Miercom

2019

Cisco Catalyst 9200 Switch Series

CISCO

Detailed Report DR190710E

Performance Validation Testing

CONTENTS

EXECUTIVE SUMMARY

1

Modern day enterprises whether small or large require their networks to be dynamic, scalable and secure. Their networks need to be flexible and accommodating to allow organizations to grow and evolve without adding burden on IT resources and degrading the performance or security of their network. Cisco Catalyst 9200 series switches address these requirements by extending the intent based networking (IBN) and simplifying the deployment of advanced technologies without compromising the network performance. These switches are ideal for any mid-sized organization or branch access deployment as they help simplify the network complexity and deliver security and reliability while delivering the benefits of automation and assurance through IBN architecture.

Cisco released its line of Catalyst 9200 switches – bringing the services and features previously afforded by the enterprise Catalyst 9300 line to branch and mid-market enterprises. Cisco has proven in testing that this line of switches has the same technology as its enterprise-grade switch and engaged Miercom to provide third-party validation.

Having tested similar features on Catalyst 9300 testing, we were impressed to find the same sophistication in the Catalyst 9200 series. The device was deployed in a real-world business network environment with generated dataflows to observe use case behavior.

From our testing, we noted the following key takeaways that demonstrate the cost-effective functionality of the Catalyst 9200 switch series for branch and mid-sized enterprises environments:

Key Findings

- **Experience** through flexible onboarding and management. Getting the device up and running is expedited with three onboarding options (Plug and Play, Zero Touch Provisioning or WebUI). Plug in the device for instant onboarding or use optional remote custom setup with Python scripting. Then with Cisco DNA Center – a single pane-of-glass management with built-in workflows – provides simple design, provisioning and control that automates and optimizes endpoint monitoring and troubleshooting for dynamic organizations' needs. Network-based Application Recognition (NBAR2) enables application-aware services for optimized policies and resource usage.
- **Always on.** Like enterprise switching counterparts, the Catalyst 9200 line has resilient power and fan redundancy components, as well as hot-swapping of 1/10 GE uplink modules to prevent switch failure. StackWise Stateful Switchover (SSO) supports stacking of two or more switches for virtually linked, synchronized configurations for failover situations. Single-feature patches help avoid vulnerabilities between releases that could put the switch and network at risk.

- **Security.** MACsec encryption protects Ethernet downlinks against Man-in-the-Middle (MiTM) attacks and other intrusions, and Control Plane Policing (CoPP) protects ingress traffic from Denial-of-Service attacks. Trustworthy Systems (Secure Boot) ensures all software images are Cisco- verified to protect hardware and software against digital signature-based corruption. The Catalyst 9200 series switches support Full Flexible NetFlow which combined with Cisco Stealthwatch provides real-time insights into network trends, analysis, and breach alerts. Cisco SD-Access network fabric accelerates and simplifies your enterprise network operations by enabling policy-based automation from edge to cloud with Group-based policies and network virtualization and segmentation.
- **Uninterrupted operations for IoT deployments.** Catalyst 9200 switches also support Perpetual Power over Ethernet (PoE) and Fast PoE to avoid downtime and incurred costs by providing uninterrupted power during reloading and remember power drawn on PoE ports for immediate power-on and reboot without having to wait for the IOS to finish booting. Two-event PoE and classification can intelligently identify the device class to provide enough power for switch power-on and operation.
- **Overall Cost Savings.** With enterprise feature set and security, network management and operations can be carried out with increased automation and simplicity that reduces the need for costly IT expertise and reduces downtime to ensure optimal business productivity and profit.

Based on our observations, the Cisco Catalyst 9200 Switch Series delivers enterprise functionality and security for the benefit of mid-market and branch networks. In recognition of its integrated unified management, high-efficiency architecture, novel monitoring technology and enhanced security measures, we award the Cisco Catalyst 9200 series with the ***Miercom Performance Verified*** certification.

Robert Smithers

CEO

Miercom

Product Tested

2

The Cisco Catalyst 9200 Switch Series takes on the challenge of the ever increasing network demands spurred by Internet of Things (IoT) and in particular – support for security, increased deployment of sensors, evolving higher densities of endpoints (via high concentrations of access points), and the necessary scalability of a growing business. By creating a switch with sophisticated functionality, as well as compatibility with advancing technology, Cisco created a straightforward but reliable way to deliver quality service, software defined access fabric technology with smooth policy management and onboarding. The Catalyst 9200 line brings a new experience for enterprises branch from both the technical and front-end perspective.

While the Catalyst 9200 series is intended for smaller scale networks than the enterprise-level Cisco Catalyst 9000 line, it maintains the same high-end enterprise capabilities. This is useful for enterprises that may expand over time, or for large businesses that want to extend functionality to new branches of their existing network.

This switch series comes with the same consistent interface and excellent quality of user experience as the Catalyst 9000 line, as well as its enterprise- grade features and advanced network security.

Source: Cisco

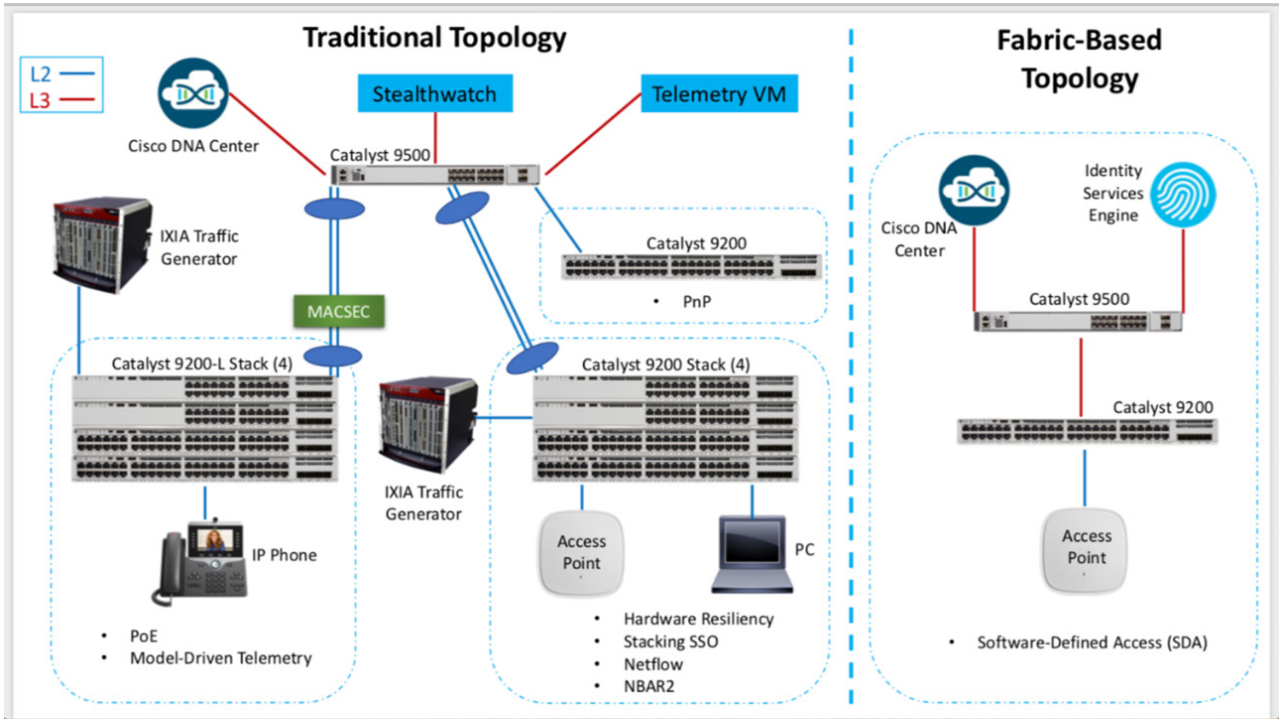
The Cisco Catalyst 9200 Series include modular uplinks models (C9200) and fixed uplinks(C9200L) switch models that range from 24 to 48 ports, available with or without full PoE+ capabilities, and optional modular uplinks, 4x1/10G fixed uplinks or 2x25G fixed uplinks.

How We Did It

3

Enterprise-grade functionality and security of the branch-level Catalyst 9200 switch series was tested using a realistic network of switch stacks, common network endpoints and cutting-edge test equipment to validate each feature.

Test Environment



Source: Cisco

The test bed used to evaluate the Cisco Catalyst 9200 switch capabilities consisted of a stack of four switches, providing reliability of redundant servers. Redundant hot swappable interface modules, fans and power supplies were also included.

For the traditional topology (left), there were two stacks of Catalyst 9200 switches. One stack included two Catalyst 9200-24P switches and two 9200-48P PoE+ switches. The other stack consisted of 9200L-24P switches and 9200L-48 PoE+ switches. Then, there was also a standalone 9200-48P PoE+ switch. Both stacks, and the standalone switch, were connected over Layer 2 to a single Catalyst 9500-24P switch.

