Cisco 7600 Troubleshooting Guide

This document contains troubleshooting information for the Cisco 7600 Routers.

Contents

This publication contains these sections:

Document Revision History

Revision	Date	Change Summary
OL-28248-01	November 2012	Initial version.

Cisco 7600 Troubleshooting Issues

This section describes the probable causes and solutions for the troubleshooting issues:

Isolated BFD Flaps

Issue: Bidirectional Forwarding Detection (BFD) is implemented to detect the faults between two routers as quickly as possible. Logs indicate that BFD detected an issue due to loss of keepalive signals. But there were no packet drops on either end, no errors on the links, and no other protocol flaps.

Probable Cause: On the Cisco 7600 routers, the BFD is implemented on supervisors, and there are instances of BFD flaps due to delay of the keepalive messages within the platform.

Solution:

- A high CPU utilization can delay the BFD keepalive messages. To prevent the CPU unavailability, use the **process-max-time 50** or **hw-module rp process-max-time 50** commands. This prevents the CPU unavailability for aggressive BFD timers. It also decreases the maximum duration of a process run from the default 200ms to 50ms.
- Do not configure very aggressive timers. The minimum recommended configuration is to use the **bfd interval 100 min_rx 100 multiplier 3** commands.
- Offload the BFD sessions to a line card (only for ES+). This moves the processing from the Supervisor to the line card. For more information see the following link: http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html#wp1720514.
  Also, reduce the maximum processing time if the CPU utilizations of the line card is high. Use the **hw-module slot 'x' process-max-time 50** command.
- BFD sessions configured on interfaces belonging to non-DFC cards may flap during a physical online insertion and removal (OIR) of any other line card in the router. This is because of a short bus stall caused on the backplane bus during the physical OIR. We recommend you to increase the BFD timers to 999 for the interfaces of the non-DFC cards.

If the above troubleshooting does not help, open a case with Cisco Technical Assistance Center (TAC) or High Touch Technical Support (HTTS).

High CPU Utilization on the Processors

Issue: High CPU utilization on the route processors (RP) or switch processors (SP) due to a high rate of punted traffic.

Probable Cause: The RP and the SP are mainly used for control plane packets, while the Policy Feature Card (PFC) and the Distributed Forwarding Card (DFC) handle packet forwarding at Application Specific Integrated Circuit (ASIC) level. Because of this, the CPU utilization of the processors remains low. If the processor utilization is high (over 50%), then this needs to be checked. The most common cause of high CPU utilization is a high rate of traffic punted by the PFC or DFC to the processors.

Solution:

First identify the source of traffic. See the guide at the following URL to know more:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_tech_note09186a00804916e0.shtml

Use these options to capture the ingress packets sent to the processors. You can use these options even if the CPU utilization is 100% because the packet capturing does not occur at the processors:

Option A: Use the Netdr tool

- This tool captures the packet headers on the System Controller ASIC that connects directly to the processors. It is the last ASIC before the packet reaches the processor. It captures a maximum of 4096 packets.
- Use the **debug netdr capture rx** command. You can view the packets using the **show netdr capture** command. Similarly, for the SP, use the **remote command switch debug netdr capture rx** command to capture packets. Use the **remote command switch show netdr capture** command to view the captured packets. Open a case with TAC or HTTS, and send the output for further analysis.

Option B: Use an Inband RP or SP monitoring session

- A span session for the RP or the SP is optional. The traffic is replicated and sent out of a port where a network analyzer or sniffer is connected.
- First, configure a monitoring session with any source interface that is administratively shutdown. The destination interface is the interface connected to an external analyzer.

  monitor session *session_number* **source interface** *interface*
  monitor session *session_number* **destination interface** *interface*
- Next, apply the following configuration from the SP console (Use the **remote login switch** command to reach the SP console).

  test monitor session *session_number* **add rp-inband rx** <-- to enable SPAN for the RP

  t**est monitor session** *session_number* **add sp-inband rx** <-- to enable SPAN for the SP

See the guides at these URLs for various measures present on the 7600 routers to prevent the high CPU utilization:

http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html#9

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/dos.html

Inaccurate or nil Rate Counters on Show Interface for a VLAN Interface

Issue: The output of the **show int vlan** command shows a zero rate counter for the switched virtual interface (SVI) on all the layer 2 switched traffic. The output of the **show int vlan** command shows a wrong rate counter for SVI for the layer 3 switched traffic.

