WHITE PAPER

GENERIC ONLINE DIAGNOSTICS ON THE CISCO CATALYST 6500 SERIES SWITCH

INTRODUCTION

The Cisco® Catalyst® 6500 Series, the Cisco Systems® flagship modular LAN switch, delivers highly available and secure converged network services throughout enterprise and service provider networks. Although high-availability and reliability features are primary integrated technologies on the Cisco Catalyst 6500 Series, the platform also offers another integral component to delivering maximum uptime: fault detection. When anomalies in a system are identified, fault-detection mechanisms trigger fault-recovery mechanisms. Keepalives can be used as a general means for intersystem fault detection. However, an internal resiliency mechanism is also needed in order to guarantee that a given running system is healthy. This function has converged into a generic diagnostics framework known as Generic Online Diagnostics, or GOLD. With the GOLD functions integrated on the Cisco Catalyst 6500 Series, the platform goes one step further in delivering highly available networks.

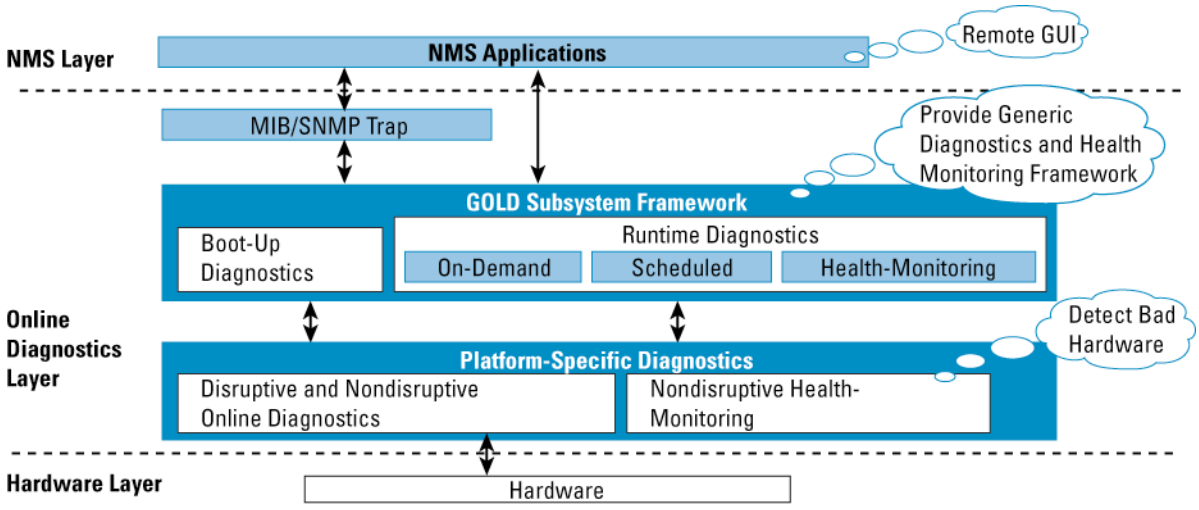
This paper provides information about GOLD on the Cisco Catalyst 6500 Series. It begins with an overview of GOLD and then covers the main diagnostic mechanisms available on the Cisco Catalyst 6500 Series. Although GOLD implements many mechanisms to ensure that a unit is healthy, this paper does not provide an exhaustive list of diagnostics tests available on the Cisco Catalyst 6500 Series. GOLD was integrated on the Cisco Catalyst 6500 Series in Supervisor Engine 2 Cisco IOS® Software Release 12.1(13)E and 12.2(17d)SXB and in the Supervisor Engine 720 Cisco IOS Software Release 12.2(14)SX. Later releases on the Cisco Catalyst 6500 Series increase diagnostic coverage with more tests.

OVERVIEW OF GOLD

GOLD Framework

GOLD defines a common framework for diagnostics operations across Cisco platforms running Cisco IOS Software. Figure 1 illustrates the GOLD framework and how it interacts with platform-dependant diagnostics operations and network-management systems.

Figure 1. GOLD Framework



The GOLD framework specifies the platform-independent fault-detection architecture for centralized and distributed systems. This includes the common diagnostics CLI and the platform-independent fault-detection procedures for boot-up and runtime diagnostics. The platform-specific diagnostics provide hardware-specific fault-detection tests and take appropriate corrective action in response to diagnostics test results. Given that much of the forwarding intelligence in the Cisco Catalyst 6500 Series is hardware-based, testing the hardware functions regularly is critical.

