

Chapter 5

Managing the System

5

This chapter describes the EXEC commands you use to monitor and troubleshoot general system processes on your network server. These processes include:

- System memory allocator and buffer pools
- System configuration and processes
- Stack utilization
- System error message logs

This chapter also provides a general overview of these system tasks:

- Using the **debug** commands to troubleshoot network problems
- Testing connectivity
- Tracing routes
- Testing the system

See the chapters containing information about the interfaces and the protocols supported by Cisco software for descriptions of the interface- and protocol-specific debugging and monitoring commands.

Most of the network management commands are executed at the privileged-level prompt, although there is a subset of monitoring commands that you may enter at the user-level prompt.

An alphabetically arranged summary of the commands described in this chapters is included at the end of this chapter.

Monitoring System Processes

Use the EXEC show commands to display data structures, configuration parameters, and usage statistics for the network server. To list all the available **show** command options, enter this command at the EXEC prompt.

show ?

Two different lists may be displayed, one at the user-level prompt, and one at the enabled, privileged-level prompt. The lists include a summary of the command function, for easy ref-

erence. See the chapter “First-Time Startup and Basic Configuration” for the procedure to enter these levels.

Monitoring the Environmental Monitor Card

Use this EXEC command to monitor the Environmental Monitor card:

show env

The command displays measurement statistics for this card.

Displaying Buffer Pool Statistics

The network server has one pool of queuing elements and five pools of packet buffers of different sizes. For each pool, the network server keeps counts of the number of buffers outstanding, the number of buffers in the free list, and the maximum number of buffers allowed in the free list. To display statistics for the buffer pools on the network server, use the **show buffers** command. Enter this command at the EXEC prompt:

show buffers [*interface*]

The optional argument *interface* causes a search of all buffers that have been associated with that interface for longer than one minute. The contents of these buffers will be printed to the screen. This option is useful in diagnosing problems where the input queue count on an interface is consistently nonzero.

Following is sample output without the optional *interface* argument. Table 5-1 describes the fields seen.

```
Buffer elements:
    250 in free list (250 max allowed)
    10816 hits, 0 misses, 0 created
Small buffers, 104 bytes (total 120, permanent 120):
    120 in free list (0 min, 250 max allowed)
    26665 hits, 0 misses, 0 trims, 0 created
Middle buffers, 600 bytes (total 90, permanent 90):
    90 in free list (0 min, 200 max allowed)
    5468 hits, 0 misses, 0 trims, 0 created
Big buffers, 1524 bytes (total 90, permanent 90):
    90 in free list (0 min, 300 max allowed)
    1447 hits, 0 misses, 0 trims, 0 created
Large buffers, 5024 bytes (total 0, permanent 0):
    0 in free list (0 min, 100 max allowed)
    0 hits, 0 misses, 0 trims, 0 created
Huge buffers, 12024 bytes (total 0, permanent 0):
    0 in free list (0 min, 30 max allowed)
    0 hits, 0 misses, 0 trims, 0 created

0 failures (0 no memory)
```

Table 5-1 Show Buffers Field Descriptions

Field	Description
Buffer elements	Blocks of memory used in internal operating system queues
Small buffers Middle buffers Big buffers Large buffers Huge buffers	Blocks of memory used to hold network packets
hits	Count of successful attempts to allocate a buffer when needed
misses	Count of allocation attempts which failed for lack of a free buffer in the pool
created	Count of new buffers created
trims in free list	Count of buffers destroyed Number of buffers of a given type which are not currently allocated and are available for use
max allowed	The maximum number of buffers of a given type allowed in the system
failures	The total number of allocation requests that have failed for lack of a free buffer
no memory	Number of failures due to a lack of memory to create a new buffer

Displaying System Memory Statistics

To show statistics about the memory, use the **show memory** command. Enter this command at the EXEC prompt:

show memory

This command displays memory free pool statistics. These statistics include summary information about the activities of the system memory allocator, and a block-by-block listing of memory use. Sample output follows. Table 5-2 describes the fields seen; Table 5-3 lists the characteristics of each block of memory in the system.

