

Troubleshooting High CPU Utilization on Cisco Routers

Document ID: 15095

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

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Symptoms of High CPU Utilization

Initial Troubleshooting

Determining Causes and Solving the Problem

- High CPU Utilization due to Interrupts
- High CPU when Enabling Netflow NDE on Cisco 7600 Series Router
- High CPU Utilization due to Processes
- PCI and FAST Memory Pools Show Very High Utilization

%SNMP-4-HIGHCPU: Process exceeds [dec]ms threshold ([dec]ms IOS quantum) for [chars] of [chars]---result [chars]

- High CPU due to Software Encryption
- High CPU Utilization due to Fragmentation

Commands for Obtaining More Information

- show processes cpu Command
- show interfaces Command
- show interfaces switching Command
- show interfaces stat Command
- show ip nat translations
- show align Command
- show version Command
- show log Command

UNIX Shell Script for Periodically Collecting Data

Related Information

Introduction

This document describes common symptoms and causes of high CPU utilization on Cisco routers, and provides troubleshooting guidelines and solutions.

Prerequisites

Requirements

Troubleshooting high CPU utilization on Cisco routers requires understanding of Cisco IOS® software switching paths. For information on Cisco IOS software switching paths, see Performance Tuning Basics.

Components Used

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

Conventions

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

Symptoms of High CPU Utilization

This list describes common symptoms of high CPU utilization. If you notice any of these symptoms, follow the troubleshooting steps in this document to alleviate the problem.

- High percentages in the **show processes cpu** command output

If you have the output of a **show processes cpu** 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.

- Slow performance
- Services on the router fail to respond, for instance:
 - ◆ Slow response in Telnet or unable to Telnet to the router
 - ◆ Slow response on the console
 - ◆ Slow or no response to ping
 - ◆ Router does not send routing updates to other routers
- High buffer failures

Initial Troubleshooting

Once you notice any of the symptoms from the Symptoms of High CPU Utilization:

- Check for a possible security issue. Commonly, high CPU utilization is caused by a security issue, such as a worm or virus operating in your network. This is especially likely to be the cause if there have not been recent changes to the network. Usually, a configuration change, such as adding additional lines to your access lists can mitigate the effects of this problem. Cisco Product Security Advisories and Notices contains information on detection of the most likely causes and specific workarounds.

For additional information, refer to:

- ◆ 100 Questions and Answers about Internet Threats
- ◆ Cisco Product Security Advisories and Notices
- ◆ Cisco Threat Control
- Make sure all debugging commands in your router are turned off by issuing the **undebg all** or **no debug all** commands. For more information on the use of debugging commands, refer to Using Debug Commands.
- Are you able to issue **show** commands on the router? If yes, start collecting more information immediately, using these **show** commands.
- Is the router inaccessible? Can you reproduce this problem? If yes, power-cycle the router and, before

reproducing the problem, configure the **scheduler interval 500** command. This schedules low priority processes to run every 500 milliseconds, which provides time for you to run some commands, even if CPU usage is at 100 percent. On Cisco 7200 and Cisco 7500 Series Routers, use the **scheduler allocate 3000 1000** command.

- Does the router show symptoms of high CPU utilization at brief and unpredictable intervals? If yes, periodically collect the output of the **show processes cpu** command, which shows if the high CPU utilization is caused by interrupts or by a certain process. Use this UNIX script and, based on the first findings, modify the script to collect data needed for further investigation of the issue.

Determining Causes and Solving the Problem

Use the **show processes cpu** command to check if CPU utilization is high due to interrupts or processes.

High CPU Utilization due to Interrupts

For more information, refer to Troubleshooting High CPU Utilization Caused by Interrupts. If the level of the CPU rises due to interrupts that are likely due to CEF switching packets, the level of CPU does not affect the router performance.

High CPU when Enabling Netflow NDE on Cisco 7600 Series Router

If NetFlow is configured for version 7, the flow is performed by the Routing Processor, which could cause high CPU utilization.

For troubleshooting high CPU utilization due to Netflow version 7, configure **mls nde sender** version 5, as the Netflow export is performed by the SP, which is the default for version 5 or version 9.

High CPU Utilization due to Processes

Check which process is loading the CPU. Unusual activity related to a process results in an error message in the log. Therefore, the output of the **show logging exec** command should be checked first for any errors related to the process which consumes lots of CPU cycles.

