUG	Indicates a debugging message.

Related Commands

Command	Description
clear logging	Clears messages from the logging buffer.
logging count	Enables the error log count capability.
logging history size	Changes the number of syslog messages stored in the history table of the router.
logging linecard	Logs messages to an internal buffer on a line card and limits the logging messages displayed on terminal lines other than the console line to messages with a level at or above level.
service timestamps	Configures the system to timestamp debugging or logging messages.
show logging count	Displays a summary of system error messages (syslog messages) by facility and severity.
show logging xml	Displays the state of system logging and the contents of the XML-specific logging buffer.

show logging count

To display a summary of the number of times certain system error messages are occurring, use the **show logging** command in privileged EXEC mode.

show logging count

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(8)T	This command was introduced.

Usage Guidelines To enable the error log count capability (syslog counting feature), use the **logging count** command in global configuration mode.

This feature works independently of the various settings of the other logging commands (such as **[no] logging on**, **[no] logging buffered**, and so on). In other words, turning off logging by other means does not stop the counting and timestamping from occurring.

This command displays information such as the number of times a particular system error message occurs and the time stamp of the last occurrence of the specified message. System error messages are grouped into logical units called “Facilities” based on Cisco IOS software components.

To determine if system error message counting is enabled, use the **show logging** command.

The **service timestamps** command configuration determines the timestamp format (shown in the “Last Time” column) of **show logging count** command output. There is not quite enough space for all options of the possible options (datetime, milliseconds, and timezone) of the **service timestamps datetime** command to be displayed at the same time. As a result, if **msec** is selected, **timezone** will not be displayed. If **show-timezone** is selected but not **msec**, then the time zone will be displayed.

Occasionally, the length of the message name plus the facility name contains too many characters to be printed on one line. The CLI attempts to keep the name and facility name on one line but, if necessary, the line will be wrapped, so that the first line contains the facility name and the second line contains the message name and the rest of the columns.

Examples The following example shows the number of times syslog messages have occurred and the most recent time that each error message occurred. In this example, the **show logging** command is used to determine if the syslog counting feature is enabled:

```
Router# show logging | include count
Count and timestamp logging messages: enabled

Router# show logging count

Facility      Message Name                               Sev  Occur  Last Time
=====
```

show logging count

```

SYS          BOOTTIME          6   1   00:00:12
SYS          RESTART          5   1   00:00:11
SYS          CONFIG_I         5   1   00:00:05
-----
SYS TOTAL                    3

LINEPROTO    UPDOWN              5  13  00:00:19
-----
LINEPROTO TOTAL              13

LINK         UPDOWN              3   1   00:00:18
LINK         CHANGED           5  12   00:00:09
-----
LINK TOTAL                    13

SNMP         COLDSTART          5   1   00:00:11
-----
SNMP TOTAL                    1
    
```

Table 85 describes the significant fields shown in the display.

Table 85 show logging count Field Descriptions

Field	Description
Facility	The facility, such as syslog, from which these error messages are occurring.
Message Name	The name of this message.
Sev	The severity level of this message.
Occur	How many times this message has occurred.
Last Time	The last (most recent) time this message occurred. Timestamping is by default based on the system uptime (for example “3w1d” indicates 3 weeks and 1 day from the last system reboot.)
Sys Total / Lineproto Total / Link Total / SNMP Total	Total number of error messages that have occurred for the specified Facility.

In the following example, the user is interested only in the totals:

```

Router# show logging count | include total
SYS TOTAL                    3
LINEPROTO TOTAL              13
LINK TOTAL                   13
SNMP TOTAL                    1
    
```

Related Commands

Command	Description
clear logging	Clears messages from the logging buffer.
logging count	Enables the system error message log count capability.
service timestamps	Configures the system to time-stamp debugging or logging messages.
show logging	Displays general information about the state of system logging.

show logging history

To display information about the state of the syslog history table, use the **show logging history** command in privileged EXEC mode.

show logging history

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

CommandHistory	Release	Modification
	10.0	This command was introduced.

Usage Guidelines This command displays information about the syslog history table, such as the table size, the status of messages, and text of messages stored in the table. Messages stored in the table are governed by the **logging history** global configuration command.

Examples The following example shows sample output from the **show logging history** command. In this example, notifications of severity level 5 (notifications) through severity level 0 (emergencies) are configured to be written to the logging history table.

```
Router# show logging history
Syslog History Table: 1 maximum table entries,
saving level notifications or higher
0 messages ignored, 0 dropped, 15 table entries flushed,
SNMP notifications not enabled
  entry number 16: SYS-5-CONFIG_I
  Configured from console by console
  timestamp: 1110
Router#
```

Table 86 describes the significant fields shown in the output.

Table 86 show logging history Field Descriptions

Field	Description
maximum table entry	Number of messages that can be stored in the history table. Set with the logging history size command.
saving level notifications <x> or higher	Level of messages that are stored in the history table and sent to the SNMP server (if SNMP notification is enabled). The severity level can be configured with the logging history command.

Table 86 show logging history Field Descriptions (continued)

Field	Description
messages ignored	Number of messages not stored in the history table because the severity level is greater than that specified with the logging history command.
dropped	Number of messages that could not be processed due to lack of system resources. Dropped messages do not appear in the history table and are not sent to the SNMP server.
table entries flushed	Number of messages that have been removed from the history table to make room for newer messages.
SNMP notifications	Whether syslog traps of the appropriate level are sent to the SNMP server. The sending of syslog traps are enabled or disabled through the snmp-server enable traps syslog command.
entry number:	Number of the message entry in the history table. In the example above, the message "SYS-5-CONFIG_I Configured from console by console" indicates a syslog message consisting of the facility name (SYS), which indicates where the message came from, the severity level (5) of the message, the message name (CONFIG_I), and the message text.
timestamp	Time, based on the up time of the router, that the message was generated.

Related Commands

Command	Description
clear logging	Clears messages from the logging buffer.
logging history	Limits syslog messages sent to the router's history table to a specified severity level.
logging history size	Changes the number of syslog messages that can be stored in the history table.
logging linecard	Logs messages to an internal buffer on a line card. This command limits the logging messages displayed on terminal lines other than the console line to messages with a level at or above level.
snmp-server enable traps	The [no] snmp-server enable traps syslog form of this command controls (enables or disables) the sending of system-logging messages to a network management station.

show logging xml

To display the state of system message logging in an XML format, and to display the contents of the XML syslog buffer, use the **show logging xml** command in privileged EXEC mode.

show logging xml

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(15)T	This command was introduced.

Usage Guidelines This command displays the same syslog state information as the standard **show logging** command, but displays the information in XML format. This command also displays the content of the XML syslog buffer (if XML-formatted buffer logging is enabled).

Examples The following example compares the output of the standard **show logging** command with the output of the **show logging xml** command so that you can see how the standard information is formatted in XML.

```
Router# show logging

Syslog logging: enabled (10 messages dropped, 6 messages rate-limited, 0 flushes, 0
overruns, xml enabled)
  Console logging: level debugging, 28 messages logged, xml enabled
  Monitor logging: level debugging, 0 messages logged, xml enabled
  Buffer logging: level debugging, 2 messages logged, xml enabled (2 messages logged)
  Logging Exception size (8192 bytes)
  Count and timestamp logging messages: disabled
  Trap logging: level informational, 35 message lines logged
    Logging to 1.2.3.4, 1 message lines logged, xml disabled
    Logging to 4.3.2.1, 1 message lines logged, xml enabled

Log Buffer (8192 bytes):

00:04:20: %SYS-5-CONFIG_I: Configured from console by console
00:04:41: %SYS-5-CONFIG_I: Configured from console by console

Router#show logging xml

<syslog-logging status="enabled" msg-dropped="10" msg-rate-limited="6" flushes="0"
overruns="0"><xml>enabled</xml></syslog-logging>
  <console-logging level="debugging"
messages-logged="28"><xml>enabled</xml></console-logging>
  <monitor-logging level="debugging"
messages-logged="0"><xml>enabled</xml></monitor-logging>
  <buffer-logging level="debugging" messages-logged="2"><xml>
messages-logged="2">enabled</xml></buffer-logging>
  <logging-exception size="8192 bytes"></logging-exception>
```

show logging xml

```

<count-and-timestamp-logging status="disabled"></count-and-timestamp-logging>
<trap-logging level="informational" messages-lines-logged="35"></trap-logging>
  <logging-to><dest id="0" ipaddr="1.2.3.4"
message-lines-logged="1"><xml>disabled</xml><dest></logging-to>
  <logging-to><dest id="1" ipaddr="4.3.2.1"
message-lines-logged="1"><xml>enabled</xml><dest></logging-to>

<log-xml-buffer size="44444 bytes"></log-xml-buffer>

<ios-log-msg><facility>SYS</facility><severity>5</severity><msg-id>CONFIG_I</msg-id><time>
00:04:20</time><args><arg id="0">console</arg><arg
id="1">console</arg></args></ios-log-msg>
<ios-log-msg><facility>SYS</facility><severity>5</severity><msg-id>CONFIG_I</msg-id><time>
00:04:41</time><args><arg id="0">console</arg><arg
id="1">console</arg></args></ios-log-msg>
Router#

```

Table 82 describes the significant fields shown in the displays.