Probable Cause: By definition, the rate displayed by the **show int vlan x** command does not include the layer 2 switched packets in the rate computation. Therefore, the rate counter will remain zero for layer 2 switched packets.

The rate counters for layer 3 traffic on an SVI can be erratic because the counters are received from various line cards, and the values received are cached values, not real time values. At times, the rate counters can show either a lower or a higher value than the actual rate.

Solution: This is a platform limitation and there is no software solution available. The input and output packet counters are accurate. Also, the counters for the physical ports are accurate because these are the real time counters received from the line cards. Interface counters are periodically sent from line cards to the Supervisor. The interval is typically around 10 seconds. This may also contribute to occasional erratic rate reporting.

Bad Payload CRC Causing Packet Drop

Issue: A SIP-400 or Enhanced Felxwan with MPLS configured shows the following error message:

Error Message `%HYPERION-5-HYP_INTR_INFO: HY_FD_PP_EC_EC_ERR_INT[0x1] bad payload CRC exceeds threshold.`

The error message indicates that there is a bad payload cyclic redundancy check (CRC) causing the packet drop.

Probable Cause: This is probably due to the way the hyperion ASIC calculates the CRC for the MPLS packet before and after the rewrite. Once the error is detected, the packet is dropped. The miscalculation can occur for an ES20 line card as well. In the case of an ES20, the line card crashes.

Solution: Use the **mls mpls recir-agg** command. Use the **mls mpls tunnel-recir** command if multicast VPN or point-to-point GRE tunnels are configured for traffic engineering.

Error Message Indicates Switching Bus is Idle

Issue: The error message from the PFC indicates that the switching bus is idle. On the Supervisor, the following error message is shown for the PFC:

Error Message `%EARL-2-SWITCH_BUS_IDLE: Switching bus is idle for two seconds.`

On the line card, the following error message is shown for the DFC:

Error Message `%EARL-DFC2-2-SWITCH_BUS_IDLE: Switching bus is idle for five seconds. The card grant is 0.`

Probable Cause: A timer regularly checks whether any packet is forwarded by the EARL (PFC on the Supervisor) to the EARL bus. Similar timer exists for each DFC present on the router. If the EARL did not switch any packets within two seconds for the PFC, and within five seconds for the DFC, then the error message is printed. The platform recovery mechanisms are invoked when the router detects the idle bus.

Solution: You may see this error during online insertion and removal (OIR) of a line card. If you insert the card too fast or too slow, then this error may appear. If you do not see this error during an OIR, then it indicates a hardware issue. You have to reseat the line card. If that does not resolve the issue, then you have to replace the line card. Collect the output of the following commands and send to TAC or HTTS.

- **show platform software module 'x' swbus idle info** <-- Module where error is seen
- **show platform software earl reset data**
- **show platform software earl reset history**
- **show tech-support**

Cross-connect under SVI or VPLS not Working

Issue: Cross-connect under SVI or VPLS not working

Probable Cause:

Hardware requirements are not met, so the cross-connect under SVI or Virtual Private LAN Services (VPLS) does not work from the start. Also in some cases, after link flap, VPLS or cross-connect under SVI is not working any more.

Solution:

If you are configuring cross-connect under SVI or VPLS, check whether the following restrictions apply:

- VPLS VC is not active with core facing SVI on an ES20 10 gigabyte interface
- SVI aggregate policer cannot be configured above 2.48 Gbps with cross-connect
- The core facing line card should be SIP-400, SIP-600, ES20 or ES+ line card.

Modular or Generic Online Diagnostic Failures

Issue: Modular failures or Generic Online Diagnostic Failures

Probable Cause: Generic Online Diagnostic (GOLD) failures indicate a problem in the module, the occupied slot, on the supervisor, or the chassis itself. In some rare situations, GOLD failures may also occur due to a software defect.

Note See the information about generic online diagnostic tests at: http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/diagtest.html

Solution:

1. Reload the module using the **hw-module module X reset** command.
2. Reseat the module.

Note In case a new module is inserted in the chassis, remove the module and verify that the backplane pins are not bent.

3. Perform a supervisor switchover in case of a dual supervisor.
4. Move the module into another slot of the chassis.
5. Insert the module into another chassis.

Connectivity Issues

Issue: Connectivity Issues

Probable Cause: Connectivity issues can occur because of physical issues, queue wedges or configuration mistakes.

Solution:

1. Perform a general sanity check:
   a. Check if the interfaces are up.
   b. Check if the linecard status is OK.
   c. Check if there is any error message in the logs.
2. Check if the ARP configuration is correct on both devices.
3. Check the direction in which packet flow is affected by using the packet sniffer or the **debug netdr cap rx** command.

