Technical Validation

Cognitive Networking with the Arista Campus Solution

Simplifying and Optimizing the Behavior, Visibility, Security, and Management of Networks

By Alex Arcilla, Validation Analyst; Tony Palmer, Senior Validation Analyst; and Bob Laliberte, Senior Analyst

June 2019

This ESG Technical Validation was commissioned by Arista and is distributed under license from ESG.

Contents

Introduction 3
Challenges – The Campus Network Is Rapidly Changing 3
The Solution: Arista’s Cognitive Campus Network Solution 4
ESG Technical Validation 5
Software Consistency 5
ESG Testing 5
Cognitive WiFi Edge 8
ESG Testing 8
Management and Monitoring 12
ESG Testing 12
The Bigger Truth 15

ESG Technical Validations

The goal of ESG Technical Validations is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Technical Validations are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team’s expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

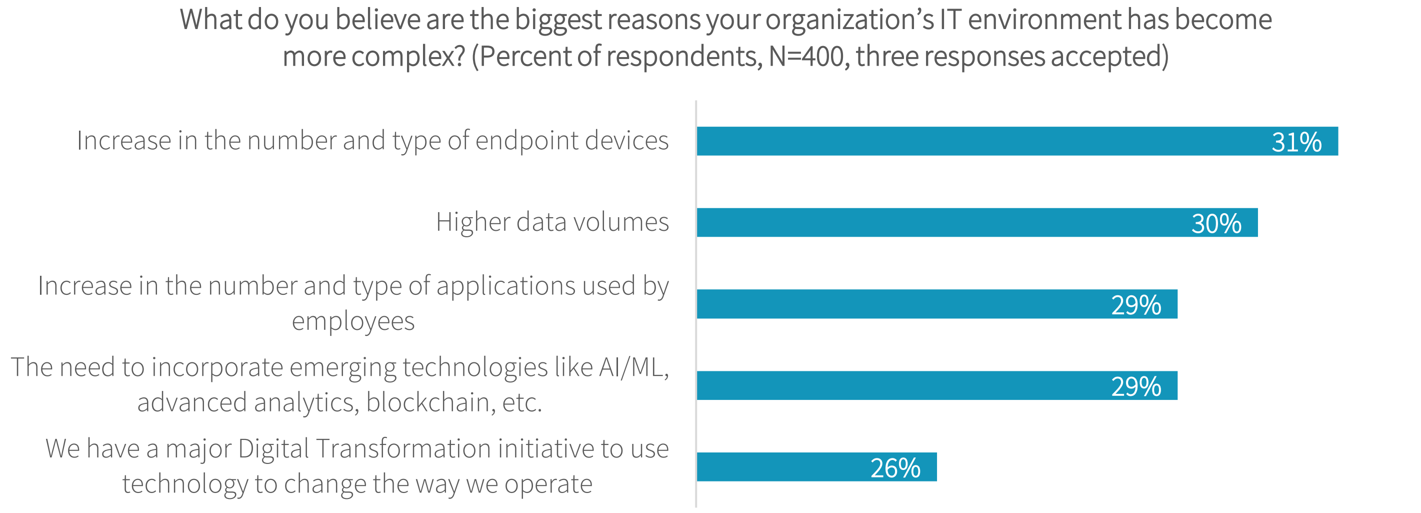
Introduction

This ESG Technical Validation documents hands-on testing of the Arista Cognitive Campus solution, comprised of the Arista campus spline switches, PoE access/leaf switches, Arista WiFi access points, and CloudVision network management software. We validated that the Arista solution provides the functionality customers expect in campus networking solutions, such as IP Phone support and integrated wired and wireless network management leveraging a single software platform. Furthermore, ESG tested Arista's Cognitive Campus for flow and device visibility, management, and security.

Challenges – The Campus Network Is Rapidly Changing

ESG research recently uncovered that 66% of organizations view their IT environments as more or significantly more complex than they were two years ago. The three most cited reasons provided by respondents for this increased complexity were the increase in the number and type of endpoint devices, higher data volumes, and the increase in the number and type of applications used within an organization.[1]

Figure 1. Top Five Reasons for Increase in IT Network Complexity



Source: Enterprise Strategy Group

This complexity is due in part to the increasing number of applications hosted in cloud environments (SaaS and IaaS), requiring hybrid cloud networks, the increasing use of IoT devices, and the need to secure a wide range of devices to protect against the latest threat vectors. Issues related to security, segmentation, and monitoring need to be considered for both smart endpoints that contain an 802.1X supplicant and simple plug and play IoT devices that lack the ability to authenticate to the network.

