Testing, Packaging & Shipping Procedures

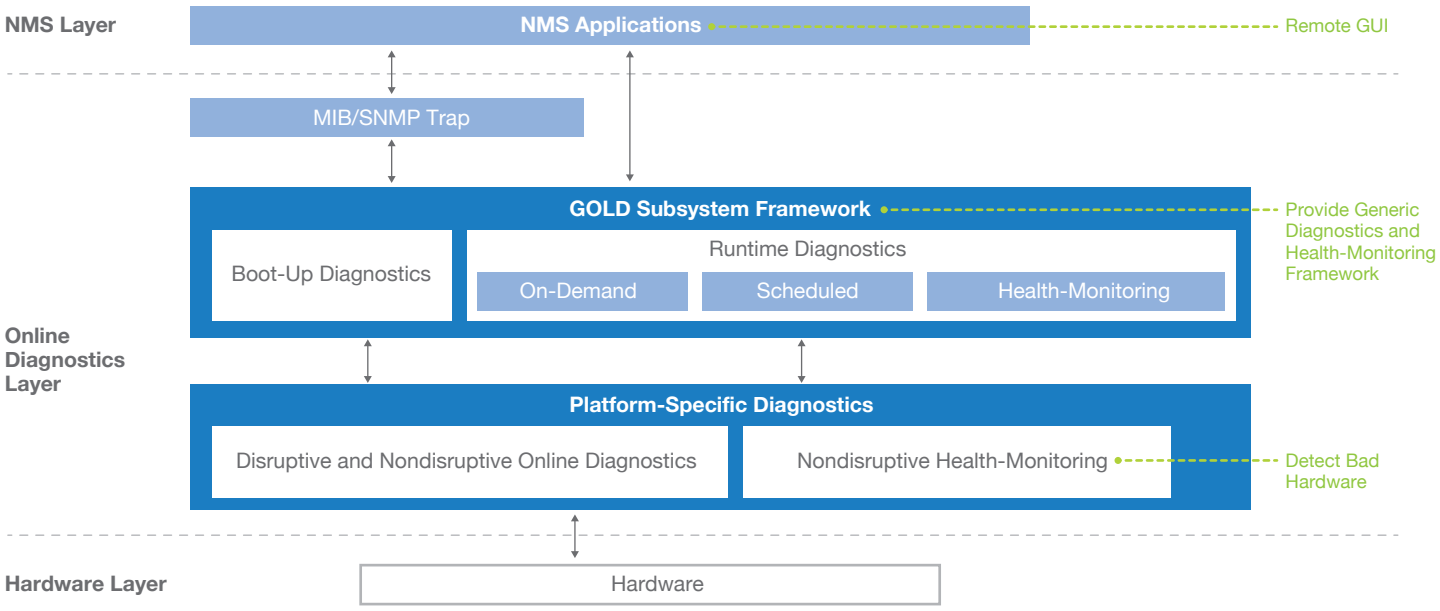
Hula Networks Standard 12 Point Certification Process

We physically inspect all equipment for noticeable damage	Port by port diagnostic testing	Clean chassis and modules from dust and debris
Ensure fans are operational	Restore factory default configurations	Remove any passwords
Live network testing	24 hour stability testing	Test all power supplies
Verify all serial numbers are valid	Verify all chassis are error free	Verify all modules and Interfaces are error free

In addition to the above 12 point Certification Process Hula Networks Inc will perform the following for all orders.

- Verify that all cards are recognized in chassis running on specific IOS.
- Verify that the cards are 100% functional while running specific IOS.
- Verify and use the most recent built card if a build date is available and an option.
- Latest revision available
- Power all DC power supplies with -48v
- Power cycle both power supplies 10 times
- Verify that the LED is green and the chassis boots up
- All cards to be run with the specified software version for a minimum of 48 hours

Line Card Testing



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 no disruptive diagnostics tests. Although no disruptive 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 no disruptive 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 no disruptive, 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 no disruptive (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.

