



Troubleshooting the Router

This chapter describes basic tasks that you can perform to troubleshoot your router and network in Cisco IOS Release 12.1. For detailed troubleshooting procedures and a variety of scenarios, see the *Internetwork Troubleshooting Guide*. For complete details on all **debug** commands, see the *Cisco IOS Debug Command Reference*.

For a complete description of the troubleshooting commands in this chapter, refer to the “Troubleshooting Commands” chapter in “Cisco IOS System Management Commands” part of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.1*. To locate documentation of other commands that appear in this chapter, use the command reference index or search online.

Understanding Fault Management

To manage network faults, you need to discover, isolate, and fix the problems. You can discover problems with the system’s monitoring commands, isolate problems with the system’s test commands, and resolve problems with other commands, including **debug** commands.

To perform general fault management, use the commands in the following sections:

- [Displaying System Information Using Show Commands](#)
- [Receiving Automatic Warning Messages](#)
- [Receiving the Automatic Shutdown Message](#)
- [Testing Network Connectivity](#)
- [Testing Memory and Interfaces](#)
- [Logging System Error Messages](#)
- [Using Field Diagnostics](#)
- [Troubleshooting Specific Line Cards](#)
- [Storing Line Card Crash Information](#)
- [Creating Core Dumps for System Exceptions](#)
- [Enable Debug Operations](#)
- [Enable Conditionally Triggered Debugging](#)

In addition, some chapters in the Cisco IOS software configuration guides include fault management tasks in a monitoring and maintaining section.

Displaying System Information Using Show Commands

To provide information about system processes, the Cisco IOS software includes an extensive list of EXEC commands that begin with the word **show**, which, when executed, display detailed tables of system information. Following is a partial list of system management **show** commands. Use these commands in EXEC mode to display the information described:

Command	Purpose
<code>show c2600</code>	Display information about the Cisco 2600 platform, including interrupts, IOS Priority Masks, and IDMA status, for troubleshooting.
<code>show c7200</code>	Display information about the CPU and midplane for the Cisco 7200 series routers.
<code>show context</code>	Display information stored in NVRAM when the router crashes. This command is only useful to your technical support representative. This command is supported on the Cisco 2600 and 7000 series routers.
<code>show controllers (GRP image)</code>	Display information that is specific to the Cisco 12000 series Gigabit Switch Router hardware options listed with this command.
<code>show controllers (line card image)</code>	Display information specific to the hardware on a line card installed in the Cisco 12000 series Gigabit Switch Router.
<code>show controllers logging</code>	Display logging information about a VIP card.
<code>show controllers tech-support</code>	Display general information about a VIP card when reporting a problem.
<code>show diag</code>	Display hardware information including DRAM and SRAM on the line cards.
<code>show environment [all last table]</code>	Display a message indicating whether an environmental warning condition currently exists, the temperature and voltage information, the last measured value from each of the six test points stored in nonvolatile memory, or the environmental specifications. This command is supported on the Cisco 7000 series routers.
<code>show gsr</code>	Display hardware information on the Cisco 12000 series Gigabit Switch Router.
<code>show gt64010</code>	Display all GT64010 internal registers and interrupt status on the Cisco 7200 series routers.
<code>show memory [memory-type] [free] [summary]</code>	Display memory pool statistics including summary information about the activities of the system memory allocator and a block-by-block listing of memory use.
<code>show pci {hardware bridge [register]}</code>	Display information about the peripheral component interconnect (PCI) hardware registers or bridge registers for the Cisco 2600 and 7000 series routers.
<code>show processes [cpu]</code>	Display information about all active processes.
<code>show processes memory</code>	Display information about memory usage.
<code>show protocols</code>	Display the configured protocols.
<code>show stacks</code>	Display stack usage of processes and interrupt routines, including the reason for the last system reboot. This command is only useful to your technical support representative.
<code>show subsys [class class name name]</code>	Display subsystem information.

Command	Purpose
<code>show tcp [line-number]</code>	Display the status of TCP connections.
<code>show tcp brief [all]</code>	Display a concise description of TCP connection endpoints.
<code>show tdm connections [motherboard slot number]</code>	Display a snapshot of the time-division multiplexing (TDM) bus connection or data memory in a Cisco AS5200 access server.
<code>show tech-support [page] [password]</code> <code>show controllers vip slot-number</code> <code>tech-support</code>	Display general information about the router or VIP card when reporting a problem.

Look for specific **show** commands in the tables of configuration commands found throughout the chapters in Cisco IOS software configuration guides. See the Cisco IOS software command references for detailed descriptions of the commands.

Receiving Automatic Warning Messages

Some routers have an environmental monitor which monitors the physical condition of the router. If a measurement exceeds acceptable margins, a warning message is printed to the system console. The system software collects measurements once every 60 seconds, but warnings for a given test point are printed at most once every four hours. If the temperature measurements are out of specification more than the shutdown margin, the software shuts the router down but the fan will stay on. The router has to be manually turned off and on after such a shutdown. You can query the environmental monitor using the **show environment** command at any time to determine whether a measurement is out of tolerance. Refer to the *System Error Messages* publication for a description of environmental monitor warning messages.

