# Cisco Catalyst 9000 Switches: Independent Feature Validation

DR171114H

January 2018

Miercom
www.miercom.com

# Contents





Miercom Copyright © 2018

# 1 - Executive Summary

Miercom was engaged by Cisco Systems to independently configure, operate and validate the performance and features of the new Catalyst 9000 switches. The switches tested – the Catalyst 9300, 9400 and 9500 – represent the next generation of Cisco's Catalyst switch line. Although this report does not focus on Software-Defined Access (SD-Access), it is worth noting that the Catalyst 9000 switches are the best platform for Cisco's SD-Access solution.

Tests were conducted in several areas:

- **Higher Availability –** exercising new features including StackWise Virtual pooling of data ports, Graceful Insertion and Removal (GIR), and Software Maintenance Upgrades (SMU).
- **Security, and programming support –** assessing the latest trustworthy system protections, as well as the platforms' model-driven telemetry, and application hosting.
- **Basic Operation & Ease of Use –** examining new aspects of the Catalyst 9000 switches including: RFID for simplifying inventory, 'Blue Beacon' for locating a specific device, and shorter boot-up times.

**Key Findings and Observations:**

- **Solid software**. The proven Cisco IOS XE operating system, which has run for years on the Catalyst 3850, performed flawlessly on the Catalyst 9000 models tested. The Catalyst 9300 also supports Catalyst 3850 uplink modules, power supplies, fans, and cables.
- **Super switch survivability**. Verified sub-second failover high-availability (HA) features, like stateful switch-over (SSO) and non-stop forwarding (NSF), and new HA capabilities tested with the Catalyst 9000 models. New features include Graceful Insertion and Removal (GIR) and in-service software patching. Additional features include: Hot Insertion and Removal of power supplies, fans, even uplink modules while the switch continues to operate (FRU/OIR).
- **Best-in-class Stack support**. Besides redundant and shared-power options, stacked switches can deliver up to 480 Gbps of collective switch bandwidth, and combinable data ports to create a single, virtual switch. StackPower provides pooling of power supplies between members of a stack for redundancy and load-sharing purposes.

- **Other new features**. We verified that collected data could be continually delivered via HTTP in near real-time using Streaming Telemetry. Plus, RFID now makes switch inventory much easier, and the new "Blue Beacon" helps identify and locate specific switches and switch modules. New Security enhancements are provided through ETA (Encrypted Traffic Analytics) which entails the detection of Malware in encrypted traffic without decrypting the traffic, together with 256-bit AES MACSEC encryption across all ports and speeds. Catalyst 9000 switches also supports Application Hosting in a Container or Virtual Machine directly on the switch as well a Netconf/YANG programmable interfaces.

Based on the results of this testing, and in recognition of its significant new features, we proudly award the ***Miercom Performance Verified Certification*** to Cisco's impressive new Catalyst 9000 switches.


Robert Smithers
CEO
Miercom

# 2 - Products Tested

Cisco developed the new Catalyst 9000 switches as its latest answer to network convergence, unprecedented survivability and virtually impenetrable security. The models we tested – the stackable Catalyst 9300, the modular chassis Catalyst 9400 and the aggregation and core Catalyst 9500 switches – all are built with a common ASIC (application-specific integrated circuit): the UADP (Unified Access Data Plane) 2.0, and run the same operating system Cisco IOS XE 16 with a single binary image for all members of the Catalyst 9000 family. For our testing, we used Cisco IOS XE version 16.6.1.

**Catalyst 9300**

Up to eight switches of any Catalyst 9300 model can be stacked, taking advantage of many redundancy options, and yielding up to 384 Power over Ethernet (PoE) access ports and 480 Gbps of local stackable switching bandwidth. Power stacking using Stackpower, facilitates the pooling of power supplies across members for redundancy and efficiency purposes. WiFi support is integrated in the SD-Access fabric and consistent policies can be applied for wired and wireless endpoints.

Source: Cisco

The 9300 models support up to 48 UPoE/PoE/Data/mGig Gigabit Ethernet ports with a variety of uplink modules, including 40G, 10G, mGig and 1G. Migrating from the predecessor Catalyst 3850 to the Catalyst 9300 is straightforward, as the uplink modules, power supplies, stacking cables and power stacking cables are compatible.

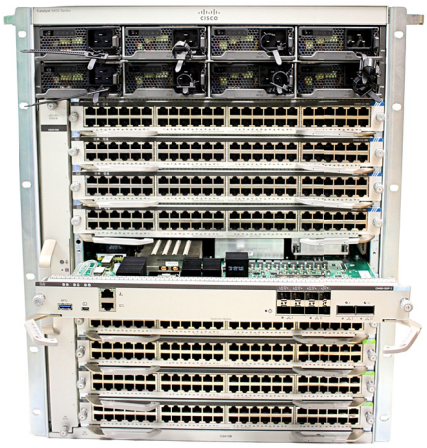
**Catalyst 9400**

The Cisco Catalyst 9400 switch offers two chassis options: a 7-slot and 10-slot, shown below, with a wide range of copper, mGig and Fiber line card options. The system supports five and eight line cards, respectively. It provides a common architecture that can scale up to 392 ports (10-slot chassis).

Source: Cisco


Miercom Copyright © 2018

The Catalyst 9400 chassis features efficient side-to-side airflow and full front access to all removable components, including supervisors, line cards, power supplies and fan tray – shown below. The chassis also supports optional rear access to fan tray.



Source: Miercom

Among other new features, the Catalyst 9400 Series chassis, supervisor modules, line cards, power supplies and fan trays all have embedded RFID tags, which facilitate easy asset and inventory management using commercial RFID readers. This and other new features of the Catalyst 9400 Series are examined and discussed in this report.

**Catalyst 9500**

Three models of the Catalyst 9500 core and aggregation layer switch are offered. A fixed-configuration model, pictured below, supports 24 x 40-Gb QSFP+ fiber-optic ports.

Source: Cisco

A pared-down version, shown below, is also a fixed-configuration model, supporting 12 x 40-Gb QSFP+ fiber-optic ports.

Source: Cisco

The third model, supporting 40 x 10-Gb SFP/SFP+ ports, also accepts one of two uplink modules: an 8 x 10-Gb SFP/SFP+ module or a 2 x 40-Gb QSFP+ module, pictured below.