In many cases, organizations have built out and managed datacenter and campus networks using multiple point solutions potentially from different vendors, each with its own architecture, OS software, and management systems. As the campus becomes an integral part of the hybrid cloud experience, this traditional approach becomes less effective as point solutions do not integrate seamlessly. Organizations face the challenge of operating their networks via a patchwork of these solutions, making workflows less efficient and fragmenting end-to-end network visibility, from the campus core to the access layer, down to the end devices generating network traffic.

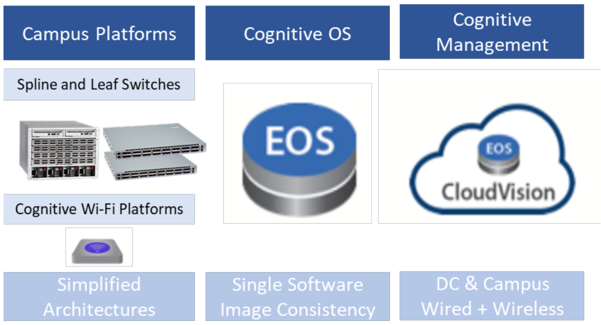
What is needed is a solution that enables organizations to build and manage their campus networks (and end-to-end networks) with a common architecture and software system that will enable greater efficiencies in network operations. It is

[1] Source: ESG Master Survey Results, *2019 Technology Spending Intentions Survey*, March 2019.

not uncommon for large enterprises to be running 10+ different versions of network OS software from the same vendor. Managing multiple versions of software is not only operationally time consuming but also less secure. A single software version should be used to reduce complexity, and standards-based features should be used for operational leverage and to avoid vendor lock-in.

Campus solutions should be capable of managing both wired and wireless network devices via a single management interface. From a security perspective, being able to identify all unique wired and wireless devices within the campus network, determine how they are connected, and monitor traffic continuously to baseline network behavior would be an advantage. Baselining this behavior will help organizations to identify and address anomalous behavior quickly with little manual intervention into individual devices, thus helping to improve both network performance and security. This interface will aggregate relevant details at the device and network traffic level to increase and improve network visibility.

The Solution: Arista's Cognitive Campus Network Solution



The Arista Cognitive Campus solution extends the cloud networking principles employed in designing Arista's datacenter solutions into the campus network. All Arista switch platforms are supported by the Arista Extensible Operating System (EOS), providing consistent operations, workflow automation, and high availability; in fact, all Arista switches leverage the same software binary. Other features that organizations can leverage within the campus network include Smart System Upgrade (SSU), high availability with Stateful Switchover (SSO), dynamic path selection, secure macro segmentation services, flow telemetry, and NetDB streaming—specifically for device data collection to facilitate network monitoring activities. The following components comprise this solution:

- **Modular 7300X3 and fixed 7050X3 switch platforms** – Arista has designed these spline (or distribution) switches for high availability and simplicity. The platform's uniform performance, supported by balanced forwarding tables and dynamic buffers, enables organizations to manage the growth of mobile and bursty traffic generated by endpoint devices such as phones and IoT devices.

- **720XP Power-over-Ethernet (PoE) switch series** – Arista introduces the 720XP series as a PoE leaf (or access) switch for the campus network. The platform has been designed to support power negotiation over all IEEE PoE standards (802.3af, 802.3at, 802.3bt), such that it will support the growing number of endpoint devices currently accessing the campus network.

- **Arista WiFi access point (AP) product line** – Arista launched its WiFi access point product line in 2018 to address the growth of WiFi access in today's campus networks. The Client Journey is a dashboard that can simplifiy troubleshooting and remediation of network issues such as WiFi association and authentication. Solving other encountered network issues is facilitated by an inference engine that can automate root cause analysis and recommendation of possible solutions.