Tested Switches	Firmware	Version
Catalyst 9200-24P (2)	Cisco IOS-XE	16.11.1
Catalyst 9200-48P PoE+ (2)	Cisco IOS-XE	16.11.1
Catalyst 9200L-24P (2)	Cisco IOS-XE	16.11.1
Catalyst 9200L-48P PoE+ (2)	Cisco IOS-XE	16.11.1
Catalyst 9200L-48P	Cisco IOS-XE	16.11.1
Cisco DNA Center	-	1.2.10

All switches, except the standalone 9200-48P, were running Cisco IOS-XE software, version 16.11.1. The standalone switch was used to test Plug and Play tests; it was running Cisco IOS-XE, version 16.12.1, in conjunction with the Cisco DNA Center, version 1.2.10.

The fabric-based topology (right) was used to test and demonstrate Cisco Software-Defined Access (SDA) capabilities. All other tests were run using the traditional topology.

Equipment

The **Ixia XGS12 with IxOS,** version 8.4, generated Layer 2 and Layer 3 data flows within the working business network. This tool is capable of large-scale application performance and security validation and optimization testing for both physical and virtual networks. (For more information, visit https://ixia.keysight.com/).

Experience

4

Device Onboarding

Why It Matters

Setting up network devices can mean manual configurations of each switch and can take days or in some cases weeks. Businesses can benefit from an intuitive and quick way to deploy network switches.

The Cisco Advantage

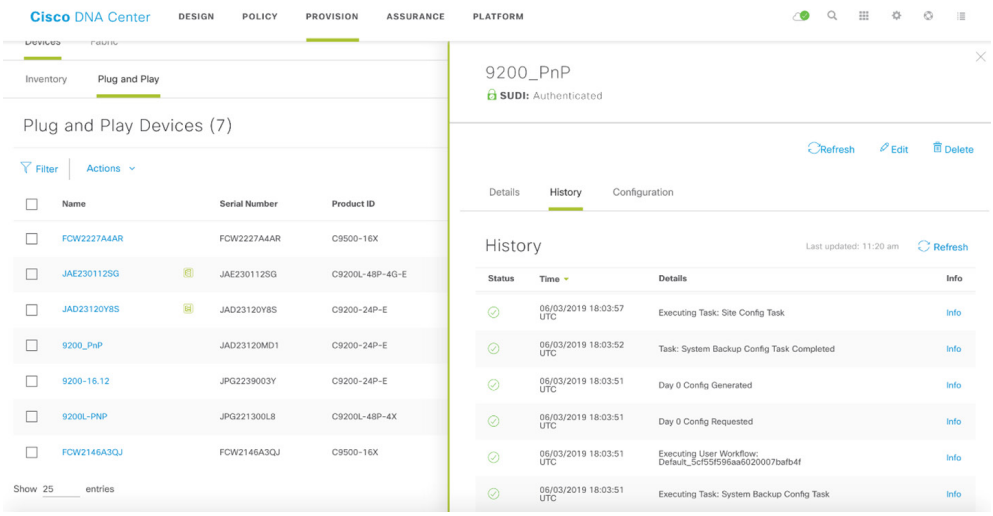
The Cisco Catalyst 9200 switch makes it simple to set up, configure and deploy using three options for onboarding: Plug and Play (PnP), Zero-Touch Provisioning (ZTP) and a Web User Interface (Web UI). We explored each of these options during testing and found these setup options to be fast and significantly cut down downtime and labor of traditional deployment from days to hours.

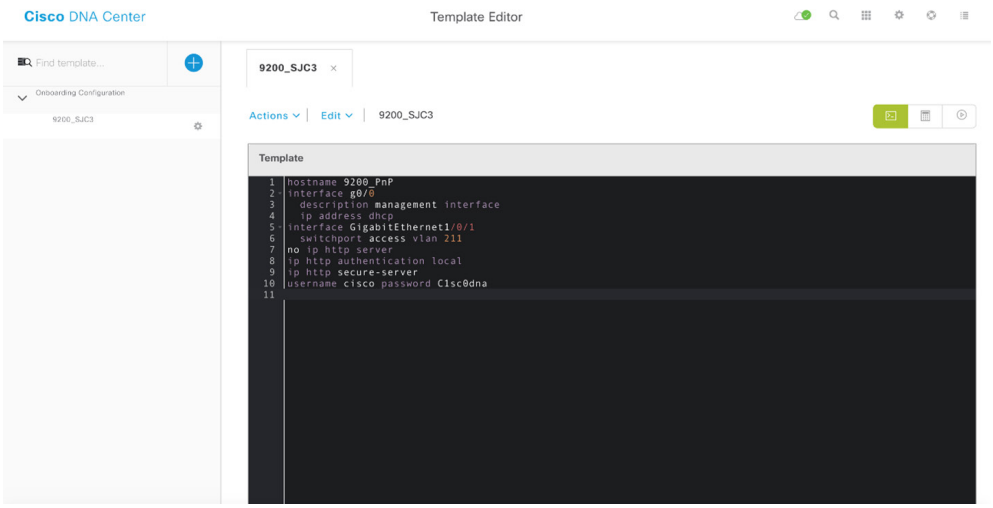
Test 1: Plug and Play (PnP)

For this test, we looked at the process for provisioning a switch using PnP through the Cisco DNA Center. This onboarding option offers an easy branch or campus device installation or update to an existing network that is fully secure. It works for any Cisco device that supports PnP and uses a DHCP address for configuring new routers.

PnP works with Cisco Catalyst 9200 switches, in tandem with Cisco Digital Networking Architecture Center, to create a clear, unified approach to provision new switches. Switches are provisioned based on zones, allowing configuration templates to be applied upon connection and power-on without the need for physical access. Using the only the DHCP server, the switch can be loaded with software images and configured with details about the PnP server – automatically initiating PnP as soon as it becomes active.

Using the Plug and Play interface in Cisco DNA Center, an IT administrator can track provisioning changes for a particular device. Details such as serial number and configuration status are visible, as well as the history of the device with timestamps. Plug and Play makes network switches easily identified and monitored.





Efficient deployment of switches was demonstrated using the Cisco DNA Center Template Editor. We were able to create configurations based on a set of criteria and apply them upon connection and power-on without physically accessing the device.

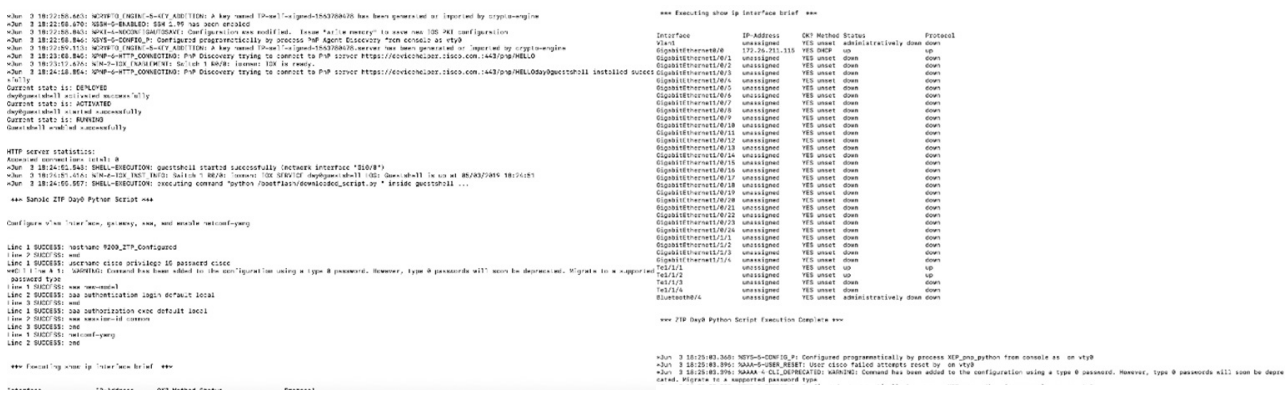
Test 2: Zero-Touch Provisioning (ZTP)

Another option for onboarding devices is Zero-Touch Provisioning. ZTP automates all installation or update processes for software images or configuration files on first-deployment Cisco devices.

Cisco IOS XE on Catalyst 9200 switches also support ZTP. Like PnP, ZTP supports template configuration implementation on a wide range of new switches without any physical interaction. But the distinction for ZTP comes from its ability to apply processes to a wider variety of devices that do not necessarily also support PnP.

Device configuration was very straightforward and streamlined by receiving a DHCP address from a DHCP Server, then a HTTP/TFTP server that hosts the configuration template is used. The switch then enables Guest Shell, downloads the configuration template with a Python script.

To test this feature, we factory-reset a PnP switch and observed the process for provisioning a switch using ZTP by having the switch enable its guest shell, download and execute the Python script from a TFTP server for a successful self-configured device.