Receiving the Automatic Shutdown Message

On routers with an environmental monitor, if the software detects that any of its temperature test points have exceeded maximum margins, it performs the following steps in this order:

1. Saves the last measured values from each of the six test points to internal nonvolatile memory.
2. Interrupts the system software and causes a shutdown message to be printed on the system console.
3. Shuts off the power supplies after a few milliseconds of delay.

The following is the message the system displays if temperatures exceed maximum margins, along with a message indicating the reason for the shutdown:

```
Router#
%ENVM-1-SHUTDOWN: Environmental Monitor initiated shutdown
%ENVM-2-TEMP: Inlet temperature has reached SHUTDOWN level at 64(C)
```

Refer to the hardware installation and maintenance publication for your router for more information about environmental specifications.

Testing Network Connectivity

Use the commands in the following sections to test basic network connectivity:

- [Setting Up the TCP Keepalive Packet Service](#)
- [Testing Connections with the Ping Command](#)
- [Tracing Packet Routes](#)

Setting Up the TCP Keepalive Packet Service

The TCP keepalive capability allows a router to detect when the host with which it is communicating experiences a system failure, even if data stops being transmitted (in either direction). This is most useful on incoming connections. For example, if a host failure occurs while talking to a printer, the router might never notice, because the printer does not generate any traffic in the opposite direction. If keepalives are enabled, they are sent once every minute on otherwise idle connections. If five minutes pass and no keepalives are detected, the connection is closed. The connection is also closed if the host replies to a keepalive packet with a reset packet. This will happen if the host crashes and comes back up again.

To set up the TCP keepalive packet service, use the following command in global configuration mode:

Command	Purposes
<code>service {tcp-keepalives-in tcp-keepalives-out}</code>	Generate TCP keepalive packets on idle network connections, either incoming connections initiated by a remote host, or outgoing connections initiated by a user.

Testing Connections with the Ping Command

As an aid to diagnosing basic network connectivity, many network protocols support an echo protocol. The protocol involves sending a special datagram to the destination host, then waiting for a reply datagram from that host. 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.

To use the echo protocol, use the following command in either user or privileged EXEC mode:

Command	Purposes
<code>ping [protocol] {host address}</code>	Invoke a diagnostic tool for testing connectivity.

Look for specific **ping** commands in the tables of configuration commands found throughout the chapters in Cisco IOS software configuration guides. See the Cisco IOS software command references for detailed descriptions of the command.

Tracing Packet Routes

To discover the routes that packets will actually take when traveling to their destinations, use the following command in either user or privileged EXEC mode:

Command	Purposes
<code>trace [protocol] [destination]</code>	Trace packet routes through the network (privileged level).

Testing Memory and Interfaces

You can test the status of the following items:

- Flash memory
- System memory
- Interfaces



Caution

We do not recommend using these test commands; they are intended to aid manufacturing personnel in checking system functionality.

Testing Flash Memory

To test the status of Flash memory, use the following command in privileged EXEC mode:

Command	Purposes
<code>test flash</code>	Test Flash memory on MCI and envm Flash EPROM interfaces.

Testing System Memory

To test the status of system memory, use the following command in privileged EXEC mode:

Command	Purposes
<code>test memory</code>	Diagnose Multibus memory, including nonvolatile memory.

Testing Interfaces



Caution

Do not use this test to diagnose problems with an operational server.

To test the status of the interfaces, use the following command on a nonoperational server in privileged EXEC mode:

Command	Purposes
<code>test interfaces</code>	Check network interfaces.

Logging System Error Messages

By default, routers send the output from the **debug** EXEC command and system error messages to a logging process. The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, terminal lines, or a UNIX syslog server, depending on your configuration. The process also sends messages to the console. When the logging process is on, the messages are displayed on the console after the process that generated them has finished.



Note

The syslog format is compatible with 4.3 BSD UNIX.

When the logging process is disabled, messages are sent only to the console. The messages are sent as they are generated, so error and debug output will be interspersed with prompts or output from the command.

You can set the severity level of the messages to control the type of messages displayed for the console and each of the destinations. You can timestamp log messages or set the syslog source address to enhance real-time debugging and management.

Refer to the *System Error Messages* publication for information on possible error messages.

Enabling System Message Logging

Message logging is enabled by default. It must be enabled in order to send messages to any destination other than the console.

To disable message logging, use the **no logging on** command. Disabling the logging process can slow down the router because a process must wait until the messages are written to the console before continuing.

To reenabling message logging after it has been disabled, use the following command in global configuration mode:

Command	Purposes
<code>logging on</code>	Enable message logging.

Enabling Message Logging for a Slave Card

To enable slave Versatile Interface Processor (VIP) cards to log important messages to the console, use the following command in global configuration mode:

Command	Purposes
<code>service slave-log</code>	Enable slave message logging.

