Miercom

2019

Cisco Catalyst 9800

Wireless Controller

CISCO

MIERCOM.COM

Detailed Report DR190220E

Competitive test data for HPE-Aruba, Ruckus Networks and Huawei Technologies

CONTENTS

EXECUTIVE SUMMARY

1

Miercom was engaged by Cisco Systems Inc. to conduct an independent competitive analysis of leading wireless infrastructure packages – Wireless Controllers and their corresponding Access Points (APs). The vendors comparatively tested were: Cisco Systems, HPE-Aruba, Ruckus Networks and Huawei Technologies.

Miercom and Cisco jointly developed a test plan in which key features of these packages would be assessed. Comparable configurations of the four vendors' packages were then obtained and assembled. Testing was conducted in early 2019 using the current product releases.

The test plan and comparative criteria focused on four feature areas: High Availability, Security, Deployment Flexibility, and Programmability/Telemetry.

Key Findings of the Cisco 9800 Series Wireless Controller

- **Sustained high-availability when other vendors couldn't.** Many typical interruptions to ongoing operations were exercised, which includes bug fixes, system upgrades, introduction of a new AP model, and unexpected failure of the wireless controller. Cisco maintained system functionality through all scenarios.
- **Effectively detected threats in encrypted traffic.** Additionally, Cisco outperformed its competitors in tests for flow-tracking accuracy, application identification, multi-level segmentation and threat detection with encrypted traffic.
- **Deployable in all environments tested.** Products and software versions were tested for suitability of deployment in different forms: appliance, embedded on the switch, private and public clouds – with scalability and feature parity. Cisco was the only vendor to meet all deployment scenario requirements.
- **Only vendor to support broad programmability and telemetry options.** The Cisco 9800 wireless controller distinguished itself among competitors through broad support of standard programming models, including: NETCONF, RESTCONF, YANG, and on-box Python, as well as its ability to capture and export full traffic flows.

The testing validated the Cisco Catalyst 9800's leading stature against competitive Wireless Controller offerings from Aruba, Ruckus and Huawei. The Cisco product package outshined the competition in areas including high availability and security, and we proudly award the Catalyst 9800 the ***Miercom Performance Verified*** certification.

Robert Smithers

CEO

Miercom

PRODUCT OVERVIEW

2

The objective of this project was to compare key features of the industry-leading offerings for enterprise network control of the wireless infrastructure. This encompasses Wireless Controllers, which manage the vendor's associated Access Points, or APs.

We acquired and built comparable, competitive configurations to test deployed vendors' packages interchangeably in an enterprise network.

The vendors and products we examined were:

- Cisco Systems: with its new Catalyst 9800 Wireless Controller and AP 4800 Access Point
- HPE-Aruba: with its 7200 Series Mobility Controller and AP 335 Access Point
- Ruckus Networks: with its SmartZone Network Controller and R720 Access Point
- Huawei Technologies: with its AC6600 Access Controller and AP5030DN Access Point

Cisco Catalyst 9800 Series Wireless Controller

The Catalyst 9800 Series of Wireless Controllers is offered in a variety of sizes and forms. At the high end is the 9800-80, an IOS-XE based hardware package that supports up to 80 Gbps of wireless throughput. Cisco IOS-XE is powerful, modern and modular operating systems which also runs on Cisco Catalyst Switches and Cisco Routers as well. A standalone 9800-80 can handle up to 6,000 APs and up to 64,000 wireless clients. A mid-size version, also a hardware package, is the 9800-40, handling up to 40 Gbps of throughput and up to 2,000 APs and 32,000 wireless clients.


Catalyst 9800 Series Wireless Controller

In addition to these fixed hardware models there is the 9800-CL, which we also tested for this competitive analysis. CL stands for Cloud, which denotes one of the targets for this software package. The 9800-CL embodies the same IOS-XE software as on the higher-end hardware models. The wireless controller package is deployed in various modes, including Centralized, FlexConnect and Fabric Enabled Wireless.

The 9800-CL model can run in virtual environments on hypervisors like VMWare ESXI and KVM; its capacity is based on the underlying hardware and allocated computing resources. The Cisco 9800-CL also supports scalability for up to 6,000 AP and 64,000 wireless clients. The 9800-CL is also available on public cloud, like Amazon AWS Marketplace, as Infrastructure as a Service (IaaS).