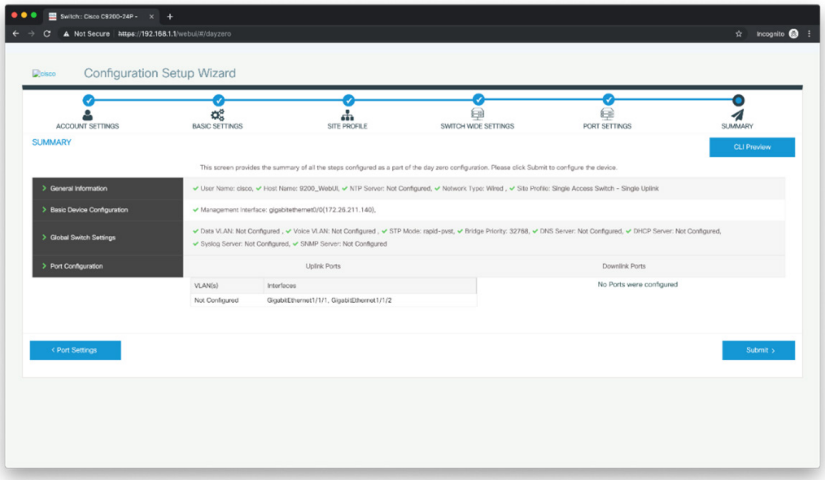
A Python script was run for ZTP Day 0 configuration of the Cisco Catalyst 9200 switch. The device was successfully deployed, activated and running.

Test 3: WebUI Onboarding

The last option for onboarding we tested was WebUI Day 0 Provisioning which, unlike PnP and ZTP, required physical access to the hardware. We went through the process for connecting a new Cisco switch using the WebUI to show initial configuration steps and options.

With the WebUI available on Cisco Catalyst 9200 switches, a user can configure a PC as a DHCP client and then connect it via any downlink port to the switch. The switch then acts as a DHCP server, providing an address for the PC, after which a web browser can be utilized to open the WebUI page with a GUI to provision the switch. Since the switch comes with a default image, there is no need to enable or install licenses, but users can quickly employ the WebUI to build configurations and manage devices without any costly CLI expertise.

The Configuration Setup Wizard allows for seamless deployment of a new Cisco Catalyst 9200 switch.



RFID

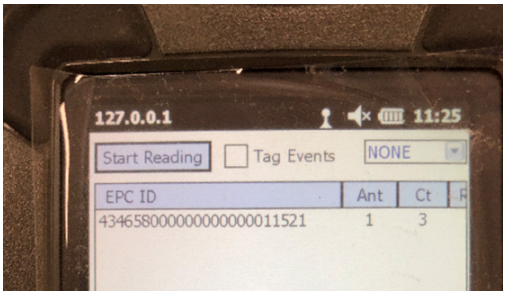
Why It Matters

Enterprise networks use dozens, and sometimes even hundreds, of Cisco Catalyst switches which make inventory management cumbersome and time consuming. From labeling each device, to entering and managing details in a database, it creates a considerable amount of manual labor that is highly prone to error.

The Cisco Advantage

Cisco Catalyst 9200 switches have a solution to tracking so many key network components – integrated, passive SGTIN (Serialized Global Trade Item Number)-198-bit encoded RFID tags within the chassis, as well as on supervisor, line cards, power supplies and fan trays.

The built-in RFID tag on the front panel allows users with compatible RFID readers to utilize these tags for more efficient inventory management. Tags are read by an RFID reader and readily imported into the inventory databases. Since these are passive RFID tags, they require no additional power source to be read by the reader, and the device or module does not have to powered up for the tags to be read.



We scanned a system for its EPIC ID by using a standard RFID reader. The tag made auto-identification made asset tracking and management much simpler and more accurate.

Blue Beacon

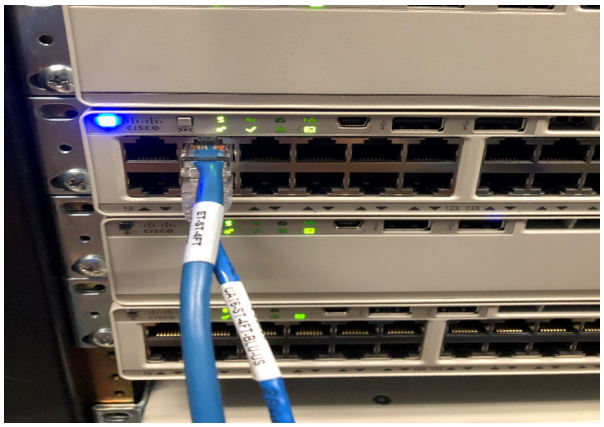
Why It Matters

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.

The Cisco Advantage

For a large enterprise, device location can be complicated and time consuming. To resolve this, Cisco has placed a bright blue LED on the top left corner of the front panel on all members of the Catalyst 9200 switch family. This blue LED, or "Blue Beacon", can be turned on and off through a console command or physically by pressing the UID button on the front panel. When the Blue Beacon is turned on or off, a repeated informational message appears in the machine's syslog.

The Blue Beacon LED can be used to identify a particular switch or set of switches in rows of racked machines, possibly containing the same models, as well as indicate a switch requiring attention at a later date.



(Left) The Blue Beacon LED may be turned on or off manually, or remotely through the CLI, to help IT staff quickly locate particular switches that require attention now or in the future.

(Below) The state of the Blue Beacon LED indicator is visible through the CLI.

```
C92L-Stack#
C92L-Stack#
C92L-Stack#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
C92L-Stack(config)#hw-module beacon on switch 2

Jun  5 20:43:59.345: %PLATFORM_LED-6-BEACON_LED_TURNED: Switch 2 Beacon LED turned ON
C92L-Stack(config)#
C92L-Stack(config)#hw-module beacon off switch 2

Jun  5 20:44:12.810: %PLATFORM_LED-6-BEACON_LED_TURNED: Switch 2 Beacon LED turned OFF
C92L-Stack(config)#
C92L-Stack(config)#_
```

Bluetooth OTA

Why It Matters

There's a problem with the switch, and an IT staff member needs to quickly access the port on-the-go with configuration changes, image uploads and possible troubleshooting. Bluetooth can help wireless laptops or tablets access the WebUI or Command Line Interface (CLI) if the hardware supports it, saving the network from downtime and operation costs.

The Cisco Advantage

Cisco Catalyst 9200 switches support the connection of third-party Bluetooth dongles to its hardware for device management via Bluetooth interface. A user connected to a Catalyst 9200 via Bluetooth can interact with the WebUI and CLI to troubleshoot issues, modify configurations or transfer files to the switch wirelessly.

We tested the Bluetooth wireless access by setting up a new system. The Catalyst 9200 switches can use Bluetooth to discover the management IP address of the controller through an Over-the-Air Provisioning (OTAP) technique. The IP addressed machine can then provide all necessary information for initial configuration of the Catalyst 9200 and then install it in the network with all relevant addressing and policies for a secure working system.

The Bluetooth dongle was supported by the Cisco Catalyst 9200 switch hardware, allowing wireless access to the system CLI for initial configuration of a new system with all necessary networking details.

Model-Driven Telemetry

Why It Matters

Networks are always expanding, creating more complexity that requires costly IT expertise to handle. Businesses using manual methods to manage network operations run into continual issues, never identifying the root cause, and leave the organization without an intent-based architecture. In order to manage and meet the demands of scalable networks requires automation as a solution.

The Cisco Advantage

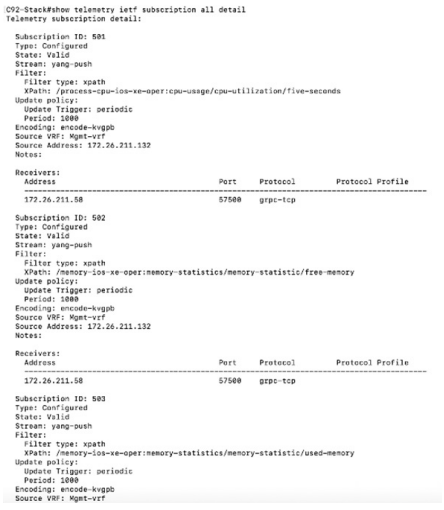
Model-driven telemetry inherits the power of models (such as YANG models) to make it easier to define, consume and subscribe to the data you want. By structuring that data with YANG, model-driven telemetry ensures that those vast quantities of data are programmatically usable. And by having such data sent from data sources automatically, it eliminates the extra communication formerly needed to request data.

So instead of trying to choose and extract information to resolve issues, model-driven telemetry is a structured approach to automatically collect and export YANG-modeled data to monitoring tools that help administrators reduce application-based resource usage.

The Cisco Catalyst 9200 switches can act as a publisher and send switch-related data (e.g. CPU and memory consumption) to a receiver where users can configure dashboards to monitor specific switch metrics.

Applications consuming data can subscribe to only the particular YANG-model data they need, over NETCONF, RESTTCONF, or gNMI.

