

# Understanding Software–forced Crashes

Document ID: 26145

---

***Interactive:*** This document offers customized analysis of your Cisco device.

---

**Introduction**

**Prerequisites**

Requirements

Components Used

Conventions

**Identify a Software–forced Crash**

**Possible Causes**

**Troubleshoot**

**Configuration Procedures**

Router Configuration Procedure

TFTP Server Host Configuration Procedure

**Information to Collect if You Open a TAC Service Request**

**NetPro Discussion Forums – Featured Conversations**

**Related Information**

---

## Introduction

This document explains the most frequent causes of software–forced crashes, and describes the information you must collect in order to troubleshoot. If you open a TAC service request for a software–forced crash, the information you will be asked to collect will be essential to solve the problem.

## Prerequisites

### Requirements

Readers of this document should have knowledge of these topics:

- How to Troubleshoot Router Crashes.

### Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

# Identify a Software–forced Crash

A software–forced crash occurs when the router detects a severe, unrecoverable error, and reloads itself so that it does not transmit corrupted data. A vast majority of software–forced crashes are caused by Cisco IOS® software bugs, although some platforms (such as the old Cisco 4000) can report a hardware problem as a software–forced crash.

If you have not power–cycled or manually reloaded the router, output from the **show version** command displays this:

```
Router uptime is 2 days, 21 hours, 30 minutes
System restarted by error - Software-forced crash, PC 0x316EF90 at 20:22:37 edt
System image file is "flash:c2500-is-1.112-15a.bin", booted via flash
```

If you have the output of a **show version** command from your Cisco device, you can use Output Interpreter (registered customers only) to display potential issues and fixes.

## Possible Causes

This table explains the possible reasons for software–forced crashes:

Reason	Explanation
Watchdog timeouts	<p>The processor uses timers to avoid infinite loops, and causes the router to stop responding. In normal operation, the CPU resets those timers at regular intervals. Failure to do so results in a system reload.</p> <p>Watchdog timeouts that are reported as software–forced crashes are software–related. Refer to Troubleshooting Watchdog Timeouts for information about other types of watchdog timeouts. The system was stuck in a loop before the reload. Therefore, the stack trace is not necessarily relevant. You can recognize this type of software–forced crash in these lines of the console logs:</p> <pre>%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Exec  and  *** System received a Software forced crash *** signal = 0x17, code = 0x24, context= 0x60ceca60</pre>
Low memory	<p>When a router runs too low on memory, it can eventually reload itself and report it as a software–forced crash. In this case, memory allocation failure error messages appear in the console logs:</p> <pre>%SYS-2-MALLOCFAIL: Memory allocation of 734 bytes failed from 0x6015EC84, pool Processor, alignment 0</pre>
Corrupt software image	<p>At the time of bootup, a router can detect that a Cisco IOS software image is corrupt, return the compressed image checksum is incorrect message, and attempt to reload. In this case, the event is reported as a software–forced crash.</p> <pre>Error : compressed image checksum is incorrect 0x54B2C70A Expected a checksum of 0x04B2C70A  *** System received a Software forced crash *** signal= 0x17, code= 0x5, context= 0x0</pre>

	<p>PC = 0x800080d4, Cause = 0x20, Status Reg = 0x3041f003</p> <p>This can be caused by a Cisco IOS software image that has actually been corrupted during transfer to the router. In this case, you can load a new image onto the router to resolve the issue. [For a ROMMON recovery method for your platform, refer to ROMmon Recovery Procedure for the Cisco 7200, 7300, 7400, 7500, RSP7000, Catalyst 5500 RSM, uBR7100, uBR7200, uBR10000, and 12000 Series Routers.]</p> <p>It can also be caused by faulty memory hardware or by a software bug.</p>
Other faults	<p>The errors that cause crashes are often detected by processor hardware, which automatically calls special error-handling code in the ROM monitor. The ROM monitor identifies the error, prints a message, saves information about the failure, and restarts the system.</p> <p>There are crashes in which none of this can happen (see Watchdog timeouts), and there are crashes in which software detects the problem and calls the crashdump function. This is a true "software-forced" crash.</p> <p>On Power PC platforms, "software-forced crash" is not the restart reason printed when the crashdump function gets called – at least until very recently. On those platforms (prior to Cisco IOS Software Release 12.2(12.7)), these are referred to as "SIGTRAP" exceptions. In all other ways, SIGTRAPs and SFCs are the same.</p>

## Troubleshoot

Software-forced crashes are typically caused by Cisco IOS software bugs. If memory allocation failure error messages are present in the logs, see [Troubleshooting Memory Problems](#).

If you do not see memory allocation failure error messages, and you have not manually reloaded or power-cycled the router after the software-forced crash, the best tool you can use is the Output Interpreter (registered customers only) to search for a known matching bug ID. This tool incorporates the functionality of the old Stack Decoder tool.