Tested with the 9800-CL was the Aironet AP 4800 Access Point. This is one of the latest high-end AP models in the Cisco Aironet line, fully supporting the 802.11ac Wave 2 standard. The AP supports two radios, 2.4- and 5-GHz, and can dynamically reconfigure to run in dual-5-GHz mode. The AP supports multi-gigabit uplink speeds.

Aruba Networks 7200 Series Mobility Controller

Aruba employs a two-level wireless controller implementation. Aruba APs connect with and converse through a Mobility Controller, containing much of the wireless controller functionality. But then a separate, higher-level Mobility Master is required for handling a cluster of Mobility Controllers to offer premium features like ISSU, multi-zone AP and more.

The Aruba 7200 Mobility Controller we tested supports a max of 2,048 APs and up to 32,728 wireless clients. Aruba offers a virtual Mobility Controller which can be installed om VMWare ESXI as a virtual machine (VM) in the private cloud deployments.

The Aruba Mobility Master is a separate, and additional, specialty software package that can either be deployed as a VM or hardware appliance. A Mobility Master can manage a cluster of up to 12 Mobility Controllers. Pricing of the software is based on the total number of wireless controllers and clients.

The AP 335 AP we used in the Aruba test configuration is a mainstay of Aruba's, with integrated radios that support 2.4- and 5-GHz operation. Up to 256 wireless clients are supported per radio.

Aruba 7200 Series Mobility Controller

Ruckus Networks SmartZone Network Controller

Ruckus Networks' SmartZone family of wireless controllers comes in a physical appliance form, or as a software package. The SmartZone Controller is software that runs either in a virtual hypervisor environment – several are supported – or on a commodity x86 server. We tested the wireless controller running in a VMWare environment. Each wireless controller manages a cluster of APs; according to the vendor, a single controller can scale up to 10,000 APs and up to 100,000 wireless clients – this depends, of course, on the computing power and resources of the underlying wireless controller platform.

The Ruckus R720 AP was used in the Ruckus configuration tested. The R720 supports Wi-Fi standards including 802.11ac Wave 2, a multi-gigabit uplink and up to 512 clients per AP. Both 2.4- and 5-GHz radios are integral.

Ruckus SmartZone

Huawei Technologies AC6600 Access Controller

Huawei's wireless controllers are hardware. Some are boards that insert in the vendor's switches; others are standalone appliances. The Huawei wireless controller models range from the low-end AC6003 – managing 48 APs and 1,000 wireless clients with 2 Gbps of wireless throughput, to the high-end, AC6800V supporting 10,000 APs and 100,000 wireless clients with 60 Gbps of wireless throughput.

We tested with Huawei's mid-level AC6605 Access Controller, which manages up to 1,000 APs and 10,000 wireless clients. The controller supports standards up through 802.11ac Wave 2 and up to 10 Gbps of wireless throughput.

Tested with the AC6605 controllers was the AP5030DN AP. The AP supports both 2.4- and 5-GHz radios, 2 x Gbps uplinks and up to 256 wireless clients.