Setting the Error Message Display Device

If message logging is enabled, you can send messages to specified locations, in addition to the console.

To specify the locations that receive messages, use one or more of the following commands in global configuration mode:

Command	Purposes
<code>logging buffered</code> <i>[size]</i>	Log messages to an internal buffer.
<code>terminal monitor</code>	Log messages to a nonconsole terminal.
<code>logging host</code>	Log messages to a UNIX syslog server host.

The **logging buffered** command copies logging messages to an internal buffer. The buffer is circular, so newer messages overwrite older messages after the buffer is full. To display the messages that are logged in the buffer, use the **show logging EXEC** command. The first message displayed is the oldest message in the buffer. To clear the current contents of the buffer, use the **clear logging** privileged EXEC command.

The EXEC command **terminal monitor** locally accomplishes the task of displaying the system error messages to a nonconsole terminal.

The **logging** command identifies a syslog server host to receive logging messages. The argument *host* is the name or Internet address of the host. By issuing this command more than once, you build a list of syslog servers that receive logging messages. The **no logging** command deletes the syslog server with the specified address from the list of syslogs.

Configuring Synchronization of Logging Messages

You can configure the system to synchronize unsolicited messages and **debug** command output with solicited device output and prompts for a specific line. You can identify the types of messages to be output asynchronously based on the level of severity. You can also determine the maximum number of buffers for storing asynchronous messages for the terminal after which messages are dropped.

When synchronous logging of unsolicited messages and **debug** command output is turned on, unsolicited device output is displayed on the console or printed after solicited device output is displayed or printed. Unsolicited messages and **debug** command output is displayed on the console after the prompt for user input is returned. Therefore, unsolicited messages and **debug** command output are not interspersed with solicited device output and prompts. After the unsolicited messages are displayed, the console displays the user prompt again.

To configure for synchronous logging of unsolicited messages and **debug** command output with solicited device output and prompts, use the following commands beginning in global configuration mode:

	Command	Purposes
Step 1	<code>line [aux console vty] line-number</code> <code>[ending-line-number]</code>	Specify the line to be configured for synchronous logging of messages.
Step 2	<code>logging synchronous [level severity-level all]</code> <code>[limit number-of-buffers]</code>	Enable synchronous logging of messages.

Enabling Timestamps on Logging (Syslog) Messages

By default, logging messages are not timestamped. You can enable timestamping of logging messages by using the following command in global configuration mode:

Command	Purposes
<code>service timestamps log uptime</code>	Enable log timestamps.
or	
<code>service timestamps log datetime [msec] [localtime]</code> <code>[show-timezone]</code>	

Defining the Logging Message Severity Level and Facilities

You can limit messages displayed to the selected device by specifying the severity level of the error message. To do so, use one of the following commands in global configuration mode:

Command	Purposes
<code>logging console level</code>	Limit messages logged to the console.
<code>logging monitor level</code>	Limit messages logged to the terminal lines.
<code>logging trap level</code>	Limit messages logged to the syslog servers.

If you have enabled syslog messages traps to be sent to an SNMP network management station with the **snmp-server enable trap syslog** command, you can also change the level of messages sent and stored in a history table on the router. You can also change the number of messages that get stored in the history table.

Messages are stored in the history table because SNMP traps are not guaranteed to reach their destination. By default, one message of the level warning and above (see Table 20) is stored in the history table even if syslog traps are not enabled.

To change the level and table size defaults, use the following commands in global configuration mode:

	Command	Purposes
Step 1	<code>logging history <i>level</i></code>	Change the default level of syslog messages stored in the history file and sent to the SNMP server.
Step 2	<code>logging history size <i>number</i></code>	Change the number of syslog messages that can be stored in the history table.



Note

Table 20 lists the level keywords and severity level. For SNMP usage, the severity level values use +1. For example, **emergency** equals 1 instead of 0 and **critical** equals 3 instead of 2.

The **logging console** command limits the logging messages displayed on the console terminal to messages with a level number at or below the specified severity level, which is specified by the *level* argument. Table 20 lists the error message *level* keywords and corresponding UNIX syslog definitions in order from the most severe level to the least severe level.

Table 20 Error Message Logging Keywords

Level Keyword	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

The **no logging console** command disables logging to the console terminal.

The default is to log messages to the console at the **debugging** level and those level numbers that are lower, which means all levels. The **logging monitor** command defaults to **debugging** also. The **logging trap** command defaults to **informational**.

To display logging messages on a terminal, use the **terminal monitor EXEC** command.

Current software generates four categories of error messages:

- Error messages about software or hardware malfunctions, displayed at levels **warnings** through **emergencies**
- Output from the **debug** commands, displayed at the **debugging** level
- Interface up/down transitions and system restart messages, displayed at the **notifications** level
- Reload requests and low-process stack messages, displayed at the **informational** level

Defining the UNIX System Logging Facility

You can log messages produced by UNIX system utilities. To do this, enable this type logging and define the UNIX system facility from which you want to log messages. Table 21 lists the UNIX system facilities supported by the Cisco IOS software. Consult the operators manual for your UNIX operating system for more information about these UNIX system facilities.