Source: Cisco

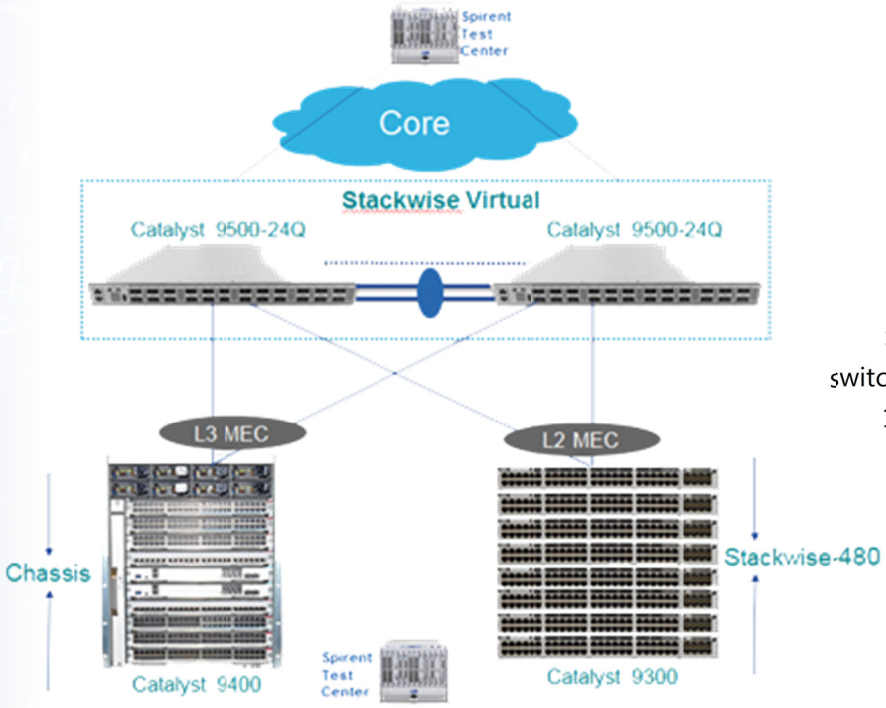

Miercom Copyright © 2018

# 3 - Test Bed: How We Did It

Two different test beds were used due to the nature of the features tested. The first we called the "StackWise Virtual" topology (see diagram). It consisted of Catalyst 9300 and 9400 access switches, and 9500 aggregation and core switches, all connected via failover and redundant/alternate-route links, called Multichassis EtherChannel (MEC), a Layer 2 or Layer-3 multipathing technology.

A Spirent test system generated all traffic and analyzed returned data. Spirent test software version 4.53 was run for all testing except one; version 4.73 of Spirent test software was run for the Multigigabit testing discussed in Section 4.

## Miercom "StackWise Virtual" Test Bed Topology




Switch-to-switch links are 10-Gigabit

Source: Miercom

This test bed was used to exercise and assess these Catalyst 9000 features:

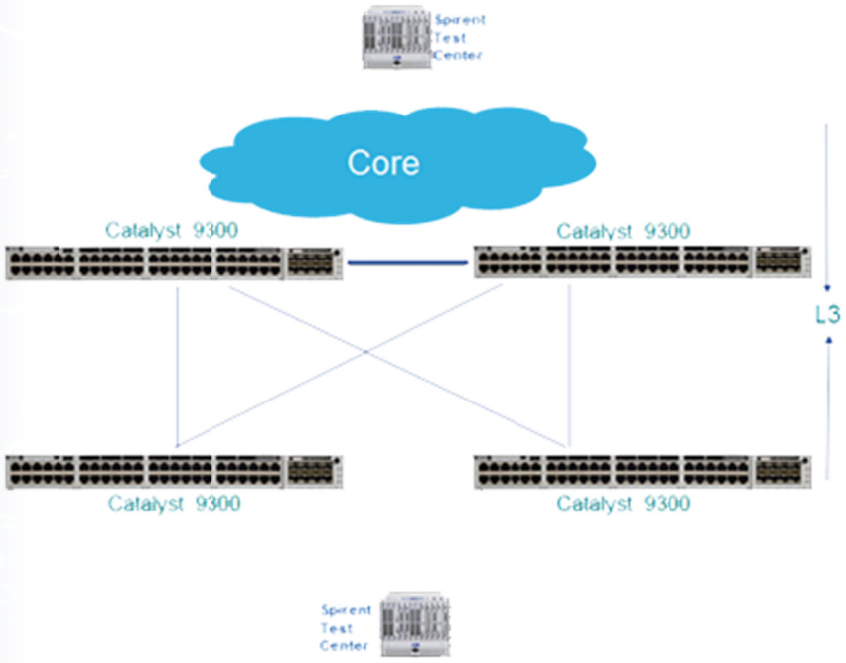
- RFID
- Blue Beacon
- Shorter Boot Times
- Online Insertion and Removal (OIR)
- Multigigabit (mGig) Support
- StackWise Virtual
- StackWise-480
- StackPower*
- Stateful Switchover (SSO)**

* For StackPower testing the latest Cisco IOS XE version 16.6.2 was used. For all other testing Cisco IOS XE 16.6.1 was run.

** Stateful Switchover (SSO) on Catalyst 9400 also uses 16.6.2 software

The second test bed, called the "Routed Access" topology, is shown below. In this case Catalyst 9300 models were deployed for access and intermediate aggregation, and two Catalyst 9500 models for the core. Alternate/failover links were used throughout.

## Miercom "Routed Access" Test Bed Topology




Source: Miercom

This test bed was used to exercise and assess these Catalyst 9000 features:

- WebUI
- Streaming Telemetry
- Software Patching
- Graceful Insertion and Removal (GIR)
- Trustworthy Systems
- App Hosting
- MACsec
- Programming (Python/NetConf/Yang)

The results of testing of these features are individually detailed in the following sections.

# 4 - Basic Operations & Ease of Use

In this category, we exercised newly delivered features with Catalyst 9000 family, as well as other key capabilities Cisco recently implemented in the new Catalyst 9000 switches, to validate that these, too, are supported in the new Catalyst 9000 switches.

In this Basic Operations & Ease of Use section we examined:

- Multigigabit (mGig) Connectivity
- Shorter Boot Times
- RFID
- Blue Beacon
- WebUI

## Multigigabit (mGig) Connectivity

Catalyst 9000 devices support Multigigabit technology, which can deliver data rates up to 10 Gbps over 8-conductor Category 5e (Cat 5e) and higher (Cat6 and 6a) UTP cabling. Data rates supported can be 100 Mbps, 1 Gbps, 2.5 Gbps, 5 Gbps and 10 Gbps – depending on cable type, installation quality and distance. Generally, speeds up to 5 Gbps are supported over Cat 5e cabling, while Cat 6 and Cat 6a support up to 10 Gbps.

New to the Catalyst family is support of 48 mGig ports.

We tested mGig connectivity on the Catalyst 9000 using the mGig models over lengths of Cat 5e and Cat 6a cable. We ran the tests using the Spirent Test Center, changing the mGig card's line rate and the Spirent bi-directional output to match – at 1 Gbps, 2.5 Gbps, 5 Gbps, and 10 Gbps. Each test ran for two minutes. The result: No packets were dropped in any of these tests.

## Shorter Boot Times

It has traditionally taken a while to boot or re-boot a Catalyst switch, even with the Linux-based Cisco IOS XE operating software. Cisco software engineers have worked to reduce that delay with the new Catalyst, with some success.

Using the **reload** command we restarted a Catalyst 9500 switch and carefully measured the time until the system completely rebooted. The result: Total elapsed time for reboot: 3 minutes, 18 seconds. This is notably faster than predecessor Catalyst reboot times.