Diagnostics Operations

The GOLD implementation checks the health of hardware components and verifies proper operation of the system data and control planes. Some tests take effect when the system is booting up, whereas other tests take effect when the system is operational. As shown in Figure 1, tests are categorized into two categories: boot-up diagnostics and runtime diagnostics. Multiple tests can run in parallel.

Boot-Up Diagnostics

A booting module goes through a series of checks before coming online. This allows the system to detect faults in the hardware components at boot-up time and helps ensure that a failing module is not introduced in a live network.

When boot-up diagnostics detects a diagnostics failure on a Cisco Catalyst 6500 Series, the failing modules are shut down. The administrator can configure the level of boot-up diagnostics to be minimal, complete, or disabled. Though complete diagnostics is recommended, the default on the Catalyst 6500 Series is to run minimal diagnostics, allowing the system to come online faster. The boot-up diagnostics level CLI is as follows:

```
Router (config)#diagnostic bootup level ?
  complete Complete level
  minimal Minimal level
```

Runtime Diagnostics

Defects are also diagnosed during system operation or runtime. A series of diagnostics checks can be enabled to determine the condition of an online system. Care must be taken to distinguish between disruptive and nondisruptive diagnostics tests. Although nondisruptive tests occur in the background and do not affect the system data or control planes, disruptive tests do affect live packet flows and should be scheduled during special maintenance windows. The **`show diagnostic content module`** CLI output displays test attributes such as disruptive or nondisruptive tests (refer to the configuration in the section “Supervisor Engine 720 Diagnostics Coverage”).

The impact of disruptive tests is usually minimal, with tests taking in the order of seconds to complete. Note, however, that extensive memory tests can take several hours to complete. Few runtime diagnostics tests are enabled by default. The main reason behind this decision is to avoid unnecessary testing: customers running exclusively IPv4 traffic in their network do not need to have IPv6 and Multiprotocol Label Switching (MPLS) hardware functions tested. Examples of such MPLS- and IPv6-specific tests for the Supervisor Engine 720 include TestMplsFibShortcut and TestIPv6FibShortcut. For a complete list of tests enabled on the Supervisor Engine 720, refer to the section “Supervisor Engine 720 Diagnostics Coverage.” It is the administrator’s responsibility to enable more diagnostics tests if deemed necessary.

Runtime diagnostics checks can be run on demand, can be scheduled to run at a specific time, or can run continually in the background:

- *Health-monitoring diagnostics tests*
  - Health-monitoring diagnostics tests are nondisruptive, and they run in the background while the system is in operation. The role of online diagnostics health monitoring is to proactively detect hardware failures in the live network environment and inform appropriate entities of a failure. It is up to the administrator to determine the number of health-monitoring checks to run and the interval at which to run them. Health-monitoring tests do not affect system performance. However, software restricts the health-monitoring interval to a minimum threshold to prevent affecting the CPU performance. Upon detecting several consecutive failures, health-monitoring diagnostics can reset a module. By default, health-monitoring tests include data- and control-plane verification, as well as proper function of hardware registers. The output of the **`show diagnostics content`** CLI gives an exhaustive list of health-monitoring tests: all tests marked as nondisruptive (N) can be configured to run as health-monitoring tests. For example, the following CLI schedules an inband ping test

(test number 2) on a supervisor in slot 5 every 15 seconds. Notice that the inband test in the following CLI output is test 2. The mapping to test number can be obtained by typing a "?".

```
Router(config)#diagnostic monitor interval module 5 test ?
Router(config)#diagnostic monitor interval module 5 test 2 00:00:15 0 0
```

- *On-demand diagnostics*
  - An administrator issuing a **diagnostic start** command triggers on-demand diagnostics tests statically. An administrator can specify how many times a test runs and whether to continue running the test upon failure detection. On-demand diagnostics is useful primarily as a troubleshooting tool to verify hardware functions when an administrator suspects a hardware fault. Note that on-demand diagnostics does not cause the faulty hardware to reset or power down the Cisco Catalyst 6500 Series. Syslog messages warn about the faulty hardware, and the administrator needs to check the diagnostics results to see if the tests passed or failed and take appropriate action. As an example, the following command triggers two on-demand module memory tests (test number 12) on a module in slot 2. If the first memory test fails, no further testing is performed.

```
Router#diagnostic ondemand iterations 2
Router#diagnostic ondemand action-on-failure stop
Router#diagnostic start module 2 test ?
Router#diagnostic start module 2 test 12
```