Define UNIX system facility message logging by using the following command in global configuration mode:

Command	Purposes
<code>logging facility facility-type</code>	Configure system log facilities.

Table 21 Logging Facility Type Keywords

Facility Type Keyword	Description
auth	Indicates the authorization system.
cron	Indicates the cron facility.
daemon	Indicates the system daemon.
kern	Indicates the Kernel.
local0–7	Reserved for locally defined messages.
lpr	Indicates line printer system.
mail	Indicates mail system.
news	Indicates USENET news.
sys9	Indicates system use.
sys10	Indicates system use.
sys11	Indicates system use.
sys12	Indicates system use.
sys13	Indicates system use.
sys14	Indicates system use.
syslog	Indicates the system log.
user	Indicates user process.
uucp	Indicates UNIX-to-UNIX copy system.

Refer also to your syslog manual pages.

Displaying Logging Information

To display logging information, use the following command in EXEC mode:

	Command	Purposes
Step 1	<code>show logging</code> <code>show controllers vip slot-number logging</code>	Display the state of syslog error and event logging, including host addresses, whether console logging is enabled, and other logging statistics.
Step 2	<code>show logging history</code>	Display information in the syslog history table such as the table size, the status of messages, and the text of the messages stored in the table.

Logging Errors to a UNIX Syslog Daemon

To set up the syslog daemon on a 4.3 BSD UNIX system, include a line such as the following in the `/etc/syslog.conf` file:

```
local7.debugging /usr/adm/logs/cisco.log
```

The **debugging** keyword specifies the syslog level; see Table 20 for a general description of other keywords. The **local7** keyword specifies the logging facility to be used; see Table 21 for a general description of other keywords.

The syslog daemon sends messages at this level or at a more severe level to the file specified in the next field. The file must already exist, and the syslog daemon must have permission to write to it.

Setting the Syslog Source Address

By default, a syslog message contains the IP address of the interface it uses to leave the router. To require that all syslog messages contain the same IP address, regardless of which interface they use, use the following command in global configuration mode:

Command	Purposes
<code>logging source-interface type number</code>	Set the syslog source address.

Using Field Diagnostics

Each line card on the Cisco 12000 series can perform field diagnostic testing to isolate faulty hardware without disrupting normal operation of the system. However, performing field diagnostic testing on a line card does halt all activity on the line card for the duration of the testing. After successful completion of the field diagnostic testing, the Cisco IOS software is automatically reloaded on the line card.



Note

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

To perform field diagnostic testing on a line card, perform the following commands in privileged EXEC mode:

Command	Purposes
Step 1 <code>diag slot-number [previous post verbose wait]</code>	<p>Specify the line card that you want to perform diagnostic testing on.</p> <p>Optionally, specify that previous test results are displayed, that only extended power-on self-tests (POST) be performed, that the maximum messages are displayed, or that the Cisco IOS software not be reloaded on the line card after successful completion of the tests. The following prompt is displayed.</p> <pre>Running Diags will halt ALL activity on the requested slot. [confirm]</pre> <p>At the prompt, press Return to confirm that you want to perform field diagnostic testing on the specified line card, or type no to stop the testing.</p>

To stop field diagnostic testing on a line card, use the following commands in privileged EXEC mode:

Command	Purpose
<code>diag slot-number halt</code> or <code>no diag slot-number</code>	Specify the line card that you want to stop perform diagnostic testing on.



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, on-line), you must use the **microcode reload** global configuration command or power cycle the line card.

Troubleshooting Specific Line Cards

Cisco IOS provides the **execute-on** command to allow you issue IOS commands (such as **show** commands) to a specific line card for monitoring and maintenance. For example, you could show what Cisco IOS image is loaded on the card in slot 3 of a Cisco 12012 GSR by issuing the command **execute-on slot 3 show version**. You can also use this command for troubleshooting cards in the dial shelf of Cisco Access Servers. For complete documentation of this command see the “Troubleshooting” chapter of the *Cisco IOS Configuration Fundamentals Command Reference*.

Storing Line Card Crash Information

This section explains how to enable storing of crash information for a line card and optionally specify the type and amount of information stored. 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 the **exception linecard** global configuration command only when directed by a technical support representative and only enable options that the technical support representative requests you to enable.

To enable and configure the crash information options for a line card, use the following command in global configuration mode:

Command	Purpose
<code>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]]</code>	Specify the line card that you want crash information for when a line card resets. Optionally, specify the type and amount of memory to be stored.

Creating Core Dumps for System Exceptions

“System exceptions” are any unexpected system shutdowns or reboots (most frequently caused by a system failure, commonly referred to as a “system crash”). When an exception occurs, it is sometimes useful to obtain a full copy of the memory image (called a core dump) to identify the cause of the unexpected shutdown. Not all exception types will produce a core dump.