The reduced boot time was checked and confirmed on all the Catalyst 9000 switches we tested: the Catalyst 9300, 9400 and 9500.

## RFID

Enterprise Campus Networks which use dozens, even hundreds, of Catalyst switches are not uncommon. And so inventory management in large enterprise networks is a time consuming chore. From labeling each device to entering and managing all the particulars in a database, considerable manual labor is involved and highly prone to error.

Keeping track of so many key network components has now been made a little easier. Cisco's solution, new with the Catalyst 9000 product line, is to integrate passive SGTIN (Serialized Global Trade Item Number)-198 bit encoded RFID tags within the Catalyst 9000 chassis, as well as on supervisor, line cards, power supplies and fan trays.

These RFID tags are easily read by commercial RFID readers (like the one shown below) and then readily imported into inventory databases. The tags are integral to the component and not easily removed. Passive RFID tags such as these are powered by the signal from the RFID reader and require no additional power source to be read by such readers. And the device or module does not have to be powered up for the RFID tags to be read.

The RFID tags contain all pertinent device information, including serial number, Product ID and manufacturing date. What's more, the Cisco RFIDs offer a 240-bit user partition, where the customer can store inventory numbers and other customer-specified data, password-protected.

We tested the RFID feature by scanning Catalyst 9400 equipment. With one pull of the RFID scanner trigger from about 6 feet away, all the equipment inventory codes appeared in the scanner. We were then able to load these into a compatible database.


Source: Miercom

*All Catalyst 9400 device-identity data was picked up by this RFID scanner from 10 feet away.*

## Blue Beacon

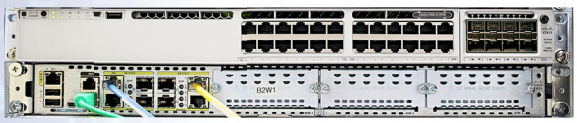
When troubleshooting, configuring or moving equipment in a large enterprise network, it is often difficult to locate the exact device, whether it's rack-mounted or a component within a multi-slot chassis. It can take a few tests, each time checking back with an operator at a management console, to confirm that the device in question has been located and identified.

To resolve this, Cisco has placed a bright blue LED on all members of the new Catalyst 9000 switch family. This blue LED, dubbed the "Blue Beacon," can be turned on and off either via console command for all components, or physically on some components. When turned on, a repeated informational message appears in the machine's syslog. A message also appears when the LED is turned off.

This LED is visible from the end of a row of equipment racks, making it simple and quick to locate and identify a particular device or component. On the modular 9400 switches, the fan tray, supervisors, line-card modules, and power supplies have their own addressable Blue Beacons.

Source: Cisco

*Catalyst 9300 Blue Beacon is ON*



Source: Cisco

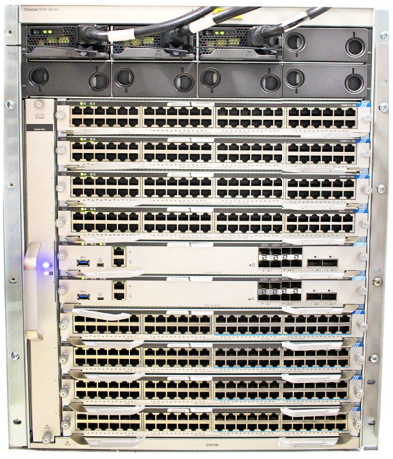
*Catalyst 9300 Blue Beacon is OFF*

A fairly straightforward command-line dialog turns the Blue Beacon on and off. To check beacon status and turn on the Blue Beacon for a Catalyst 9300 switch (Switch 1 in a stack):

```
C9300#show hardware led | incl BEACON
        BEACON: BLACK
C9300#conf t
        C9300(config)#
C9300(config)#hw-module beacon on switch 1
C9300#show hardware led | incl BEACON
        BEACON: BLUE
```

The dialog is similar for a module, in this case a fan tray, in a Catalyst 9400 modular chassis:

```
C9400#hw-module beacon fan-tray ?
        off  Turn off
        on   Turn on
C9400#hw-module beacon fan-tray on
C9400#show hardware led | incl FANTRAY BEACON
        FANTRAY BEACON: BLUE
```



Source: Cisco

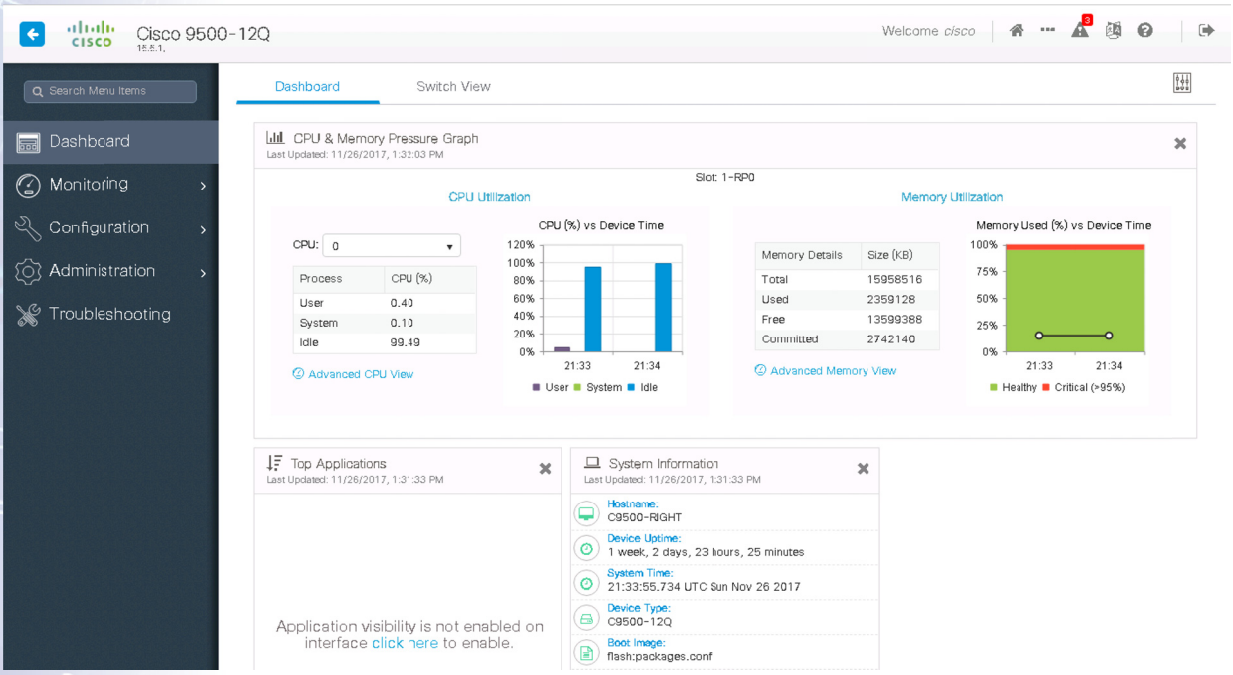
*Catalyst 9400 Blue Beacon is ON – Fan Tray*

## Web User Interface (WebUI)

An alternative to the IOS command line for managing Catalyst 9000 switches is the graphical Web User Interface, or WebUI, which was first introduced in an earlier Cisco IOS XE version. WebUI simplifies device deployment by enabling a user to perform many switch configurations and monitoring operations without IOS command-line expertise.