Head	Free Start	Total Bytes	Used Bytes	Free Bytes
Processor	148B8C	1D66B0	2847860	561252
				2286608

Address	Bytes	Prev.	Next	Free?	PrevF	NextF	Alloc PC	What
148B8C	916	0	148F20				7B8E	*Init*
148F20	2024	148B8C	149708				ADEE	*Init*
149708	536	148F20	149920				AE18	*Init*
149920	2024	149708	14A108				4A7C	*Init*
14A108	72	149920	14A150				2492C	*Init*
14A150	44	14A108	14A17C				36114	*Init*
14A17C	152	14A150	14A214				1DBC	*Init*
14A214	2024	14A17C	14A9FC				1DE0	*Init*
14A9FC	152	14A214	14AA94				1DBC	*Init*
14AA94	2024	14A9FC	14B27C				1DE0	*Init*
14B27C	100	14AA94	14B2E0				3F2FE	Logger
14B2E0	152	14B27C	14B378				1DBC	Router Init
14B378	480	14B2E0	14B558	y	1CE270	1CA938	5E85A	IGRP Router
14B558	100	14B378	14B5BC				57A8E	DECnet Input
14B5BC	60	14B558	14B5F8	y	1CAFC4	1CA508	5EF08	IGRP Router
14B5F8	72	14B5BC	14B640				7B830	XNS Router
14B640	72	14B5F8	14B688				7B830	XNS Router
14B688	52	14B640	14B6BC				7B840	XNS Router
14B6BC	88	14B688	14B714				C724C	Virtual Exec
14B714	60	14B6BC	14B750				C7602	Virtual Exec
14B750	480	14B714	14B930	y	1D1768	1CAFC4	5E85A	IGRP Router

Table 5-2 Show Memory Field Descriptions

Field	Description
Head	The hexadecimal address of the head of the memory allocation chain
Free Start	The hexadecimal address of the base of the free list
Total Bytes	The total amount of system memory
Used Bytes	The amount of memory in use
Free Bytes	The amount of memory not in use

Table 5-3 Characteristics of Each Block of Memory

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)
Free?	Tells if the block is free
Alloc PC	Address of the system call that allocated the block
What	Name of process that owns the block

Displaying Active System Processes

To see information about the active processes, use the **show processes** command. Enter this command at the EXEC prompt:

show processes

Following is a partial display of the command output. Table 5-4 describes the fields seen.

PID	Q	T	PC	Runtime (ms)	Invoked	uSecs	Stacks	TTY	Process
1	M	E	17518	40072	830	48279	606/800	0	Net Background
2	M	E	5040	932	11	84727	486/800	0	Logger
32	M	E	4C390	73012	6141	11889	480/800	0	IGRP Router
4	M	E	22984	172	252	682	662/800	0	BOOTP Server
5	H	E	5040	100324	66619	1505	606/900	0	IP Input
6	M	E	21278	12188	22451	542	508/800	0	IP Protocols
7	M	E	32F32	32	10926	2	592/800	0	TCP Timer
8	L	E	33C1E	508	28	18142	576/800	0	TCP Protocols
9	L	E	5040	1104	935	1180	666/800	0	ARP Input
10	L	E	5040	352	458	768	674/800	0	Probe Input
11	H	E	5040	2636	9077	290	710/800	0	Net Input
12	M	T	2CF2	36976	49175	751	602/800	0	TTY Background
13	H	E	5040	0	2	0	852/900	0	DECnet Input
14	M	E	44AE4	21964	18029	1218	742/900	0	DECnet Routing
15	H	E	5040	2848	6556	434	686/800	0	XNS Input
16	L	E	5040	220	1642	133	748/800	0	XNS Protocols
17	L	E	59794	13660	3310	4126	632/800	0	XNS Router
18	H	E	5040	16652	59410	280	832/1000	0	AT Input
19	L	E	5040	13508	59201	228	884/1000	0	AT Protocols
20	L	E	73E0C	107496	40799	2634	832/1000	0	AT RTMP
21	L	E	5040	56	31	1806	814/1000	0	AT NBP
22	L	E	73E4A	84928	28526	2977	736/1000	0	AT ZIP

Table 5-4 Show Processes Field Descriptions

Field	Description
PID	Process ID
Q	Queue priority (high, medium, low)
T	Scheduler test (Event, Time, Suspended)
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 invocation
Stacks	Low water mark/Total stack space available
TTY Process	Terminal that controls the process and name of process

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.

Displaying Stack Utilization

To show stack utilization, use the **show stacks** command. Enter this command at the EXEC prompt:

show stacks

The **show stacks** command monitors the stack utilization of processes and interrupt routines. Its display 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 can be useful for analyzing crashes in the field.

