Configuring Online Diagnostics

This chapter contains the following sections:

Information About Online Diagnostics

Online diagnostics provide verification of hardware components during switch bootup or reset, and they monitor the health of the hardware during normal switch operation.

Cisco Nexus Series switches support bootup diagnostics and runtime diagnostics. Bootup diagnostics include disruptive tests and nondisruptive tests that run during system bootup and system reset.

Runtime diagnostics (also known as health monitoring diagnostics) include nondisruptive tests that run in the background during normal operation of the switch.

Bootup Diagnostics

Bootup diagnostics detect faulty hardware before bringing the switch online. Bootup diagnostics also check the data path and control path connectivity between the supervisor and the ASICs. The following table describes the diagnostics that are run only during switch bootup or reset.

Table 1: Bootup Diagnostics

Diagnostic	Description
PCIe	Tests PCI express (PCIe) access.
NVRAM	Verifies the integrity of the NVRAM.
In band port	Tests connectivity of the inband port to the supervisor.
Management port	Tests the management port.

Diagnostic	Description
Memory	Verifies the integrity of the DRAM.

Bootup diagnostics also include a set of tests that are common with health monitoring diagnostics.

Bootup diagnostics log any failures to the onboard failure logging (OBFL) system. Failures also trigger an LED display to indicate diagnostic test states (on, off, pass, or fail).

You can configure Cisco Nexus device to either bypass the bootup diagnostics or run the complete set of bootup diagnostics.

Health Monitoring Diagnostics

Health monitoring diagnostics provide information about the health of the switch. They detect runtime hardware errors, memory errors, software faults, and resource exhaustion.

Health monitoring diagnostics are nondisruptive and run in the background to ensure the health of a switch that is processing live network traffic.

The following table describes the health monitoring diagnostics for the switch.

Table 2: Health Monitoring Diagnostics Tests

Diagnostic	Description
LED	Monitors port and system status LEDs.
Power Supply	Monitors the power supply health state.
Temperature Sensor	Monitors temperature sensor readings.
Test Fan	Monitors the fan speed and fan control.

Note When the switch reaches the intake temperature threshold and does not go within the limits in 120 seconds, the switch will power off and the power supplies will have to be re-seated to recover the switch

The following table describes the health monitoring diagnostics that also run during system boot or system reset.

Table 3: Health Monitoring and Bootup Diagnostics Tests

Diagnostic	Description
SPROM	Verifies the integrity of backplane and supervisor SPROMs.
Fabric engine	Tests the switch fabric ASICs.
Fabric port	Tests the ports on the switch fabric ASIC.
Forwarding engine	Tests the forwarding engine ASICs.
Forwarding engine port	Tests the ports on the forwarding engine ASICs.

Diagnostic	Description
Front port	Tests the components (such as PHY and MAC) on the front ports.

Note When the switch exceeds the internal temperature threshold of 70 degrees Celsius and does not decrease below the threshold limit within 120 seconds, the switch powers off and the switch must be properly power-cycled in order to recover the switch.

Expansion Module Diagnostics

During the switch bootup or reset, the bootup diagnostics include tests for the in-service expansion modules in the switch.

When you insert an expansion module into a running switch, a set of diagnostics tests are run. The following table describes the bootup diagnostics for an expansion module. These tests are common with the bootup diagnostics. If the bootup diagnostics fail, the expansion module is not placed into service.

Table 4: Expansion Module Bootup and Health Monitoring Diagnostics

Diagnostic	Description
SPROM	Verifies the integrity of backplane and supervisor SPROMs.
Fabric engine	Tests the switch fabric ASICs.
Fabric port	Tests the ports on the switch fabric ASIC.
Forwarding engine	Tests the forwarding engine ASICs.
Forwarding engine port	Tests the ports on the forwarding engine ASICs.
Front port	Tests the components (such as PHY and MAC) on the front ports.

Health monitoring diagnostics are run on in-service expansion modules. The following table describes the additional tests that are specific to health monitoring diagnostics for expansion modules.

Table 5: Expansion Module Health Monitoring Diagnostics

Diagnostic	Description
LED	Monitors port and system status LEDs.
Temperature Sensor	Monitors temperature sensor readings.

Guidelines and Limitations for Online Diagnostics

Online diagnostics has the following configuration guidelines and limitations:

- You cannot run disruptive online diagnostic tests on demand.

- The BootupPortLoopback test is not supported.
- Interface Rx and Tx packet counters are incremented (approximately four packets every 15 minutes) for ports in the shutdown state.
- On admin down ports, the unicast packet Rx and Tx counters are incremented for GOLD loopback packets. The PortLoopback test is on demand for releases prior to Cisco NX-OS 7.0(3)I1(2), so the packet counter is incremented only when you run the test on admin down ports. Starting with Cisco NX-OS Release 7.0(3)I1(2), the PortLoopback test is periodic, so the packet counter is incremented on admin down ports every 30 minutes. The test runs only on admin down ports. When a port is unshut, the counters are not affected.

Configuring Online Diagnostics

You can configure the bootup diagnostics to run the complete set of tests, or you can bypass all bootup diagnostic tests for a faster module boot up time.

Note We recommend that you set the bootup online diagnostics level to complete. We do not recommend bypassing the bootup online diagnostics.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **diagnostic bootup level** [**complete** | **bypass**]	Configures the bootup diagnostic level to trigger diagnostics when the device boots, as follows: • **complete**—Performs all bootup diagnostics. This is the default value. • **bypass**—Does not perform any bootup diagnostics.
Step 3	(Optional) switch# **show diagnostic bootup level**	Displays the bootup diagnostic level (bypass or complete) that is currently in place on the switch.