Table 87 show logging and show logging XML Field Descriptions

Field	Description	XML Tag
Syslog logging	The global state of system message logging (syslog); “enabled” or “disabled.”	syslog-logging
Console logging	State of logging to console connections.	console-logging
Monitor logging	State of logging to monitor (TTY and Telnet) connections.	monitor-logging
Buffer logging	State of logging to the local system logging buffer.	buffer-logging
Count and timestamp logging messages:	Indicates whether the logging count feature is enabled. Corresponds to the logging count command.	count-and-timestamp-logging
Trap logging	State of logging to a remote host.	trap-logging

Related Commands

Command	Description
show logging count	Displays counts of each system error message.
show logging history	Displays the contents of the SNMP syslog history table.
show logging	Displays the contents of the standard syslog buffer.

show memory

To show statistics about memory, including memory-free pool statistics, use the **show memory** command in EXEC mode.

show memory [*memory-type*] [**free**] [**summary**]

Syntax Description	
<i>memory-type</i>	(Optional) Memory type to display (processor , multibus , io , or fast). If <i>memory-type</i> is not specified, statistics for all memory types present are displayed.
free	(Optional) Displays free memory statistics.
summary	(Optional) Displays a summary of memory usage including the size and number of blocks allocated for each address of the system call that allocated the block.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The **show memory** command displays information about memory available after the system image decompresses and loads.

Examples The following is sample output from the **show memory** command:

```
Router# show memory

Processor          Head    Total (b)    Used (b)    Free (b)    Lowest (b)    Largest (b)
-----
Processor memory
Address  Bytes Prev.    Next    Ref  PrevF  NextF  Alloc PC  What
-----
B0EE38   1056 0         B0F280    1         18F132  List Elements
B0F280   2656 B0EE38    B0FD08    1         18F132  List Headers
B0FD08   2520 B0F280    B10708    1         141384  TTY data
B10708   2000 B0FD08    B10F00    1         14353C  TTY Input Buf
B10F00    512 B10708    B11128    1         14356C  TTY Output Buf
B11128   2000 B10F00    B11920    1         1A110E  Interrupt Stack
B11920    44 B11128    B11974    1         970DE8  *Init*
B11974   1056 B11920    B11DBC    1         18F132  messages
B11DBC    84 B11974    B11E38    1         19ABCE  Watched Boolean
B11E38    84 B11DBC    B11EB4    1         19ABCE  Watched Boolean
B11EB4    84 B11E38    B11F30    1         19ABCE  Watched Boolean
B11F30    84 B11EB4    B11FAC    1         19ABCE  Watched Boolean
Router#
```

The following is sample output from the **show memory free** command:

```
Router# show memory free
```

show memory

```

Processor      Head    Total (b)    Used (b)    Free (b)    Lowest (b)    Largest (b)
Processor      B0EE38    5181896     2210076     2971820     2692456     2845368

Processor memory
Address  Bytes  Prev.    Next      Ref  PrevF    NextF    Alloc PC  What
CEB844   24     Free list 1
          32     CEB7A4   CEB88C    0  0        0        96B894    SSE Manager
          52     Free list 2
          72     Free list 3
          76     Free list 4
          80     Free list 5
D35ED4   80     D35E30   D35F4C    0  0        D27AE8   96B894    SSE Manager
D27AE8   80     D27A48   D27B60    0  D35ED4   0        22585E    SSE Manager
          88     Free list 6
          100    Free list 7
D0A8F4   100    D0A8B0   D0A980    0  0        0        2258DA    SSE Manager
          104    Free list 8
B59EF0   108    B59E8C   B59F84    0  0        0        2258DA    (fragment)
    
```

The display of **show memory free** contains the same types of information as the **show memory** display, except that only free memory is displayed, and the information is displayed in order for each free list.

The first section of the display includes summary statistics about the activities of the system memory allocator. [Table 88](#) describes the significant fields shown in the first section of the display.

Table 88 *show memory Field Descriptions—First Section*

Field	Description
Head	Hexadecimal address of the head of the memory allocation chain.
Total(b)	Sum of used bytes plus free bytes.
Used(b)	Amount of memory in use.
Free(b)	Amount of memory not in use.
Lowest(b)	Smallest amount of free memory since last boot.
Largest(b)	Size of largest available free block.

The second section of the display is a block-by-block listing of memory use. [Table 89](#) describes the significant fields shown in the second section of the display.

Table 89 *Characteristics of Each Block of Memory—Second Section*

Field	Description
Address	Hexadecimal address of block.
Bytes	Size of block (in bytes).
Prev.	Address of previous block (should match Address on previous line).
Next	Address of next block (should match address on next line).
Ref	Reference count for that memory block, indicating how many different processes are using that block of memory.
PrevF	Address of previous free block (if free).
NextF	Address of next free block (if free).

Table 89 Characteristics of Each Block of Memory—Second Section (continued)

Field	Description
Alloc PC	Address of the system call that allocated the block.
What	Name of process that owns the block, or “(fragment)” if the block is a fragment, or “(coalesced)” if the block was coalesced from adjacent free blocks.

The **show memory io** command displays the free I/O memory blocks. On the Cisco 4000 router, this command quickly shows how much unused I/O memory is available.

The following is sample output from the **show memory io** command:

```
Router# show memory io

Address  Bytes Prev.  Next    Ref  PrevF  NextF  Alloc PC  What
6132DA0  59264 6132664 6141520 0    0      600DDEC 3FCF0    *Packet Buffer*
600DDEC    500 600DA4C 600DFE0 0    6132DA0 600FE68 0
600FE68    376 600FAC8 600FFE0 0    600DDEC 6011D54 0
6011D54    652 60119B4 6011FE0 0    600FE68 6013D54 0
614FCA0    832 614F564 614FFE0 0    601FD54 6177640 0
6177640 2657056 6172E90 0      0    614FCA0 0      0
Total: 2723244
```

The **show memory sram** command displays the free SRAM memory blocks. For the Cisco 4000 router, this command supports the high-speed static RAM memory pool to make it easier to debug or diagnose problems with allocation or freeing of such memory.

The following is sample output from the **show memory sram** command:

```
Router# show memory sram

Address  Bytes Prev.  Next    Ref  PrevF  NextF  Alloc PC  What
7AE0    38178 72F0    0      0    0      0      0
Total    38178
```

The following example of the **show memory** command used on the Cisco 4000 router includes information about SRAM memory and I/O memory:

```
Router# show memory

          Head  Total (b)  Used (b)  Free (b)  Lowest (b)  Largest (b)
Processor 49C724    28719324 1510864   27208460 26511644    15513908
  I/O    6000000    4194304 1297088   2897216 2869248     2896812
  SRAM    1000      65536   63400    2136     2136      2136

Address  Bytes Prev.  Next    Ref  PrevF  NextF  Alloc PC  What
1000    2032 0      17F0    1      3E73E  *Init*
17F0    2032 1000   1FE0    1      3E73E  *Init*
1FE0    544 17F0   2200    1      3276A  *Init*
2200    52 1FE0   2234    1      31D68  *Init*
2234    52 2200   2268    1      31DAA  *Init*
2268    52 2234   229C    1      31DF2  *Init*
72F0    2032 6E5C   7AE0    1      3E73E  Init
7AE0    38178 72F0    0      0    0      0      0
```

The **show memory summary** command displays a summary of all memory pools and memory usage per Alloc PC (address of the system call that allocated the block).

The following is a partial sample output from the **show memory summary** command. This command shows the size, blocks, and bytes allocated. Bytes equal the size multiplied by the blocks. For a description of the other fields, see Table 20 and Table 21.

show memory

Router# **show memory summary**

Head	Total (b)	Used (b)	Free (b)	Lowest (b)	Largest (b)	
Processor	B0EE38	5181896	2210216	2971680	2692456	2845368

Processor memory

Alloc PC	Size	Blocks	Bytes	What
0x2AB2	192	1	192	IDB: Serial Info
0x70EC	92	2	184	Init
0xC916	128	50	6400	RIF Cache
0x76ADE	4500	1	4500	XDI data
0x76E84	4464	1	4464	XDI data
0x76EAC	692	1	692	XDI data
0x77764	408	1	408	Init
0x77776	116	1	116	Init
0x777A2	408	1	408	Init
0x777B2	116	1	116	Init
0xA4600	24	3	72	List
0xD9B5C	52	1	52	SSE Manager
.....				
0x0	0	3413	2072576	Pool Summary
0x0	0	28	2971680	Pool Summary (Free Blocks)
0x0	40	3441	137640	Pool Summary(All Block Headers)
0x0	0	3413	2072576	Memory Summary
0x0	0	28	2971680	Memory Summary (Free Blocks)

Related Commands

Command	Description
show processes memory	Displays memory used.

show memory ecc

To display single-bit Error Code Correction (ECC) error logset data, use the **show memory ecc** command in privileged EXEC mode.

show memory ecc

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	11.1(30)CC	This command was introduced in Cisco IOS Release 11.1(30)CC.
	12.0(4)XE	This command was integrated into Cisco IOS Release 12.0(4)XE.
	12.0(6)S	This command was integrated into Cisco IOS Release 12.0(6)S.
	12.1(13)	This command was integrated into Cisco IOS Release 12.1(13).

Usage Guidelines Use this command to determine if the router has experienced single-bit parity errors.

Examples The following is sample output from the **show memory ecc** command from a 12000-series router running Cisco IOS Release 12.0(23)S:

```
Router# show memory ecc
ECC Single Bit error log
-----
Single Bit error detected and corrected at 0x574F3640
- Occured 1 time(s)
- Whether a scrub was attempted at this address: Yes
- Syndrome of the last error at this address: 0xE9
- Error detected on a read-modify-write cycle ? No
- Address region classification: Unknown
- Address media classification : Read/Write Single Bit error detected and corrected at
0x56AB3760
- Occured 1 time(s)
- Whether a scrub was attempted at this address: Yes
- Syndrome of the last error at this address: 0x68
- Error detected on a read-modify-write cycle ? No
- Address region classification: Unknown
- Address media classification : Read/Write

Total Single Bit error(s) thus far: 2
```

Table 88 describes the significant fields shown in the first section of the display.