- *Scheduled diagnostics*
  - Scheduled diagnostics tests run at either one specific time or periodically. This can be especially useful when scheduling disruptive tests during maintenance windows. When failures are detected, appropriate syslog messages are displayed; diagnostics results can be accessed by issuing the **show diagnostic result** command on the switch. Scheduled diagnostics does not cause the faulty hardware to reset or power down the Cisco Catalyst 6500 Series. The following CLI schedules a loopback test (test number 1) on a module situated in module 2 every Monday at 3 a.m.:

```
Router(config)#diagnostic schedule module 2 test ?
Router(config)#diagnostic schedule module 2 test 1 weekly MON 03:00
```

Diagnostics Results

GOLD collects diagnostics results and detailed statistics for all tests: last execution time, first and last test pass time, first and last test failure time, total run count, total failure count, consecutive failure count, and error code. These test results help administrators determine the condition of a system and understand the reason for a system failure. Diagnostics results can be viewed by issuing the **show diagnostic result** command on the switch.

Platform-dependant software helps ensure that the system takes specific actions following the discovery of a fault. On the Cisco Catalyst 6500 Series, appropriate syslog messages are displayed on the console or terminal to inform an administrator of a failure. Failures are classified into minor and major failures. For minor failures, the error is reported with a syslog message. Major failures are also reported by syslog messages, and may also result in a module being powered down. The following is an example of a syslog message displayed upon detection of an error:

```
%DIAG-SP-3-MAJOR: Module 2: Online Diagnostics detected a Major Error. Please use 'show diagnostic
Module 2' to see test results.
```

At the hardware level, a module that does not pass boot-up diagnostics is not brought online, and a module that is detected to be in an unstable condition in a running system can be powered down. This applies to supervisors as well: if the software detects a fault in the active or standby supervisor, it can bring the supervisor down. Note that a port failure does not necessarily cause a module to reset or power down. At a minimum, the software disables a faulty port.

GOLD Applications

GOLD reduces the MTTR by monitoring systems and identifying hardware and software faults proactively.

Boot-up diagnostics declares a module “online” only if it passes boot-up diagnostics: this helps ensure that a system is put into a live network only if it is healthy.

Nondisruptive tests are useful high-availability switchover triggers. Fault-detection diagnostics mechanisms are enabled on an active and a standby supervisor. With GOLD integration on the Cisco Catalyst 6500 Series, switchover triggers are not limited to software exceptions. Instead, switchovers can be triggered when the control and data paths of the supervisor are inconsistent or faulty, or when a piece of hardware is detected to be malfunctioning. In addition to helping trigger switchover decisions, diagnostics regularly monitors the standby supervisor to make sure that it is ready to take over if the need to switch over occurs. Diagnostics also integrates a feature that allows scheduling of switchovers: an administrator can schedule a switchover at a specific time through the online diagnostics CLI.

When coupled with the stateful-switchover (SSO) mechanism between supervisors, the Cisco Catalyst 6500 Series can achieve availability close to 100-percent. GOLD is also SSO-aware: diagnostics test results are synchronized between an active and a standby supervisor. This helps troubleshoot problems upon switchover and helps ensure that diagnostics results are not lost upon switchover.

GOLD can detect the following problems: faulty hardware components, faulty connectors, faulty interfaces, faulty memory, and inconsistencies that cause the data and control paths to be erroneous. GOLD also can detect software misbehaviors or failures. These problems can be detected at boot-up time and in a live environment.

GOLD is a very powerful troubleshooting tool for customers and technical assistance to differentiate between software faults and hardware faults. If a hardware fault is to blame, the Return Materials Authorization (RMA) process can be handled effectively.

CISCO CATALYST 6500 SERIES DIAGNOSTICS COVERAGE

Each of the platforms using GOLD must define its own hardware tests to check consistency and functions of the hardware components. This is referred to as platform-specific diagnostics. The Cisco Catalyst 6500 Series provides specific tests to verify the functions of hardware components. These tests are implemented using packet-switching tests.