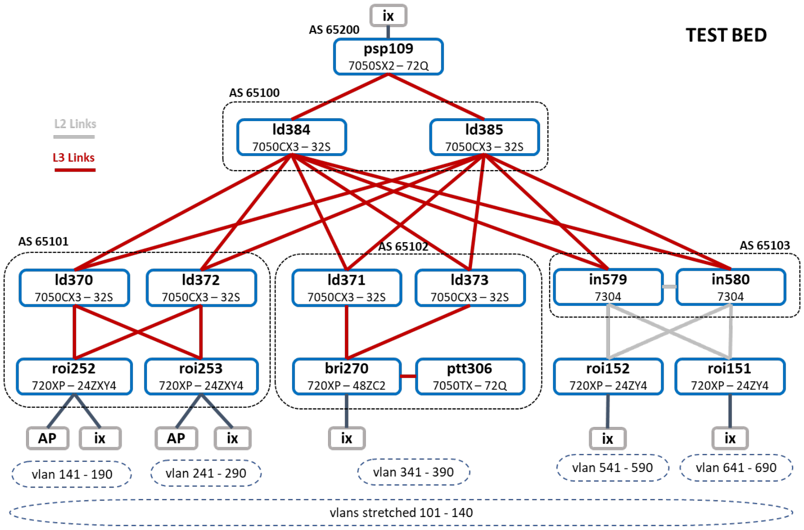
Why This Matters

Analyzing non-sampled flow communication patterns is increasingly important to guard against malware with IoT devices and users. IoT devices typically only communicate with a few other devices and leverage known communication patterns. Understanding communication patterns can be used to quickly identify an IoT device.

- **CloudVision** – With network management features such as configuration management, automation, monitoring and analytics tools, organizations can simplify network operations and administration, identify problems proactively, and avoid network outages. Arista has also incorporated additional capabilities to improve upon CloudVision's management capabilities to meet the specific needs of the campus. The Device Analyzer builds and updates an inventory of all endpoint devices connected to the campus network. Organizations can use this inventory to track endpoint devices, monitor their connectivity to the network, and collect traffic statistics in real time. The Flow Monitoring capability enables organizations to monitor client traffic flows. Reports are provided describing what clients are connected to the network, who is talking to whom, and what L4 ports are in use per client. The flow information can then be used to identify anomalous behavior such as unusual lateral communication or communication patterns indicative of malware.

ESG Technical Validation

ESG evaluated and tested Arista's Cognitive Campus solution at its headquarters in Santa Clara, CA. Testing was designed to evaluate the performance of switches using industry-standard tools and methodologies, while emulating real-world use patterns typically encountered in today's campus network. Our test network consisted of Arista spine (network core), Spline, and leaf (network access) switches. Spine switches included the 7050CX3 model. Spline switches include the 7050CX3 and 7304X3 models. Access switches included the 720XP PoE switches, which are providing power to the attached APs or IP phones. The top switch (7050SX2) provides Internet access, acting as a border router attached to the campus spine. The left side of the test network represented routed access (designated by the red L3 links). Switches on the right side of the test network are bridging up to the Spline layer (designated by the grey L2 links).



Software Consistency

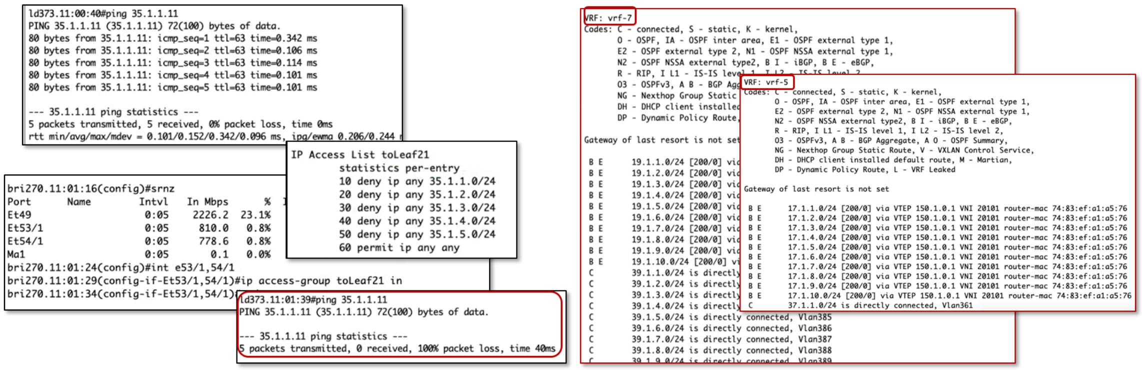
Currently, organizations often operate and manage disparate point solutions to architect the campus core, distribution, and access layers. Consequently, campus network architectures, operations, and management become complicated as the administrator designs topologies and workflows accounting for the lack of solution uniformity. Arista offers a common software architecture in its campus network solution that simplifies operations and management yet supports the base capabilities that a campus network administrator expects. We specifically address how the Arista 720XP handles security via segmentation and device authentication.