Displaying the System Configuration

To display the contents of the nonvolatile memory, if present and valid, use the **show configuration** command. Enter this command at the EXEC prompt:

show configuration

The nonvolatile memory stores the configuration information in the network server in text form as configuration commands.

Displaying the Error Logging Conditions

To show the state of logging (syslog), use the **show logging** command. Enter this command at the EXEC prompt:

show logging

This command displays the state of syslog error and event logging, including host addresses, and whether console logging is enabled. This command also displays SNMP (Simple Network Management Protocol) configuration parameters and protocol activity. See the section “Redirecting System Error Messages” in the chapter “Configuring the System” for an explanation of how to configure message logging. Following is a sample output. Table 5-5 describes the fields seen.

```
Syslog logging: enabled
  Console logging: disabled
  Monitor logging: level debugging, 266 messages logged.
  Trap logging: level informational, 266 messages logged.
  Logging to 131.108.2.238

SNMP logging: disabled, retransmission after 30 seconds
  0 messages logged
```

Table 5-5 Show Logging Field Descriptions

Field	Description
Syslog logging	When enabled, system logging messages are sent to a UNIX host which 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	The minimum level of severity required for a log message to be sent to a monitor terminal (not the console).
Trap logging	The minimum level of severity required for a log message to be sent to syslog server.
SNMP logging	Shows whether SNMP logging is enabled and the number of messages logged, and the retransmission interval.

Displaying Protocol Information

To display the configured protocols, use the **show protocols** command. Enter this command at the EXEC prompt:

show protocols

The `show protocols` command shows the global and interface-specific status of any configured Level 3 protocol; for example, IP, DECnet, Novell, AppleTalk, and so forth. The following is sample output:

```
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 131.108.1.1, 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 192.31.7.49, subnet mask is 255.255.255.240
Ethernet 1 is up, line protocol is up
  Internet address is 131.108.2.1, 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 192.31.7.177, subnet mask is 255.255.255.240
  AppleTalk address is 999.1, zone Magnolia Estates
```

Troubleshooting Network Operations

The network server includes software to aid in tracking down problems with the network server or with other hosts on the network. The privileged EXEC command **debug** enables the display of several classes of network events on the console terminal. The privileged **undebug** command turns off the display of these classes. The EXEC command **show debugging** displays the state of each debugging option. See the section “Redirecting System Error Messages” in the chapter “Configuring the System” for an explanation of how to configure message logging.

Note: Debugging output is given high priority by the system. For this reason, debugging commands should be turned on only for troubleshooting specific problems, or during troubleshooting sessions with Cisco engineers. Excessive debugging output can render the system unusable.

To list and briefly describe all the **debug** command options, enter the **debug ?** command at the privileged-level EXEC prompt. This section provides an overview of how to use the debugging commands. See the interface and protocol-specific chapters for the **debug** command descriptions.

To turn on all system diagnostics, enter this command at the EXEC prompt:

debug all

Its converse, the **undebug all** command, turns off all diagnostic output.

Testing Connectivity with the Ping Command

As an aid to diagnosing basic network connectivity, many network protocols support the *packet internet groper* (ping) program, which sends an echo request packet to an address, then awaits a reply. Results from this echo protocol can help in evaluating the path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

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

To implement this program, use the privileged EXEC command ping. When the ping command is entered, the system issues a prompt for one of the following protocol keywords—**appletalk**, **clns**, **ip**, **novell**, **pup**, or **xns**.

The default protocol is IP. After determining the protocol type, the **ping** command prompts for an address or host name, repeat count (default is 5), datagram size (default is 100 bytes), time-out interval (default is 2 seconds), and extended commands (default is none). The precise dialog varies from protocol to protocol.

If a host name or address is typed on the same line as the EXEC **ping** command, the default actions will be taken as appropriate for the protocol type of that name or address.

The **ping** command uses the exclamation point (!) and period (.) in its display. Each exclamation point indicates receipt of a reply. A period (.) indicates the network server timed out while waiting for a reply. Other characters may appear in the **ping** output display, depending on the protocol type. The output concludes with the success rate and minimum, average, and maximum round-trip times.

To abort a ping session, type the escape sequence (by default, Ctrl-^, X).

Sample displays and tips for using these protocols are included in the chapters describing the protocols supported by the Cisco **ping** command.