Huawei AC6605 Access Controller

TEST BED OVERVIEW

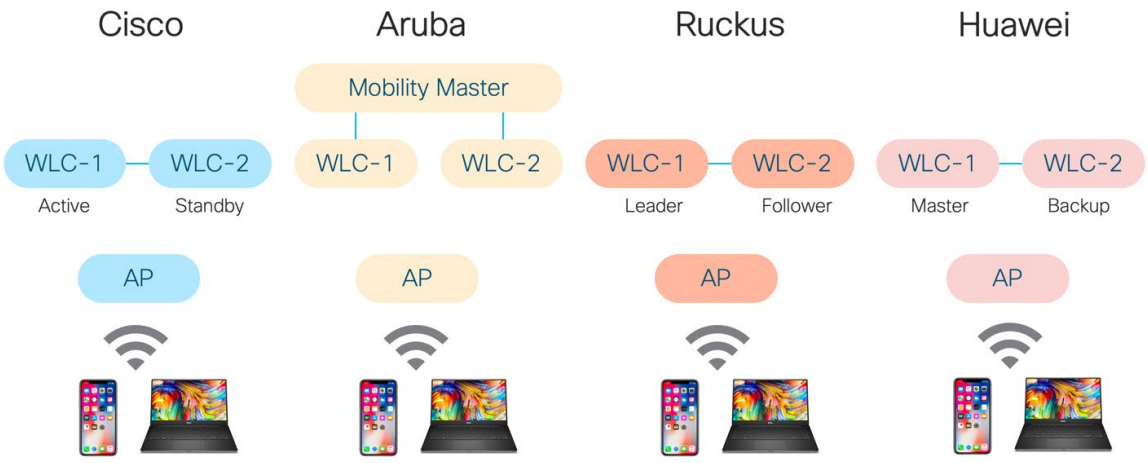
3

To the extent possible, comparable product configurations of the four vendors were acquired and assembled, each according to that vendor's specific deployment instructions and/or Best Practices recommendations.

To test failover redundancy, we deployed two of each vendor's wireless controllers. Cisco and Ruckus offered software versions of their respective controllers, and so we deployed two instances of each in a VM environment. Aruba and Huawei controllers come in hardware form, so pairs of their appliances were deployed.

As noted in the previous section, Aruba has placed some of its controller and cluster management functionality in a higher-level "Mobility Master." So, we also deployed Mobility Master software in addition to the two Aruba Mobility Controllers.

The test bed configuration was set up as shown below. The same user devices, like Dell laptop/Apple MacBook and iPhone, were used in each test: disconnected, powered down, and then reconnected to the appropriate vendor AP.



Source: Miercom

RESULTS: Availability

4

We define availability as the ability of users to access and use a system or service. "High availability" implies that immediate and ongoing access is offered all of the time.

High availability was tested in five scenarios, examining the effect on wireless controller availability during events of interrupted access. The first four scenarios are predictable and schedulable, performed typically during off hours or on weekends, but today's mission critical networks demand these to be done on the live production network. The last scenario is an unpredictable event.

1. Bug fixes: Apply necessary, minor code "patches" to the wireless controller
2. Feature enhancements: Addition of code that adds or expands feature capabilities
3. New AP hardware: Addition of new AP model without need to upgrade the entire wireless controller software
4. System upgrades: Installation of a new system software release
5. Failover of a wireless controller or network during the unplanned event

Applying Bug Fixes

Fixing bugs are essential but traditionally requires entire wireless controller system software upgrade. This has its own drawback like interoperability validation which adds operational cost. Small, necessary software patches (bug fixes) are usually applied for pressing security or operational reasons which can impact availability of a wireless controller. For this reason, we provisioned two of each vendor's controllers. We found this process is handled very differently by the products.

Cisco: Excellent
Bug patches can be installed on any of the components while the wireless infrastructure keeps running; there is no impact on availability or system operation. The patch file was copied to the bootflash location on one of the Cisco wireless controllers and then a file-commit command was executed. In addition, a straightforward command-line process allows the patch to be undone and removed, also with no interruption to system operation.

Aruba: Poor
Patching of Aruba Access points or wireless controllers is not supported. Rather, bug patches need to be applied as a whole system upgrade, which necessarily involves down time.

Ruckus: Fair
Patching of Ruckus Access points or wireless controller is not supported. Rather, bug patches need to be applied as a whole system upgrade, which necessarily involves down time. Ruckus does support separate software image for Access Points, so admin restrict downtime to certain APs at a time.

Huawei: Excellent
Bug fixes can be installed on Huawei wireless controllers without down time. The wireless controller patch can be applied using CLI or web interface.

Feature Enhancements

Similar to bug fixes, software changes and/or reconfigurations are applied to activate new features. One such feature enhancement is updating the application signature database. This pack was installed in the Cisco controllers for this test.

Cisco: Excellent
Protocol pack releases for feature enhancements are applied and installed, or uninstalled, without down time or interruption to system operation.

Aruba: Excellent
Aruba has "service modules" for applications, which allow for enhancements to be applied and configured with no disruption or downtime.

Ruckus: Fair
Ruckus requires a full system upgrade to support feature enhancements. It is a disruptive process, as it involves a wireless controller reboot.

Huawei: Fair
As with Ruckus, feature enhancements to the Huawei controller are installed only as part of a new system installation, which typically entails downtime.

New AP Model Hardware

Onboarding a new AP model is an essential part of a wireless network and often requires an entire system software upgrade – disrupting services and impacting users.