ESG Testing

ESG began its validation by first testing that the 720XP can perform both ACL and VxLAN-based segmentation. We first segmented the network such that the leaf switch "ld373" could not communicate with "bri270" (see test bed). We first confirmed that we could ping "bri270" (see left-hand side of Figure 2). Next, we configured the interfaces of "bri270" with an ACL group that prevented any switch from reaching the IP addresses named in the group. We pinged "bri270" using the IP address "35.1.1.11," and the attempt failed.

For VxLAN segmentation, ESG saw that one can segment via the VRFs (see right-hand side of Figure 2). We checked the VRFs associated with vrf-5 and vrf-7 and found that the IP routing tables were isolated. We noted that VxLAN segmentation with EVPN control can enable an administrator to interconnect these VRFs with security rules (e.g., a firewall) without having the VRFs configured on higher-level devices (i.e., Spline devices). This helps to collapse the network into fewer layers.

Figure 2. ACL and EVPN-based Segmentation



```
ld373.11:00:40#ping 35.1.1.11
PING 35.1.1.11 (35.1.1.11) 72(100) bytes of data.
80 bytes from 35.1.1.11: icmp_seq=1 ttl=63 time=0.342 ms
80 bytes from 35.1.1.11: icmp_seq=2 ttl=63 time=0.106 ms
80 bytes from 35.1.1.11: icmp_seq=3 ttl=63 time=0.114 ms
80 bytes from 35.1.1.11: icmp_seq=4 ttl=63 time=0.101 ms
80 bytes from 35.1.1.11: icmp_seq=5 ttl=63 time=0.101 ms

--- 35.1.1.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.101/0.152/0.342/0.096 ms, ipg/ewma 0.206/0.244
```

```
IP Access List toLeaf21
        statistics per-entry
        10 deny ip any 35.1.1.0/24
        20 deny ip any 35.1.2.0/24
        30 deny ip any 35.1.3.0/24
        40 deny ip any 35.1.4.0/24
        50 deny ip any 35.1.5.0/24
        60 permit ip any any
```

```
bri270.11:01:16(config)#srnz
Port       Name          Intvl    In Mbps      %
Et49                      0:05     2226.2  23.1%
Et53/1                    0:05      810.0   0.8%
Et54/1                    0:05      778.6   0.8%
Ma1                       0:05        0.1   0.0%
bri270.11:01:24(config)#int e53/1,54/1
bri270.11:01:29(config-if-Et53/1,54/1)#ip access-group toLeaf21 in
bri270.11:01:34(config-if-Et53/1,54/1)
```