Example

The following example shows how to configure the bootup diagnostics level to trigger the complete diagnostics:

```
switch# configure terminal
switch(config)# diagnostic bootup level complete
```

Verifying the Online Diagnostics Configuration

Use the following commands to verify online diagnostics configuration information:

Command	Purpose
show diagnostic bootup level	Displays the bootup diagnostics level.
show diagnostic result module *slot*	Displays the results of the diagnostics tests.

Default Settings for Online Diagnostics

The following table lists the default settings for online diagnostics parameters.

Table 6: Default Online Diagnostics Parameters

Parameters	Default
Bootup diagnostics level	complete

Parity Error Diagnostics

Clearing Parity Errors

You can clear a corresponding Layer 2 or Layer 3 table entry (with 0s) when a parity error is detected by using the **hardware profile parity-error {l2-table | l3-table} clear** command. This command is effective when it is present in the running configuration and the system is booting up. In addition, the command must be enabled and after the configuration is saved, the system should be rebooted for the command to take effect.

Important This command is not supported on Cisco NX-OS Release 6.0(2)U2(1) and higher versions.

The following guidelines apply:

- When the command is used for an l2_entry table, the cleared entry should be relearned due to the traffic pattern.
- When the command is used for an l3_entry_only (host) table, the cleared entry is not be relearned.

The command is useful in the following customer configurations:

- L2_Entry table, with no static L2_entry table entries

  If the L2_Entry table entry is cleared, the entry should be dynamically learned through the traffic pattern. It should not be learned through IGMP or multicast.

- L3_Entry_only (host) table

Customers should not use the host table. The **hardware profile unicast enable-host-ecmp** command should be enabled. In this case, the customer node does not have any valid entries in the L3_Entry_only table, so clearing the L3_Entry_only entry table should not have any impact.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **hardware profile parity-error l2-table clear**	Clears parity error entries in a Layer 2 table.
Step 3	switch(config)# **hardware profile parity-error l3-table clear**	Clears parity error entries in a Layer 3 table.

Example

This example shows how to clear parity errors in a Layer 2 table:

```
switch# configure terminal
switch(config)# hardware profile parity-error l2-table clear
switch(config)# copy running-config startup-config
switch(config)# reload
```

This example shows how to clear parity errors in a Layer 3 table:

```
switch# configure terminal
switch(config)# hardware profile parity-error l3-table clear
switch(config)# copy running-config startup-config
switch(config)# reload
```

Soft Error Recovery

Cisco NX-OS Release 6.0(2)U2(1) introduces software error recovery (SER) for soft errors in the internal memory tables of the forwarding engine. This feature is enabled by default.

The forwarding engine internal control tables and packet memories are protected through various mechanisms such as error-correcting code (ECC), parity protection, or software scan based parity check of the tables. Software caches are maintained for most of the hardware tables. Parity and ECC errors are detected when the traffic hits the affected entries. For ternary content addressable memories (TCAMs), an error is detected when the CPU compares the software shadow entries to the hardware entries. When any of these types of errors are detected, an interrupt is generated to report an error for that memory.

The correction mechanism is different for different hardware tables. For hardware tables that have a software shadow, the affected entry is copied from the software cache and the interrupt is cleared. Hardware tables, such as the Layer 3 host lookup table and the ACL TCAM tables, are detected and corrected in this way. For hardware tables that do not have a software shadow, the affected entry is cleared or zeroed out. Hardware tables, such as the hardware-learned Layer 2 entry table, and the counters' memory are detected and corrected in this way.

When a parity error is encountered in the hardware in the forwarding lookup for the packet, the packet is subject to a drop depending on the table encountering the parity error. The recovery time from the parity error

detection to correction, in this case, for an entry can be over 600 microseconds. If the traffic is hitting this entry, there will be traffic loss for this duration.

For TCAM tables that do not have parity protection, a periodic software scan is done for the table entries to detect parity errors. In case of parity error detection, the system copies the affected memory location from the software shadow to correct the error. Software initiated scan is done every 10 seconds with 4,000 entries scanned per interval. There are about 36,000 TCAM entries to be scanned in the forwarding engine. In the worst case scenario, it can take over 90 seconds for parity error detection and correction for these tables, the recovery time is based on the system load.

In case of unrecoverable parity errors, the software generates a syslog event notification as shown in the following example:

```
2013 Nov 14 12:37:32 switch %USER-3-SYSTEM_MSG: bcm_usd_isr_switch_event_cb_log:658: slot_num
 0, event 2, memory error type: Detection(0x1), table name: Ingress ACL result
table(0x830004b5), index: 1790  - bcm_usd
```

Verifying Memory Table Health

To display a summary of parity error counts encountered in ASIC memory tables, run the following command:

Command	Purpose
show hardware forwarding memory health summary	Displays a summary of parity error counts in ASIC memory tables.

Example

The following example shows how to display a summary of parity error counts in ASIC memory tables:

```
switch# show hardware forwarding memory health summary
Parity error counters:
Total parity error detections: 7
Total parity error corrections: 7
Total TCAM table parity error detections: 1
Total TCAM table parity error corrections: 1
Total SRAM table parity error detections: 6
Total SRAM table parity error corrections: 6
Parity error summary:
Table ID: L2 table      Detections: 1   Corrections: 1
Table ID: L3 Host table Detections: 1   Corrections: 1
Table ID: L3 LPM table  Detections: 1   Corrections: 1
Table ID: L3 LPM result table   Detections: 1   Corrections: 1
Table ID: Ingress pre-lookup ACL result table   Detections: 1   Corrections: 1
Table ID: Ingress ACL result table      Detections: 1   Corrections: 1
Table ID: Egress ACL result table       Detections: 1   Corrections: 1
```