We observed a dashboard containing numerous, helpful charts and graphs that displayed switch data and YANG models that drive further insight of resource usage.



```
C92-Stack#show telemetry ietf subscription all detail
Telemetry subscription detail:

  Subscription ID: 501
  Type: Configured
  State: Valid
  Stream: yang-push
  Filter:
    Filter type: xpath
    XPath: /process-cpu-ios-xe-oper:cpu-usage/cpu-utilization/five-seconds
  Update policy:
    Update Trigger: periodic
    Period: 1000
  Encoding: encode-kvgpb
  Source VRF: Mgmt-vrf
  Source Address: 172.26.211.132
  Notes:

  Receivers:
    Address                                                 Port     Protocol         Protocol Profile
    ------------------------------------------------------------------------------------------------
    172.26.211.58                                           57500    grpc-tcp

  Subscription ID: 502
  Type: Configured
  State: Valid
  Stream: yang-push
  Filter:
    Filter type: xpath
    XPath: /memory-ios-xe-oper:memory-statistics/memory-statistic/free-memory
  Update policy:
    Update Trigger: periodic
    Period: 1000
  Encoding: encode-kvgpb
  Source VRF: Mgmt-vrf
  Source Address: 172.26.211.132
  Notes:

  Receivers:
    Address                                                 Port     Protocol         Protocol Profile
    ------------------------------------------------------------------------------------------------
    172.26.211.58                                           57500    grpc-tcp

  Subscription ID: 503
  Type: Configured
  State: Valid
  Stream: yang-push
  Filter:
    Filter type: xpath
    XPath: /memory-ios-xe-oper:memory-statistics/memory-statistic/used-memory
  Update policy:
    Update Trigger: periodic
    Period: 1000
  Encoding: encode-kvgpb
  Source VRF: Mgmt-vrf
```

Cisco supports different coding (e.g.encode-kvgpb protocol) that determines which attributes the dashboard should display. In this case, the CPU usage over the course of five seconds was commanded for collection, implemented with a periodic trigger. The dashboard shows the model-driven telemetry in a visual interface, using an open source software such as Grafana, to display memory and CPU usage.

Model-driven telemetry is visible in an interface, such as Grafana, to display memory, CPU and interface statistics.

Network-Based Application Recognition (NBAR2)

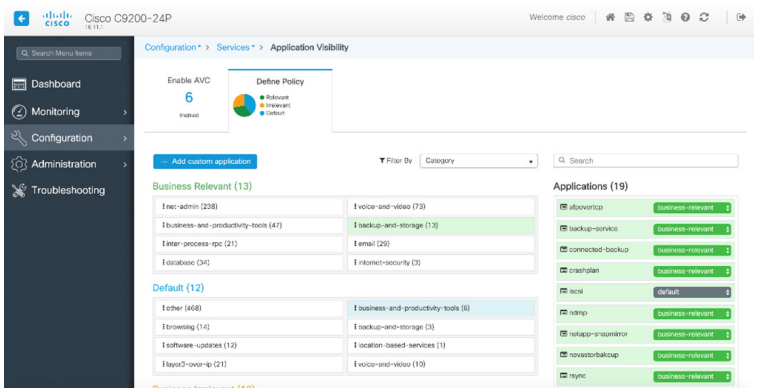
Why It Matters

Application-based threats can penetrate a network, putting the entire enterprise at risk. The IT staff required to remediate this would be time consuming and costly, but by tracking applications, administrators have full visibility of HTTP-based traffic. Since web applications can be accessed from any location, there is less security control over these services and can result in overused network resources or attacks.

The Cisco Advantage

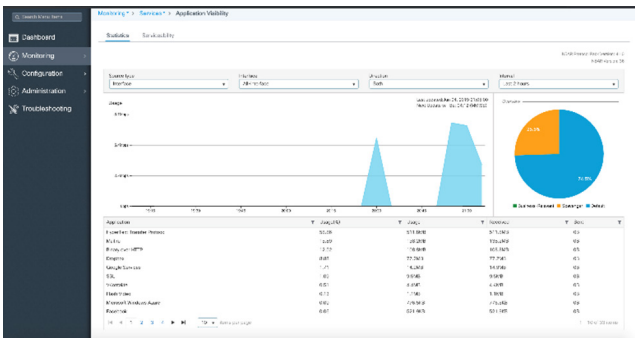
NBAR enable Cisco Catalyst 9200 switches to become application-aware and allow for switch metrics to be measured on a per-application basis. Using NBAR, applications can be intelligently identified and classified, letting critical applications to be policy routed or guaranteed allotted bandwidth. Non-critical applications can also be policed or even blocked.

Charts and graphs, as shown below, describe application metrics while also being configurable from the switch WebUI.



NBAR dashboard shows application visibility, demonstrating the monitoring of business application usage metrics across a switch.

Unlike the monitoring NetFlow and Stealthwatch tools, NBAR has the ability to classify and carry out actions for different services on the application layer. Cisco can recognize up to 1,400 applications (e.g. mail traffic, Dropbox, Microsoft Azure) in real-time. Unlike standard monitoring tools, NBAR does not replicate applications and analyze after traffic has been processed but in real-time before data is received by the client side. Once classified, IT administrators can perform actions on applications that are business-oriented or non-business related. This is done at the low-level hardware on the switch.



Cisco DNA Center

Why It Matters

Businesses should be focused on exactly that – business. Unfortunately, organizations waste a lot of time and money on setting up or fixing network issues that would be better spent on being productive.

Ever-expanding networks bring an overwhelming amount of complexity that requires the cost and talent of expert IT staff. And to make matters worse, this needs to be accomplished quickly or productivity and profit are sacrificed.

Ways networking becomes a burden on businesses:

- Multiple tools, each with their own interface, that can lead to human error in configuration and management
- Incorrectly configured devices and communication allow vulnerabilities to be exploited by attackers
- Unsupported third-party integration makes changes and troubleshooting difficult and time consuming
- Limited remediation of virtualized networks falls short of integrated analytics and automation tools
- Extensive real-time data flow shared between third-party vendors is not efficiently shared, creating holes in the intent-based architecture for configuration, security, analytics and automation

The solution: a centralized management system for the entire architecture, on a global scale, that can provision and configure all devices as well as monitoring, troubleshooting and optimizing at the same time for accurate, automated and robust real intent-based networking.

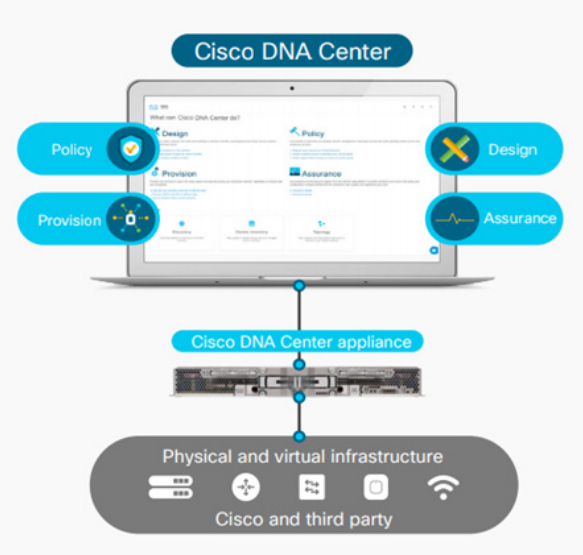
The Cisco Advantage

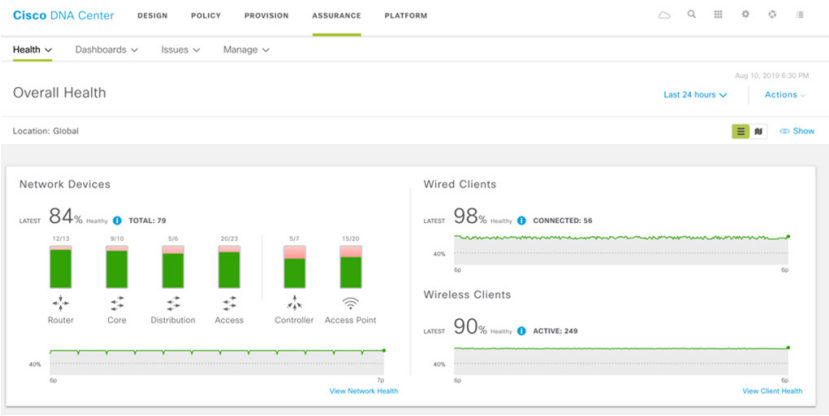
The Cisco Digital Network Architecture (Cisco DNA) is Cisco's architecture for networks – across the campus, branch, WAN, and the extended enterprise. It provides an open, extensible, and software-driven approach called the Cisco DNA Center to make the network simpler to manage, and more agile for business needs.

Cisco DNA Center provides an intuitive, single pane of glass command center that is accessible as a graphical user interface via a web service for easy end-to-end management in one place.