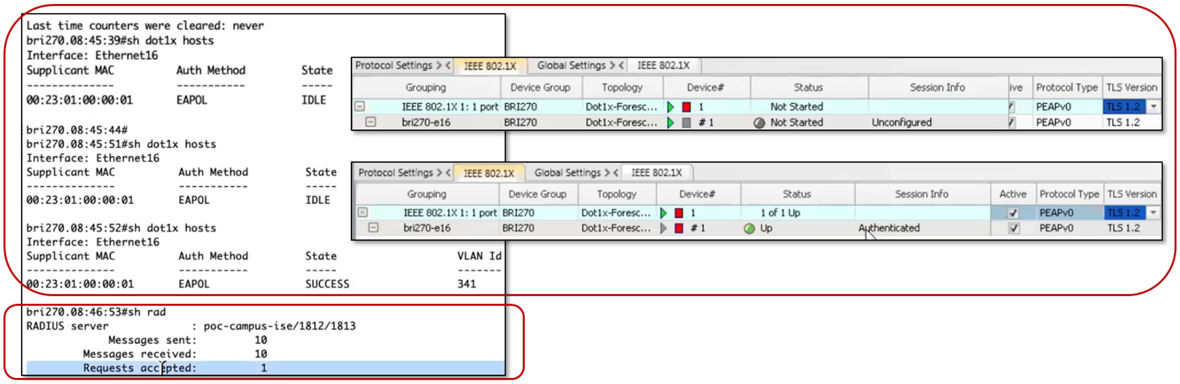
```
ld373.11:01:39#ping 35.1.1.11
PING 35.1.1.11 (35.1.1.11) 72(100) bytes of data.

--- 35.1.1.11 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 40ms
```

```
VRF: vrf-7
Codes: C - connected, S - static, K - kernel,
       O - OSPF, IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type2, B I - iBGP, B E - eBGP,
       R - RIP, I L1 - IS-IS level
       O3 - OSPFv3, A B - BGP Agg
       NG - Nexthop Group Static
       DH - DHCP client installed
       DP - Dynamic Policy Route,

Gateway of last resort is not set

 B E      19.1.1.0/24 [200/0] vi
 B E      19.1.2.0/24 [200/0] vi
 B E      19.1.3.0/24 [200/0] vi
 B E      19.1.4.0/24 [200/0] vi
 B E      19.1.5.0/24 [200/0] vi
 B E      19.1.6.0/24 [200/0] vi
 B E      19.1.7.0/24 [200/0] vi
 B E      19.1.8.0/24 [200/0] vi
 B E      19.1.9.0/24 [200/0] vi
 B E      19.1.10.0/24 [200/0] vi
 C        39.1.1.0/24 is directly
 C        39.1.2.0/24 is directly
 C        39.1.3.0/24 is directly
 C        39.1.4.0/24 is directly
 C        39.1.5.0/24 is directly connected, Vlan385
 C        39.1.6.0/24 is directly connected, Vlan386
 C        39.1.7.0/24 is directly connected, Vlan387
 C        39.1.8.0/24 is directly connected, Vlan388
 C        39.1.9.0/24 is directly connected, Vlan389
```

```
VRF: vrf-5
Codes: C - connected, S - static, K - kernel,
       O - OSPF, IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type2, B I - iBGP, B E - eBGP,
       R - RIP, I L1 - IS-IS level 1, I L2 - IS-IS level 2,
       O3 - OSPFv3, A B - BGP Aggregate, A O - OSPF Summary,
       NG - Nexthop Group Static Route, V - VXLAN Control Service,
       DH - DHCP client installed default route, M - Martian,
       DP - Dynamic Policy Route, L - VRF Leaked

Gateway of last resort is not set

 B E      17.1.1.0/24 [200/0] via VTEP 150.1.0.1 VNI 20101 router-mac 74:83:ef:a1:a5:76
 B E      17.1.2.0/24 [200/0] via VTEP 150.1.0.1 VNI 20101 router-mac 74:83:ef:a1:a5:76
 B E      17.1.3.0/24 [200/0] via VTEP 150.1.0.1 VNI 20101 router-mac 74:83:ef:a1:a5:76
 B E      17.1.4.0/24 [200/0] via VTEP 150.1.0.1 VNI 20101 router-mac 74:83:ef:a1:a5:76
 B E      17.1.5.0/24 [200/0] via VTEP 150.1.0.1 VNI 20101 router-mac 74:83:ef:a1:a5:76
 B E      17.1.6.0/24 [200/0] via VTEP 150.1.0.1 VNI 20101 router-mac 74:83:ef:a1:a5:76
 B E      17.1.7.0/24 [200/0] via VTEP 150.1.0.1 VNI 20101 router-mac 74:83:ef:a1:a5:76
 B E      17.1.8.0/24 [200/0] via VTEP 150.1.0.1 VNI 20101 router-mac 74:83:ef:a1:a5:76
 B E      17.1.9.0/24 [200/0] via VTEP 150.1.0.1 VNI 20101 router-mac 74:83:ef:a1:a5:76
 B E      17.1.10.0/24 [200/0] via VTEP 150.1.0.1 VNI 20101 router-mac 74:83:ef:a1:a5:76
 C        37.1.1.0/24 is directly connected, Vlan361
```

Next, ESG verified that the Arista 720XP can perform 802.1X and MAC-based RADIUS authentication with a variety of NAC/RADIUS products. We first tested 802.1X authentication with the Cisco Identity Services Engine (ISE) using both an Ixia traffic generator and CLI access to leaf switch “bri270” (see Figure 3). Using the Ixia GUI, we stopped, then restarted traffic on the 802.1X port, simulating a client device attached to “bri270.” We then typed “sh dot1x hosts” on the switch’s CLI and saw that the port initially detected no devices. Eventually, the CLI showed that a device was recognized and was assigned to VLAN 341. We also saw that our simulated device was authenticated on the IxNetwork interface.