As shown below, most aspects of switch operation can be monitored via easy-to-read graphics.

The WebUI comes with default images; there is no need to enable anything or install any license on the Catalyst 9000 device. Via the WebUI the user can build configurations and monitor and troubleshoot any Catalyst 9000 device.




Source: Miercom


Miercom Copyright © 2018

# 5 - High Availability

From the results of this testing and in our independent assessment, the combination of redundancy and fail-over capabilities supported by the Cisco Catalyst 9000 switches is unprecedented in the industry.

Power options, including pooled and redundant power supplies, are offered as StackPower capabilities which were delivered with earlier Catalyst switches. The StackWise-480 features, also delivered with earlier Catalyst switches, include pooling of data ports, non-stop forwarding and stateful switchover.

New with the Catalyst 9000 family is StackWise Virtual, which unites two of the same switches into a single logical unit, with especially resilient failover capabilities.

In this High Availability section we examined:

- Power Redundancy and StackPower
- StackWise-480
- StackWise Virtual
- Redundant Fans
- Stateful Switchover (SSO)
- Nonstop Forwarding (NSF

## Power Redundancy & StackPower

### Catalyst 9300

Catalyst 9300 Series switches support dual redundant power supplies. The two power supplies can run in combined or redundant mode. In addition, the Catalyst 9300 Series switches also support StackPower. StackPower interconnects power supplies on the Catalyst 9300, creating a pool of power. Power is budgeted first to 9300 operation and then to active ports. Remaining power is used for the PoE and Universal PoE (UPoE) connections.

Interconnected power supplies can be configured in any of the following two modes:

- **Combined**, where the power from interconnected power supplies is pooled into one power pool for all interconnected switches. Power is prioritized for the switch systems and interface ports and remaining power on the PoE ports.
- **Redundant**, where the highest output power supply is redundant (in standby mode) and backs up any of the several active power supplies.

### Catalyst 9400

Catalyst 9400 (7 and 10 slot chassis) supports 8 slots for power supplies. There are three modes of operation supported by Cisco Catalyst 9400 power supplies:

- **Combined,** where the power from all power supplies is pooled into one power pool in the switch. Power is prioritized for the switch systems and interface ports and remaining power on the PoE ports.
- **Redundant N+1,** where one power supply is redundant (in standby mode) and backs up any of the several active power supplies.
- **N+N Redundant**, where two sets of power supplies are interconnected to act as two independent power


Miercom Copyright © 2018

sources. When failure is detected in the active set, standby will become active. This may be particularly useful when there are two separate external power sources, such as line power and a standby generator. In the event of a line power failure, the standby generator kicks in and the second set of power supplies takes over.

The **show power** command yields a useful display of power and fan states for the entire chassis:

```
C9400 #show power
Power
Fan States
Supply  Model No            Type
Capacity  Status      1    2    3    4
------ -------------------- ----
-------- ------------ ----------
-------------
PS1    C9400-PWR-3200AC AC    3200
W   active      good  good  good  good
PS2    C9400-PWR-3200AC AC    3200
W   active      good  good  good  good
PS3    C9400-PWR-3200AC AC    3200
W   active      good  good  good  good
PS4    C9400-PWR-3200AC AC    3200
W   active      good  good  good  good
PS6    C9400-PWR-3200AC 3200 W
active      good  good  good  good
PS7    C9400-PWR-3200AC AC    3200
W   active      good  good  good  good
PS8    C9400-PWR-3200AC AC    3200
W   active      good  good  good  good

PS Current Configuration Mode :
Combined
Default power mode is Combined
PS Current Operating State  : Combined

Power supplies currently active    : 7
Power supplies currently available : 7


Power Summary       Maximum
(in Watts)    Used    Available
------------- ------ ---------
System Power  1720    1720
Inline Power  0       20680
------------- ------ ---------
Total         1720    22400
```

We varied the configurations of power redundant mode and then selectively disabled power supplies to see that switch operations and line power (PoE) continued without interruption. The displays correctly reflected the status and redundant power-supply configurations. All the power-supply sharing and redundant failover scenarios were tested responded appropriately.

## StackWise-480

Cisco StackWise-480 allows up to eight Catalyst 9300 switches together to be interconnected to form one logical switch with up to 480 Gbps of bandwidth available for inter-switch communication (total bi-directional bandwidth through the switching fabric).

In our test of StackWise-480, we had traffic passing bi-directionally through the complete 9300 stack. We then performed a switchover between active and standby switch nodes. Switchover on switch nodes without uplinks showed no impact on the traffic.

Some traffic was impacted when a switch node with uplinks was switched over. This is because a network state has to be reset on the standby switch after it becomes the active. There are ways of mitigating even this brief disruption: the Catalyst 9300 Series also supports Stateful Switchover (SSO) and Nonstop Forwarding (NSF) with the StackWise-480 as well. These are discussed individually later in this section.

## StackWise Virtual

StackWise Virtual is a stacking technology that is supported in distribution roles. It provides system virtualization at the network layer. The Catalyst 9500 supports StackWise Virtual with a two-node topology. Access and core-layer switches interact with the Stackwise Virtual nodes in distribution as if it were a single logical switch. An access/core switch connects to both switches of the StackWise Virtual switch using a logical port channel called a Multichassis EtherChannel (MEC). The MEC enables StackWise Virtual switches to provide redundancy and load balancing on the port channel.

This capability enables a Layer 2 network topology without loops, since the StackWise Virtual switches are treated as one logical switch from the point of view of both access and core switches. The StackWise Virtual switch also simplifies the Layer-3 network topology by presenting itself as one logical switch, thus reducing the number of (Layer-3) routing peers in the network.

To test StackWise Virtual we cabled together a pair of Catalyst 9500 Series switches, forming a StackWise Virtual switch.

A bi-directional Spirent data stream was then delivered between the systems – that is, traffic was routed through the StackWise Virtual switch.

To simulate a switch failure, the active switch in the virtual pool was shut down and restarted. The standby switch became the active and the traffic proceeded virtually uninterrupted.

The first switch – the original active, now the standby – took approximately 3 minutes to fully reboot. The Spirent Test Center recorded traffic loss in sub-seconds during this active-to-standby transition.

On switching back, by rebooting the now active switch, Spirent recorded similar traffic loss in sub-seconds. The amount of packets lost would depend, of course, on how much data was passing at the time. Still, we observed that, with the Layer-3 resilience offered by the StackWise Virtual configuration (two tightly coupled Catalyst 9500 Series switches), the interruption for a switch failure and failover was sub-second in all scenarios.