The Cisco Catalyst 6500 Series diagnostics tests cover specific hardware components and are tied very closely to the Cisco Catalyst 6500 Series architecture. An example of these tests is based on the Supervisor Engine 720 and the WS-X6748-GE-TX architecture. However, the same logic applies to any of the other Cisco Catalyst 6500 Series modules. Although it is not a goal of this paper to cover all the Cisco Catalyst 6500 Series-related test scenarios, all diagnostics tests are important because they each cover a specific hardware component.

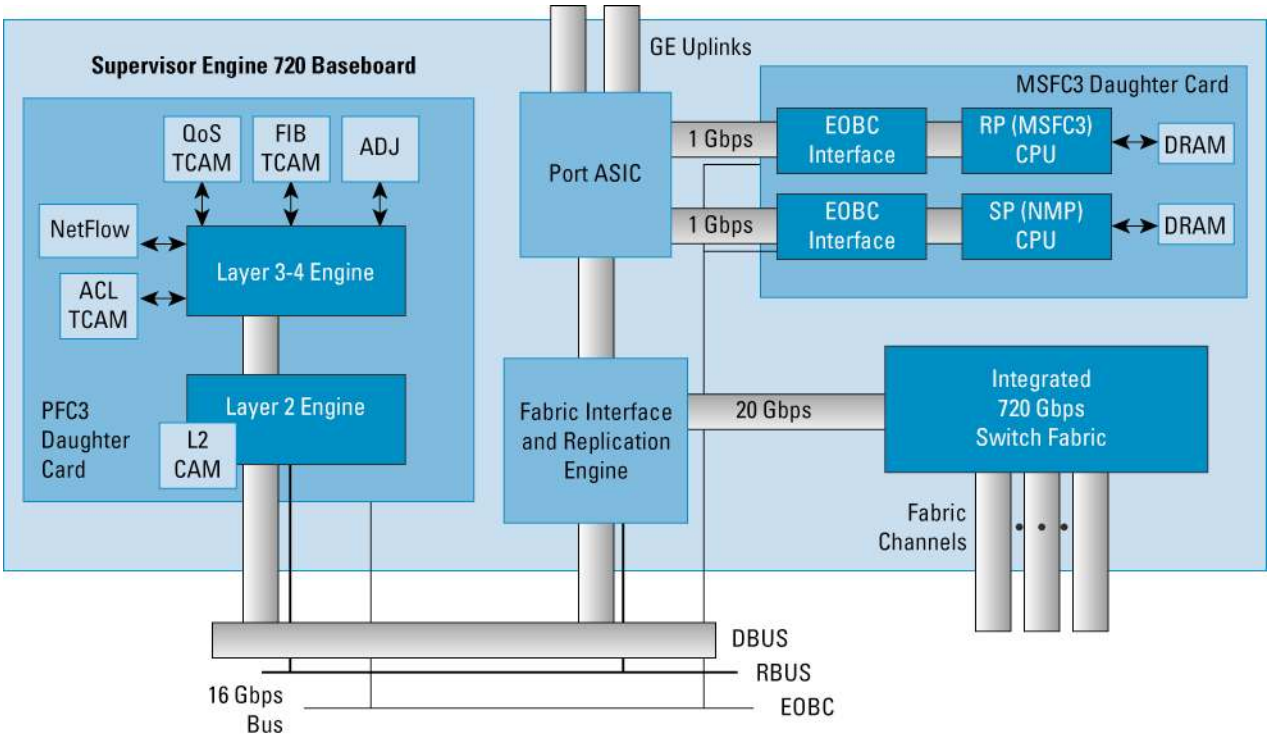
The following sections categorize diagnostics tests for the Cisco Catalyst 6500 Series to help you decide which tests to run.