Example:

1. Collect the output of **show stack** from the router.
2. Go to the Output Interpreter (registered customers only) tool.
3. Select **show stack** from the pull-down menu.
4. Paste in the output you have collected.
5. Click **submit**.

If the decoded output from the **show stack** command matches a known software bug, you will receive the bug IDs of the most likely software bugs that could have caused the software-forced crash.

6. Click on the bug ID hyperlinks to view additional bug details from the Cisco Bug Toolkit (registered customers only) which can help you determine the correct bug ID match.

When you have identified a bug ID that matches your error, refer to the "fixed in" field to determine the first Cisco IOS software version that contains the fix for the bug.

If you are uncertain about the bug ID, or the Cisco IOS software version that contains the fix for the problem, upgrade your Cisco IOS software to the latest version in your release train. This helps because, the latest version contains fixes for a large number of bugs. Even if this fails to resolve the problem, bug reporting and the resolution process is simpler and quicker when you have the latest version of the software.

If, after you use the Output Interpreter tool, you either suspect or have positively identified a bug which remains unresolved, we recommend that you open a TAC service request to provide additional information to help resolve the bug, and for quicker notification when the bug is ultimately resolved.

## Configuration Procedures

If the problem is identified as a new software bug, a Cisco TAC engineer can request that you configure the router to collect a *core dump*. A core dump is sometimes required to identify what can be done to fix the software bug.

To collect more useful information in the core dump, we recommend that you use the hidden **debug sanity** command. This causes every buffer that is used in the system to be sanity-checked when it is allocated and when it is freed. The **debug sanity** command has to be issued in privileged EXEC mode (enable mode) and involves some CPU, but does not significantly affect the functionality of the router. If you want to disable sanity checking, use the **undebug sanity** privileged EXEC command.

For routers that have 16 MB or less of main memory, you can use Trivial File Transfer Protocol (TFTP) to collect the core dump. It is recommended that you use File Transfer Protocol (FTP) if the router has more than 16MB of main memory. Use the configuration procedures in this section. Alternatively, refer to Creating Core Dumps.

## Router Configuration Procedure

Complete these steps to configure your router:

1. Configure the router with the **configure terminal** command.
2. Type **exception dump n.n.n.n**, where n.n.n.n is the IP address of the remote Trivial File Transfer Protocol (TFTP) server host.
3. Exit the configuration mode.

## TFTP Server Host Configuration Procedure

Complete these steps to configure a TFTP server host:

1. Create a file under the /tftpboot directory on the remote host with the help of an editor of your choice. The file name is the Cisco router hostname-core.
2. On UNIX systems, change the permission mode of the "hostname-core" file to be globally compatible (666). You can check the TFTP setup through the **copy running-config tftp** command on that file.
3. Make sure you have more than 16 MB of free disk space under /tftpboot.

If the system crashes, the **exception dump** command creates its output to the above file. If the router has more than 16 MB of main memory, use File Transfer Protocol (FTP) or Remote Copy Protocol (RCP) to get the core dump. On the router, configure this:

```
exception protocol ftp
exception dump n.n.n.n
ip ftp username <string>
ip ftp password <string>
ip ftp source-interface <slot/port/interface>
exception core-file <core-filename>
```

When you have collected a core dump, upload it to ftp://ftp-sj.cisco.com/incoming (in UNIX, type

**pftp ftp–sj.cisco.com** and then **cd incoming**), and notify the owner of your case and include the filename.

## Information to Collect if You Open a TAC Service Request

If you still need assistance after following the troubleshooting steps above and want to create a service request with the Cisco TAC, be sure to include the following information:

- **show technical–support** output The output of the **show technical–support** command gives information about the current state of the router, and also key information stored by the router before a crash.
- Console logs The console logs, often saved out to a syslog server, can provide valuable information about the events that occur on the router before a crash. These clues are often the most important information you can collect.
- crashinfo file (if present) Cisco recommends that you use a Cisco IOS software release that supports the crashinfo feature in order to troubleshoot successfully. For this, the version must meet the other needs of your network.

See Retrieving Information from the Crashinfo File or use the Software Advisor (registered customers only) tool to locate a Cisco IOS software version that supports the crashinfo feature.

A potential bonus is that if you have an older version of Cisco IOS software, the newer IOS software releases which support this feature could already have your bug fixed.

In order to attach information to your service request, upload it through the TAC Service Request Tool (registered customers only) . If you cannot access the TAC Service Request Tool, you can send the information in an email attachment to [attach@cisco.com](mailto:attach@cisco.com) with your case number in the subject line of your message.



**Caution:** Please do not manually reload or power–cycle the router before you collect the above information, if possible, as this can cause important information to be lost that is needed to determine the root cause of the problem.

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

## Related Information

- **Troubleshooting Router Crashes**
  - **Retrieving Information from the Crashinfo File**
  - **Creating Core Dumps**
  - **Troubleshooting Memory Problems**
  - **Technical Support – Cisco Systems**
- 

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Jul 31, 2006

Document ID: 26145

---