Miercom Copyright © 2018

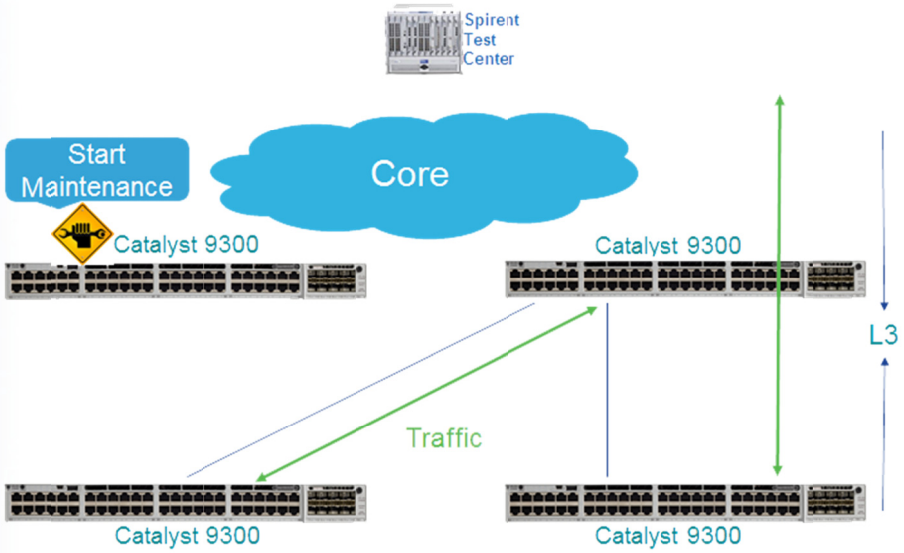
## GIR – Graceful Insertion and Removal

Graceful Insertion and Removal, or GIR, a new capability introduced with the Catalyst 9000 switches, lets the user isolate a node for maintenance, with minimal impact on network operations and traffic flow.

GIR, as shown in the below graphic, is a network-layer High Availability (HA) capability (where IP packets are re-routed via routing control protocols). Patching and In-Service Software Updates, by comparison, can be viewed as application-layer HA capabilities.

With GIR, the specific device or switch is put into maintenance mode via console command. This signals the network to automatically re-route traffic around the switch, so that network traffic continues uninterrupted during the maintenance process. Indeed, about the only impact of GIR on network traffic is that remaining switches will see more traffic – the diverted traffic flows – until the switch maintenance is finished and it is returned into service.

GIR is supported consistently across the Catalyst 9000 product line.




Source: Cisco


Miercom Copyright © 2018

When put in maintenance mode (via the command: **start maintenance**), the switch can be removed and replaced – while the network remains fully functioning and operational.

To test GIR we put one of the Catalyst 9300 switches into maintenance mode – which might be done to change the operating system, install or replace a module, replace cabling, and so on.

We ran and observed a streaming video of a helicopter in flight during the GIR test (see above). Traffic was running through the switch that we then put in maintenance mode.

The video ran with no glitches or detectable effect all during the GIR process.


Source: Miercom

*This video of a flying helicopter showed no glitches during the sub-second packet drop for the Patch test below.*

## Redundant Fans

Also new with the Catalyst 9000 family: The Catalyst 9400 modular chassis introduces user-configurable dual serviceable fan tray, allowing users to service the same fan-tray from the front and rear of the chassis, shown in the picture to the right.

Source: Cisco

## Patching

Patching is a point fix which only touches the affected components of the operating system, without the need of upgrading the entire operating system.

Patches are small in size and, when applied, fix only the affected components in the operating system and avoid long certification cycles.

Some bug fixes will entail a "Cold Patch", where the system needs a restart to complete the install process. Other fixes can be applied in a "Hot Patch", where the patch can be installed without reloading the system, and where there is no effect on network traffic.

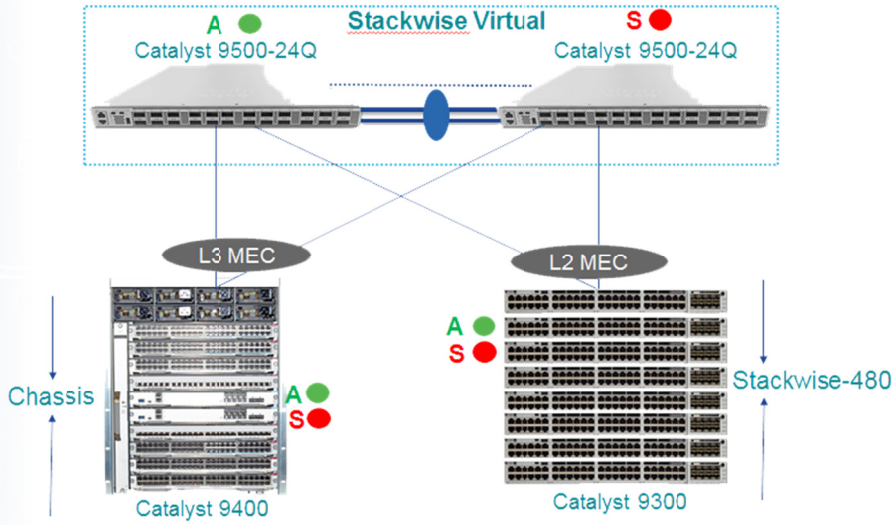
Patching is supported across all Catalyst 9000 models.

## Stateful Switchover (SSO)

With the Catalyst 9300 StackWise-480, Catalyst 9500 in StackWise Virtual and Catalyst 9400 with Dual Supervisors, there is a high availability mechanism called Stateful Switchover (SSO). SSO takes care of synching all states between the active and standby systems.

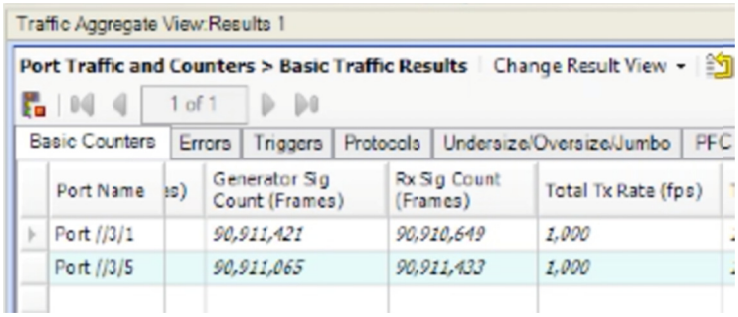
In the event of an active node/supervisor failover or a forced manual switchover, a standby device immediately takes over all the responsibilities of the active device with minimal impact on the forwarding traffic.

SSO tests were performed by manually switching over from active to standby in Catalyst 9300 StackWise-480, Catalyst 9500 StackWise Virtual and Catalyst 9400 with Dual Supervisors. Traffic loss was recorded in sub-seconds.




Source: Cisco

As shown, Spirent's 3/1 interface connected to the Supervisor in slot 5 (Te5/0/1), and Spirent 3/5 connected to the Supervisor in slot 6 (Te6/0/1). The Spirent system confirmed the traffic flow (see below). Traffic was sent continuously.