Supervisor Engine 720 Diagnostics Coverage

Figure 2 illustrates the Supervisor Engine 720 architecture. The Supervisor Engine 720 consists of:

- A policy feature card (PFC3) that contains a Layer 2 and a Layer 3–4 engine; these engines are responsible for hardware switching functions
- A Multilayer Switching Feature Card (MSFC3) that contains the route processor and the switch processor
- An integrated switch fabric that provides dedicated data-plane bandwidth to each of the Cisco Catalyst 6500 Series slots
- A fabric interface and replication engine that provide the interface connection to the switch fabric and the hardware multicast and Switched Port Analyzer (SPAN) capabilities
- A port application-specific integrated circuit (ASIC) that provides port-related functions and bandwidth to uplink ports and CPUs

Figure 2. Supervisor 720 Architecture



The Supervisor Engine 720 main components are tested by online diagnostics. The following output is a list of the 30 diagnostics tests available on a Supervisor Engine 720 in Cisco IOS Software Release 12.2(18)SXD. Notice that many of listed tests mention the components shown in the Supervisor Engine 720 architecture diagram. The **`show diagnostics content module`** CLI output displays the diagnostics tests available for a particular module:

```
Sup720#show diagnostic content module 5
Module 5:
  Diagnostics test suite attributes:
    M/C/* - Minimal bootup level test / Complete bootup level test / NA
      B/* - Basic ondemand test / NA
    P/V/* - Per port test / Per device test / NA
    D/N/* - Disruptive test / Non-disruptive test / NA
      S/* - Only applicable to standby unit / NA
      X/* - Not a health monitoring test / NA
      F/* - Fixed monitoring interval test / NA
      E/* - Always enabled monitoring test / NA
      A/I - Monitoring is active / Monitoring is inactive
      R/* - Power-down line cards and need reset supervisor / NA
      K/* - Require resetting the line card after the test has completed / NA

                                                    Testing Interval
  ID   Test Name                           Attributes   (day hh:mm:ss.ms)
  ==== ================================== ============ =================
    1) TestScratchRegister -------------> ***N****A**  000 00:00:30.00
    2) TestSPRPInbandPing --------------> ***N****A**  000 00:00:15.00
    3) TestTransceiverIntegrity --------> **PD****I**  not configured
    4) TestActiveToStandbyLoopback -----> M*PDS***I**  not configured
    5) TestLoopback --------------------> M*PD****I**  not configured
    6) TestNewIndexLearn ---------------> M**N****I**  not configured
    7) TestDontConditionalLearn --------> M**N****I**  not configured
    8) TestBadBpduTrap -----------------> M**D****I**  not configured
    9) TestMatchCapture ----------------> M**D****I**  not configured
   10) TestProtocolMatchChannel --------> M**D****I**  not configured
   11) TestFibDevices ------------------> M**N****I**  not configured
   12) TestIPv4FibShortcut -------------> M**N****I**  not configured
   13) TestL3Capture2 ------------------> M**N****I**  not configured
   14) TestIPv6FibShortcut -------------> M**N****I**  not configured
   15) TestMPLSFibShortcut -------------> M**N****I**  not configured
   16) TestNATFibShortcut --------------> M**N****I**  not configured
   17) TestAclPermit -------------------> M**N****I**  not configured
   18) TestAclDeny ---------------------> M**D****A**  000 00:00:05.00
   19) TestQoSTcam ---------------------> M**D****I**  not configured
```

Health monitoring

Per-port tests

PFC Layer 2 engine tests

PFC Layer 3–4 engine tests

```
   20) TestL3VlanMet ------------------> M**N****I**  not configured
   21) TestIngressSpan ----------------> M**N****I**  not configured   Replication engine tests
   22) TestEgressSpan -----------------> M**N****I**  not configured
   23) TestNetflowInlineRewrite --------> C*PD****I**  not configured   Per-port tests
   24) TestFabricSnakeForward ----------> M**N****I**  not configured   Fabric tests
   25) TestFabricSnakeBackward ---------> M**N****I**  not configured
   26) TestFibTcamSSRAM ----------------> ***D****IR*  not configured
   27) TestAsicMemory ------------------> ***D****IR*  not configured   Memory tests
   28) TestAclQosTcam ------------------> ***D****IR*  not configured
   29) TestNetflowTcam -----------------> ***D****IR*  not configured
   30) ScheduleSwitchover --------------> ***D****I**  not configured   Switchover schedule
```