Table 90 *show memory ecc Field Descriptions*

Field	Description
Occured <i>n</i> time(s)	Number of single-bit errors that has occurred.
Whether a scrub was attempted at this address:	Indicates whether a scrub has been performed.
Syndrom of the last error at this address:	Describes the syndrome of last error.
Error detected on a read-modify-write cycle ?	Indicates whether an error has occurred.
Address region classification: Unknown	Describes the region of the error.
Address media classification :	Describes the media of the error and correction.

Related Commands

Command	Description
show memory	Displays statistics about memory, including memory-free pool statistics.

show pci

To display information about the peripheral component interconnect (PCI) hardware registers or bridge registers for the Cisco 7200 series routers, use the **show pci** command in EXEC mode.

show pci { **hardware** | **bridge** [*register*]

Syntax Description	hardware	Displays PCI hardware registers.
	bridge	Displays PCI bridge registers.
	<i>register</i>	(Optional) Number of a specific bridge register in the range from 0 to 7. If not specified, this command displays information about all registers.

Command Modes EXEC

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines The output of this command is generally useful for diagnostic tasks performed by technical support only.



Note

The **show pci hardware** EXEC command displays a substantial amount of information.

Examples The following is sample output for the PCI bridge register 1 on a Cisco 7200 series router:

```
Router# show pci bridge 1

Bridge 4, Port Adaptor 1, Handle=1
DEC21050 bridge chip, config=0x0
(0x00): cfid = 0x00011011
(0x04): cfcs = 0x02800147
(0x08): cfccid = 0x06040002
(0x0C): cfpm1t = 0x00010010

(0x18): cfsm1t = 0x18050504
(0x1C): cfsis = 0x22805050
(0x20): cfmla = 0x48F04880
(0x24): cfpm1a = 0x00004880

(0x3C): cfbc = 0x00000000
(0x40): cfseed = 0x00100000
(0x44): cfstwt = 0x00008020
```

The following is partial sample output for the PCI hardware register, which also includes information on all the PCI bridge registers on a Cisco 7200 series router:

```
Router# show pci hardware

GT64010 External PCI Configuration registers:
```

■ show pci

```
Vendor / Device ID      : 0xAB114601 (b/s 0x014611AB)
Status / Command       : 0x17018002 (b/s 0x02800117)
Class / Revision       : 0x00000006 (b/s 0x06000000)
Latency                : 0x0F000000 (b/s 0x0000000F)
RAS[1:0] Base         : 0x00000000 (b/s 0x00000000)
RAS[3:2] Base         : 0x00000001 (b/s 0x01000000)
CS[2:0] Base          : 0x00000000 (b/s 0x00000000)
CS[3] Base            : 0x00000000 (b/s 0x00000000)
Mem Map Base          : 0x00000014 (b/s 0x14000000)
IO Map Base           : 0x01000014 (b/s 0x14000001)
Int Pin / Line        : 0x00010000 (b/s 0x00000100)
```

Bridge 0, Downstream MB0 to MB1, Handle=0

DEC21050 bridge chip, config=0x0

(0x00): cfid = 0x00011011

(0x04): cfcs = 0x02800143

(0x08): cfccid = 0x06040002

(0x0C): cfpmult = 0x00011810

(0x18): cfsmlt = 0x18000100

(0x1C): cfsis = 0x02809050

(0x20): cfmla = 0x4AF04880

(0x24): cfpmpla = 0x4BF04B00

(0x3C): cfbc = 0x00000000

(0x40): cfseed = 0x00100000

(0x44): cfstwt = 0x00008020

.

.

.

show pci hardware

To display information about the Host-PCI bridge, use the **show pci hardware** command in EXEC mode.

show pci hardware

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines The output of this command is generally useful for diagnostic tasks performed by technical support only:

```
router# show pci hardware
```

```
hardware PCI hardware registers
```

Each device on the PCI bus is assigned a PCI device number. For the C2600, device numbers are as follows:

Device	Device number
0	First LAN device
1	Second LAN device
2	AIM device (if present)
3	Not presently used
4	Port module - first PCI device
5	Port module - second PCI device
6	Port module - third PCI device
7	Port module - fourth PCI device
8-14	Not presently used
15	Xilinx PCI bridge

Examples The following is partial sample output for the PCI hardware register, which also includes information on all the PCI bridge registers. [Table 91](#) describes the significant fields shown in the display.

```
router# show pci hardware
```

```
XILINX Host-PCI Bridge Registers:
Vendor / Device ID: 0x401310EE
Status / Command: 0x040001C6
PCI Slave Base Reg 0: 0x00000000
PCI Slave Base Reg 1: 0x04000000
```

Table 91 *show pci hardware Field Descriptions*

Field	Description
Device/Vendor ID	Identifies the PCI vendor and device. The value 0x401310EE identifies the device as the Xilinx-based Host-PCI bridge for the Cisco 2600 router.
Status/Command	Provides status of the Host-PCI bridge. Refer to the PCI Specification for more information.
PCI Slave Base Reg 0	The base address of PCI Target Region 0 for the Host-PCI bridge. This region is used for Big-Endian transfers between PCI devices and memory.
PCI Slave Base Reg 1	The base address of PCI Target Region 1 for the Host-PCI bridge. This region is used for Little-Endian transfers between PCI devices and memory.

show processes

To display information about the active processes, use the **show processes** command in EXEC mode.

show processes [history]

Syntax Description	history (Optional) Displays the process history in an ordered format.
---------------------------	--

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	10.0	This command was introduced.
	12.2(2)T	The history keyword was added.

Examples The following is sample output from the **show processes** command:

```
Router# show processes

CPU utilization for five seconds: 21%/0%; one minute: 2%; five minutes: 2%
PID QTy PC Runtime (ms) Invoked uSecs Stacks TTY Process
 1 Mwe 2FEA4E 1808 464 3896 1796/3000 0 IP-EIGRP Router
 2 Lst 11682 10236 109 93908 1828/2000 0 Check heaps
 3 Mst 3AE9C 0 280 0 1768/2000 0 Timers
 4 Lwe 74AD2 0 12 0 1492/2000 0 ARP Input
 5.ME 912E4 0 2 0 1892/2000 0 IPC Zone Manager
 6.ME 91264 0 1 0 1936/2000 0 IPC Realm Manager
 7.ME 91066 0 30 0 1784/2000 0 IPC Seat Manager
 8.ME 133368 0 1 0 1928/2000 0 CXBus hot stall
 9.ME 1462EE 0 1 0 1940/2000 0 Microcode load
10 Msi 127538 4 76 52 1608/2000 0 Env Mon
11.ME 160CF4 0 1 0 1932/2000 0 MIP Mailbox
12 Mwe 125D7C 4 280 14 1588/2000 0 SMT input
13 Lwe AFD0E 0 1 0 1772/2000 0 Probe Input
14 Mwe AF662 0 1 0 1784/2000 0 RARP Input
15 Hwe A1F9A 228 549 415 3240/4000 0 IP Input
16 Msa C86A0 0 114 0 1864/2000 0 TCP Timer
17 Lwe CA700 0 1 0 1756/2000 0 TCP Protocols
18.ME CCE7C 0 1 0 1940/2000 0 TCP Listener
19 Mwe AC49E 0 1 0 1592/2000 0 BOOTP Server
20 Mwe 10CD84 24 77 311 1652/2000 0 CDP Protocol
21 Mwe 27BF82 0 2 0 1776/2000 0 ATMSIG Input
```

The following is sample output from the **show processes history** command:

```
Router# show process history
PID Exectime(ms) Caller PC Process Name
 3 12 0x0 Exec
16 0 0x603F4DEC GraphIt
21 0 0x603CFEF4 TTY Background
22 0 0x6042FD7C Per-Second Jobs
67 0 0x6015CD38 SMT input
39 0 0x60178804 FBM Timer
```

show processes

```

16          0 0x603F4DEC GraphIt
21          0 0x603CFEF4 TTY Background
22          0 0x6042FD7C Per-Second Jobs
16          0 0x603F4DEC GraphIt
21          0 0x603CFEF4 TTY Background
22          0 0x6042FD7C Per-Second Jobs
67          0 0x6015CD38 SMT input
39          0 0x60178804 FBM Timer
24          0 0x60425070 Compute load avgs
11          0 0x605210A8 ARP Input
69          0 0x605FD4F4 DHCPD Database
69          0 0x605FD568 DHCPD Database
51          0 0x60670B3C IP Cache Ager
69          0 0x605FD568 DHCPD Database
36          0 0x606E96DC SSS Test Client
69          0 0x605FD568 DHCPD Database
--More--
PID Exectime(ms) Caller PC Process Name
16          0 0x603F4DEC GraphIt
21          0 0x603CFEF4 TTY Background
22          0 0x6042FD7C Per-Second Jobs
34          0 0x60679D74 CDP Protocol
19          0 0x6041FBA4 Net Background
36          0 0x606E97AC SSS Test Client
12          0 0x60722A40 HC Counter Timers
69          0 0x605FD568 DHCPD Database
44          0 0x6031AD14 Adj Manager
65          4 0x60BC5BE0 SAA Event Processor
25          8 0x6042FD7C Per-minute Jobs
16          0 0x603F4DEC GraphIt
21          0 0x603CFEF4 TTY Background
22          0 0x6042FD7C Per-Second Jobs
67          0 0x6015CD38 SMT input
39          0 0x60178804 FBM Timer
2          0 0x60496768 Load Meter
16          0 0x603F4DEC GraphIt
21          0 0x603CFEF4 TTY Background
22          0 0x6042FD7C Per-Second Jobs
16          0 0x603F4DEC GraphIt
21          0 0x603CFEF4 TTY Background
22          0 0x6042FD7C Per-Second Jobs
--More--
. . .