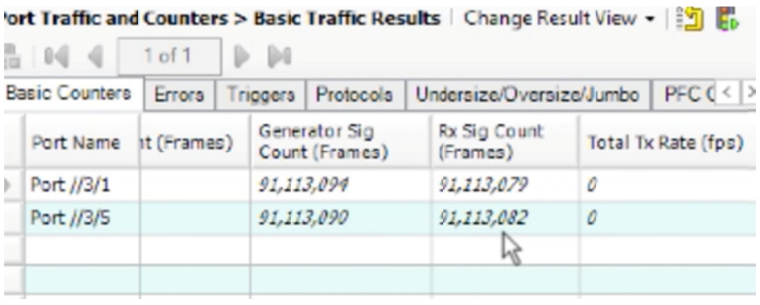

Source: Miercom

Then the active Supervisor was powered down to simulate a failure such as a power failure or intentional power down to upgrade the node's operating software, forcing a switchover.

The result: Traffic immediately re-routed through the standby Supervisor, which became the active Supervisor and took over very quickly since it had been keeping up to date with routing information.

We stopped the traffic generator and looked at the final sent/receive packet counts during the switchover, shown below.

Some packets were lost, but very few. That is unavoidable during a switchover, as some packets are in transit and already in the active node's pipeline at the time of the failure and switchover. In the IP world, higher-level software is tasked with retransmitting packets that are lost in route. At Spirent port 3/1, subtracting the values shows 15 packets were lost. In the other direction, at Spirent port 3/5, eight packets were lost. To summarize, our tests showed that, at a traffic rate of 1,000 packets per second, an average of just 12 packets are lost in each direction, which represents 0.012 seconds of "packet downtime" in each direction.




Source: Miercom

## Nonstop Forwarding (NSF)

Cisco NSF works with the Stateful Switchover (SSO) feature that is common in the base IOS software of all Catalyst 9000 devices. In fact, running SSO is a prerequisite to running NSF. The goal of NSF is to continue forwarding IP packets following a switchover from an active to standby node.

To appreciate what NSF does, it is necessary to understand how a switchover affects a routed network. Usually, when a routing device restarts, all routing peers of that device detect that the device went down and then came back up. This transition results in what is called a routing flap, which can spread across multiple routing domains. Routing flaps caused by such routing restarts, create routing instabilities which can impact the whole routed network's performance.

NSF helps to suppress routing flaps in SSO-enabled devices. It does this by allowing the forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. As a result of NSF, peer networking devices do not experience routing flaps. The ability of intelligent line cards and the standby node to remain up through a switchover – and to be kept current with the same routing table of the active node – is key to how Cisco's Nonstop Forwarding works.

NSF has to be configured. If enabled in the SSO configuration, the standby node is then kept up to date with routing-protocol information. This is supported both by dual active/standby Supervisors in the Catalyst 9400, as well as by StackWise Virtual with dual Catalyst 9300 and Catalyst 9500 configurations. This is supported both by dual active/standby Supervisor in the Catalyst 9400, StackWise Virtual with Catalyst 9500, and StackWise-480 in the Catalyst 9300.


Miercom Copyright © 2018

# 6 – Security

## Trustworthy Systems - Safe Hardware and Software

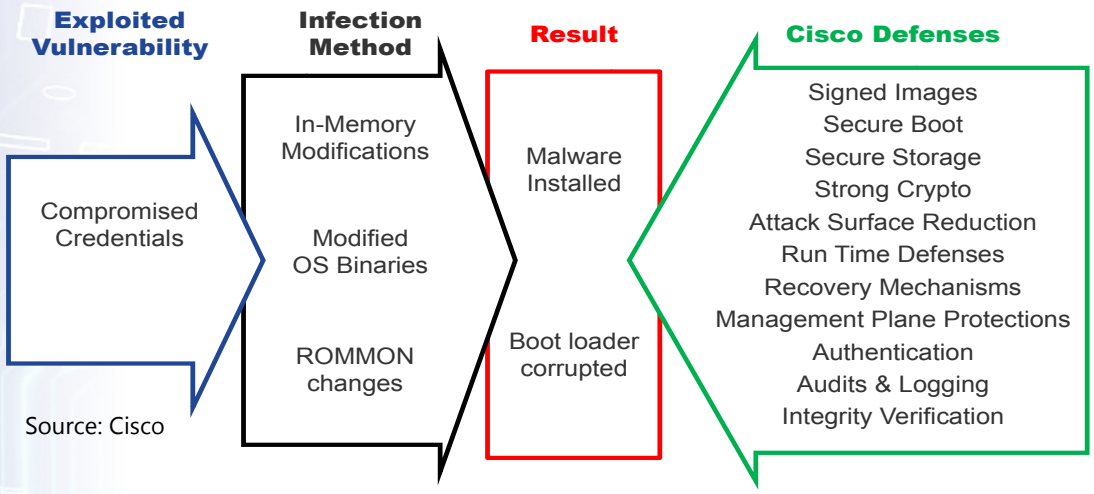
We noted the inclusion of several new features to bolster network and system security, and the ability of the user to monitor and identify security problems and threats. These include:

- **Image Signing**, where digitally signed software is used to protect against the use of counterfeit images and to assure that the image has not been modified or tampered with. The code signing uses a hashing algorithm, similar to a checksum; the hash is then encrypted using a signing key. The signed code is checked at runtime and validated by a trusted system element to ensure it has not changed. The trusted element is a piece of code known to be authentic and is unable to change (immutable).
- **Secure Boot**, which ensures that only authentic Cisco software boots up (through a secure processor, memory, and boot ROM) on the Cisco platform. This enhances image signing by using a hardware "trust anchor," also unchangeable, and helps prevent physical possession attacks and part-replacement attacks.

No one can ever guarantee that a system is invulnerable to surreptitious attack, but in our ongoing assessment of network-equipment vendors, Cisco seems more aware and proactive about security than most. Cisco provided us the below flow-chart graphic that defines the current state of threats and defenses.

Cisco collectively calls its unending security campaign "Trustworthy Systems." The objective, in a nutshell, is to assure that hardware is secure and has not been tampered before it's deployed. Software is verified as the same secure software that Cisco shipped.

The below chart summarizes many of the actual components of the Trustworthy Systems program. Many are unseen by typical customers, but all are constantly revised and improved.





Miercom Copyright © 2018

**Key Features Delivered by Cisco Catalyst 9000 Trustworthy Systems**

| | Image Signing & Secure Boot | Secure Device ID & Trust Anchor | Runtime Defenses | Integrity Verification | SSH2 Factor X.509v3 Authentication |
|---|---|---|---|---|---|
| **Protects Against:** | Compromised software and boot code | Counterfeit hardware | Attacks against the running software | Subtle penetrations | Unauthorized command line access |
| **Benefits:** | Secures the boot-code & ensures Open IOS-XE is authentic & unmodified | Includes built-in hardware ID root-of-trust, and that hardware is unaltered Cisco; provides secure plug and play | Protects the running OS; eliminates vulnerabilities | Detects potential loss of integrity | Eliminates passwords; protects the configuration |

In our review, we examined details of the Cisco security mechanisms, such as validating the SHA-1 hash algorithm result. Several system IOS commands show the particulars and results of integrity checking. We were able to verify the packages SHA-1 hash, verifying that the software had not been altered during boot up:

```
calculated
CD1D6169:9734AA81:75A57880:A969A4F8:3362CB
65
expected
CD1D6169:9734AA81:75A57880:A969A4F8:3362CB
65
Switch#show software authenticity
running
```

This command produces a list of authentication information about the system and software.