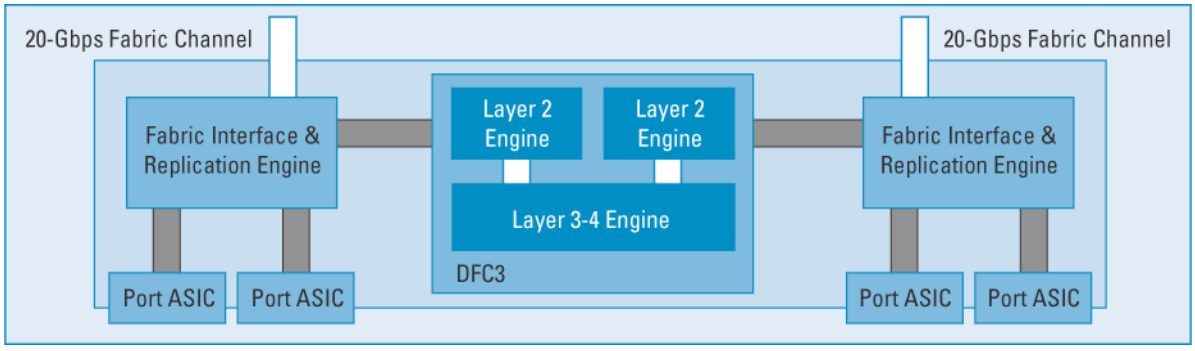
In this CLI output, some of the test procedures are disruptive (entries marked with D), and some are nondisruptive (entries marked with N). Nondisruptive tests are candidate health-monitoring tests. You can also notice which tests occur at boot-up time when the switch is configured in minimal (entries marked with M) or complete (entries marked with C) boot-up diagnostics level. Tests can be broken down into test categories listed on the right side. These categories were added to help administrators understand how these tests apply to the supervisor architecture. An explanation for these test categories is provided in the "Main Diagnostics Coverage" section later in this document.

WS-X6748-GE-TX Diagnostics Coverage

Figure 3 illustrates the WS-X6748-GE-TX architecture. It comprises:

- A fabric interface and replication engine that provide the interface connection to the switch fabric and the multicast and SPAN capabilities
- Port ASICs that provide port functions
- A central forwarding card (CFC) that provides the interface to the shared system bus for central replication capabilities or an optional distributed forwarding card 3 (DFC3) that contains a Layer 2 and a Layer 3–4 engine responsible for hardware switching functions

Figure 3. WS-X6748-GE-TX with WS-F6700-DFC3 Architecture



Most module components are tested by online diagnostics. The following output is an exhaustive list of the 28 diagnostics tests available on a WS-X6748-GE-TX with WS-F6700-DFC3A in Cisco IOS Software Release 12.2(18)SXD. The reader can recognize the same components as listed on the WS-X6748-GE-TX architecture diagram. The output of the **`show diagnostics content module`** CLI is given for a module that carries a WS-F6700-DFC3A.

```
Sup720#show diagnostic content module 7

Module 7:

  Diagnostics test suite attributes:
    M/C/* - Minimal bootup level test / Complete bootup level test / NA
      B/* - Basic ondemand test / NA
    P/V/* - Per port test / Per device test / NA
    D/N/* - Disruptive test / Non-disruptive test / NA
      S/* - Only applicable to standby unit / NA
      X/* - Not a health monitoring test / NA
      F/* - Fixed monitoring interval test / NA
      E/* - Always enabled monitoring test / NA
      A/I - Monitoring is active / Monitoring is inactive
      R/* - Power-down line cards and need reset supervisor / NA
      K/* - Require resetting the line card after the test has completed / NA

                                                    Testing Interval
  ID   Test Name                           Attributes   (day hh:mm:ss.ms)
  ==== ================================== ============ =================
1) TestLoopback --------------------> M*PD****I**  not configured        Per-port tests
   2) TestScratchRegister -------------> ***N****A**  000 00:00:30.00   Health monitoring
   3) TestTxPathMonitoring ------------> M**N****A**  000 00:00:02.00
   4) TestDontLearn -------------------> C**D****I**  not configured
   5) TestConditionalLearn ------------> M**D****I**  not configured
   6) TestNewLearn --------------------> C**D****I**  not configured
   7) TestStaticEntry -----------------> C**D****I**  not configured   DFC Layer 2 engine tests
   8) TestIndexLearn ------------------> C**D****I**  not configured
   9) TestCapture ---------------------> C**D****I**  not configured
  10) TestTrap ------------------------> C**D****I**  not configured
  11) TestMacNotification -------------> M**N****A**  000 00:00:15.00   Health monitoring
  12) TestFibDevices ------------------> M**D****I**  not configured
  13) TestIPv4FibShortcut -------------> M**D****I**  not configured
  14) TestIPv6FibShortcut -------------> M**D****I**  not configured
  15) TestL3HealthMonitoring ----------> ***N****A**  000 00:00:05.00   DFC Layer 3–4 engine tests
  16) TestNATFibShortcut --------------> M**D****I**  not configured
  17) TestMPLSFibShortcut -------------> M**D****I**  not configured
```