```

Table 92 describes the significant fields shown in the displays.

Table 92 show processes Field Descriptions

Field	Description
CPU utilization for five seconds	CPU utilization for the last 5 seconds. The second number indicates the percent of CPU time spent at the interrupt level.
one minute	CPU utilization for the last minute.
five minutes	CPU utilization for the last 5 minutes.
PID	Process ID.
Q	Process queue priority. Possible values: H (high), M (medium), L (low).

Table 92 *show processes Field Descriptions (continued)*

Field	Description
Ty	Scheduler test. Possible values: * (currently running), E (waiting for an event), S (ready to run, voluntarily relinquished processor), rd (ready to run, wakeup conditions have occurred), we (waiting for an event), sa (sleeping until an absolute time), si (sleeping for a time interval), sp (sleeping for a time interval (alternate call), st (sleeping until a timer expires), hg (hung; the process will never execute again), xx (dead: the process has terminated, but has not yet been deleted.).
PC	Current program counter.
Runtime (ms)	CPU time the process has used (in milliseconds).
Invoked	Number of times the process has been invoked.
uSecs	Microseconds of CPU time for each process invocation.
Stacks	Low water mark/Total stack space available (in bytes).
TTY	Terminal that controls the process.
Process	Name of the process.
5Sec	CPU utilization by task in the last 5 seconds.
1Min	CPU utilization by task in the last minute.
5Min	CPU utilization by task in the last 5 minutes.



Note

Because the network server has a 4-millisecond clock resolution, run times are considered reliable only after a large number of invocations or a reasonable, measured run time.

For a list of process descriptions, see http://www.cisco.com/warp/public/63/showproc_cpu.html .

Related Commands

Command	Description
show processes memory	Displays amount of system memory used per system process.

show processes cpu

To display CPU utilization information about the active processes in a device, use the **show processes cpu** command in privileged EXEC mode.

show processes cpu [history | sorted]

Syntax Description	history	(Optional) Displays CPU history in a graph format.
	sorted	(Optional) Displays CPU utilization sorted by percentage.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0	This command was introduced.
	12.2(2)T	The history keyword was added.
	12.3(8)T	This command was enhanced to display Address Resolution Protocol (ARP) output.

Usage Guidelines When you use the optional **history** keyword, output shows (in ASCII graphical form) the total CPU usage on the device over a period of time. Time periods are one minute, one hour, and 72 hours, displayed in increments of one second, one minute, and one hour, respectively. Maximum usage is measured and recorded every second; average usage is calculated on periods of more than one second.

Consistently high CPU utilization over an extended period of time indicates a problem and using the **show processes cpu** command is useful for troubleshooting. Also, you can use the output of this command in the Cisco [Output Interpreter](#) tool to display potential issues and fixes. Output Interpreter is available to registered users of Cisco.com who are logged in and have Java Script enabled.

For a list of system processes, go to http://www.cisco.com/warp/public/63/showproc_cpu.html.

Examples The following is sample output from the **show processes cpu** command without keywords:

```
Router# show processes cpu

CPU utilization for five seconds: 5%/2%; one minute: 3%; five minutes: 2%
  PID  Runtime (ms)  Invoked  uSecs   5Sec  1Min  5Min  TTY  Process
    1      1736         58  29931    0%   0%   0%   0   Check heaps
    2         68        585   116    1.00% 1.00%  0%   0   IP Input
    3          0        744    0      0%   0%   0%   0   TCP Timer
    4          0          2    0      0%   0%   0%   0   TCP Protocols
    5          0          1    0      0%   0%   0%   0   BOOTP Server
    6         16        130   123    0%   0%   0%   0   ARP Input
    7          0          1    0      0%   0%   0%   0   Probe Input
    8          0          7    0      0%   0%   0%   0   MOP Protocols
    9          0          2    0      0%   0%   0%   0   Timers
   10        692         64  10812    0%   0%   0%   0   Net Background
   11          0          5    0      0%   0%   0%   0   Logger
   12          0          38    0      0%   0%   0%   0   BGP Open
```


Table 93 *show processes cpu Field Descriptions*

Field	Description
CPU utilization for five seconds	CPU utilization for the last 5 seconds and the percent of CPU time spent at the interrupt level.
one minute	CPU utilization for the last minute and the percent of CPU time spent at the interrupt level.
five minutes	CPU utilization for the last 5 minutes and the percent of CPU time spent at the interrupt level.
PID	Process ID.
Runtime (ms)	CPU time the process has used (in milliseconds).
Invoked	Number of times the process has been invoked.
uSecs	Microseconds of CPU time for each process invocation.
5Sec	CPU utilization by task in the last 5 seconds.
1Min	CPU utilization by task in the last minute.
5Min	CPU utilization by task in the last 5 minutes.
TTY	Terminal that controls the process.
Process	Name of the process.



Note

Because platforms have a 4- to 8-millisecond clock resolution, run times are considered reliable only after several invocations or a reasonable, measured run time.

Related Commands

Command	Description
show processes memory	Displays the amount of system memory used per system process.

show processes memory

To show memory used, use the **show processes memory** command in EXEC mode.

show processes memory [*pid* | *sorted*]

Syntax Description	<i>pid</i>	(Optional) Process ID number of a specific process. This keyword shows detail for only the specified process.
	<i>sorted</i>	(Optional) Displays CPU history sorted by percentage of utilization.

Command Modes Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Examples The following is sample output from the **show processes memory** command:

```
Router# show processes memory

Total: 5611448, Used: 2307548, Free: 3303900
PID  TTY  Allocated    Freed    Holding    Getbufs    Retbufs Process
 0    0    199592      1236    1907220      0           0 *Init*
 0    0      400        76928     400         0           0 *Sched*
 0    0    5431176    3340052    140760    349780      0 *Dead*
 1    0      256         256     1724         0           0 Load Meter
 2    0      264          0     5032         0           0 Exec
 3    0          0          0     2724         0           0 Check heaps
 4    0    97932          0     2852    32760      0 Pool Manager
 5    0      256         256     2724         0           0 Timers
 6    0      92           0     2816         0           0 CXBus hot stall
 7    0          0          0     2724         0           0 IPC Zone Manager
 8    0          0          0     2724         0           0 IPC Realm Manager
 9    0          0          0     2724         0           0 IPC Seat Manager
10   0      892         476     3256         0           0 ARP Input
11   0      92           0     2816         0           0 SERIAL A'detect
12   0      216          0     2940         0           0 Microcode Loader
13   0          0          0     2724         0           0 RFSS watchdog
14   0    15659136   15658584    3276         0           0 Env Mon
.
.
.
77   0      116          0     2844         0           0 IPX-EIGRP Hello
2307224 Total
```

Table 94 describes the significant fields shown in the display.

Table 94 show processes memory Field Descriptions

Field	Description
Total:	Total amount of memory held.
Used:	Total amount of used memory.
Free:	Total amount of free memory.
PID	Process ID.
TTY	Terminal that controls the process.
Allocated	Bytes of memory allocated by the process.
Freed	Bytes of memory freed by the process, regardless of who originally allocated it.
Holding	Amount of memory currently allocated to the process.
Getbufs	Number of times the process has requested a packet buffer.
Retbufs	Number of times the process has relinquished a packet buffer.
Process	Process name.
Init	System initialization.
Sched	The scheduler.
Dead	Processes as a group that are now dead.
Total	Total amount of memory held by all processes.

The following is sample output from the show process memory command when a PID is specified:

```
Router# show process memory 1

Proc Memory Summary for pid = 1
Holding = 6844

pc = 0x6049B900, size = 000006044, count = 0001
pc = 0x60480650, size = 000000612, count = 0001
pc = 0x6048254C, size = 000000188, count = 0001

Router#
```

Related Commands

Command	Description
show memory	Displays statistics about memory, including memory-free pool statistics.
show processes	Displays information about the active processes.

show protocols

To display configured Level 3 protocols, use the **show protocols** command in EXEC mode.

show protocols

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines This command shows the global and interface-specific status of any configured Level 3 protocol; for example, IP, DECnet, IPX, AppleTalk, and so on.

Examples The following is sample output from the **show protocols** command:

```
Router# show protocols

Global values:
  Internet Protocol routing is enabled
  DECNET routing is enabled
  XNS routing is enabled
  Appletalk routing is enabled
  X.25 routing is enabled
Ethernet 0 is up, line protocol is up
  Internet address is 192.168.1.1, subnet mask is 255.255.255.0
  Decnet cost is 5
  XNS address is 2001.AA00.0400.06CC
  AppleTalk address is 4.129, zone Twilight
Serial 0 is up, line protocol is up
  Internet address is 192.168.7.49, subnet mask is 255.255.255.240
Ethernet 1 is up, line protocol is up
  Internet address is 192.168.2.1, subnet mask is 255.255.255.0
  Decnet cost is 5
  XNS address is 2002.AA00.0400.06CC
  AppleTalk address is 254.132, zone Twilight
Serial 1 is down, line protocol is down
  Internet address is 192.168.7.177, subnet mask is 255.255.255.240
  AppleTalk address is 999.1, zone Magnolia Estates
```

For more information on the parameters or protocols shown in this sample output, see the *Cisco IOS Network Protocols Configuration Guide*.

show stacks

To monitor the stack usage of processes and interrupt routines, use the **show stacks** command in EXEC mode.

show stacks

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The display from this command includes the reason for the last system reboot. If the system was reloaded because of a system failure, a saved system stack trace is displayed. This information is of use only to your technical support representative in analyzing crashes in the field. It is included here in case you need to read the displayed statistics to an engineer over the phone.