Debugging can also be of great help in troubleshooting high CPU utilization in processes. Nevertheless, debugging should be carried out with extreme caution because it may raise the CPU utilization even more. These prerequisites should be met in order to make debugging safe and useful:

- All logging destinations except buffer logging should be either disabled or their logging severity level should be lowered from 7 (debugging) to 6 (informational) or less, using the appropriate **logging destination [severity-level]** configuration command. To see which logging destinations and corresponding levels are enabled, read the header lines of the **show logging exec** command.
- Logging buffer size should be increased in order to capture sufficient information. For more details, refer to the description of the **logging buffered** global configuration command.
- In order to be able to better read and understand debugs, the datetime and millisecond timestamps should be enabled. For more details, refer to the description of the **service timestamps** global configuration command.

A sample debugging session of IP packets is provided in Troubleshooting High CPU Utilization in the IP Input Process.

For troubleshooting high CPU utilization in specific processes, refer to the appropriate link:

- ARP Input ARP Input section of the document Troubleshooting High CPU Utilization Due to Processes
- BGP Router High CPU due to BGP Router Process section of the document Troubleshooting High CPU Caused by the BGP Scanner or BGP Router Process
- BGP Scanner High CPU due to BGP Scanner section of the document Troubleshooting High CPU Caused by the BGP Scanner or BGP Router Process
- EXEC High CPU Utilization in the EXEC and Virtual EXEC Processes
- HyBridge Input Troubleshooting High CPU Utilization Caused by the HyBridge Input Process on Routers With ATM Interfaces
- IP Input Troubleshooting High CPU Utilization Due to the IP Input Process
- IP Simple Network Management Protocol (SNMP) IP Simple Network Management Protocol (SNMP) Causes High CPU Utilization
- LC ADJ Updater What Causes High CPU Utilization in the LC Adjacency Updater Process on a Cisco 12000 Series Internet Router?
- TCP Timer TCP Timer section of the document Troubleshooting High CPU Utilization due to Processes
- TTY Background TTY Background section of the document Troubleshooting High CPU Utilization due to Processes
- Virtual EXEC High CPU Utilization in Exec and Virtual Exec Processes
- Vtemplate Backgr Virtual Template Background section of the document Troubleshooting High CPU Utilization due to Processes
- SSH Process Might go high if capturing a **show tech** or some debug is enabled.
- Other processes Other Processes section of the document Troubleshooting High CPU Utilization due to Processes

PCI and FAST Memory Pools Show Very High Utilization

It is normal to see low free memory with PCI and Fast memory pools. The PCI memory is used for memory access to the GT64260 controller on the PRP mainboard for the PCI buses connected to it. This memory is used for internal communication between the system controller and other parts, so it appears to be high all the time.

If more memory is needed, it falls back to processor pool memory. The Fast memory is a small amount of memory that has been set aside for use by the hardware Interface Descriptor Block (IDB) data structures. This memory is also completely reserved throughout bootup, so it is always shows as high since the memory is completely used. Because of this, it is normal to see low free memory with the Fast memory pool.

%SNMP-4-HIGHCPU: Process exceeds [dec]ms threshold ([dec]ms IOS quantum) for [chars] of [chars]--result [chars]

The CPU hog message looks like this:

```
SNMP-4-HIGHCPU: Process exceeds 200ms threshold (200ms IOS quantum)
for GET of rmon.19.16.0--result rmon.19.16.0
```

A new syslog message (HIGHCPU) was added to IOS in 12.4(13). If a process holds on to the CPU for more than 200 ms, it reports a HIGHCPU message. The HIGHCPU message has no impact on the router. It just lets you know what process has caused the high CPU. The HIGHCPU message is similar to the CPUHOG message, but the HIGHCPU message has a much lower tolerance threshold, at 1/10 the amount of time compared to a CPUHOG message, that is, measured in milliseconds). In versions prior to 12.4(13) on the 2600, the processes ran for longer times but did not generate messages because the IOS versions did not have this enhancement.

SNMP PDU processing (MIB object queries) are supposed to be performed in a single CPU time quantum to ensure that each object in the PDU is retrieved as if simultaneously. This is a requirement imposed by the SNMP protocol standard. Some objects are aggregates of a lot of data in the system, so, even though they are single objects, there is a lot of processing involved due to the way they are instrumented. If they do not relinquish the CPU, as required by MIB instrumentation rules, there is a possibility of this error message. Additionally, if you poll several different objects in the same object group/table and get the error message, is not unusual because of this same reason.

This message is used to identify objects that use more CPU time than expected (but still not CPUHOG). Some NMS/instrumentation tools do not behave well when polling. This issue is documented in Cisco bug ID CSCsl18139 (registered customers only) .

High CPU due to Software Encryption

When there is no hardware encryption module installed in the device, then all encrypted traffic coming through the device will have to be encrypted by the software. This is very CPU intensive. It is not recommend to use software encryption for any encryption deployment with a reasonable throughput requirement. One option to resolve this issue is to reduce the volume of encrypted traffic (re-route traffic or limit the flows that are encrypted). However, the best way to address this issue is to get a Hardware Encryption module installed for this device which eliminates the need for encryption to take place through the software.