18) TestL3Capture ------------------> C**D****I**	not configured	Replication engine tests
19) TestL3VlanMet ------------------> M**D****I**	not configured	
20) TestIngressSpan ----------------> M**D****I**	not configured	
21) TestEgressSpan -----------------> M**D****I**	not configured	
22) TestAclPermit ------------------> M**D****I**	not configured	DFC Layer 3–4 engine tests
23) TestAclDeny --------------------> C**D****I**	not configured	
24) TestQos ------------------------> M**D****I**	not configured	
25) TestNetflowShortcut -------------> M**D****I**	not configured	
26) TestLinecardMemory --------------> ***D****I*K	not configured	Memory tests
27) TestEobcStressPing --------------> ***D****I**	not configured	Stress tests
28) TestFibTcamSSRAM ----------------> ***D****I*K	not configured	Switchover schedule

Looking closely at CLI output, one can distinguish the same test categories as specified in the section “Supervisor Engine 720 Diagnostics Coverage.” Note that the DFC-related categories would not show up if the module did not have a DFC.

Main Diagnostics Coverage

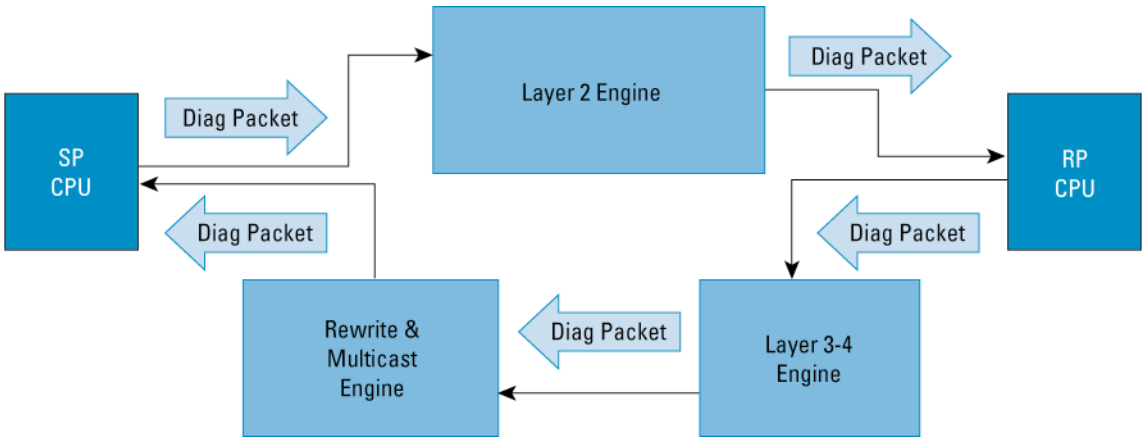
The test categories specified in the Supervisor Engine 720 and the WS-X6748-GE-TX Diagnostics coverage sections are listed as follows along with a short description:

- *Health-monitoring tests*—Health-monitoring tests run in the background. On a Supervisor Engine 720, the TestInbandSPRPing and TestScratchRegister, which are enabled by default, play an important role in fault detection. The TestTxPathMonitoring is enabled by default on the WS-X6748-GE-TX module.
  - The TestInbandSPRPing verifies the control and data path between the switch processor and the route processor through the forwarding engine using pings. “Inband” refers to the internal data-path communication through the port ASIC and the fabric interface, as opposed to Ethernet out-of-band channel (EOBC). This test is different from the regular heartbeat test between the switch processor and route processor that only uses the EOBC. By default, the test runs every 15 seconds, and 10 consecutive failures are treated as fatal, initiating a supervisor switchover. Note that the route processor-switch processor ping test is skipped at high traffic or CPU usage.
  - The TestScratchRegister is also enabled by default. It monitors the health of ASICs by writing values into registers and reading back values from registers. Tests run periodically every 30 seconds, and five consecutive failures are treated as fatal, leading to supervisor switchover.
  - The TestTxPathMonitoring monitors the data and control paths between a module and the active supervisor.
  - The TestMacNotification verifies the data and control paths between modules and supervisors. It also helps ensure MAC address table consistency across Layer 2 MAC address tables in a system.
- *PFC and DFC Layer 2 tests*—These tests cover the proper Layer 2 engine lookup operations. They comprise MAC address learning, capture, and other Layer 2 function-related tests. Note that the TestMacNotification is enabled by default on the WS-X6748-GE-TX with a DFC. The TestMacNotification is a nondisruptive health-monitoring test.
- *PFC and DFC Layer 3–4 engine tests*—These tests cover the proper Layer 3–4 engine lookup operations. Access control lists (ACLs), quality of service (QoS), NetFlow, and Forwarding Information Base (FIB) functions are covered. The adjacency table function is also covered by the FIB-related tests. Some tests are feature- or protocol-specific; for example, one can pinpoint IPv4-, IPv6-, or MPLS-specific tests in the CLI output. In general, the tests program diagnostics entries or shortcuts in the hardware using reserved addresses and make sure the shortcuts are operational.
- *Port ASIC functions*—These tests cover the port ASICs and transceivers. Loopback tests verify the data path between the processors, the forwarding engine, and the port ASIC by putting a port in loopback mode. Loopback tests can be disruptive or nondisruptive, depending on the modules. However, disruptive loopback tests complete in the order of one second. Inline rewrite tests verify the Layer 2 rewrite functions of port ASICs.
- *Fabric tests*—These tests cover the proper operation of the active and standby fabric. This is done by testing the switching ability from one fabric channel to another fabric channel and the data path between the forwarding engine and the fabric interface.

- *Replication engine tests*—These tests verify the SPAN, central-rewrite, and multicast-replication capabilities of the hardware.
- *Memory tests*—A malfunctioning memory can cause forwarding error or data corruption. Two types of memory tests are provided: memory error correlation tests and extensive memory tests. Nondisruptive memory tests monitor excessive cyclic redundancy check (CRC), error checking and correction (ECC), fabric, or forwarding errors to make fault-detection decisions. Extensive buffer, synchronous static RAM (SSRAM), and ternary content addressable memory (TCAM) memory tests are disruptive and time-consuming because they can take hours to complete. Proper care should be taken before running such tests in a live environment. Refer to the following document for recommendations about how to run these tests: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/diags.htm - wp1040287.
- *Stress tests*—Stress tests are disruptive tests that stress the control and data planes to verify proper functioning.
- *Schedule Switchover feature*—This feature allows an administrator to schedule supervisor switchover.

Figure 4 shows a graphical illustration of the switch processor-route processor inband ping test (TestInbandSPRPing). The figure should help an administrator understand how the data and control paths can be effectively tested in the background by diagnostics packets.

Figure 4. Switch Processor-Route Processor In-Band Ping Test



A diagnostic packet is sent from the switch processor to the route processor through the Layer 2 engine. The diagnostics packet is sent back to the switch processor using the Layer 3–4 engine and the rewrite and multicast engine functions. This test reveals faulty ASICs, faulty connectors, and software faults.

Note that the categories cited previously are not extensive. More diagnostics tests are available, and more are being implemented. Diagnostics tests also are not exclusive to supervisors and modules. Health-monitoring capabilities also are implemented for power supplies, fan trays, temperature, and other Cisco Catalyst 6500 Series-related components. An embedded event manager also extends health-monitoring capabilities to various software and hardware threshold parameters.

Summary

Experience has shown that boot-up and runtime diagnostics are both very effective ways of detecting hardware and software defects. Boot-up diagnostics has proven to detect faulty connector issues, badly seated daughter cards, faulty ports, and faulty modules; and health-monitoring tests have proven to detect software, memory, and other hardware component-related issues.

Together with platform-specific online diagnostics, GOLD provides resilient fault-detection mechanisms. GOLD is thus a very important integrated part of the Cisco Catalyst 6500 Series platform, providing yet another degree of reliability and high-availability protection.

REFERENCES

For complete diagnostics configuration information about the Cisco Catalyst 6500 Series, refer to:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/diags.htm.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

204108.66_ETMG_CC_12.04

Printed in the USA