Examples The following is sample output from the **show stacks** command following a system failure:

```
Router# show stacks

Minimum process stacks:
Free/Size  Name
 652/1000  Router Init
 726/1000  Init
 744/1000  BGP Open
 686/1200  Virtual Exec

Interrupt level stacks:
Level      Called Free/Size  Name
 1          0 1000/1000 env-flash
 3          738 900/1000 Multiport Communications Interfaces
 5          178 970/1000 Console UART

System was restarted by bus error at PC 0xAD1F4, address 0xD0D0D1A
GS Software (GS3), Version 9.1(0.16), BETA TEST SOFTWARE
Compiled Tue 11-Aug-92 13:27 by jthomas
Stack trace from system failure:
FP: 0x29C158, RA: 0xACFD4
FP: 0x29C184, RA: 0xAD20C
FP: 0x29C1B0, RA: 0xACFD4
FP: 0x29C1DC, RA: 0xAD304
FP: 0x29C1F8, RA: 0xAF774
FP: 0x29C214, RA: 0xAF83E
FP: 0x29C228, RA: 0x3E0CA
FP: 0x29C244, RA: 0x3BD3C
```

Related Commands

Command	Description
show processes	Displays information about the active processes.

show subsys

To display the subsystem information, use the **show subsys** command in privileged EXEC mode.

show subsys [**class** *class* | **name** *name*]

Syntax Description	class <i>class</i>	(Optional) Displays the subsystems of the specified class. Valid classes are driver , kernel , library , management , protocol , and registry .
	name <i>name</i>	(Optional) Displays the specified subsystem. Use the asterisk (*) as a wildcard at the end of the name to list all subsystems, starting with the specified characters.

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	11.1	This command was introduced.

Usage Guidelines	Use the show subsys command to confirm that all required features are in the running image.
------------------	--

Examples In the following example, partial sample output is shown from the **show subsys** command:

```
Router# show subsys

static_map      Class      Version
arp             Kernel     1.000.001
ether          Kernel     1.000.001
compress       Kernel     1.000.001
alignment      Kernel     1.000.002
monvar         Kernel     1.000.001
slot           Kernel     1.000.001
oir            Kernel     1.000.001
atm            Kernel     1.000.001
ip_addrpool_sys Library    1.000.001
chat           Library    1.000.001
dialer         Library    1.000.001
flash_services Library    1.000.001
ip_localpool_sys Library    1.000.001
nvram_common   Driver     1.000.001
ASP            Driver     1.000.001
sonict         Driver     1.000.001
oc3suni        Driver     1.000.001
oc12suni       Driver     1.000.001
ds3suni        Driver     1.000.001
.
.
.
```

Table 95 describes the significant fields shown in the display.

Table 95 *show subsys Field Descriptions*

Field	Description
static_map	Name of the subsystem.
Class	Class of the subsystem. Possible classes include Kernel, Library, Driver, Protocol, Management, Registry, and SystemInit.
Version	Version of the subsystem.

show tcp

To display the status of TCP connections, use the **show tcp** command in EXEC mode.

show tcp [*line-number*]

Syntax Description	<i>line-number</i>	(Optional) Absolute line number of the line for which you want to display Telnet connection status.
---------------------------	--------------------	---

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	10.0	This command was introduced.

Examples The following is sample output from the **show tcp** command:

```
Router# show tcp

tty0, connection 1 to host cider
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 172.31.232.17, Local port: 11184
Foreign host: 172.31.1.137, Foreign port: 23

Enqueued packets for retransmit: 0, input: 0, saved: 0

Event Timers (current time is 67341276):
Timer:      Retrans  TimeWait  AckHold    SendWnd  KeepAlive  GiveUp     PmtuAger
Starts:      30         0         32         0         0         0         0
Wakeups:     1         0         14         0         0         0         0
Next:        0         0         0         0         0         0         0

iss: 67317172 snduna: 67317228 sndnxt: 67317228 sndwnd: 4096
irs: 1064896000 rcvnxt: 1064897597 rcvwnd: 2144 delrcvwnd: 0

SRTT: 317 ms, RTTO: 900 ms, RTV: 133 ms, KRTT: 0 ms
minRTT: 4 ms, maxRTT: 300 ms, ACK hold: 300 ms
Flags: higher precedence, idle user, retransmission timeout

Datagrams (max data segment is 536 bytes):
Rcvd: 41 (out of order: 0), with data: 34, total data bytes: 1596
Sent: 57 (retransmit: 1), with data: 35, total data bytes: 55
```

[Table 96](#) describes the first five lines of output shown in the display.

Table 96 *show tcp* Field Descriptions—First Section of Output

Field	Description
tty0	Identifying number of the line.
connection 1	Number identifying the TCP connection.
to host xxx	Name of the remote host to which the connection has been made.

Table 96 show tcp Field Descriptions—First Section of Output (continued)

Field	Description
Connection state is ESTAB	<p>A connection progresses through a series of states during its lifetime. These states follow in the order in which a connection progresses through them.</p> <ul style="list-style-type: none"> • LISTEN—Waiting for a connection request from any remote TCP and port. • SYNSENT—Waiting for a matching connection request after having sent a connection request. • SYNRCVD—Waiting for a confirming connection request acknowledgment after having both received and sent a connection request. • ESTAB—Indicates an open connection; data received can be delivered to the user. This is the normal state for the data transfer phase of the connection. • FINWAIT1—Waiting for a connection termination request from the remote TCP or an acknowledgment of the connection termination request previously sent. • FINWAIT2—Waiting for a connection termination request from the remote TCP host. • CLOSEWAIT—Waiting for a connection termination request from the local user. • CLOSING—Waiting for a connection termination request acknowledgment from the remote TCP host. • LASTACK—Waiting for an acknowledgment of the connection termination request previously sent to the remote TCP host. • TIMEWAIT—Waiting for enough time to pass to be sure the remote TCP host has received the acknowledgment of its connection termination request. • CLOSED—Indicates no connection state at all. <p>For more information, see RFC 793, <i>Transmission Control Protocol Functional Specification</i>.</p>
I/O status:	Number describing the current internal status of the connection.
unread input bytes:	Number of bytes that the lower-level TCP processes have read, but the higher-level TCP processes have not yet processed.
Local host:	IP address of the network server.
Local port:	Local port number, as derived from the following equation: <i>line-number + (512 * random-number)</i> . (The line number uses the lower nine bits; the other bits are random.)
Foreign host:	IP address of the remote host to which the TCP connection has been made.
Foreign port:	Destination port for the remote host.

Table 96 show tcp Field Descriptions—First Section of Output (continued)

Field	Description
Enqueued packets for retransmit:	Number of packets waiting on the retransmit queue. These are packets on this TCP connection that have been sent but have not yet been acknowledged by the remote TCP host.
input:	Number of packets that are waiting on the input queue to be read by the user.
saved:	Number of received out-of-order packets that are waiting for all packets comprising the message to be received before they enter the input queue. For example, if packets 1, 2, 4, 5, and 6 have been received, packets 1 and 2 would enter the input queue, and packets 4, 5, and 6 would enter the saved queue.

The following line of output shows the current time according to the system clock of the local host:

```
Event Timers (current time is 67341276):
```

The time shown is the number of milliseconds since the system started.

The following lines of output display the number of times that various local TCP timeout values were reached during this connection. In this example, the local host re-sent data 30 times because it received no response from the remote host, and it sent an acknowledgment many more times because there was no data on which to piggyback.

```
Timer:      Retrans   TimeWait   AckHold    SendWnd    KeepAlive   GiveUp     PmtuAger
Starts:      30          0          32         0          0          0          0
Wakeups:     1           0          14         0          0          0          0
Next:        0           0          0          0          0          0          0
```

Table 97 describes the fields in the preceding lines of output.

Table 97 show tcp Field Descriptions—Second Section of Output

Field	Description
Timer:	The names of the timers in the display.
Starts:	The number of times the timer has been started during this connection.
Wakeups:	Number of keepalives sent without receiving any response. (This field is reset to zero when a response is received.)
Next:	The system clock setting that will trigger the next time this timer will go off.
Retrans	The Retransmission timer is used to time TCP packets that have not been acknowledged and are waiting for retransmission.
TimeWait	The TimeWait timer is used to ensure that the remote system receives a request to disconnect a session.
AckHold	The Acknowledgment timer is used to delay the sending of acknowledgments to the remote TCP in an attempt to reduce network use.
SendWnd	The Send Window is used to ensure that there is no closed window due to a lost TCP acknowledgment.
KeepAlive	The KeepAlive timer is used to control the transmission of test messages to the remote TCP to ensure that the link has not been broken without the local TCP's knowledge.

Table 97 show tcp Field Descriptions—Second Section of Output (continued)

Field	Description
GiveUp	The GiveUp timer determines the amount of time a local host will wait for an acknowledgement (or other appropriate reply) of a transmitted message after the the maximum number of retransmissions has been reached. If the timer expires, the local host gives up retransmission attempts and declares the connection dead.
PmtuAger	The PMTU age timer is a time interval for how often TCP reestimates the path MTU with a larger maximum segment size (MSS). When the age timer is used, TCP path MTU becomes a dynamic process. If the MSS is smaller than what the peer connection can manage, a larger MSS is tried every time the age timer expires. The discovery process stops when the send MSS is as large as the peer negotiated or the timer has been manually disabled by setting it to infinite.