Cisco: Excellent
Installed new AP device pack on the existing wireless controller software. This allowed us to onboard new AP hardware such as new Wi-Fi 6 AP to join the controller without upgrading the base wireless controller software. This process does not required reboot or does not impact wireless service.

Aruba: Poor
An installed wireless controller software had to be completely upgraded with a system reboot to support new AP model hardware.

Ruckus: Fair
Ruckus offers separate AP images which are de-coupled from the wireless controller software, so a new AP can be added without disrupting wireless service. But all AP images are not available for the latest wireless controller software. For example, a new Ruckus Wi-Fi 6 AP R730 image was only available for the old wireless controller software release v3.6 but was not available for the latest software release v5.0

Huawei: Excellent
New APs can be added with no downtime or wireless controller restart.

System Upgrades

In a system upgrade, the operating code currently running in the primary or active controller is replaced with a whole new release. To do this without interrupting availability, a secondary standby system is usually first upgraded, then control is shifted from the primary to the standby. The other controller becomes upgraded. Here are how the vendors fared in this task:

Cisco: Excellent
With Cisco's intelligent RRM based rolling AP upgrade, the entire system was upgraded with new software with zero downtime and with automated operation.

Aruba: Good
It turns out that performing a system upgrade with no downtime requires a second high-level Mobility Master package, which adds more touchpoints and cost.

Ruckus: Poor
Upgrading a wireless controller's system software requires that traffic across that controller be stopped, which impacts end user experience.

Huawei: Poor
System upgrades require taking down one (of the two) wireless controllers, which causes the other controller to become the new Master. The Master then keeps looking for the Secondary and waits for it to come up before traffic flows again, so there is traffic-flow disruption.

Controller Failover

We procured two of each vendor's wireless controllers to exercise the ability to failover from one to the other in the event of wireless controller or network failure. The AP in each vendor's test configuration had direct access to both controllers (see test bed diagram in Section 2).

Cisco: Excellent
One wireless controller is designated the Active and the other the Standby. The Standby remains synchronized with the Active on both AP and client states. In the event the Active controller fails, the Standby assumes control as the Active, with no interruption to AP, clients and services.

Aruba: Good
Aruba also offers sub-second failover (ISSU) like Cisco, but Aruba requires an additional Mobility Master controller appliance or VM to implement this feature which adds cost and complexity.

Ruckus: Fair
A minimum three-controller cluster is required to support sub-second failover. With three controllers appropriately configured, traffic continues uninterrupted if a controller failure occurs.

Huawei: Poor
With Huawei's N+1 support, an extra controller could be used to back up the active controller. But Huawei does not offer sub-second failover which impacts end user and application experience.

AVAILABILITY RESULTS SUMMARY

	Cisco	Aruba, a Hewlett Packard Enterprise company	Ruckus, an ARRIS company	Huawei
Competitive Rating	✓✓✓	✓	✓	✓
Bug Fixes	Excellent	Poor	Fair	Excellent
Feature Enhancements	Excellent	Excellent	Fair	Fair
New AP Model	Excellent	Poor	Fair	Excellent
System Upgrades	Excellent	Good	Poor	Poor
Controller Failover	Excellent	Good	Fair	Poor

RESULTS: Security

5

This section reviews aspects of security offered by the different vendors in their wireless infrastructures. In comparing these products for these features, we did take into account other, often optional, security-oriented packages that the vendor offers, which would run on servers elsewhere in the user's network, typically in a secure, central data center.

1. Application visibility: How accurately can the system identify specific applications?
2. Flow tracking: Can the system accurately report on the specifics of a particular traffic flow?
3. Encrypted traffic visibility: Can the system identify threats in encrypted traffic without need to decrypt the traffic?

Application Visibility and Identification Accuracy

We found there are differences in how well the products identify traffic by application. Cisco, for example, says it can identify 1,400 applications. Aruba says it can identify 2,300 applications, but it seems many of these are actually web sites, not unique applications.

In addition, we observed that the products vary in the accuracy of their application identification. For example, the below table shows the differences in how the packages identified two traffic applications: a WebEx audio-video and a CNN Live Video (and/or "Akamai," referring to the content-delivery service).