Core dumps are generally useful only to your technical support representative. The core dump file, which is a very large binary file, must be transferred to a Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), or Remote Copy Protocol (RCP) server and subsequently interpreted by technical personnel who have access to source code and detailed memory maps.

The following commands are used to create core dumps:

Command	Purpose
<code>ip ftp password [type] password</code>	Specifies the password to be used for FTP connections.
<code>ip ftp username username</code>	Configures the user name for FTP connections.
<code>exception protocol {ftp rcp tftp}</code>	Configures the protocol used for core dumps.
<code>exception flash</code>	Configures the router for a core dump using a flash disk.
<code>exception core-file name</code>	Specifies the name of the core dump file when your router has generated a core dump file after crashing.
<code>exception dump ip-address</code>	Configures the router to dump a core file to a particular server when the router crashes.

Command	Purpose
<code>exception memory {fragment size minimum size}</code>	Causes the router to create a core dump and reboot when certain memory size parameters are violated.
<code>exception spurious-interrupt [number]</code>	Causes the router to create a core dump and crash after a specified number of spurious interrupts.

Specifying the Destination for the Core Dump File

Core dumps can be sent to a remote server using the trivial file transfer protocol (TFTP), the file transfer protocol (FTP), or the remote copy protocol (rcp). Additionally, core dumps can be written to a local flash disk. To configure the destination for a core dump file, perform one or more of the tasks in the following sections:

- [Core Dumps Using TFTP](#)
- [Core Dumps Using FTP](#)
- [Using RCP](#)
- [Core Dumps Using a Flash Disk](#)

Core Dumps Using TFTP

Due to a limitation of most TFTP applications, the router will only dump the first 16 MB of the core file. Therefore, if your router's main memory is larger than 16 MB, use of TFTP is not recommended.

To configure a router for a core dump using TFTP, use the following commands in global configuration mode:

	Command or Action	Purpose
Step 1	<code>exception protocol tftp</code>	(Optional) Explicitly specifies TFTP as the protocol to be used for router exceptions (core dumps for unexpected system shutdowns). Note Because TFTP is the default exception protocol, the exception protocol tftp command does not need to be used unless the protocol has been previously changed to ftp or rcp in your system's configuration. To determine if the exception protocol has been changed, use the show running-config command in EXEC mode.
Step 2	<code>exception dump ip-address</code>	Configures the router to dump a core file to the specified server if the router crashes.
Step 3	<code>exception core-file [filepath/] filename</code>	(Optional) Specifies the name to be used for the core dump file. The file usually must pre-exist on the TFTP server, and be writable.

For example, the following command configures a router to send a core file to the server at the IP address 172.17.92.2. As the exception protocol is not specified, the default protocol of TFTP will be used.

```
exception dump 172.17.92.2
```

The core dump is written to a file named "*hostname-core*" on the TFTP server, where *hostname* is the name of the router. You can change the name of the core file by adding the **exception core-file filename** configuration command.

Depending on the TFTP server application used, it may be necessary to create, on the TFTP server, the empty target file to which the router can write the core. Also, make sure there is enough memory on your TFTP server to hold the complete core dump.

Core Dumps Using FTP

To configure the router for a core dump using FTP, use the following configuration commands:

Command	Purpose
<code>ip ftp username <i>username</i></code>	Configures the user name for FTP connections.
<code>ip ftp password [<i>type</i>] <i>password</i></code>	Specifies the password to be used for FTP connections.
<code>exception protocol {ftp rcp tftp}</code>	Configures FTP as the protocol to use for sending core dump files.
<code>exception dump <i>ip-address</i></code>	Configures the router to dump a core file to the specified server if the router crashes.
<code>exception core-file <i>filename</i></code>	(Optional) Specifies the name to be used for the core dump file.

This example configures a router to use FTP to dump a core file named “dumpfile” to the FTP server at 172.17.92.2 if there is a system failure.

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

Using RCP

The remote copy protocol can also be used to send a core dump file. To configure the router to send core dump files using rcp, use the following commands:

	Command or Action	Purpose
Step 1	<code>ip rcmd remote-username <i>username</i></code>	(Optional) Specifies the username sent by the router to the remote server with an rcp copy/write request. The remote rcp server must be configured to grant write access to the specified username (in other words, an account must be defined on the network server for the username).
Step 2	<code>exception protocol rcp</code>	Configures the rcp as the protocol to use for sending core dump files.
Step 3	<code>exception dump <i>ip-address</i></code>	Configures the router to dump a core file to the specified server if the router crashes.
Step 4	<code>exception core-file <i>filename</i></code>	(Optional) Specifies the name to be used for the core dump file.

When an rcp username is not configured through the **ip rcmd remote-username** command, the rcp username defaults to the username associated with the current terminal (tty) connection. For example, if the user is connected to the router through Telnet and was authenticated through the username command, the router software sends the Telnet username as the rcp username. If the terminal username is not available, the router hostname will be used as the rcp username.