Benefits we observed include:

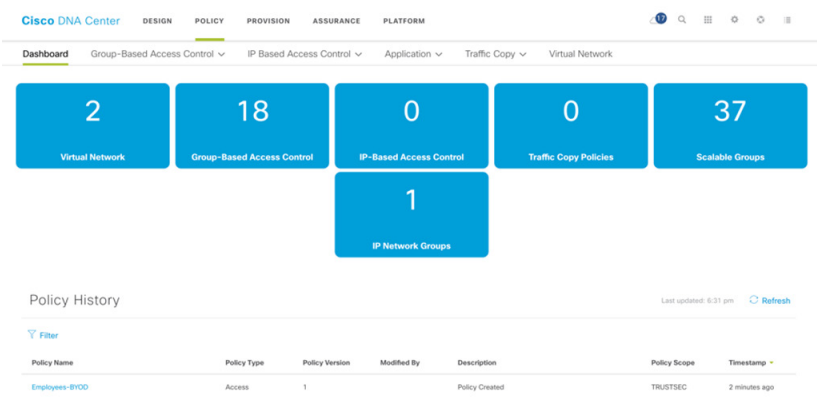
- **Single pane of glass dashboard** for a more organized, centrally controlled network
- **Built-in workflows** for easy network design, provisioning, and policy-driven control
- **Secure network segmentatio**n via user and device profiles to create policy-based configurations according to business needs and constraints
- **Drag-and-drop provisioning** with automated, zero touch assignment of devices to policies based on identities (e.g. users, devices, applications)
- **Advanced monitoring with insightful analytics** for quick remediation
- **Quick deployment in minutes**, instead of traditional methods that take days
- **Comprehensive software-defined automation** reduces the need, time and cost of IT maintenance
- **Assurance Engine** provides consistent, high-performance user experience
- **Visual design** using physical maps and logical topologies for quick upgrades
- **Device discovery** that automatically finds devices through the Cisco Discovery Protocol or IP address range





The Assurance Engine displays the overall health of the network, showing the operational status of every provisioned device. Any poorly connected devices come with a suggested remediation to restore system health. This ensures consistent and optimized service levels in accordance with business demands. IT maintenance and costs can therefore be dramatically reduced with the Assurance Engine monitoring, troubleshooting and proactive performance optimization tools for clients, applications and services.

Group-based policies ensure the most optimally configured and secure network devices and users for network segments that support business needs. Policies can be defined as network-specific or device-specific according to different models, roles, operating systems and other parameters or constraints to create virtual networks, access control policies, traffic policies, and application policies.



Programmability

Why It Matters

With more agile and complex networks becoming more common, traditional configuration and data extraction are not enough. On the network layer, NETCONF/YANG/OpenConfig Model are well known methods to achieve programmability.

However, many products support proprietary APIs that are not open-source and may limit third-party development. One of the most common standard models for network equipment operations is NETCONF (Network Configuration Protocol) – an XML-based protocol that applications can use to request information from, and make configuration changes to, network devices like switches.

The Cisco Advantage

Cisco IOS-XE, running on the Catalyst 9200 switch series, supports Guestshell with the ability to run Python scripts. Python can be used to configure features through NETCONF/RESTCONF/gNMI/gRPC in both interactive and script modes within the Guest Shell or on the switch itself.

The Guest Shell is a virtualized Linux container for running custom Linux scripts, including Python. The supported Python module allows users to run IOS CLI commands inside a Python script to enable remote and automated control or management of switch features. Using the Guest Shell, users can install, update and operate third-party Linux applications.

For example, a user could configure Fast Power over Ethernet (PoE) on devices using a Python script via Guest Shell. For our testing, we successfully configured a 2-event PoE on a PoE light using this method (discussed in Section 7).

WebUI

Why It Matters

A switch has been deployed and now requires configuration, management and monitoring throughout its lifecycle. Using CLI commands requires expert IT knowledge that can consume allotted maintenance budgets. Having a web-based User Interface (UI) can greatly reduce the time and experience needed to explore the resource and application usage that should be consistently monitored and configured for optimal service.

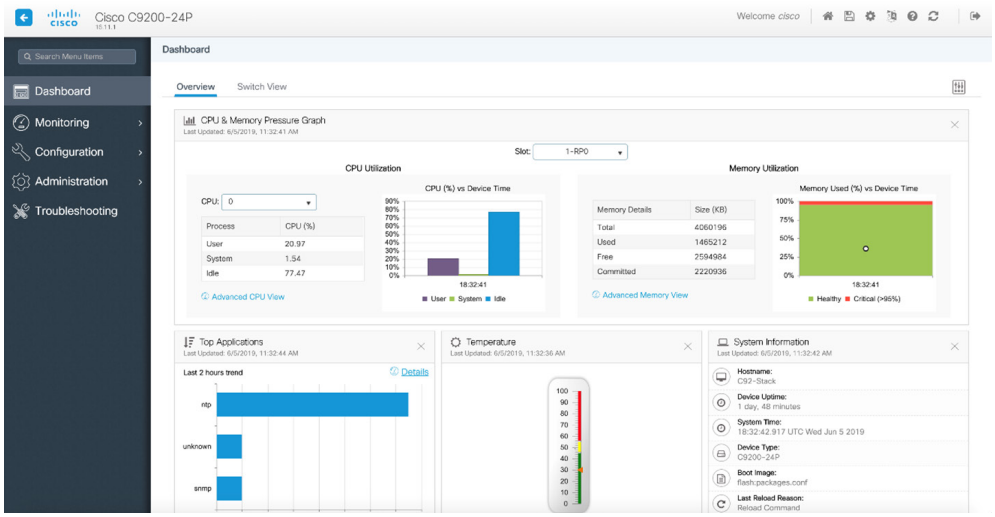
The Cisco Advantage

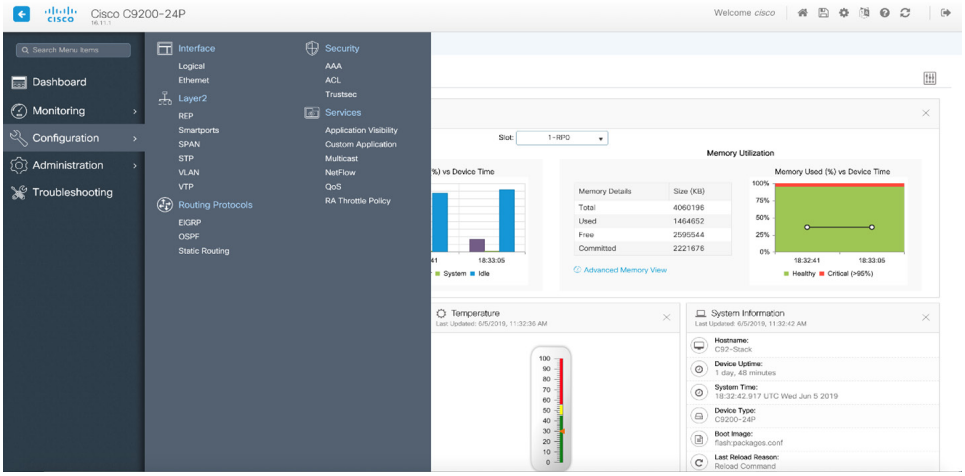
In addition to being useful for Day 0 provisioning, the Cisco Catalyst 9200 switch series has a WebUI with features that simplify configuration, management and monitoring. Once a switch has been provisioned and is online, the WebUI is readily accessible via a web browser at the management IP address of the switch.

The WebUI dashboard shows several charts and graphs, detailing information about the switch CPU, memory and application usage. Its menu offers numerous options for configuring, monitoring, administering and troubleshooting the switch as well.

The WebUI comes with a default image, eliminating the need to enable or install anything on the device. Having a WebUI feature allows users to make device alterations without needing CLI expertise, reducing cost of expert IT labor.

The WebUI shows visual charts of the Cisco Catalyst 9200 switch health – display metrics such as CPU and memory utilization, commonly used applications, device temperature and other system details.





Other configurations options are available in the WebUI, requiring no use of CLI to operate. Users can access the interface, data link layer protocols, routing protocols, security features and useful services through the left-side menu.

Always On

5

Hardware Resiliency

Why It Matters

Without High Availability (HA), the enterprise communication and activity are at the mercy of its hardware. Without some sort of resiliency measures in place, poor performance or, in the worst case, network downtime can severely impact business operations and overall user experience. Effective HA designs, particularly in hardware, can reduce the number of failures, the time between failures and the time taken to repair these inadequacies to keep business communications, devices and services running smoothly.

The Cisco Advantage

The Cisco Catalyst 9200 switch has several hardware components that provide high availability capabilities like redundancy and hot-swapping.

The switches provide the option to install a secondary power supply module, as well as a second fan module, as backups that immediately take effect in the event of primary module failure. This prevents switch downtime and the costs associated to remediate such outages.

Additionally, the uplink modules in the front of the switch for 1G/10GE uplink ports can be hot-swapped without causing the switch to be inoperable.

The following table details the Cisco Catalyst 9200 switch models and associated power supply modules, uplink ports and fan modules:

Switch Model	Description
C9200-24P	Stackable 24x1G PoE+ ports; 4x1G and 4x10G modular ports; 2 power supply slots; 2 field-replaceable fans; supports StackWise-160
C9200-24T	Stackable 24x1G ports; 4x1G and 4x10G modular uplink ports; 2 power supply slots; 2 field-replaceable fans; supports StackWise-160
C9200-48P	Stackable 48x1G PoE+ ports; 4x1G and 4x10G modular uplink ports; 2 power supply slots; 2 field-replaceable fans; supports StackWise-160
C9200-48T	Stackable 48x1G ports; 4x1G and 4x10G fixed modular ports; 2 power supply slots; 2 field-replaceable fans; supports StackWise-160

During testing, we observed the following:

- Dual Power Supply: Showed no system downtime when removing a power supply; immediate doubling of power budget when reinserted
- Dual Fan: Showed no system downtime during fan removal and installation
- Uplink Module: Hot-swapped a 4x1G FRU uplink module with 4x10G FRU uplink module and saw no switch failures during that time

In each test case, the system showed a temporary reduction in capability but still had more than enough power, cooling and uplink capability until high availability features took effect, showing no loss of data.