The following lines of output display the sequence numbers that TCP uses to ensure sequenced, reliable transport of data. The local host and remote host each use these sequence numbers for flow control and to acknowledge receipt of datagrams. [Table 98](#) describes the significant fields shown in the display.

```
iss: 67317172 snduna: 67317228 sndnxt: 67317228 sndwnd: 4096
irs: 1064896000 rcvnxt: 1064897597 rcvwnd: 2144 delrcvwnd: 0
```

Table 98 show tcp Field Descriptions—Sequence Number

Field	Description
iss:	Initial send sequence number.
snduna:	Last send sequence number that the local host sent but has not received an acknowledgment for.
sndnxt:	Sequence number the local host will send next.
sndwnd:	TCP window size of the remote host.
irs:	Initial receive sequence number.
rcvnxt:	Last receive sequence number that the local host has acknowledged.
rcvwnd:	TCP window size of the local host.
delrcvwnd:	Delayed receive window—data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field.

The following lines of output display values that the local host uses to keep track of transmission times so that TCP can adjust to the network it is using.

[Table 99](#) describes the significant fields shown in the display.

```
SRTT: 317 ms, RTTO: 900 ms, RTV: 133 ms, KRTT: 0 ms
minRTT: 4 ms, maxRTT: 300 ms, ACK hold: 300 ms
Flags: higher precedence, idle user, retransmission timeout
```

Table 99 show tcp Field Descriptions—Line Beginning with “SRTT”

Field	Description
SRTT:	A calculated smoothed round-trip timeout.
RTTO:	Round-trip timeout.
RTV:	Variance of the round-trip time.
KRTT:	New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been re-sent.
minRTT:	Smallest recorded round-trip timeout (hard-wire value used for calculation).
maxRTT:	Largest recorded round-trip timeout.
ACK hold:	Time the local host will delay an acknowledgment in order to piggyback data on it.
Flags:	Properties of the connection.

For more information on these fields, refer to *Round Trip Time Estimation*, P. Karn & C. Partridge, ACM SIGCOMM-87, August 1987.

Table 100 describes the significant fields shown in the display.

```
Datagrams (max data segment is 536 bytes):
Rcvd: 41 (out of order: 0), with data: 34, total data bytes: 1596
Sent: 57 (retransmit: 1), with data: 35, total data bytes: 55
```

Table 100 show tcp Field Descriptions—Last Section of Output

Field	Description
Rcvd:	Number of datagrams the local host has received during this connection (and the number of these datagrams that were out of order).
with data:	Number of these datagrams that contained data.
total data bytes:	Total number of bytes of data in these datagrams.
Sent:	Number of datagrams the local host sent during this connection (and the number of these datagrams that needed to be re-sent).
with data:	Number of these datagrams that contained data.
total data bytes:	Total number of bytes of data in these datagrams.

Related Commands

Command	Description
show tcp brief	Displays a concise description of TCP connection endpoints.

show tcp brief

To display a concise description of TCP connection endpoints, use the **show tcp brief** command in EXEC mode.

show tcp brief [all]

Syntax Description	all	(Optional) Displays status for all endpoints. Without this keyword, endpoints in the LISTEN state are not shown.
---------------------------	------------	--

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	11.2	This command was introduced.

Examples The following is sample output from the **show tcp brief** command while a user has connected into the system via Telnet:

```
Router> show tcp brief

TCB      Local Address      Foreign Address      (state)
609789AC Router.cisco.com.23  cider.cisco.com.3733 ESTAB
```

Table 101 describes the significant fields shown in the display.

Table 101 show tcp brief Field Descriptions

Field	Description
TCB	An internal identifier for the endpoint.
Local Address	The local IP address and port.
Foreign Address	The foreign IP address and port (at the opposite end of the connection).
(state)	The state of the connection. States are described in the syntax description of the show tcp command.

Related Commands	Command	Description
	show tcp	Displays the status of TCP connections.

show tdm connections

To display a snapshot of the time-division multiplexing (TDM) bus connection memory in a Cisco AS5200 access server, use the **show tdm connections** command in EXEC mode.

show tdm connections [**motherboard** | **slot** *slot-number*]

Syntax Description	motherboard	(Optional) Motherboard in the Cisco AS5200 access server.
	slot <i>slot-number</i>	(Optional) Slot number.

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines The **show tdm connections** command shows the connection memory for all TDM bus connections in the access server if you do not limit the display to the motherboard or a slot.

Examples In the following example, source stream 3 (ST3) channel 2 switched out of stream 6 (ST6) channel 2 is shown:

```
AS5200# show tdm connections motherboard

MT8980 motherboard unit 0, Control Register = 0x1F, ODE Register = 0x06
Connection Memory for ST6:
Ch0: 0x62, Ch1: 0x00, Ch2: 0x00, Ch3: 0x00
Ch4: 0x00, Ch5: 0x00, Ch6: 0x00, Ch7: 0x00
Ch8: 0x00, Ch9: 0x00, Ch10: 0x00, Ch11: 0x00
Ch12: 0x00, Ch13: 0x00, Ch14: 0x00, Ch15: 0x00
Ch16: 0x00, Ch17: 0x00, Ch18: 0x00, Ch19: 0x00
Ch20: 0x00, Ch21: 0x00, Ch22: 0x00, Ch23: 0x00
Ch24: 0x00, Ch25: 0x00, Ch26: 0x00, Ch27: 0x00
Ch28: 0x00, Ch29: 0x00, Ch30: 0x00, Ch31: 0x00
```

To interpret the hexadecimal number 0x62 into meaningful information, you must translate it into binary code. These two hexadecimal numbers represent a connection from any stream and a channel on any stream. The number 6 translates into the binary code 0110, which represents the third-source stream. The number 2 translates into the binary code 0010, which represents the second-source channel.

Stream 6 (ST6) channel 0 is the destination for ST3 channel 2 in this example.

Related Commands	Command	Description
	show tcp	Displays the status of TCP connections.

show tdm data

To display a snapshot of the time-division multiplexing (TDM) bus data memory in a Cisco AS5200 access server, use the **show tdm data** command in EXEC mode.

show tdm data [**motherboard** | **slot** *slot-number*]

Syntax Description	motherboard	(Optional) Motherboard in the Cisco AS5200 access server.
	slot <i>slot-number</i>	(Optional) Slot number.

Command Modes EXEC

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines The data memory for all TDM bus connections in the access server is displayed if you do not specify a motherboard or slot.

Examples In the following example, a snapshot of TDM memory is shown where the normal ISDN idle pattern (0x7E) is present on all channels of the TDM device resident on the motherboard:

```
AS5200# show tdm data motherboard

MT8980 motherboard unit 0, Control Register = 0x1F, ODE Register = 0x06
Data Memory for ST0:
Ch0: 0x7E, Ch1: 0x7E, Ch2: 0x7E, Ch3: 0x7E
Ch4: 0x7E, Ch5: 0x7E, Ch6: 0x7E, Ch7: 0x7E
Ch8: 0x7E, Ch9: 0x7E, Ch10: 0x7E, Ch11: 0x7E
Ch12: 0x7E, Ch13: 0x7E, Ch14: 0x7E, Ch15: 0x7E
Ch16: 0x7E, Ch17: 0x7E, Ch18: 0x7E, Ch19: 0x7E
Ch20: 0x7E, Ch21: 0x7E, Ch22: 0x7E, Ch23: 0x7E
Ch24: 0x7E, Ch25: 0x7E, Ch26: 0x7E, Ch27: 0x7E
Ch28: 0x7E, Ch29: 0x7E, Ch30: 0x7E, Ch31: 0x7E
Data Memory for ST1:
Ch0: 0x7E, Ch1: 0x7E, Ch2: 0x7E, Ch3: 0x7E
Ch4: 0x7E, Ch5: 0x7E, Ch6: 0x7E, Ch7: 0x7E
Ch8: 0x7E, Ch9: 0x7E, Ch10: 0x7E, Ch11: 0x7E
Ch12: 0x7E, Ch13: 0x7E, Ch14: 0x7E, Ch15: 0x7E
Ch16: 0x7E, Ch17: 0x7E, Ch18: 0x7E, Ch19: 0x7E
Ch20: 0x7E, Ch21: 0x7E, Ch22: 0x7E, Ch23: 0x7E
Ch24: 0x7E, Ch25: 0x7E, Ch26: 0x7E, Ch27: 0x7E
Ch28: 0x7E, Ch29: 0x7E, Ch30: 0x7E, Ch31: 0x7E
```

Related Commands	Command	Description
	show tdm connections	Displays data about the TDM bus connection memory in a Cisco AS5200 access server.

show tech-support

To display general information about the router when reporting a problem to Cisco technical support, use the **show tech-support** command in privileged EXEC mode.

show tech-support [**page**] [**password**] [**ipmulticast** | **rsvp**]

Syntax Description	
page	(Optional) Causes the output to display a page of information at a time. Press the Enter key to display the next line of output or press the space bar to display the next page of information. If this keyword is not used, the output scrolls (that is, does not stop for page breaks).
password	(Optional) Leaves passwords and other security information in the output. If this keyword is not used, passwords and other security-sensitive information in the output are replaced with the label “<removed>” (this is the default).
ipmulticast	(Optional) Displays the IP multicast related information from the show ip pim , show ip igmp , show ip mroute , and other IP multicast show commands.
rsvp	(Optional) Displays the IP RSVP related information that is generated by the different show ip rsvp commands.

Defaults Displays output without page breaks and remove passwords and other security information.