Core Dumps Using a Flash Disk

Some router platforms support the flash disk as an alternative to the linear flash memory or PCMCIA flash card. The large storage capacity of these flash disks make them good candidates for another means of capturing a core dump. To configure a router for a core dump using a flash disk, use the following router configuration command:

Command	Purpose
exception flash [procmem iomem all] [<i>device-name[:partition-number]</i>] [erase no_erase]	Configures the router for a core dump using a flash disk.
exception core-file <i>filename</i>	(Optional) Specifies the name to be used for the core dump file.

The **show flash all** command will give you a list of devices you can use for the **exception flash** command above.

Creating an Exception Memory Core Dump

As a debugging procedure, you can cause the router to create a core dump and reboot when certain memory size parameters are violated. The following **exception memory** commands are used to trigger a core dump:

Command	Purpose
exception memory minimum <i>bytes</i>	Triggers a core dump and system reload when the amount of free memory falls below the specified number of bytes. <ul style="list-style-type: none"> Do not specify too low a memory value, as the router needs some amount of free memory to provide the core dump. If you enter a size that is greater than the free memory (and the exception dump command has been configured), a core dump and router reload is generated after 60 seconds.
memory check-interval <i>seconds</i>	(Optional) Increases the interval at which memory will be checked. The default is 60 seconds, but much can happen in 60 seconds to mask the cause of corruption. Reducing the interval will increase CPU utilization (by around 12 %) which will be acceptable in most cases, but will also increase the chance of getting a usable core. To make sure CPU utilization doesn't hit 100%, you should gradually decrease the interval on busy routers. The ideal interval is as low as possible without causing other system problems.

Command	Purpose
<code>exception memory fragment bytes</code>	Triggers a core dump and system reload when the amount of contiguous (non-fragmented) free memory falls below the specified number of bytes.
<code>exception core-file filename</code>	(Optional) Specifies the name to be used for the core dump file. The file usually must exist on the TFTP server, and be writable. Note that the file will be the same size as the amount of processor memory on the router.

Note that the **exception memory minimum** command is primarily useful if you anticipate running out of memory before a core dump can be triggered or other debugging can be performed (rapid memory leak); if the memory leak is gradual (slow drift), you have generally have time to perform debugging before the system runs out of memory and must be reloaded.

By default, the number of free memory bytes is checked every 60 seconds when these commands are configured. The frequency of this checking can be increased using the **memory check-interval seconds** command.

The **exception dump ip-address** command must be configured with these commands. If the **exception dump** command is not configured, the router reloads without triggering a core dump.

The following example configures the router to monitor the free memory. If the memory falls below 250000 bytes, the core dump is created and the router reloads.

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

Creating a Spurious Interrupt Core Dump

During the debugging process, you can configure the router to create a spurious interrupt core dump and reboot when a specified number of interrupts have occurred.



Caution

Use the **exception spurious-interrupt** global configuration command only when directed by a technical support representative, and only enable options requested by the technical support representative.

To enable and configure the crash information for spurious interrupts, use the following command

Command	Purposes
<code>exception spurious-interrupt [number]</code>	Specify a number between 1 and 4294967295 to set the maximum number of spurious interrupts to include in the core dump before rebooting.
<code>exception dump ip-address</code> or <code>exception flash</code>	Specifies the destination for the core dump file.

The following example configures a router to create a core dump with a limit of 2 spurious interrupts:

```
exception spurious-interrupt 2
exception dump 209.165.200.225
```

Enable Debug Operations

Your router includes hardware and software to aid in tracking down internal problems and problems with other hosts on the network. The **debug** privileged EXEC mode commands start the console display of several classes of network events. The following commands describe in general the system debug message feature. Refer to the *Debug Command Reference* for detailed information on specific **debug** commands. Also refer to the *Internetwork Troubleshooting Guide* publication for additional information.

Command	Purposes
<code>show debugging</code>	Display the state of each debugging option.
<code>debug ?</code>	Display a list and brief description of all the debug command options.
<code>debug command</code>	Begin message logging for the specified debug command.
<code>no debug command</code>	Turn message logging off for the specified debug command.



Caution

The system gives high priority to debugging output. For this reason, debugging commands should be turned on only for troubleshooting specific problems or during troubleshooting sessions with technical support personnel. Excessive debugging output can render the system inoperable.

You can configure timestamping of system debug messages. Timestamping enhances real-time debugging by providing the relative timing of logged events. This information is especially useful when customers send debugging output to your technical support personnel for assistance. To enable timestamping of system debug messages, use the following command in global configuration mode:

Command	Purposes
<code>service timestamps debug uptime</code>	Enable timestamping of system debug messages.
or <code>service timestamps debug datetime [msec] [localtime] [show-timezone]</code>	

Normally, the messages are displayed only on the console terminal. See the section “[Setting the Error Message Display Device](#)” earlier in this chapter to change the output device.

Enable Conditionally Triggered Debugging

When the Conditionally Triggered Debugging feature is enabled, the router generates debugging messages for packets entering or leaving the router on a specified interface; the router will not generate debugging output for packets entering or leaving through a different interface. You can specify the interfaces explicitly. For example, you may only want to see debugging messages for one interface or subinterface. You can also turn on debugging for all interfaces that meet specified condition. This feature is useful on dial access servers, which have a large number of ports.