How Vendors Identify Test Applications

	Cisco	Aruba (a Hewlett Packard Enterprise company)	Ruckus (an ARRIS company)	Huawei
WebEx A/V Call	"cisco spark and cisco spark-video"	"stun ? https ?"	"stun rctp"	"stun https"
CNN Live Video (Akamai)	"cnn video, akamai"	"cnn, akamai"	"miscellaneous"	"cnn"

Two notes on the above table: "https" and "stun" are the underlying protocols used by WebEx for audio and video, but the application is WebEx, or Spark. Spark is an adjunct application that Cisco recently integrated with, and now encompasses, WebEx.

With all results considered, here is a summary of each product's application visibility aptitude:

Cisco: Excellent
Application identification was consistently accurate – including Jabber, Netflix, Dropbox, and YouTube. Cisco can dive deeper into data packets with its DPI (Deep Packet Inspection). Only Cisco correctly identified the WebEx as a separate audio-video application and the CNN Live Video with Akamai as the actual video source, offering more granular control.

Aruba: Good
Many applications are identified: Jabber, Netflix, Dropbox, and YouTube – as well as specific web sites. It had incorrect identification on many applications. For example: WebEx.

Ruckus: Poor
Many applications were incorrectly identified. Ruckus offers no DPI. Application identification was hit or miss.

Huawei: Fair
Limited application identification and DPI. Some applications are correctly identified; some were incorrect, including WebEx misidentification.

Flow Tracking

Another security-based test we conducted was to see whether the system could accurately track and report flows (e.g. large file movements). To test this, we sent a 6.5 megabyte (MB) file via the File Transfer Protocol (FTP) through the system under test. Each vendor's system recognized FTP as the application, but some of the vendors apparently got a late start in recognizing and then reporting this file transfer. The table below shows the difference between reporting of the same file transmission.

Reporting a 6.5 MB File Transfer

	Cisco	Aruba (a Hewlett Packard Enterprise company)	Ruckus (an ARRIS company)	Huawei
File Size Reported	6.5 MB	4.9 MB	1.2 MB	6.5 MB
When Reported	Immediately on transfer	~5 minutes	~5 minutes	A few minutes

The incorrect short size of this transferred file reported by Aruba and Ruckus may be due to the sampling technique these vendors use for traffic monitoring. Where Cisco is able to track 100 percent of traffic – made possible through NetFlow and a special hardware that tracks every packet through the system – competitors use a sampling process that only "sees" a fraction of monitored traffic flows.

Here is a summary of the products' flow-tracking capability:

Cisco: Excellent
Applications were detected immediately with the accurate amount of data passed for that application.

Aruba: Fair
Reports application activity long after transmission begins and reports considerably less data transmitted than actually sent.

Ruckus: Poor
Reports application activity long after transmission begins and reports much less data transmitted than actually sent.

Huawei: Good
Reports application activity accurately, unless monitoring is started after the transfer already began; reporting of application activity is delayed.

Detecting Threats in Encrypted Data

User data traffic is increasingly being encrypted to protect it from being monitored or intercepted by malicious users. But also increasingly, hackers are using encryption to hide their malware and conduct other disreputable operations, like Man-in-the-Middle (MiTM) and keylogging attacks. This problem increases with proliferation of IoT devices.

Most enterprises examine some of encrypted traffic by decrypting it first, via security products like a firewall or intrusion prevention system. But this process is time consuming and drains network performance and resources. Also, after decryption, this data is then vulnerable to prying eyes.

From among the vendors in this testing, only Cisco offered a solution: Encrypted Traffic Analytics, ETA – a technology that spots malware in encrypted traffic without having to first decrypt it. ETA is an IOS-XE feature that includes Enhanced NetFlow and uses advanced behavioral algorithms to identify malicious traffic patterns hiding in encrypted traffic.

Last year, Cisco engaged Miercom to perform an independent assessment of Cisco's Encrypted Traffic Analytics solution in an enterprise network. The results of that study can be found here. In that evaluation, Miercom separately sent known and unknown threats – viruses, botnets, Trojans, ransomware, and more – in encrypted and unencrypted traffic, through large-enterprise ETA and non-ETA networks – looking to identify the threats.