Checking Routes with the Trace Command

The **trace** command is a useful debugging command which allows the network administrator to discover the routes packets will actually take when travelling to their destination. The **trace** command supports IP, CLNS and VINES route tracing.

trace [*destination*]

To invoke a simple **trace** test, enter the destination address or host name on the command line. The default parameters for the appropriate protocol are assumed and the tracing action begins.

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.

Typing the escape sequence (by default, Ctrl-^, X) terminates a **trace** command. See the IP, ISO CLNS and VINES chapters for more information about using this command.

Writing System Configuration Information

This section describes the privileged **write** commands used to manage the system configuration information.

To erase the configuration information, use the following EXEC command:

write erase

This command erases the configuration information in the nonvolatile memory. This command does not affect the configuration in use.

To copy the configuration to memory, use the following EXEC command:

write memory

This command copies the current configuration information to the nonvolatile memory.

To copy the configuration to the network, use the following EXEC command:

write network

This command sends a copy of the current configuration information to a server host. You are prompted for a destination host and a file name.

To write configuration on the terminal, use the following EXEC command:

write terminal

This command displays the current configuration information on the terminal.

Testing the System

Included as part of the EXEC command set are commands that allow testing of system interfaces and memory.



Caution: Use of these commands is not recommended, as they are intended to aid Cisco manufacturing personnel in checking out system functionality.

To test the system interfaces, use this EXEC command:

test interfaces

The EXEC **test interfaces** 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 will 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 loop back (MCI and cBus Ethernet and all serial interfaces), the **test interface** command sends a series of ICMP echoes. Error counters are examined to determine the operational status of the interface.

To test system memory, use this EXEC command:

test memory

The EXEC command **test memory** performs a test of Multibus memory, including the nonvolatile memory.



Caution: This test will overwrite the contents of memory. You will need to rewrite nonvolatile memory after running this command. If you test Multibus memory (for example, the memory used by the CSC-R four megabit Token Ring interfaces), you will need to reload the system to restore correct operation of the network interfaces.

EXEC System Management Command Summary

This section lists all the EXEC system management and user commands in alphabetical order.

debug ?

Lists and briefly describes all the **debug** command options.

[un]debug all

Enables all diagnostic output. Its converse, the **undebug all** command, turns off all diagnostic output.

ping

Provides a diagnostic tool for testing connectivity. Results help evaluate path-to-host reliability, delays over the path, and whether the host is functioning.

show ?

The **show ?** command lists all the **show** command options. Two lists may be displayed, one at the user-level prompt, and one at the enabled, privileged-level prompt.

show buffers [interface]

Displays statistics for the buffer pools on the network server. The network server has one pool of queuing elements and four pools of packet buffers of different sizes. For each pool, the network server keeps counts of the number of buffers outstanding, the number of buffers in the free list, and the maximum number of buffers allowed in the free list. With the optional argument *interface*, this command searches all buffers that have been associated with the interface for longer than one minute.

show configuration

Displays the contents of the nonvolatile memory, if present and valid. The nonvolatile memory stores the configuration information in the network server in text form as configuration commands.

show debugging

Displays the current settings of the **debug** command options.

show logging

Displays the state of syslog error and event logging, including host addresses and whether console logging is enabled. This command also displays SNMP configuration parameters and protocol activity.

show memory

Displays memory free pool statistics. These statistics include summary information about the activities of the system memory allocator, and a block-by-block listing of memory use.

show processes

Displays information about all active processes.

show protocols

Displays the global and interface-specific status of any configured Level 3 protocol.

show stacks

Monitors the stack utilization of processes and interrupt routines. Its display 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 can be useful to support personnel for analyzing crashes in the field.

test interfaces

Intended for the factory checkout of network interfaces. It is not intended for diagnosing problems with an operational router.

test memory

Performs a test of Multibus memory, including the nonvolatile memory

trace [*destination*]

Allows the network administrator to discover the routes packets will actually take when travelling to their destination. The **trace** command supports both IP and CLNS route tracing. Typing the escape sequence terminates **trace**.

write erase

Erases the configuration information in the nonvolatile memory. This command does not affect the configuration in use.

write memory

Copies the current configuration information to the nonvolatile memory.

write network

Sends a copy of the current configuration information to a server host. You are prompted for a destination host and a file name.

write terminal

Displays the current configuration information.