Normally, the router will generate debugging messages for every interface, resulting in a large number of messages. The large number of messages consumes system resources, and can make it difficult to find the specific information you need. By limiting the debugging messages, you can receive messages related to only the ports you wish to troubleshoot.

Conditionally Triggered Debugging controls the output from the following protocol-specific **debug** commands:

- **debug aaa** {accounting | authorization | authentication }
- **debug dialer** {events | packets }
- **debug isdn** {q921 | q931 }
- **debug modem** {oob | trace }
- **debug ppp** {all | authentication | chap | error | negotiation | multilink events | packet }

While this feature limits the output of the above commands, it does not automatically enable the generation of debugging output from these commands. Debugging messages are generated only when the protocol-specific **debug** command is enabled. **Debug** command output is controlled through two processes:

- The protocol-specific **debug** commands specify which protocols are being debugged. For example, the **debug dialer events** command generates debugging output related to dialer events.
- The **debug condition** commands limit these debugging messages to those related to a particular interface. For example, the **debug condition username bob** command generates debugging output only for interfaces with packets that specify a username of bob.

To configure Conditionally Triggered Debugging, perform the following tasks:

- [Enable Protocol-Specific Debug Commands](#)
- [Enable Conditional Debugging Commands](#)
- [Specify Multiple Conditions](#)

Enable Protocol-Specific Debug Commands

In order to generate any debugging output, the protocol-specific **debug** command for the desired output must be enabled. Use the **show debugging** command to determine which types of debugging are enabled. Use the **show debug condition** command to display the current debug conditions. Use the following commands in privileged EXEC mode to enable the desired protocol-specific **debug** commands:

Command	Purpose
show debugging	Determine which types of debugging are enabled.
show debug condition [<i>condition-id</i>]	Displays the current debug conditions.
debug protocol	Enable the desired debugging commands.
no debug protocol	Disable the debugging commands that are not desired.

If you wish to have no output, disable all the protocol-specific **debug** commands.

Enable Conditional Debugging Commands

If no **debug condition** commands are enabled, all debugging output, regardless of the interface, will be displayed for the enabled protocol-specific **debug** commands.

The first **debug condition** command you enter enables conditional debugging. The router will only display messages for interfaces that meet one of the specified conditions. If multiple conditions are specified, the interface must meet at least one of the conditions in order for messages to be displayed.

You can enable messages for interfaces specified explicitly or for interfaces that meet certain conditions, as described in the following sections:

- [Display Messages for One Interface](#)
- [Display Messages for Multiple Interfaces](#)
- [Limit Messages Based on Conditions](#)

Display Messages for One Interface

To disable debugging messages for all interfaces except one, use the following command in privileged EXEC mode:

Command	Purpose
<code>debug condition interface <i>interface</i></code>	Disable debugging messages for all interfaces except one.

If you enter the **debug condition interface** command, the debugging output will be turned off for all interfaces except the specified interface. To reenabling debugging output for all interfaces, use the **no debug interface** command.

Display Messages for Multiple Interfaces

To enable debugging messages for multiple interfaces, use the following commands in privileged EXEC mode:

Command	Purpose
<code>debug condition interface <i>interface</i></code>	Disable debugging messages for all interfaces except one.
<code>debug condition interface <i>interface</i></code>	Enable debugging messages for additional interfaces. Repeat this task until debugging messages are enabled for all desired interfaces.

If you specify more than one interface by entering this command multiple times, debugging output will be displayed for all of the specified interfaces. To turn off debugging on a particular interface, use the **no debug interface** command. If you use the **no debug interface all** command or remove the last **debug interface** command, debugging output will be reenabling for all interfaces.

Limit Messages Based on Conditions

The router can monitor interfaces to see if any packets contain the specified value for one of the following conditions:

- username

- calling party number
- called party number

If you enter a condition, such as calling number, debug output will be stopped for all interfaces. The router will then monitor every interface to see if a packet with the specified calling party number is sent or received on any interfaces. If the condition is met on an interface or subinterface, **debug** command output will be displayed for that interface. The debugging output for an interface is “triggered” when the condition has been met. The debugging output continues to be disabled for the other interfaces. If, at some later time, the condition is met for another interface, the debug output will become enabled for that interface as well.

Once debugging output has been triggered on an interface, the output will continue until the interface goes down. However, the session for that interface might change, resulting in a new username, called party number, or calling party number. Use the **no debug interface** command to reset the debug trigger mechanism for a particular interface. The debugging output for that interface will be disabled until the interface meets one of the specified conditions.

To limit debugging messages based on a specified condition, use the following command in privileged EXEC mode:

Command	Purpose
debug condition { username <i>username</i> called <i>dial-string</i> caller <i>dial-string</i> }	Enable conditional debugging. The router will only display messages for interfaces that meet this condition.