ETA doesn't decrypt messages. Rather, it assembles metadata profiles of encrypted traffic flows – their packet lengths, inter-packet arrival times, and so on. The metadata is then exported in NetFlow v9 records to Cisco Stealthwatch and its Global Threat Analytics – a cloud-based function of Stealthwatch – for further analysis, risk assessment and action.

A key Stealthwatch function is to continually monitor traffic and source-destination flows, and to build a baseline of normal web and network activity. With the encrypted-flow metadata sent to it by ETA, Stealthwatch applies "multi-level machine learning" to identify traffic behavioral anomalies, which may indicate suspicious events. By running a range of malware threats through each system, we determined and then compared the detection accuracy and time of each.

Our key finding: ETA Works! ETA showed as much as 36 percent higher rates of malware detection than the non-ETA system. The ETA-based system also found 100 percent of threats buried in encrypted data within three hours. We noted, too, that ETA improves its accuracy over time: In less than five minutes, ETA had already detected nearly two-thirds of all the malicious flows in encrypted flows – almost double that of the non-ETA system.

The ETA function is well integrated with Stealthwatch. Threats are ranked by severity and readily displayed with detailed information, along with remediating action options, once confirmed. Of the vendors included in this competitive analysis, only Cisco offers anything like ETA for the detection of malware in encrypted traffic. Moreover, Cisco offers this functionality across switching, routing and wireless platforms.

Cisco: Excellent
Cisco Wireless Controller successfully detected malware, trojans inside encrypted traffic.

Aruba: Poor
Aruba does not support detection of threats from encrypted traffic.

Ruckus: Poor
Ruckus does not support detection of threats from encrypted traffic.

Huawei: Poor
Huawei Wireless Controller does not support detection of threats from encrypted traffic.

SECURITY RESULTS SUMMARY

	Cisco	Aruba, a Hewlett Packard Enterprise company	Ruckus, an ARRIS company	Huawei
Competitive Rating	✓✓✓	✓	✓	✓
Application Visibility	Excellent	Good	Poor	Fair
Flow Tracking	Excellent	Fair	Poor	Good
Encrypted Threat	Excellent	Poor	Poor	Poor

RESULTS: Deployment

As already discussed, wireless LAN infrastructures differ substantively in terms of the high availability and security capabilities they support. These products also differ considerably in form, or "footprint," and the range of APs and clients they can handle.

This "Deployment" section looks at these aspects of the products:

1. Appliance-based and embedded wireless on switch: For larger campus or locations, a hardware-based wireless controller appliance can be the most appropriate solution – for centralized data forwarding. Additionally, embedding the wireless controller on a switch/router package can be an ideal solution in locations without an IT staff, especially in a distributed enterprise or branch environments.
2. Software, Virtualized, in Private or Public Clouds: In large distributed networks, it may be preferred to run the wireless controller in the data center "cloud," typically as a service in a virtualized environment (e.g. VMware, Hyper-V, KVM). For some, running the wireless controller in a public cloud (like Amazon Web Services or Google Cloud Platform) may be a consideration.
3. Scalability: Valid deployment concerns are capacity and incremental growth. Some of these concerns include: Can a wireless infrastructure supports sufficient APs and wireless clients? Can a wireless controller product line support a wide data plane capacity range? Can the wireless controller be clustered to incrementally handle enough APs and clients?

Standalone appliance or Embedded with Switch

Here are how the four vendors differ in the hardware forms their wireless controller offered:

Cisco: Excellent
Offers a range of wireless controller appliances, as well as the same full wireless functionality integrated with many of its switch hardware packages.

Aruba: Fair
Aruba offers wireless controllers in many appliance forms, but often require an additional layer of an appliance/VM called "Mobility Master" to manage clusters of the wireless controller appliances. This additional Mobility Master adds cost, complexity and another touchpoint in the network. Aruba's appliance-based controller AP scale is threefolds lower than Cisco. Aruba does not offer a product which integrates the wireless controller with a switch.

Ruckus: Fair
The vendor offers an appliance-based wireless controller platform, with the same functionality in a software package but with extremely limited data plane traffic capacity. It does not offer a product which integrates the wireless controller on a switch.

Huawei: Good
The vendor offers wireless controller in the form of standalone appliances. The wireless controller integrates into the switch, and the wireless controller line cards that insert in the vendor's modular switches are also available, though with some feature differences.