Miercom Copyright © 2018

## Encrypted Traffic Analytics (ETA)

ETA is another new capability which identifies malware in encrypted data streams, without requiring bulk decryption, using intraflow metadata –data elements within encrypted flows. Cisco security and software engineers say they are able to identify metadata elements that hint at malware, even from high-level scanning of flows, without decryption, by comparing the message characteristics with threat signatures that Cisco has catalogued.

Cisco says that ETA can provide potentially substantial benefits, among them:

- Gaining insight into encrypted threats by obtaining contextual threat intelligence with real-time analysis that can be correlated with user and device information
- Faster response time to contain infected devices and users

ETA is on the leading edge of network threat analysis and detection, and deserving of more review and testing.

## MACsec - Media Access Control Security

Cisco MACsec has become the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices. The IEEE standard was originally published in 2006, with key amendments issued through 2013. It provides security at Layer 2 between switches and hosts, similar to IPsec, which operates at Layer 3 (the IP protocol layer). MACsec is fully supported by the Catalyst 9000 switches, providing an important additional layer of encrypted security, using an extension of the EtherType field for a security tag and adding a message authentication code.

This added security measure secures potentially compromised connections between switches and hosts. As MACsec implementations proliferate, its use is spreading. Here are additional L2 connections for which MACsec is well suited:

- Host to switch
- Switch to switch
- Router to switch

We installed MACsec on a Catalyst 9300 and a connected switch, ran continuous data and then examined the link using this CLI commands:

**Switch 9000#show cts interface** ***<interface-id>*** (CTS=Cisco TrustSec)

**Switch 9000#show macsec interface** ***<interface-id>***

The resulting display confirmed that the link was secure, encrypted and that replay protection was enabled. MACsec on the Catalyst 9000 switches support the AES-128 and AES-256.


Miercom Copyright © 2018

# 7 - Programmability and Application Hosting

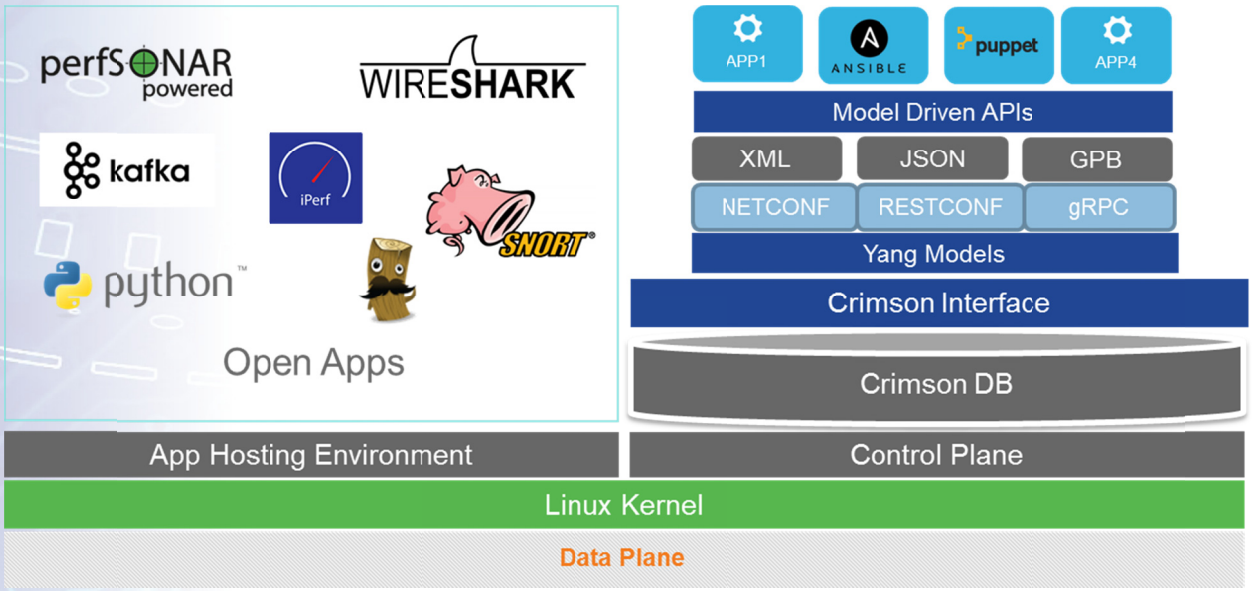
We noted during our review that the Cisco Catalyst 9000 switch software has evolved considerably from the monolithic IOS of the past. Our switches ran the latest v16.6.1 of Cisco IOS XE, which runs IOS functionality as an application atop a Linux kernel. With the Linux kernel, a popular and well-understood software environment, and x86 processor hardware, Cisco offers users and developers rich access to a Linux Guest Shell. Numerous programming interfaces for this Guest Shell enable diversified application hosting.

## Application Hosting

IOS-XE supports model-driven programmability, on-box Python object-oriented scripting, model-driven telemetry, and application hosting. Other popular programming environments supported include: The Yang Development Kit (YDK), protocol support for NETCONF (the IETF Network Configuration Protocol) and Remote Procedure Call (RPC) with XML encoding.

This below chart generally shows the rich programming support and access to the Catalyst 9000 switch Cisco IOS XE operating environment.

As noted, the Catalyst 9000 switches run x86 processors and provide storage containers for additional applications to be hosted on the switch. These can be used for custom applications as they can run on server environment in Linux KVM or LXC Container.