To reenable the debugging output for all interfaces, enter the **no debug condition all** command.

Specify Multiple Conditions

To limit debugging messages based on more than one condition, use the following commands in privileged EXEC mode:

Command	Purpose
debug condition { username <i>username</i> called <i>dial-string</i> caller <i>dial-string</i> }	Enable conditional debugging and specify the first condition.
debug condition { username <i>username</i> called <i>dial-string</i> caller <i>dial-string</i> }	Specify the second condition. Repeat this task until all conditions are specified.

If you enter multiple **debug condition** commands, debugging output will be generated if an interface meets at least one of the conditions. If you remove one of the conditions, using the **no debug condition** command, interfaces that meet only that condition will no longer produce debugging output. However, interfaces that meet a condition other than the removed condition will continue to generate output. Only if no active conditions are met for an interface will the output for that interface be disabled.

Conditionally Triggered Debugging Configuration Examples

In this example, four conditions have been set by the following commands:

- **debug condition interface serial 0**

- **debug condition interface serial 1**
- **debug condition interface virtual-template 1**
- **debug condition username fred**

The first three conditions have been met by one interface. The fourth condition has not yet been met.

```
Router# show debug condition

Condition 1: interface Se0 (1 flags triggered)
          Flags: Se0
Condition 2: interface Se1 (1 flags triggered)
          Flags: Se1
Condition 3: interface Vt1 (1 flags triggered)
          Flags: Vt1
Condition 4: username fred (0 flags triggered)
```

When any **debug condition** command is entered, debugging messages for conditional debugging are enabled. The following debugging messages show conditions being met on different interfaces as the serial 0 and serial 1 interfaces come up. For example, the second line of output indicates that serial interface 0 meets the username fred condition.

```
*Mar 1 00:04:41.647: %LINK-3-UPDOWN: Interface Serial0, changed state to up
*Mar 1 00:04:41.715: Se0 Debug: Condition 4, username fred triggered, count 2
*Mar 1 00:04:42.963: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed
state to up
*Mar 1 00:04:43.271: Vi1 Debug: Condition 3, interface Vt1 triggered, count 1
*Mar 1 00:04:43.271: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
*Mar 1 00:04:43.279: Vi1 Debug: Condition 4, username fred triggered, count 2
*Mar 1 00:04:43.283: Vi1 Debug: Condition 1, interface Se0 triggered, count 3
*Mar 1 00:04:44.039: %IP-4-DUPADDR: Duplicate address 172.27.32.114 on Ethernet 0,
sourced by 00e0.1e3e.2d41
*Mar 1 00:04:44.283: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to up
*Mar 1 00:04:54.667: %LINK-3-UPDOWN: Interface Serial1, changed state to up
*Mar 1 00:04:54.731: Se1 Debug: Condition 4, username fred triggered, count 2
*Mar 1 00:04:54.735: Vi1 Debug: Condition 2, interface Se1 triggered, count 4
*Mar 1 00:04:55.735: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed
state to up
```

After a period of time, the **show debug condition** command displays the revised list of conditions.

```
Router# show debug condition

Condition 1: interface Se0 (2 flags triggered)
          Flags: Se0 Vi1
Condition 2: interface Se1 (2 flags triggered)
          Flags: Se1 Vi1
Condition 3: interface Vt1 (2 flags triggered)
          Flags: Vt1 Vi1
Condition 4: username fred (3 flags triggered)
          Flags: Se0 Vi1 Se1
```

Next, the serial 1 and serial 0 interfaces go down. When an interface goes down, conditions for that interface are cleared.

```
*Mar 1 00:05:51.443: %LINK-3-UPDOWN: Interface Serial1, changed state to down
*Mar 1 00:05:51.471: Se1 Debug: Condition 4, username fred cleared, count 1
*Mar 1 00:05:51.479: Vi1 Debug: Condition 2, interface Se1 cleared, count 3
*Mar 1 00:05:52.443: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed
state to down
*Mar 1 00:05:56.859: %LINK-3-UPDOWN: Interface Serial0, changed state to down
*Mar 1 00:05:56.887: Se0 Debug: Condition 4, username fred cleared, count 1
*Mar 1 00:05:56.895: Vi1 Debug: Condition 1, interface Se0 cleared, count 2
```

```
*Mar 1 00:05:56.899: Vtl Debug: Condition 3, interface Vt1 cleared, count 1
*Mar 1 00:05:56.899: Vtl Debug: Condition 4, username fred cleared, count 0
*Mar 1 00:05:56.903: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to down
*Mar 1 00:05:57.907: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed
state to down
*Mar 1 00:05:57.907: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to down
```

The final **show debug condition** output is the same as the output before the interfaces came up.

```
Router# show debug condition

Condition 1: interface Se0 (1 flags triggered)
          Flags: Se0
Condition 2: interface Se1 (1 flags triggered)
          Flags: Se1
Condition 3: interface Vt1 (1 flags triggered)
          Flags: Vt1
Condition 4: username fred (0 flags triggered)
```