Virtualized Wireless Controller in Private or Public Clouds

A wireless controller in a software package provides a valuable deployment option for users who prefer their infrastructure operations to be public cloud (e.g. Amazon AWS) or private cloud (data center) based. Running a wireless controller as a tenant service in a virtualized environment addresses some users' concerns of security and perhaps easier configuration, deployment and management. Here are how the four vendors address this:

Cisco: Excellent
The vendor offers the same, singular wireless controller software code in its software version as on its wireless controller appliances. The same features and scale are supported regardless of platform footprint. Moreover, Cisco offers a virtualized wireless controller for private cloud, as well as public cloud.

Aruba: Fair
The vendor offers a wireless controller software package, for virtualized private cloud environments like VMware and KVM, but with extremely low scale for APs and users. For example, the highest-end Aruba wireless controller VM scale is sixfolds lower than Cisco wireless controller VM. Aruba does not offer wireless controller in the form of public cloud, like AWS.

Ruckus: Excellent
The vendor offers its wireless controller product as a virtualized software module, suitable for deployment in public or private cloud environments.

Huawei: Poor
The vendor does not offer its wireless controller in a software version for public or private cloud.

Scalability

The wireless controller solution should be able to cater the scale requirements of growing businesses without impacting the operational cost and with minimum footprint.

Cisco: Excellent
The high-end standalone appliance form of the wireless controller, the 9800-80, handles up to 6,000 APs and 64,000 wireless clients. The cloud software version we tested, the 9800-CL, also supports up to 6,000 APs and 64,000 clients, and scales linearly with full redundancy.

Aruba: Fair
The vendor's high-end Series 7280 wireless controller supports a max of 2,048 APs and 32,768 clients. However, up to 12 of these controllers can be clustered, expanding capacity to only 10,000 AP and 100,000 clients with additional touchpoint of Mobility Master VM/ appliance. But it increases capex and operational expenses by multiple folds.

Ruckus: Excellent
The SZ300 or SmartZone controller offers a scale of 10,000 APs and 100,000 clients. However, three of these wireless controllers can be clustered to offer a total scale of 30,000 APs and 300,000 clients.

Huawei: Good
The vendor's wireless controllers include the AC6000, AC6600 and AC6800 Series. The vendor's high-end AC6800V claims to support up to 10,000 APs and 100,000 wireless clients. No clustering is supported by Huawei wireless controllers.

DEPLOYMENT RESULTS SUMMARY

	Cisco	Aruba, a Hewlett Packard Enterprise company	Ruckus, an ARRIS company	Huawei
Competitive Rating	✓✓✓	✓	✓✓	✓
Appliance, or with Switch/Router	Excellent	Fair	Fair	Good
Software, Virtualized, Private or Public Cloud	Excellent	Fair	Excellent	Poor
Scalability	Excellent	Fair	Excellent	Good

RESULTS: Programmability & Telemetry

7

Today's networks are much more agile and complex than the yesterday's networks, and so traditional ways of configuring and extracting information from wireless controllers are not enough. As an administrator, you need modern tools for automation and analytics, prompting a lot of vendors to begin offering tools - like API to automate operations like configuration or retrieval of management or data. API was primarily used for application layer. For the network layer, NETCONF/ YANG and Open Config Model are well known methods to achieve programmability and telemetry. In addition to these methods, getting consistent data flow information in form of NetFlow/sFlow/NetFlow is very essential for better visibility and for enforcing policies. On-box Python support is an add-on to enable scripting right on the wireless controller itself. We compared the products in three main areas:

1. API/Python/NETCONF/YANG and Standard Model Support: Many products support "proprietary APIs," but these are not open, and they limit third-party software development. Some products support web-like, remote program access, such as RESTFUL, while others support open program standard models. Among the most common standard models for network-equipment operations: YANG (Yet Another Next Generation) data modeling language; Python, an interpreted high-level language; and NETCONF, (the Network Configuration protocol), standardized in IETF RFCs. NETCONF is an XML-based protocol that applications can use to request information from and make configuration changes to network devices like wireless controllers.
2. Full versus Sampled Data: For security, as well as traffic modeling, the ability to track specific flows can be a valuable tool. But copying and storing data streams at gigabit speeds takes a lot of computer resources. Vendors have implemented different solutions, one being sFlow, a traffic-sampling technology in which the device captures only about two packets out of every 100 from a stream. This may not be sufficient, however, for analysis software to adequately scrutinize and assess the stream. An alternative is NetFlow, implemented by Cisco along with special supporting hardware, which permits all packets in a specified stream, 100 percent, to be captured and exported for analysis.
3. SNMP Support: The original Simple Network Management Protocol originated as an Internet standard decades ago and became incredibly popular as a standardized way to retrieve management data and perform minor configuration actions. This is done with simple "get" and "set" operands. To enhance SNMP and add security, versions 2 and 3 of SNMP were adopted.