Command Modes Privileged EXEC

Command History	Release	Modification
	11.2	This command was introduced.
	11.3(7), 11.2(7)T, 11.2(16), 12.0	The output for this command was expanded to show additional information for boot , bootflash , context , and traffic for all enabled protocols.
	12.0 T	Support for this command was added for Cisco 800 and uBR905 series routers.
	12.1(3)T	Support for encryption module show commands was added for the Cisco 1700 series.
	12.2(13)T	Support for Cisco Easy VPN commands was added to the Cisco IOS Release 12.2 T. Support for show commands related to AppleTalk EIGRP, Apollo Domain, Banyan VINES, EGP, HP Probe, IGRP, NHRP for IPX, NLSP,SMRP for AppleTalk, and XNS were removed because these protocols are no longer supported in Cisco IOS software.

Usage Guidelines The **show tech-support** command displays a large amount of configuration, run-time status, and other information about the router for troubleshooting purposes. The output of this command can be provided to technical support representatives when reporting a problem.

**Tip**

Depending on the platform and configuration, the output from the **show tech-support** command can easily exceed the buffers found in many communications programs. To write the output to a file so that it can be sent to Cisco TAC, use the pipe (|) redirection extensions available for this command. These extensions are documented as the **show <command> append**, **show <command> redirect**, and **show <command> tee** commands. Alternatively, you can use a Telnet program that allows you to capture the output directly to disk. The output of this command can also be limited using the **| include**, **| exclude**, and **| begin** extensions. See the documentation of the **show <command> include**, **show <command> exclude**, and **show <command> begin** commands for more information.

The **show tech-support** command displays the output of a number of **show** commands at once. The output from this command will vary depending on your platform and configuration. For example, access servers will display voice-related **show** command output, and the **show protocol traffic** commands will be displayed for only the protocols enabled on your device. The output of the **show tech-support** command can include the output of the following commands:

Configuration Information

- **show version**
- **show runningconfig**

Run-time State Information

- **show stacks**
- **show interfaces**
- **show controllers**
- **show process memory**
- **show process cpu**
- **show process cpu history**
- **show controller c0 mac state**

System and Memory Information

- **show bootflash**
- **show bootvar**
- **show buffers**
- **show context**
- **show controllers**
- **show interfaces**
- **show region**

Voice Port Information

- **show voice port**
- **show dialpeer voice**
- **show gateway**
- **show call active voice**
- **show call history voice**

Traffic Information

- show clns traffic
- show decnet traffic
- show ip traffic
- show novell traffic

Cisco Easy VPN Configuration Information

- show crypto ipsec client ezvpn
- show ip nat statistics
- show ip nat translations
- show crypto map
- show access-list
- show crypto isakmp policy
- show crypto ipsec transform
- show crypto isakmp sa
- show crypto engine connection active
- show crypto ipsec sa

Examples

For a sample display of the output of the **show tech-support** command, refer to the documentation for the **show** commands listed.

Related Commands

Command	Description
show <command> append	Redirects and appends show command output to the end of an existing file.
show <command> begin	Begins the output of any show command from the specified string.
show <command> exclude	Filters show command output so that it excludes lines that contain the specified string.
show <command> include	Filters show command output so that it displays only lines that contain the specified string.
show <command> redirect	Redirects the output of any show command to a specified file.
show <command> tee	Copies the show command output to a file while displaying it on the terminal.

show tech-support

To display general information about the router when it reports a problem, use the **show tech-support** command in privileged EXEC mode.

show tech-support [page] [password]

Syntax Description	parameter	Description
	page	(Optional) Causes the output to display a page of information at a time. Use the Return key to display the next line of output or use the space bar to display the next page of information. If not used, the output scrolls (that is, does not stop for page breaks).
	password	(Optional) Leaves passwords and other security information in the output. If not used, passwords and other security-sensitive information in the output are replaced with the label “<removed>” (this is the default).

Defaults Display output without page breaks and remove passwords and other security information.

Command Modes Privileged EXEC

Command History	Release	Modification
	11.2	This command was introduced.
	11.3(7)	The output for this command was expanded to show additional information for boot , bootflash , context , and traffic for all enabled protocols.
	11.3(7)T	The output for this command was expanded to show additional information for boot , bootflash , context , and traffic for all enabled protocols
	11.2(16)	The output for this command was expanded to show additional information for boot , bootflash , context , and traffic for all enabled protocols
	12.0	The output for this command was expanded to show additional information for boot , bootflash , context , and traffic for all enabled protocols

Usage Guidelines The **show tech-support** command is useful for collecting a large amount of information about your routing device for troubleshooting purposes. The output of this command can be provided to technical support representatives when reporting a problem.

The **show tech-support** command displays the output of a number of **show** commands at once. The output from this command will vary depending on your platform and configuration. For example, access servers will display voice-related show output. Additionally, the **show protocol traffic** commands will be displayed for only the protocols enabled on your device. The output of the **show tech-support** command can include the output of the following commands:

- **show apollo traffic**
- **show appletalk traffic**
- **show bootflash**

- **show bootvar**
- **show buffers**
- **show clns traffic**
- **show context**
- **show controllers**
- **show decnet traffic**
- **show interfaces**
- **show ip traffic**
- **show novell traffic**
- **show processes cpu**
- **show processes memory**
- **show running-config**
- **show stacks**
- **show version**
- **show vines traffic**
- **show xns traffic**

For a sample display of the output of the **show tech-support** command, refer to the documentation for the **show** commands listed.

Related Commands

Command	Description
show apollo traffic	Displays information about the number and type of Apollo Domain packets sent and received by the Cisco IOS software.
show appletalk traffic	Displays statistics about AppleTalk traffic, including MacIP traffic.
show bootflash	Displays the contents of boot Flash memory.
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.
show buffers	Displays statistics for the buffer pools on the network server.
show clns traffic	Displays a list of the CLNS packets this router has seen.
show context	
show controllers	Displays information that is specific to the hardware.
show controllers tech-support	Displays general information about a VIP card when reporting a problem.
show decnet traffic	Displays the DECnet traffic statistics (including datagrams sent, received, and forwarded).
show interfaces	Displays ALC information.
show ip traffic	Displays statistics about IP traffic.
show novell traffic	Displays information about the number and type of IPX packets sent and received.
show processes cpu	Displays information about the active processes.

Command	Description
show processes memory	Displays the amount of memory used.
show running-config	Displays the current configuration of your routing device. While still operational in this release, this command has been replaced with the more system:running-config command.
show stacks	Displays the stack usage of processes and interrupt routines.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.
show vines traffic	Displays the statistics maintained about VINES protocol traffic.
show xns traffic	Displays information about the number and type of XNS packets sent and received by the Cisco IOS software.

test flash

To test Flash memory on MCI and envm Flash EPROM interfaces, use the **test flash** command in EXEC mode.

test flash

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Examples In the following example, the Flash memory is tested:

```
test flash
```

Related Commands	Command	Description
	test interfaces	Tests the system interfaces on the modular router.
	test memory	Performs a test of Multibus memory (including nonvolatile memory) on the modular router.

test interfaces

To test the system interfaces on the modular router, use the **test interfaces** command in EXEC mode.

test interfaces

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The **test interfaces** EXEC command is intended for the factory checkout of network interfaces. It is not intended for diagnosing problems with an operational router. The **test interfaces** output does not report correct results if the router is attached to a “live” network. For each network interface that has an IP address that can be tested in loopback (MCI and ciscoBus Ethernet and all serial interfaces), the **test interfaces** command sends a series of ICMP echoes. Error counters are examined to determine the operational status of the interface.

Examples In the following example, the system interfaces are tested:

```
test interfaces
```

Related Commands	Command	Description
	test flash	Tests Flash memory on MCI and envm Flash EPROM interfaces.
	test memory	Performs a test of Multibus memory (including nonvolatile memory) on the modular router.

test memory

To perform a test of Multibus memory (including nonvolatile memory) on the modular router, use the **test memory** command in EXEC mode. The memory test overwrites memory.

test memory

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The memory test overwrites memory. If you use the **test memory** command, you will need to rewrite nonvolatile memory. For example, if you test Multibus memory, which is the memory used by the CSC-R 4-Mbps Token Ring interfaces, you will need to reload the system before the network interfaces will operate properly. The **test memory** command is intended primarily for use by Cisco personnel.

Examples In the following example, the memory is tested:

```
test memory
```

Related Commands	Command	Description
	test flash	Tests Flash memory on MCI and envm Flash EPROM interfaces.
	test interfaces	Tests the system interfaces on the modular router.

trace (privileged)

To discover the routes that packets will actually take when traveling to their destination, use the **trace** command in privileged EXEC mode.

trace [*protocol*] [*destination*]

Syntax Description	<i>protocol</i>	(Optional) Protocols that can be used are appletalk , clns , ip and vines .
	<i>destination</i>	(Optional) Destination address or host name on the command line. The default parameters for the appropriate protocol are assumed and the tracing action begins.

Defaults The *protocol* argument is based on the Cisco IOS software examination of the format of the *destination* argument. For example, if the software finds a *destination* argument in IP format, the *protocol* value defaults to **ip**.

Command Modes Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The **trace** command works by taking advantage of the error messages generated by routers when a datagram exceeds its time-to-live (TTL) value.

The **trace** command starts by sending probe datagrams with a TTL value of one. This causes the first router to discard the probe datagram and send back an error message. The **trace** command sends several probes at each TTL level and displays the round-trip time for each.

The **trace** command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A “time exceeded” error message indicates that an intermediate router has seen and discarded the probe. A “destination unreachable” error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, the **trace** command prints an asterisk (*).

The **trace** command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with the escape sequence. By default, to invoke the escape sequence, type **Ctrl-^ X** by simultaneously pressing and releasing the **Ctrl**, **Shift**, and **6** keys, and then pressing the **X** key.

