Troubleshooting Watchdog Timeouts

Document ID: 7956

Contents

Introduction

This document describes the cause of Watchdog Timeouts on Cisco routers, and explains how to troubleshoot them.

Prerequisites

Requirements

Readers of this document should have knowledge of these topics:

- Troubleshooting Router Crashes

Components Used

The information in this document is based on these software and hardware versions:

- All Cisco routers
- All Cisco IOS® software versions

Note: This document does not apply to Cisco Catalyst switches or MGX platforms, but only to Cisco routers.

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 Watchdog Timeouts

Cisco processors have timers that guard against certain types of system hangs. The CPU periodically resets a watchdog timer. The watchdog timer basically controls the time of each process. If the timer is not reset, a trap occurs. If a process is longer than it must be, the watchdog timer is used to escape from this process.

This only occurs if something goes wrong. Based on the situation, the router can reset itself, or recover from the failure and generate an error message in the console logs, which looks like this:

```
*** Watch Dog Timeout ***

PC = 0x6022536C, SP = 0x00000000
```

or

```
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Exec

*** System received a Software forced crash ***

signal = 0x17, code = 0x24, context= 0x60ceca60
```

If you do not power−cycle or manually reload the router, the output of the **show version** command looks like this:

```
Router#show version
...
Router uptime is 1 hour, 47 minutes
System restarted by watchdog timer expired at 09:26:24 UTC Mon Mar 27 2000
System image file is "flash:c3640-is-mz.113-7-T.bin", booted via flash
...
```

If you have the output of a **show version** command from your Cisco device, you can use to display potential issues and fixes. To use, you must be a registered customer, be logged in, and have JavaScript enabled.

You can use Output Interpreter to display potential issues and fixes. To use Output Interpreter, you must be a registered customer, be logged in, and have JavaScript enabled.

Troubleshoot

The root cause of the watchdog timeout can be hardware− or software−related. Here are the common symptoms through which you can identify the source of the problem:

- If a router that has been properly operational for months suddenly starts to reload every 20 minutes, or if it continuously reboots and you can no longer access it, the problem is most likely a hardware−related issue. This is also the case if a new module has been installed recently, and the router crashes by watchdog timeout afterwards.
- If the router starts to crash after a configuration change or a change in the Cisco IOS software version, it is probably a software−related issue.

The first step to troubleshoot this type of issue is to identify the type of watchdog timeout that you encounter. There are two types of Watchdog Timeouts:

- The Software Watchdog Timeout, which, despite its name, is often hardware−related
- The Process Watchdog Timeout, which is often software−related

Software Watchdog Timeout

This timeout is caused by an infinite loop at interrupt level, or by a hardware problem. Here are some indications of this type of timeout:

- Console logs contain these lines:

```
*** Watch Dog Timeout ***

PC = 0x6022536C, SP = 0x00000000
```

- The **show version** output reports the reload reason as a "watchdog timer expired":

```
Router#show version
...
Router uptime is 1 hour, 47 minutes
System restarted by watchdog timer expired at 06:30:24 UTC Mon Jan 28 2000
System image file is "flash:c3640−is−mz.113−7−T.bin", booted via flash
```

- No crashinfo file is generated. See Retrieving Information from the Crashinfo File for details.

Most of the time, these messages indicate a hardware issue, either with the main processor board or with one of the modules.

After you identify a software watchdog timeout, the next step is to check the Product Field Notice Summary for your platform and all the components installed in that system for known critical hardware issues. For example, there is one Field Notice for the Cisco 3600 Series Router: Cisco 3600 T1/E1 PRI Module Watchdog Timeouts. Ensure that you check the Field Notices before you troubleshoot further.

If a new module has been recently installed, you must first try to remove it to verify whether it is the reason for the watchdog timeout. If the watchdog timeout persists, try to re−seat all removable components.

If the watchdog timeout continues at this point, there are no Field Notices for your hardware, and if no new module has been recently installed, go ahead and replace the main processor board. On high−end platforms, the processor board is a separate card (such as the NPE−400 or RSP8). On low−end platforms (Cisco 1700, 2500, 4000, 2600, 3600, and so on), the motherboard cannot be shipped separately. In this case, you have to replace the chassis itself.

Process Watchdog Timeout

This timeout is caused by an infinite loop at the process level. Here are some indications of this timeout:

- Console logs contain these lines:

```
%SYS−2−WATCHDOG: Process aborted on watchdog timeout,
         process = Exec

*** System received a Software forced crash ***

signal = 0x17, code = 0x24, context= 0x60ceca60
```

- The **show version** output reports the crash as a "software−forced crash":

```
Router#show version
...
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−l.112−15a.bin",
```

```
booted via flash
```

- A crashinfo file is generated for platforms which support it.

This problem is most likely a Cisco IOS software bug.

If you have the output of a **show stacks** command from your Cisco device, you can use to display potential issues and fixes. To use, you must be a registered customer, be logged in, and have JavaScript enabled.

However, the system was stuck in a loop before the reload. Therefore, the stack trace need not necessarily be relevant. You can upgrade to the latest Cisco IOS software version in your release train to eliminate all known Process Watchdog issues. If a crash still occurs after the upgrade, collect as much information as possible (see Troubleshooting Router Crashes), and contact your technical support representative.

Error Messages Related to Watchdog Timeout

There are other console error messages related to watchdog timers. Do not confuse these messages with a watchdog timer crash. Be sure to check the meaning of these error messages with the help of the Error Message Decoder (registered customers only) . This tool gives you a detailed explanation of many error messages, and recommends actions to resolve them.

Consider this message:

```
%SYS-2-WATCHDOG: Process aborted on watchdog timeout,
process = [chars]
```

This message indicates that the specified process has run for too long, and the processor has not been relinquished. The system has shut down the indicated process. Based on your configuration, this can lead to a system crash. If the message occurs only once, you need not take any action. However, if it occurs again, you must treat it as a Process Watchdog Timeout, and take the necessary action.

Information to Collect if You Open a TAC Service Request

If you still need assistance after following the troubleshooting steps above and want to open a service request (registered customers only) with the Cisco TAC, be sure to include the following information:
• Troubleshooting performed before opening the service request. • **show technical-support** output (in enable mode if possible). • **show log** output or console captures, if available. • **execute-on slot [***slot #***] show tech** for the slot which experienced the line card crash. • The crashinfo file (if it is available, and has not already been included in the **show technical-support** output). Please attach the collected data to your service request in non-zipped, plain text format (.txt). You can attach information to your service request by uploading it using the TAC Service Request tool (registered customers only) . If you cannot access the Service Request tool, you can send the information in an email attachment to attach@cisco.com with your service request

number in the subject line of your message.

Note: Please do not manually reload or power−cycle the router before collecting the above information unless required to troubleshoot a line card crash on the Cisco 12000 Series Internet Router, as this can cause important information to be lost that is needed for determining the root cause of the problem.

Related Information

- **Troubleshooting Router Crashes**
- **Understanding Software−forced Crashes**
- **Troubleshooting Router Problems: Cisco IOS Software Releases 12.1 EX**
- **Technical Support − Cisco Systems**

Updated: Nov 29, 2006 Document ID: 7956