Note: The enabling of crypto maps on Tunnel/Physical interfaces is a memory consumption process and can cause an increase in CPU.

High CPU Utilization due to Fragmentation

Reassemblies can drive up the CPU very high if the CPU has to reassemble a large number of packets.

For troubleshooting high CPU utilization due to fragmentation, issue the **tcp mss-adjust 1400** command on the interface which sets the maximum segment size (MSS) value of TCP synchronize/start (SYN) packets going through a router.

Commands for Obtaining More Information

These commands provide more information about the problem:

- **show processes cpu**
- **show interfaces**
- **show interfaces switching**
- **show interfaces stat**
- **show ip nat translations**
- **show align**
- **show version**
- **show log**

If the router is completely inaccessible, first power-cycle it. Then, periodically collect the output of the commands in this section, except for the **show log** command, whose messages should be logged on a syslog server. The interval for collecting output should be five minutes. You can collect the data manually or automatically, using this UNIX shell script. You can also collect data using HTTP or SNMP. For details about configuring HTTP and SNMP on a Cisco router, refer to the Cisco IOS Software Configuration document.

show processes cpu Command

This is an example of the header of the **show processes cpu** command:

```
CPU utilization for five seconds: X%/Y%; one minute: Z%; five minutes: W%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
```

This table describes the fields in the header:

Field	Description
X	Average total utilization during last five seconds (interrupts + processes)
Y	Average utilization due to interrupts, during last five seconds ¹
Z	Average total utilization during last minute ²
W	Average total utilization during last five minutes ²
PID	Process ID
Runtime	CPU time the process has used (in milliseconds)
Invoked	Number of times a process has been called
uSecs	Microseconds of CPU time for each invocation
5Sec	CPU utilization by task in the last five seconds
1Min	CPU utilization by task in the last minute ²
5Min	CPU utilization by task in the last five minutes ²
TTY	Terminal that controls the process
Process	Name of process

¹CPU utilization on process level = X – Y

²Values do not represent an arithmetical average, but an exponentially decayed average. Thus, more recent values have more influence on the calculated average.

Use this link, for a detailed explanation of the **show processes cpu** command.

Note: Total CPU utilization should not be used as a measure of the ability of the router to switch more packets. On Cisco 7500 routers, Versatile Interface Processors (VIPs) and Route/Switch Processors (RSPs) do not report linear CPU utilization. Close to half of the switching packet-per-second power comes after 90 to 95 percent CPU utilization.

show interfaces Command

The command reference contains a detailed explanation of the **show interfaces** command.

show interfaces switching Command

This command is used for determining active switching paths on interfaces. For more information about switching paths in Cisco IOS Software, refer to the Configuring Switching Paths document.

This is a sample output of the **show interfaces switching** command for one interface:

```
RouterA#show interfaces switching
Ethernet0
    Throttle count          0
    Drops                   RP          0          SP          0
    SPD Flushes             Fast          0          SSE          0
    SPD Aggress             Fast          0
    SPD Priority             Inputs        0          Drops          0

    Protocol    Path    Pkts In    Chars In    Pkts Out    Chars Out
    Other      Process  0          0          595         35700
    Cache misses
    Fast          0          0          0          0
    Auton/SSE     0          0          0          0
    IP          Process  4          456         4          456
    Cache misses
    Fast          0          0          0          0
    Auton/SSE     0          0          0          0
    IPX         Process  0          0          2          120
    Cache misses
    Fast          0          0          0          0
    Auton/SSE     0          0          0          0
    Trans. Bridge Process  0          0          0          0
    Cache misses
    Fast          11         660         0          0
    Auton/SSE     0          0          0          0
    DEC MOP      Process  0          0          10         770
    Cache misses
    Fast          0          0          0          0
    Auton/SSE     0          0          0          0
    ARP          Process  1          60          2          120
    Cache misses
    Fast          0          0          0          0
    Auton/SSE     0          0          0          0
    CDP          Process  200         63700       100         31183
    Cache misses
    Fast          0          0          0          0
    Auton/SSE     0          0          0          0
```

The output lists the switching paths for all protocols configured on the interface, so you can easily see what kind and the amount of traffic going through the router. This table explains the output fields.