To use nondefault parameters and invoke an extended **trace** test, enter the command without a *destination* argument. You will be stepped through a dialog to select the desired parameters.

Common Trace Problems

Due to bugs in the IP implementation of various hosts and routers, the IP **trace** command may behave in unexpected ways.

Not all destinations will respond correctly to a probe message by sending back an “ICMP port unreachable” message. A long sequence of TTL levels with only asterisks, terminating only when the maximum TTL has been reached, may indicate this problem.

There is a known problem with the way some hosts handle an “ICMP TTL exceeded” message. Some hosts generate an “ICMP” message but they reuse the TTL of the incoming packet. Because this is zero, the ICMP packets do not make it back. When you trace the path to such a host, you may see a set of TTL values with asterisks (*). Eventually the TTL gets high enough that the *ICMP* message can get back. For example, if the host is six hops away, the **trace** command will time out on responses 6 through 11.

Trace IP Routes

The following display shows sample IP **trace** output when a destination host name has been specified:

```
Router# trace ABA.NYC.mil

Type escape sequence to abort.
Tracing the route to ABA.NYC.mil (26.0.0.73)
  1 DEBRIS.CISCO.COM (192.180.1.6) 1000 msec 8 msec 4 msec
  2 BARNET-GW.CISCO.COM (192.180.16.2) 8 msec 8 msec 8 msec
  3 EXTERNAL-A-GATEWAY.STANFORD.EDU (192.42.110.225) 8 msec 4 msec 4 msec
  4 BB2.SU.BARNET.NET (192.200.254.6) 8 msec 8 msec 8 msec
  5 SU.ARC.BARNET.NET (192.200.3.8) 12 msec 12 msec 8 msec
  6 MOFFETT-FLD-MB.in.MIL (192.52.195.1) 216 msec 120 msec 132 msec
  7 ABA.NYC.mil (26.0.0.73) 412 msec 628 msec 664 msec
```

Table 102 describes the significant fields shown in the display.

Table 102 trace Field Descriptions

Field	Description
1	Indicates the sequence number of the router in the path to the host.
DEBRIS.CISCO.COM	Host name of this router.
192.180.1.6	Internet address of this router.
1000 msec 8 msec 4 msec	Round-trip time for each of the three probes that are sent.

Extended IP Trace Dialog

The following display shows a sample **trace** session involving the extended dialog of the **trace** command:

```
Router# trace

Protocol [ip]:
Target IP address: mit.edu
Source address:
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to MIT.EDU (18.72.2.1)
  1 ICM-DC-2-V1.ICP.NET (192.108.209.17) 72 msec 72 msec 88 msec
  2 ICM-FIX-E-H0-T3.ICP.NET (192.157.65.122) 80 msec 128 msec 80 msec
  3 192.203.229.246 540 msec 88 msec 84 msec
  4 T3-2.WASHINGTON-DC-CNSS58.T3.ANS.NET (140.222.58.3) 84 msec 116 msec 88 msec
```

```

5 T3-3.WASHINGTON-DC-CNSS56.T3.ANS.NET (140.222.56.4) 80 msec 132 msec 88 msec
6 T3-0.NEW-YORK-CNSS32.T3.ANS.NET (140.222.32.1) 92 msec 132 msec 88 msec
7 T3-0.HARTFORD-CNSS48.T3.ANS.NET (140.222.48.1) 88 msec 88 msec 88 msec
8 T3-0.HARTFORD-CNSS49.T3.ANS.NET (140.222.49.1) 96 msec 104 msec 96 msec
9 T3-0.ENSS134.T3.ANS.NET (140.222.134.1) 92 msec 128 msec 92 msec
10 W91-CISCO-EXTERNAL-FDDI.MIT.EDU (192.233.33.1) 92 msec 92 msec 112 msec
11 E40-RTR-FDDI.MIT.EDU (18.168.0.2) 92 msec 120 msec 96 msec
12 MIT.EDU (18.72.2.1) 96 msec 92 msec 96 msec

```

Table 103 describes the fields that are unique to the extended trace sequence, as shown in the display.

Table 103 trace Field Descriptions

Field	Description
Target IP address	You must enter a host name or an IP address. There is no default.
Source address	One of the interface addresses of the router to use as a source address for the probes. The router will normally pick what it feels is the best source address to use.
Numeric display	The default is to have both a symbolic and numeric display; however, you can suppress the symbolic display.
Timeout in seconds	The number of seconds to wait for a response to a probe packet. The default is 3 seconds.
Probe count	The number of probes to be sent at each TTL level. The default count is 3.
Minimum Time to Live [1]	The TTL value for the first probes. The default is 1, but it can be set to a higher value to suppress the display of known hops.
Maximum Time to Live [30]	The largest TTL value that can be used. The default is 30. The trace command terminates when the destination is reached or when this value is reached.
Port Number	The destination port used by the User Datagram Protocol (UDP) probe messages. The default is 33434.
Loose, Strict, Record, Timestamp, Verbose	IP header options. You can specify any combination. The trace command issues prompts for the required fields. Note that the trace command will place the requested options in each probe; however, there is no guarantee that all routers (or end nodes) will process the options.
Loose	Allows you to specify a list of nodes that must be traversed when going to the destination.
Strict	Allows you to specify a list of nodes that must be the only nodes traversed when going to the destination.
Record	Allows you to specify the number of hops to leave room for.
Timestamp	Allows you to specify the number of time stamps to leave room for.
Verbose	If you select any option, the verbose mode is automatically selected and the trace command prints the contents of the option field in any incoming packets. You can prevent verbose mode by selecting it again, toggling its current setting.

Table 104 describes the characters that can appear in **trace** command output.

Table 104 ip trace Text Characters

Char	Description
nn msec	For each node, the round-trip time (in milliseconds) for the specified number of probes.
*	The probe timed out.
?	Unknown packet type.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.
U	Port unreachable.

Related Commands

Command	Description
trace (user)	Discovers the CLNS routes that packets will actually take when traveling to their destination.

trace (user)

To discover the IP routes that packets will actually take when traveling to their destination, use the **trace** command in EXEC mode.

trace [*protocol*] [*destination*]

Syntax Description	
<i>protocol</i>	(Optional) Protocols that can be used are appletalk , clns , ip and vines .
<i>destination</i>	(Optional) Destination address or host name on the command line. The default parameters for the appropriate protocol are assumed and the tracing action begins.

Defaults The *protocol* argument is based on the Cisco IOS software examination of the format of the *destination* argument. For example, if the software finds a *destination* argument in IP format, the *protocol* defaults to **ip**.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The **trace** command works by taking advantage of the error messages generated by routers when a datagram exceeds its time-to-live (TTL) value.

The **trace** command starts by sending probe datagrams with a TTL value of one. This causes the first router to discard the probe datagram and send back an error message. The **trace** command sends several probes at each TTL level and displays the round-trip time for each.

The **trace** command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A “time exceeded” error message indicates that an intermediate router has seen and discarded the probe. A “destination unreachable” error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, **trace** prints an asterisk (*).

The **trace** command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with the escape sequence. By default, to invoke the escape sequence, type **Ctrl-^ X** by simultaneously pressing and releasing the **Ctrl**, **Shift**, and **6** keys, and then pressing the **X** key.

Common Trace Problems

Due to bugs in the IP implementation of various hosts and routers, the IP **trace** command may behave in unexpected ways.

Not all destinations will respond correctly to a probe message by sending back an “ICMP port unreachable” message. A long sequence of TTL levels with only asterisks, terminating only when the maximum TTL has been reached, may indicate this problem.

There is a known problem with the way some hosts handle an “ICMP TTL exceeded” message. Some hosts generate an *ICMP* message but they reuse the TTL of the incoming packet. Since this is zero, the ICMP packets do not make it back. When you trace the path to such a host, you may see a set of TTL values with asterisks (*). Eventually the TTL gets high enough that the “ICMP” message can get back. For example, if the host is six hops away, **trace** will time out on responses 6 through 11.

Trace IP Routes

The following display shows sample IP **trace** output when a destination host name has been specified:

```
Router# trace ip ABA.NYC.mil

Type escape sequence to abort.
Tracing the route to ABA.NYC.mil (26.0.0.73)
 0 DEBRIS.CISCO.COM (192.180.1.6) 1000 msec 8 msec 4 msec
 1 BARRNET-GW.CISCO.COM (192.180.16.2) 8 msec 8 msec 8 msec
 2 EXTERNAL-A-GATEWAY.STANFORD.EDU (192.42.110.225) 8 msec 4 msec 4 msec
 3 BB2.SU.BARRNET.NET (192.200.254.6) 8 msec 8 msec 8 msec
 4 SU.ARC.BARRNET.NET (192.200.3.8) 12 msec 12 msec 8 msec
 5 MOFFETT-FLD-MB.in.MIL (192.52.195.1) 216 msec 120 msec 132 msec
 6 ABA.NYC.mil (26.0.0.73) 412 msec 628 msec 664 msec
```

Table 105 describes the significant fields shown in the display.

Table 105 trace Field Descriptions

Field	Description
1	Indicates the sequence number of the router in the path to the host.
DEBRIS.CISCO.COM	Host name of this router.
192.180.1.61	Internet address of this router.
1000 msec 8 msec 4 msec	Round-trip time for each of the three probes that are sent.

Table 106 describes the characters that can appear in **trace** output.

Table 106 ip trace Text Characters

Char	Description
nn msec	For each node, the round-trip time (in milliseconds) for the specified number of probes.
*	The probe timed out.
?	Unknown packet type.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.
U	Port unreachable.

■ trace (user)

Related Commands	Command	Description
	trace (privileged)	Probes the routes that packets follow when traveling to their destination from the router.