APIs and Standard Model Support

Our assessment of the vendors' API and programmatic support is as follows:

Cisco: Excellent
Supports popular standard models including YANG and NETCONF/RESTCONF, along with traditional APIs, and on-box Python scripting is also supported. Every single CLI is offered in the form of YANG model to offer day-0 to day-n operations using programmable interfaces.

Aruba: Fair
XML/RESTFUL API support, but no support for either YANG or NETCONF models, or on-box Python.

Ruckus: Fair
RESTFUL API support, but no support for either YANG or NETCONF models, or on-box Python.

Huawei: Poor
Limited API support; no support for either YANG or NETCONF models, or on-box Python.

Access to Full vs Sampled Data

Our review of the vendors' capabilities regarding data capture concluded as follows:

Cisco: Excellent
Supports NetFlow full capture of data streams for export and analysis

Aruba: Poor
No support for NetFlow or sFlow.

Ruckus: Poor
No support for NetFlow or sFlow.

Huawei: Good
Supports NetStream but with limited sampling capture of specified flows. Optionally supports full capture using NetStream but at the cost of compromised performance.

SNMP Support

Our assessment of the vendors' SNMP support concluded the following:

Cisco: Excellent
Fully supports SNMP v1, v2 and v3.

Aruba: Excellent
Fully supports SNMP v1, v2 and v3.

Ruckus: Excellent
Fully supports SNMP v1, v2 and v3.

Huawei: Excellent
Fully supports SNMP v1, v2 and v3.

PROGRAMMABILITY & TELEMETRY RESULTS SUMMARY

	Cisco	Aruba, a Hewlett Packard Enterprise company	Ruckus, an ARRIS company	Huawei
Competitive Rating	✓✓✓	✓	✓	✓
APIs and Standard Model Support	Excellent	Fair	Fair	Poor
Full vs Sampled	Excellent	Poor	Poor	Good
SNMP Support	Excellent	Excellent	Excellent	Excellent

RESULTS SUMMARY

	Cisco	Aruba, a Hewlett Packard Enterprise company	Ruckus, an ARRIS company	Huawei
Availability	✓✓✓	✓	✓	✓
Security	✓✓✓	✓	✓	✓
Deployment	✓✓✓	✓	✓✓	✓
Programmability & Telemetry	✓✓✓	✓	✓	✓

THE BOTTOM LINE

Cisco was observed scoring Excellent in all four categories of testing: High Availability, Security, Deployment Flexibility, and Programmability/Telemetry. We found its performance to be overwhelmingly impressive in these areas:

Cisco Wireless Controller satisfies all high availability requirements, such as sub-second failover during unplanned events, zero downtime for planned events such as fixing AP/Wireless Controller bugs, adding new AP models and rolling AP upgrade etc. Whereas HPE-Aruba, Huawei, Ruckus failed to satisfy all the availability conditions.

Cisco Wireless Controller offers comprehensive security providing deep-dive packet inspection for application identification and control, full NetFlow visibility, and identification of threats hidden inside encrypted traffic. Cisco's wireless controller supports SGT (Scalable Group Tags) enabling multi-level segmentation – a unique differentiator compared to HPE-Aruba, Ruckus or Huawei.

Cisco offers deployment flexibility to implement Wireless Controller functionality on dedicated physical appliances, embedded on switch, public cloud or private cloud without compromising any features or scale. Whereas Aruba, Huawei, Ruckus offers limited wireless controller footprint options with lower scale and/or missing features.

Cisco has unbeatable programmability and telemetry using popular standard models: YANG, NETCONF, RESTCONF, traditional APIs and, uniquely, on-box Python scripting. HPE-Aruba, Ruckus, Huawei are limited to only standard APIs.

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.