StackWise Stateful Switchover (SSO) with StackWise-160/80

Why It Matters

If a switch suddenly becomes inoperable, the network will immediately experience downtime – meaning loss of communication, data and business. To remedy this, switches use a secondary standby switch to assume primary control in the event of a disruptive system fault that stops traffic on the client side.

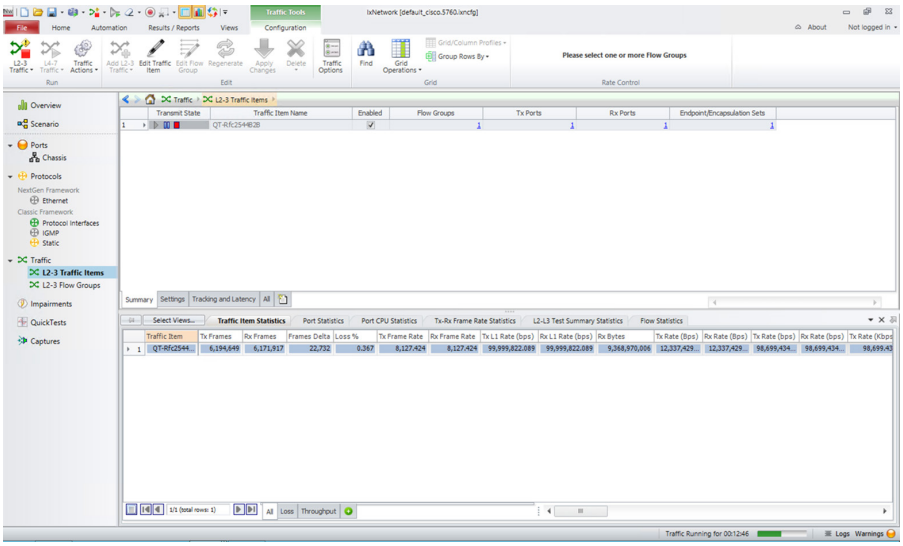
The Cisco Advantage

Cisco Catalyst 9200 switches support backplane stacking – where two or more Catalyst 9200 switches can be stacked into one logical unit, thus having unified control plane while having a distributed data plane. These members of the stack partake in StackWise Stateful Switchover (SSO) during switch failure events, creating a redundancy that can help avoid downtime.

The StackWise Virtual active switch is linked to at least one other switch, with the same aforementioned requirements, using synchronized configuration, forwarding and state information. Changes on SSO aware protocols such as STP, 802.1X, HSRP, etc. on the active switch are also propagated to the other SSO redundant switches in the stack.

During testing we observed the following:

- SSO implemented successfully with the standby switch immediately assuming primary active switch role when the original active switch in the stack experienced failure
- When running a continuous, traffic through the switch stack we saw minimal loss of traffic, proving the standby switch had assumed the state of Master switch with a transition that results in almost no downtime or data loss



StackWise-160 on Cisco Catalyst 9200 switch series saw minimal loss when the active switch on a stack of four switches was forced into a failover. Here one can see the results of RFC2544 running across the stack.

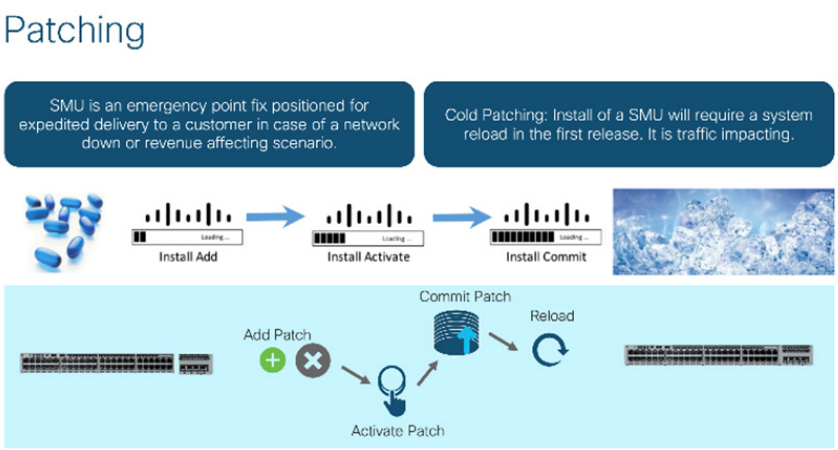
Patching

Why It Matters

Traditional architectures require an entire system software upgrade to fix bugs. But this can be time consuming to track and implement, adding cost to the patching process. What's more efficient and affordable? Adding small, necessary software patches (bug fixes) for pressing security or operational reasons on a scheduled basis.

The Cisco Advantage

- Cisco Catalyst 9200 switches allow for single-feature bug fixing. This capability provides a bug fix for individual issues between the regular quarterly releases of new operating system versions. This allows quicker, more focused responses to individual problems that arise between releases and reduces the time-to validate, as the patch does not affect any other component than the fix itself.



Cisco Catalyst 9200 switch series comes with as-needed patching between operating system releases, which can be installed and removed individually and reliably. This regular patching process removes the need for tracking and manual implementation of bug fixes, reducing cost and labor while ensuring dependable security and operation. Such patches can either be done manually via CLI or they can be pushed at once throughout the network via Cisco DNA Center.

The patch tested was easily installed and activated, showing the status "C" to indicate the SMU was "Activated & Committed".

```
9200_WebUI#show install summary
[ Switch 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
SMU   C    flash:cat9k_lite_iosxe.2019-05-08_16.01_bgajera.0.CSCvp34502.SSA.smu.bin
IMG   C    16.12.1.0.337

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

Security

MACSec

Why It Matters

Media Access Control Security (MACsec) is a standard that provides point-to-point link layer encryption and security to prevent Denial of Service (DoS), intrusion, Man-in-the-Middle (MiTM) and other types of hidden threats. MACsec helps secure protocols, like DHCP and ARP, between client and host devices communicating over Ethernet. Enterprises looking to keep communication between devices secure should be employing MACsec in their infrastructure to stay protected against the latest network attacks.

The Cisco Advantage

The Cisco Catalyst 9200 switch support MACsec encryption for different protocols – notably, MACsec Key Agreement (MKA) key-exchange protocol. While the Catalyst 9200 series supports Cisco TrustSec and Security Admission Protocol (SAP), these are for switch-to-switch links (uplinks) only and does not support switch-to-host links (downlinks). But MKA is supports on both uplinks and downlinks; this protocol allows encryption of wired networks using session and encryption keys. The MKA protocol can be used to define MKA policies and enabled MACsec between two devices, allowing peer discovery and mutual authentication with a session key. The MKA protocol manages the encryption keys of the underlying MACsec protocol.

In our testing, we observed the switch configuration which demonstrated that MACsec had been successfully configured on a port channel to protect communication on Ethernet downlinks.

Control Plane Policing (CoPP)

Why It Matters

Control Plane Policing (CoPP) is used to protect ingress traffic that affects the CPU to ensure routing security and stability. DoS attacks can drive so much traffic and exhaust physical resources of a switch; with enough control and management, CPU can be monitored and policed such that DoS attacks can be prevented. Without this protection, the switch will experience failure, and the network it belongs to will be compromised.

The Cisco Advantage

The Cisco Catalyst 9200 enables CoPP by default as a security feature to protect switch CPU from unnecessary traffic and DoS attacks. CoPP also prioritizes protocol traffic packets during high traffic volumes to ensure reliability. This prioritization of protocol packets can be further customized, if desired, based on the network requirements.

Using modular Quality of Service (QoS) CLI – or MQC – and CPU queues, different types of control plane traffic are grouped based on set criteria and assigned per queue. CPU queues are configurable through dedicated policers in hardware which do not affect CPU or data plane traffic performance. CPU loads are simply controllable, using user-based rates for each service's data.

When the switch is powered on, the system automatically scans for the policy map. If it is not found, CoPP creates and installs the policy map on the control-plane. Class maps are then created under this policy, to be detected upon the next power up. All CPU queues are enabled by default at their respective default rates.

We observed the CoPP in effect, protecting the control plane from non-management traffic. Using this information, we could ensure resources are not affected; unusual resource usage would imply an attack. The policy map auto-discover feature is enabled by default and successfully implemented.