Source: Cisco

## Model-Driven Telemetry

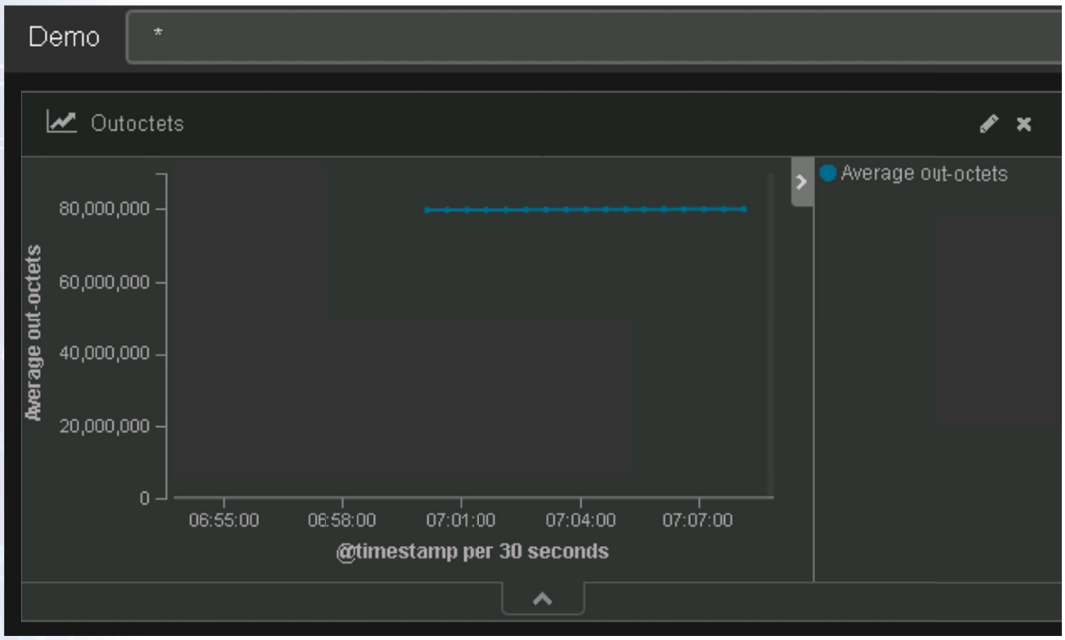
Another new capability delivered with the Catalyst 9000 switches, called model-driven telemetry, is a process that enables a user to obtain monitored data in near real-time. The user initially subscribes what information needs to be exported via the push model, enabled by telemetry, to continuously stream the user-specified data out of the switches. The streaming telemetry process consists of data collection, encoding, receipt and display.

Telemetry data is collected from the switch's data-management-engine database. Data is organized in an object model; specifying the particular path and branch.

The data can be retrieved periodically (frequency-based) or only when a change occurs in any specified object (event-based). A telemetry encoder then encapsulates the collected data into the desired format for transporting. Telemetry transport uses the secure Netconf protocol.

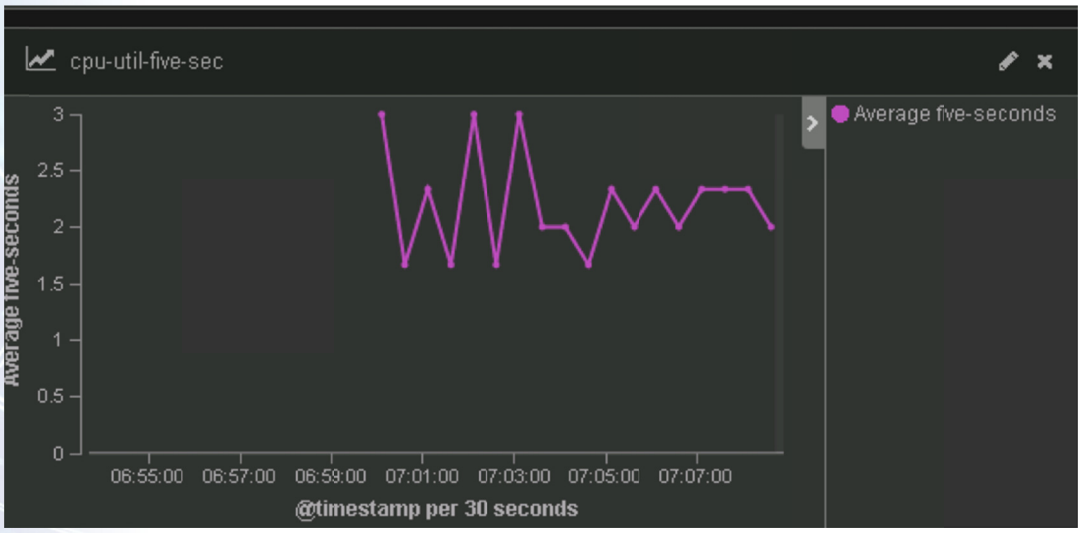
Other open-source tools, such as the Yang modeling tool can be used to categorize and send events meeting selected criteria to the telemetry receiver. The data is sent to an application, like a remote management system, which receives and stores the telemetry data. Finally, a display application formats and presents the data in a desired form (line graph, bar graph, pie chart).

The data pictured below was obtained via the streaming telemetry capability, created by subscribing to a Yang model. This image shows "out-octets" of a particular interface. This object is defined as "The total number of octets transmitted out of the interface, including framing characters." The average number of out-octets was specified per 30 second periods.




Source: Miercom


Miercom Copyright © 2018




Source: Miercom

Similarly, the screenshot above used model-driven telemetry to show the CPU utilization of a switch; we specified average CPU utilization over the last five seconds, with data points sent to the collector every 30 seconds. In this case an open-source program called Kibana receives the telemetry messages and creates the graph of CPU utilization.

## Automation Scripting

Customer applications, running in a Guest Shell portion of the Cisco IOS XE operating software on a Catalyst 9000 switch, can access the configuration, operational state and even the event data from the device. This is typically done via Python scripts.

As part of its DevNet program, Cisco makes many Python scripts, utilities and other sample code available to customers and developers. Python is not the only language that can be used for automation scripting, but it is fairly easy to learn and a favorite of network engineers.

A CLI (command line interface) script library is available from Cisco that enables Python scripts to execute CLI commands (such as **show version**). Similarly, a script can enable a TDR test (of fiber-optic link integrity) to run on every optical interface of the device that is in "up" status, or monitor configuration changes (in the Embedded Event Manager, EEM) and send a message to the administrator.

In the below example, a Python script – **sparkcfg.py** – is invoked from the IOS command line,

```
catalyst-1#
catalyst-1#sh run | sec event manager
event manager applet config_change
 event syslog pattern "SYS-5-CONFIG_I"
 action 0 cli command "enable"
 action 1 cli command "guestshell run python sparkcfg.py"
catalyst-1#
```

Source: Miercom

In the below example, the user runs Python from the guest shell and invokes various standard Python commands.

Given the access to the event log, configuration and interface data now offered on the Catalyst 9000 family of switches, it is really up to users' imagination, and their Python scripting abilities, how to best use this data for network automation.

```
catalyst-1#guestshell  run python
Python 2.7.11 (default, May 17 2017, 05:17:57)
[GCC 5.3.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>>
>>> print "hello world"
hello world
>>>
>>>
>>> import cli
>>>
>>> cli.cli("sh clock")
'\n*21:41:10.254 UTC Wed Oct 18 2017\n'
>>>
>>>
>>>
```

Source: Miercom


Miercom Copyright © 2018

# 8 - About Miercom Performance Verified Testing

This report was sponsored by Cisco Systems, Inc. The data was obtained completely and independently by Miercom engineers and lab-test staff as part of our Performance Verified assessment. Testing such as this is based on a methodology that is jointly co-developed with the sponsoring vendor. The test cases are designed to focus on specific claims of the sponsoring vendor, and either validate or repudiate those claims. The results are presented in a report such as this one, independently published by Miercom.

# 9 - About Miercom

Miercom has published hundreds of network-product-comparison analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

# 10 - Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

No part of any document may be reproduced, in whole or in part, without the specific written permission of Miercom or Cisco Systems, Inc. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.