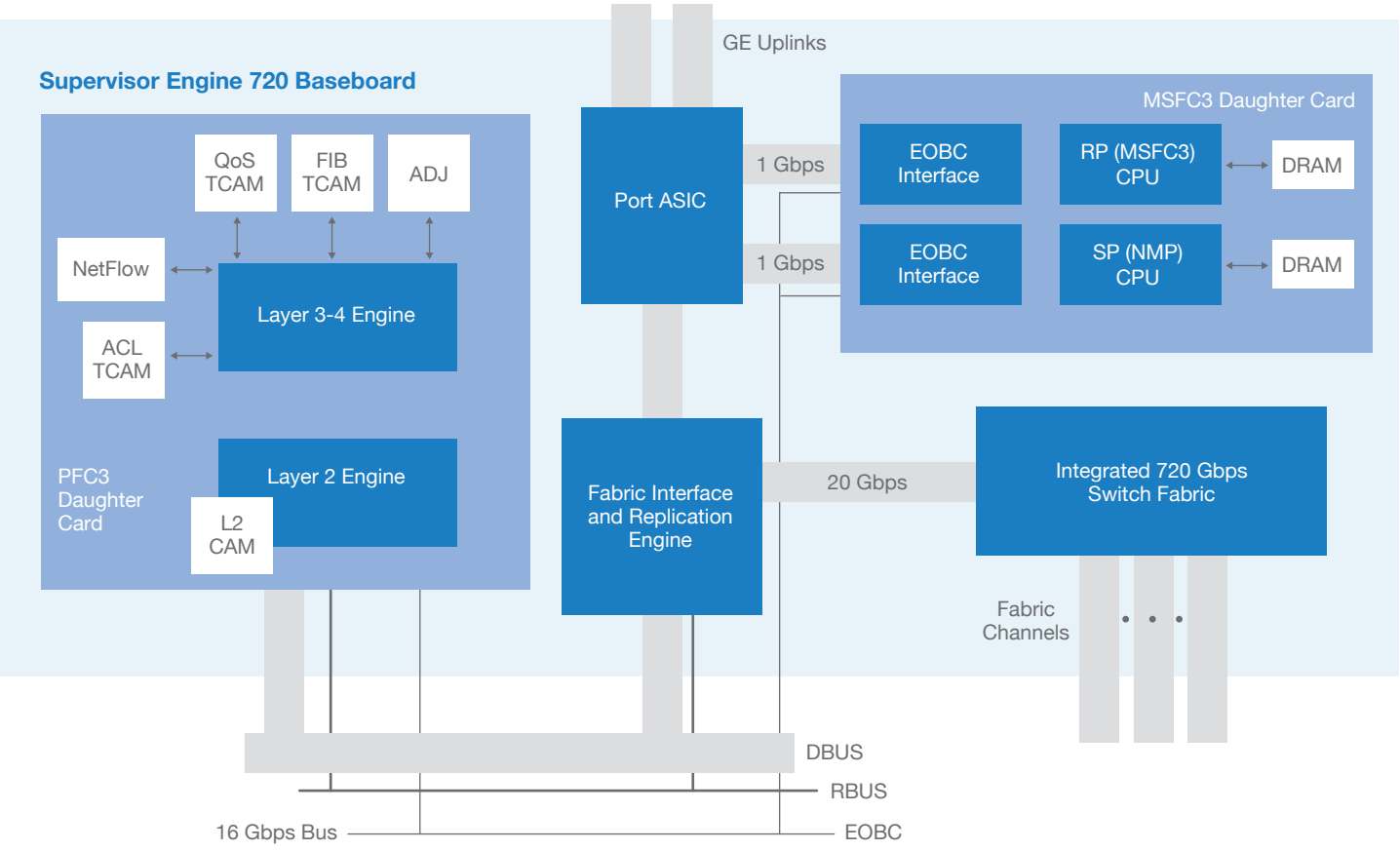
```
Router(config)#diagnostic schedule module 2 test ?
Router(config)#diagnostic schedule module 2 test 1 weekly MON 03:00
```

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

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	Health monitoring
2) TestSPRPInbandPing	***N****A** 000 00:00:15.00	
3) TestTransceiverIntegrity	**PD****I** not configured	Per-port tests
4) TestActiveToStandbyLoopback	M*PDS***I** not configured	
5) TestLoopback	M*PD****I** not configured	
6) TestNewIndexLearn	M**N****I** not configured	PFC Layer 2 engine tests
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	PFC Layer 3-4 engine tests
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	
20) TestL3VlanMet	M**N****I** not configured	Replication engine tests
21) TestIngressSpan	M**N****I** not configured	
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	Memory tests
27) TestAsicMemory	***D****IR* not configured	
28) TestAclQosTcam	***D****IR* not configured	
29) TestNetflowTcam	***D****IR* not configured	
30) ScheduleSwitchover	***D****I** not configured	Switchover schedule

Package Contents

- Verify that rack mount hardware is included.
- Verify that all port adapters are locked in.
- Remove power supplies from chassis. Package separately.
- Verify that a console cable is included with all chassis.

Shipping Guidelines

- Make sure all equipment is shipped in thick double walled cardboard boxes, wrapped in 4-5 layers of bubble wrap, foam popcorn or foam to elevate any open areas for movement in shipping.
- Secure contents so there is absolutely no movement inside the box once sealed up.
- Tip: give a healthy shake to see if contents move within.
- Enclose with at least 2 inches of padding around all sides of units.
- Cards need to be enclosed in a static bag prior to being wrapped in bubble or put in a pizza box.
- Any boxes weighing over 75 lbs. please call or email prior to shipment. Make sure equipment is palletized.
- Multiple items in a box need to be wrapped individually.
- Remove and wrap fans and power units separately to avoid bent handles.
- Include any accessories rack mounts, power and console cables needed.
- New equipment needs to be double boxed. DO NOT tape over Cisco tape or labeling.
- Palletized items need to be boxed and padded between before placing on the pallet.

CORPORATE HEADQUARTERS

Hula Networks
Servicing the Continental US, Canada, Mexico, Latin America and Europe
1153 Tasman Drive
Sunnyvale, CA 94089

Call or Fax

Direct / Local	1.650.625.4100
Toll Free	1.866.485.2638
Fax	1.650.625.4101

Contact your Hula Sales Rep for more details!