   For example:

   A -> B (ICMP Echo request dropped from A to B)

   A <- B (ICMP Echo reply is dropped from B to A)
4. Check if the packet is dropped in egress or ingress direction using the packet sniffer or counters on **show counter interface** command.
5. Check for error counters, if the faulty interface is identified.

Packet Loss

Issue: Packet loss

Probable Cause: Packet loss means that the basic bidirectional connectivity between two ends of a router is confirmed. Out of a number of packets, a fixed number of packets are lost. The connectivity between the end devices may consist out of multiple intermediate devices, which makes it difficult to isolate the specific device responsible for packet loss.

Solution:

1. Create a topology of the packet path.
2. Check if there is any noticeable pattern in the packet loss.
3. Check the direction in which packet loss is affected by using packet sniffer or the **debug netdr cap rx** command.

   For example:

A -> B (ICMP Echo request dropped from A to B)

A <- B (ICMP Echo reply is dropped from B to A)

4. Identify the device where the packet loss occurs. This can be detected with the help of packet sniffer.
5. Check if the packet is dropped in egress or ingress direction using packet sniffer or counters on interface **show counter interface** command on the device.
6. Check for error counters, if the faulty interface is identified.

Input Drops

Issue: Input drops

Probable Cause: Inputs could drop due to overruns.Overruns are situations when interface ASIC is out of buffer. Overruns represent hardware switched packet loss. Typically, this could be caused by an egress line card oversubscription when multiple ingress interfaces send traffic to the same egress interface. Another common cause is burst network traffic.

Solution:

1. Use the **TestFabricFlowControlStatus** command.
2. Use the **diagnostic monitor module test** command.

```
sup720_04(config)# diagnostic monitor module 5 test 33
```

3. Configure the frequency to 100ms.

```
diagnostic monitor interval module 5 test 33 00:00:00 100 0
```

4. Verify the presence of flow control using the **show diagnostic event** command

   Here is a sample output:

```
RateReduction: 12/0, [fpoe:7], Fab->LC = R0%/CU0%  /PU73%, LC->Fab = R100%/CU0%/PU61%,
SP CPU = 23%
```

   R0% indicates full flow control

   R100% indicates no flow control

   FAB->LC indicates direction of flow control. Here the fabric flow controls the line card, which means the line card is not allowed to send any further traffic to the fabric.

Note In an egress oversubscription, the overloaded egress line card flow controls the fabric. As a result the fabric flow controls the ingress linecards, which result in overruns on the ingress interfaces. If the direction of flow control is confirmed, the issue may be solved by rerouting some traffic through an alternate path or by increasing bandwidth.

Related Documentation

The following publications are available for the Cisco 7600 series routers:

- *Cisco 7600 Series Router Installation Guide*
- *Cisco 7600 Series Router Module Installation Guide*
- *Cisco 7600 Series Router SIP, SSC, and SPA Hardware Installation Guide*
- *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*
- *Cisco 7600 Series Router Cisco IOS Command Reference*
- *Cisco 7600 Series Internet Router System Message Guide*
- *Release Notes for Cisco IOS Release 12.2SRA on the Cisco 7600 Series Routers*
- Cisco IOS Configuration Guides and Command References—Use these publications to help you configure Cisco IOS software features not described in the Cisco 7600 series router publications:
  - *Configuration Fundamentals Configuration Guide*
  - *Configuration Fundamentals Command Reference*
  - *Bridging and IBM Networking Configuration Guide*
  - *Bridging and IBM Networking Command Reference*
  - *Interface Configuration Guide*
  - *Interface Command Reference*
  - *Network Protocols Configuration Guide*, *Parts 1, 2, and 3*
  - *Network Protocols Command Reference*, *Parts 1, 2, and 3*
  - *Security Configuration Guide*
  - *Security Command Reference*
  - *Switching Services Configuration Guide*
  - *Switching Services Command Reference*
  - *Voice, Video, and Home Applications Configuration Guide*
  - *Voice, Video, and Home Applications Command Reference*
  - *Software Command Summary*
  - *Software System Error Messages*
  - *Debug Command Reference*
  - *Internetwork Design Guide*
  - *Internetwork Troubleshooting Guide*
  - *Configuration Builder Getting Started Guide*

  The Cisco IOS Configuration Guides are located at the following URL:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html
- For information about MIBs, go to this URL:

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html