```
C92-Stack#
Jun  4 21:44:50.559: %DMI-5-SYNC_COMPLETE: Switch 1 R0/0: syncfd: The running configuration has been synchronized to the NETCONF running data store.
C92-Stack#conf t
Jun  4 21:45:06.629: %MKA-5-SESSION_SECURED: (Te4/1/1 : 134) MKA Session was secured for RxSCI 00a5.bf9c.c185/000b, AuditSessionID , CKN 01
Jun  4 21:45:06.630: %MKA-5-SESSION_SECURED: (Te3/1/1 : 101) MKA Session was secured for RxSCI 00a5.bf9c.c186/000c, AuditSessionID , show interfaces g3/0/5
GigabitEthernet3/0/5 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is dc8c.377f.af05 (bia dc8c.377f.af05)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 12/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, media type is 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 30/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 47553000 bits/sec, 92876 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     33017341 packets input, 2113107716 bytes, 558 no buffer
     Received 33017340 broadcasts (33017340 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 33017340 multicast, 0 pause input
     0 input packets with dribble condition detected

C92-Stack#sho
C92-Stack#show pr
C92-Stack#show proc
C92-Stack#show processes s
C92-Stack#show processes c
C92-Stack#show processes cpu
CPU utilization for five seconds: 1%/0%; one minute: 3%; five minutes: 2%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0          14          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2        1264        2889        437  0.00%  0.00%  0.00%   0 Load Meter
   3          84         641        131  0.00%  0.00%  0.00%   0 DiagCard2/-1
   4         228         234        974  0.00%  0.00%  0.00%   0 RF Slave Main Th
   5           0         114          0  0.00%  0.00%  0.00%   0 Retransmission o
   6           0           2          0  0.00%  0.00%  0.00%   0 IPC ISSU Dispatc
   7           0           1          0  0.00%  0.00%  0.00%   0 RO Notify Timers
   8           0         483          0  0.00%  0.00%  0.00%   0 VIDB BACKGD MGR
   9       16312        2427       6721  0.00%  0.10%  0.10%   0 Check heaps
  10          48         281        170  0.00%  0.00%  0.00%   0 Pool Manager
  11           0           1          0  0.00%  0.00%  0.00%   0 DiscardQ Backgro
```

QId	PlcIdx	Queue Name	Enabled	(default) Rate	(set) Rate	Queue Drop(Bytes)
0	11	DOT1X Auth	Yes	1000	1000	0
1	1	L2 Control	Yes	2000	2000	6531
2	14	Forus traffic	Yes	4000	3400	0
3	0	ICMP GEN	Yes	600	600	0
4	2	Routing Control	Yes	5400	1000	1452
5	14	Forus Address resolution	Yes	4000	3400	0
6	0	ICMP Redirect	Yes	600	600	0
7	16	Inter FED Traffic	Yes	2000	2000	0
8	4	L2 LVX Cont Pack	Yes	1000	1000	0
9	19	EWLC Control	Yes	13000	6000	0
10	16	EWLC Data	Yes	2000	2000	0
11	13	L2 LVX Data Pack	Yes	1000	1000	0
12	0	BROADCAST	Yes	600	600	0
13	10	Openflow	Yes	100	200	0
14	13	Sw forwarding	Yes	1000	1000	0
15	8	Topology Control	Yes	13000	6000	5971639324
16	12	Proto Snooping	Yes	2000	2000	0
17	6	DHCP Snooping	Yes	500	400	0
18	13	Transit Traffic	Yes	1000	1000	0
19	10	RPF Failed	Yes	100	200	0
20	15	MCAST END STATION	Yes	2000	2000	0
21	13	LOGGING	Yes	1000	1000	0
22	7	Punt Webauth	Yes	1000	1000	0
23	18	High Rate App	Yes	13000	6000	0
24	10	Exception	Yes	100	200	0
25	3	System Critical	Yes	1000	1000	0
26	10	NFL SAMPLED DATA	Yes	100	200	0
27	2	Low Latency	Yes	5400	1000	0
28	10	EGR Exception	Yes	100	200	0
29	5	Stackwise Virtual OOB	Yes	8000	6000	0
30	9	MCAST Data	Yes	500	400	0
31	3	Gold Pkt	Yes	1000	1000	0

With CoPP, Cisco Catalyst 9200 switches ensure: protection against DoS attacks against the infrastructure, QoS control for control plane packets, easy configuration of control plane policies, and more reliable and available switches.

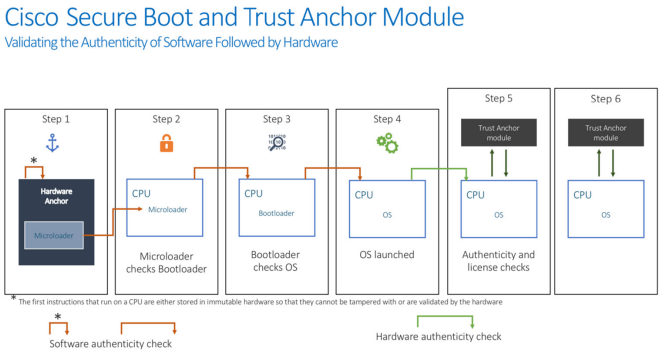
Trustworthy Systems (Secure Boot)

Why It Matters

Software should be safe to enter the network, but unless it has a signed system level driver, it may pose a direct threat. Unsigned software can come from any source and can compromise hardware, other software, and other network endpoints. Some switches use third-party sourced software, and this can put the enterprise at risk. Having Secure Boot can prevent rootkits or malware from hijacking the boot process and infecting network endpoints.

The Cisco Advantage

The Cisco Catalyst 9200 switch series guarantees trustworthy devices which are not susceptible to software image corruption. During the switch boot process, a checksum record is generated at each step and compared to a Cisco-certified record to verify software authenticity. If a checksum does not match the Cisco record, the switch will not load the software image as it can be a possible software corruption attack.



We observed a switch attempting to boot into three different software images. The images each had corrupt digital signatures which caused both the hardware and image validation to fail. These failures show that the switch would not be able to boot into unsecured, unverified images. Because of trusted hardware anchoring the secure boot, the switch did not attempt to boot the unsecured images, ensuring both hardware and software protection for the rest of the network.

Software Defined Access

Why It Matters

Manual configuration and tools are not equipped to handle the growth of dynamic enterprise networks, making policies complex to configure and inconsistent across the network. Because of this, setup or deployment of just a single switch can take hours, and a batch of switches can take weeks.

During this time, manual execution is prone to human error which can open up security vulnerabilities that put organization's resources at risk. More complexity arises when tracking VLANs, access control lists, IP addresses; wired and wireless networks are managed across multiple IT departments that yield duplicated or inconsistent management. Outdated management tools can make this process even more difficult, slowing down the network and possibly resulting in downtime that costs the business productivity and profit.

The Cisco Advantage

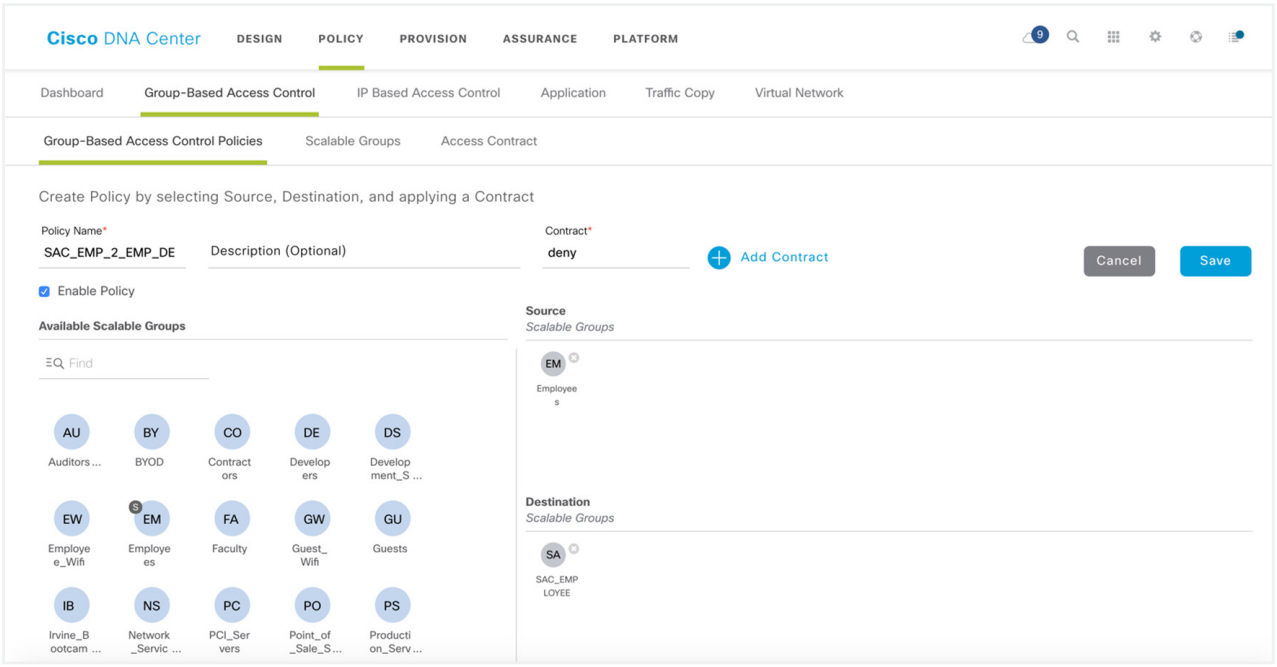
Cisco Catalyst 9200 switches come with Software Defined Access (SDA), providing network architects and engineers with a simplified way to enable business policy-based automation across the enterprise network. Automated policies can be user- or device-specific, for any application, across the network using a single network fabric.

A wide array of policies can be employed, involving several existing switch features, from a single management source to eliminate multi-department, multi-tool tracking and processing.

Cisco SDA can enable policy-based automation from the edge of the network to the cloud for segmentation, quality of service and analytics. With the ability to create Virtual Networks(VN), Cisco SDA can deliver multi-level segmentation through provisioning of embedded segmentation on Catalyst 9000 Series switches. It can also transform a chaotic, manually driven policy-controlled network into an optimized, user-friendly network that can accomplish user, device and application traffic management without constantly redesigning the network architecture to meet changing business needs.

Through Cisco SDA, enterprise end users will see an improved and consistent performance from any location because of the single network fabric, helping businesses expand dynamically without traditional network constraints.

In our testing, we observed Cisco SDA in action through the Cisco DNA Center, demonstrating powerful policy enforcement.



NetFlow

Why It Matters

Network traffic can have a powerful impact on business operations. Being able to analyze traffic for abnormalities that may be affecting performance, availability or security can help identify areas for optimization to relieve pressure on network resources and provide a better user experience. Otherwise, the organization suffers from congestion that can be costly to evaluate and fix.

The best way to manage these bottlenecks is through a network analyzer which monitors data flows for stress points that can be adjusted to prevent downtime, security vulnerabilities and maximized resources.

The Cisco Advantage

Cisco's NetFlow feature provides granular data flow visibility, detailing timed-based and application-based usage, for every single packet that enter the switch, with non-blocking line rate performance that allows for better planning and resource allocation of the network without compromising on the performance. A packet flow is uniquely identified by source/destination IP address and ports, protocol type, type of service and logical switch interface. It provides real-time networking capabilities for analyzing traffic patterns for proactive threat detection and efficient troubleshooting.

Using data captures, administrators can predictively track network trends and plan accordingly to reduce cost of network upgrades and maintenance. By maximizing performance, capacity and reliability, resources can be used efficiently to result in a higher quality services and applications.

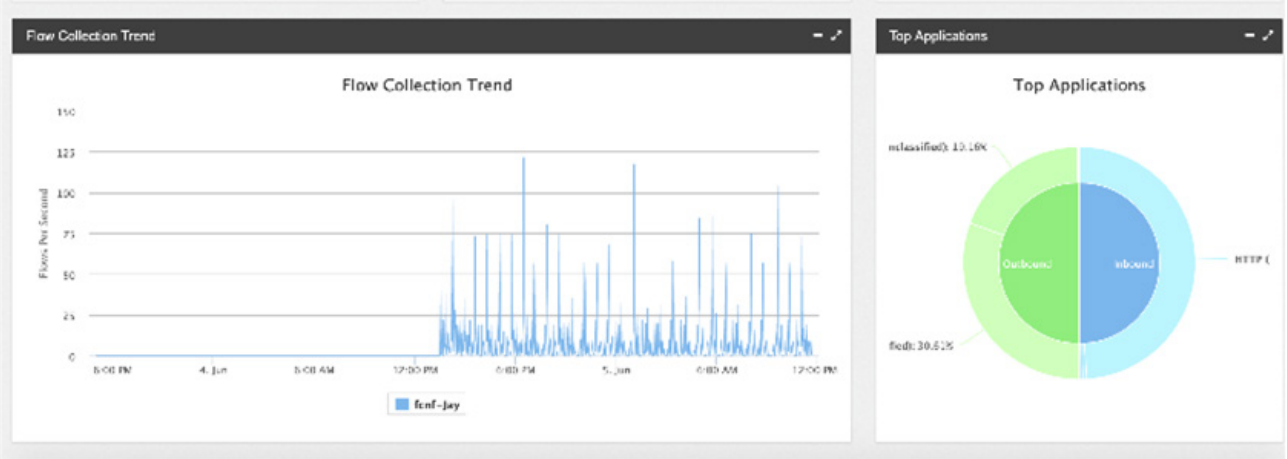
Changes in typical network behavior, as captured by NetFlow data, can indicate Denial-of-Service (DoS) attacks, viruses and other threats in real-time before they become a problem.

The NetFlow configuration above can be used to analyze data streams based on specified and collected information types. This operation can monitor traffic using hardware, in real-time, without affecting line rate.

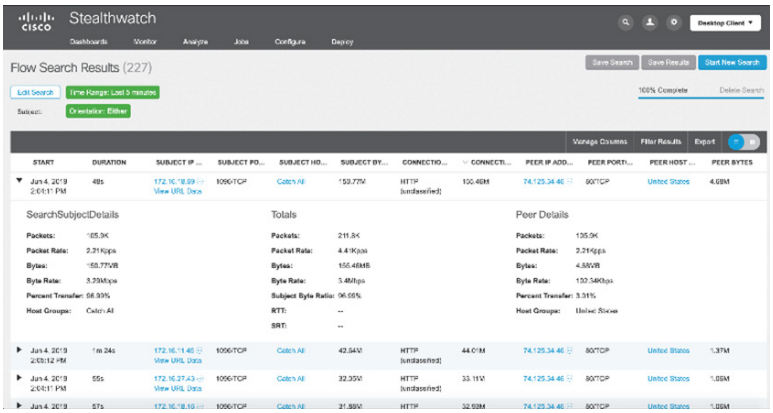
```
C92-Stack#show running-config interface g1/0/2
Building configuration...