Field	Definition
Process	Processed packets. These can be packets destined for the router, or packets for which there was no entry in the fast switching cache.
Cache misses	Packets for which there was no entry in fast switching cache. The first packet for this destination (or flow – depends on the type of fast switching configured) will be processed. All subsequent packets will be fast switched, unless fast switching is explicitly disabled on the outgoing interface.
Fast	Fast switched packets. Fast switching is enabled by default.
Auton/SSE	Autonomous switched, silicon switched or distributed switched packets. Available only on

Cisco 7000 series routers with a Switch Processor or Silicon Switch Processor (for autonomous switching or silicon switching, respectively), or on Cisco 7500 series routers with a VIP (for distributed switching).
--

show interfaces stat Command

This command is a summarized version of the **show interfaces switching** command. This is a sample output for one interface:

```
RouterA#show interfaces stat
Ethernet0
      Switching path   Pkts In   Chars In   Pkts Out   Chars Out
      Processor        52077    12245489    24646     3170041
      Route cache         0         0           0           0
      Distributed cache  0         0           0           0
      Total             52077    12245489    24646     3170041
```

The output of the **show interfaces stat** command is different for different platforms, depending on available and configured switching paths.

show ip nat translations

The **show ip nat translations** command displays the Network Address Translation (NAT) translations active on the router. Each active translation generates CPU interrupts and has an impact on the total CPU utilization of the router. A very large number of translations can have a performance impact on the router.

This is a sample output from the **show ip nat translations** command:

```
router#show ip nat translations
Pro Inside global   Inside local   Outside local   Outside global
--- 172.16.131.1    10.10.10.1    ---            ---
```

show align Command

This command is available only on reduced instruction set computing (RISC) processor-based platforms. On these platforms, the CPU can correct for mis-aligned memory reads or writes. This is some sample output:

```
Alignment data for:
4500 Software (C4500-DS40-M), Version mis-aligned RELEASE SOFTWARE (fcl)
Compiled Tue 31-Mar-98 15:05 by jdoe

Total Corrections 33911, Recorded 2, Reads 33911, Writes 0

Initial Initial
Address Count Access Type Traceback
40025F4D 15561 16bit read 0x606F4A7C 0x601C78F8 0x6012FE94 0x600102C0
40025F72 18350 32bit read 0x606FB260 0x6013113C 0x600102C0 0x60010988
```

show version Command

For the purpose of tracking high CPU utilization problems, the important part of this command output is the Cisco IOS Software version, platform, CPU type, and the uptime of the router. The command reference gives a detailed explanation of the **show version** command.

show log Command

This command shows the contents of buffered log messages. For more information about logging system messages, refer to the *Log System Error Messages* section of the Troubleshooting the Router configuration guide.

UNIX Shell Script for Periodically Collecting Data

This appendix describes a simple script for periodically capturing data from the router. The core of the script is this line:

```
(echo "show version") | telnet 192.168.1.1
```

The command in parentheses is executed in sub-shell and the output is sent to a Telnet session. This is a sample script for capturing the output from the **show version** and **show processes cpu** commands:

```
#!/opt/local/bin/bash

#####
# Router's IP address
#
IP_ADDRESS='10.200.40.53'

# Directory where the log files will be stored
#
DIR=/var/log/router

#####

if [ ! -e $DIR ]
then
    mkdir $DIR
fi

# Tag specification: mmddhhmm
DATE=`date +%m%d`\
TIME=`date +%H%M`\
TAG=$DATE$TIME

# Collect data from the router
(echo "foo";\
echo "bar";\
echo "term len 0";\
echo "show version";\
echo "show processes cpu";\
echo "term len 15";\
echo "show memory summary";\
echo "q";\
sleep 30)|telnet $IP_ADDRESS > $DIR/info.$TAG 2>$DIR/info.$TAG.msg
```

Note: In this script all data, including the password, are sent in a clear text format.

In the first section, you need to specify the IP address and the destination directory for log files. The second section contains the actual commands that are sent to the router. The first is the username, then the password, and so on. A trick for capturing only the first lines of output of certain commands is included. Terminal length is set to something short (15 in this case), and the "q" character is sent only by prompt.

If data is collected periodically, the output of **show version** shows if the problem has a periodic nature, for example, if it appears always at a certain time of day or on a particular day of the week. If you need to collect

the output of more commands, they can be added to the script in the same manner as those shown in the example. If you need to truncate the output sent to the file, first increase the sleep period (the sleep command in parenthesis).

Run this script every five minutes if the high CPU utilization problem appears often and does not last long. Otherwise, you can run it every 15 or 30 minutes. For ease of use, save the script in a file such as `/usr/bin/router-script`. Then, to run it every five minutes, add the following line to the `/etc/crontab` file:

```
* /5 * * * * /usr/bin/router-script
```

Restart the cron server. If you do not have the authority to change the `/etc/crontab` file, run the script in a separate process, like this:

```
while [ 1 ]; do ./router-script ; sleep 300; done &
```

Related Information

- [The show processes Command](#)
- [High CPU Utilization on Catalyst 2900XL/3500XL Switches](#)
- [Performance Tuning Basics](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jul 24, 2008

Document ID: 15095