Current configuration : 264 bytes
!
interface GigabitEthernet1/0/2
 ip flow monitor dsw_Vlan211_-47949611 input
 ip flow monitor dsw_Vlan211_-47949611 output
 power inline port 2-event
 service-policy input WEBUI-MARKING-IN
 service-policy output WEBUI-QUEUING-OUT
 ip nbar protocol-discovery
end

C92-Stack#show run
C92-Stack#show running-config | sec dsw_Vlan211_-47949611
flow monitor dsw_Vlan211_-47949611
 exporter export_Vlan211_-47949611
 record fnf-rec
 ip flow monitor dsw_Vlan211_-47949611 input
 ip flow monitor dsw_Vlan211_-47949611 output
C92-Stack#
Jun  5 18:41:57.966: %MKA-5-SESSION_SECURED: (Te3/1/1 : 101) MKA Session was secured for RxSCI 00a5.bf9c.c186/000c, AuditSessionID , CKN 01
C92-Stack#
Jun  5 18:41:59.967: %MKA-5-SESSION_SECURED: (Te4/1/1 : 134) MKA Session was secured for RxSCI 00a5.bf9c.c185/000b, AuditSessionID , CKN 01show
C92-Stack#show run
C92-Stack#show running-config | sec
C92-Stack#show running-config | section fnf-rec
flow record fnf-rec
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect counter bytes long
 collect counter packets long
 collect timestamp absolute first
 collect timestamp absolute last
 record fnf-rec
```



We observed a dashboard for NetFlow packet flows across the switch. The dashboard provides contextual information on network activity for administrators to investigate and remediate, if necessary. This reduces time and cost of IT departments to manually carry out forensic analysis of network issues. Instead, Stealthwatch allows administrators to quickly identify and isolate issues. In the configuration above, we collected a particular dataflow and visualize trends to determine anomalies worth exploring.



Using Stealthwatch, users can drill down into a particular flow on the network level for more details that reveal any possible malicious activity. Details include attributes such as packet rate, source IP, destination and data type. This view is different than the visual trend dashboard by displaying investigative information that helps IT administrators quarantine unwanted network behavior.

Internet-of-Things (IoT)

7

Perpetual Power-over-Ethernet (PoE)

Why It Matters

If a switch has software failure or is in th midst of a software upgrade, parts of the network will experience unnecessary downtime. Perpetual Power over Ethernet (PoE) can help powered devices avoid power loss to reduce the cost and labor to remediate.

The Cisco Advantage

Cisco Catalyst 9200 switches use Perpetual PoE to ensure if switches require reloading, connected devices are not forced to power down. Once enabled, Perpetual PoE instructs switches to keep power uninterrupted during reload of switch or switch stack, keeping devices connected and not forcing them to reboot.

Fast PoE

Why It Matters

If a switch is turned off for maintenance or if there is a power issue, switch port states can be compromised. This then entails switch rebooting and configuration applications to continue service. Like situations without Perpetual PoE, powered devices may lose power and require IT attention to get back online, incurring cost and downtime.

The Cisco Advantage

Fast PoE enables Cisco Catalyst 9200 switches to remember the last power drawn from the switch PoE ports for immediate power-on and reboot without having to wait for the IOS to finish booting.

In our testing, we observed Fast PoE enabled PoE devices to gain power within 30 to 60 seconds of the switch powering on before IOS has loaded.

2-Event PoE and Classification

Why It Matters

Sometimes powered devices draw more power than it typically uses to power on. Without an intelligent switch to detect this, the powered device may not receive adequate PoE to function. For example, network-powered lights will not receive appropriate power to turn on, requiring costly maintenance on a regular basis.

The Cisco Advantage

For Cisco Catalyst 9200 switches, when a powered device connects to an interface, the switch sends a short voltage pulse to determine how much power the device requires and identify the PoE device class. For example, a powered device identified as Class 4 tells the switch to immediately draw 30W of power, rather than its rated 15.4W. Since to power on, the Class 4 device requires more than 15.4W, the switch can react appropriately to allow the device to gain up to 30W of power instantly. IT employees no longer have to worry about whether powered devices have the resources they need to turn on and function.

About Miercom Performance Verified

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.

About Miercom

Miercom has published hundreds of network product 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.

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; Miercom accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

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.