Figure 3. 802.1X and MAC-based RADIUS Authentication on ‘bri270’ with Cisco ISE



```
Last time counters were cleared: never
bri270.08:45:39#sh dot1x hosts
Interface: Ethernet16
Supplicant MAC         Auth Method        State
--------------         -----------        -----
00:23:01:00:00:01      EAPOL              IDLE

bri270.08:45:44#
bri270.08:45:51#sh dot1x hosts
Interface: Ethernet16
Supplicant MAC         Auth Method        State
--------------         -----------        -----
00:23:01:00:00:01      EAPOL              IDLE

bri270.08:45:52#sh dot1x hosts
Interface: Ethernet16
Supplicant MAC         Auth Method        State                VLAN Id
--------------         -----------        -----                -------
00:23:01:00:00:01      EAPOL              SUCCESS              341

bri270.08:46:53#sh rad
RADIUS server                : poc-campus-ise/1812/1813
             Messages sent:          10
         Messages received:          10
         Requests accepted:           1
```

Protocol Settings > < IEEE 802.1X | Global Settings > < IEEE 802.1X

	Grouping	Device Group	Topology	Device#	Status	Session Info	ive	Protocol Type	TLS Version
⊟	IEEE 802.1X 1: 1 port	BRI270	Dot1x-Foresc...	▶ 🟥 1	Not Started		✓	PEAPv0	TLS 1.2
⊟	bri270-e16	BRI270	Dot1x-Foresc...	▶ ▨ # 1	● Not Started	Unconfigured	✓	PEAPv0	TLS 1.2

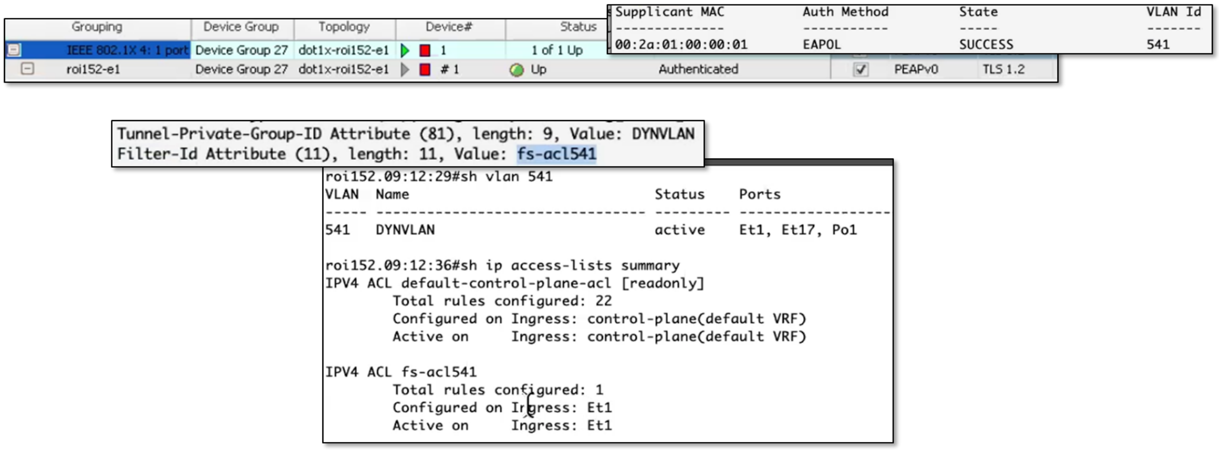
Protocol Settings > < IEEE 802.1X | Global Settings > < IEEE 802.1X

	Grouping	Device Group	Topology	Device#	Status	Session Info	Active	Protocol Type	TLS Version
⊟	IEEE 802.1X 1: 1 port	BRI270	Dot1x-Foresc...	▶ 🟥 1	1 of 1 Up		☑	PEAPv0	TLS 1.2
⊟	bri270-e16	BRI270	Dot1x-Foresc...	▶ 🟥 # 1	● Up	Authenticated	☑	PEAPv0	TLS 1.2

To confirm that “bri270” can also authenticate via RADIUS server, we typed “sh rad” and found that the server accepted one request for authentication. We also performed the same series of tests on three additional NAC/RADIUS servers—Aruba Clearpass, Forescout CounterACT, and Windows NPS - and observed similar results.

ESG also verified that the Arista 720XP can assign ACLs dynamically. Using Cisco ISE again, we first authenticated a simulated device—via the IxNetwork interface—on the leaf switch “roi152” via 802.1X (see Figure 4).

Figure 4. Assigning Dynamic ACL to Authenticated Device on ‘roi152’



Grouping	Device Group	Topology	Device#	Status				
IEEE 802.1X 4: 1 port	Device Group 27	dot1x-roi152-e1	1	1 of 1 Up				
roi152-e1	Device Group 27	dot1x-roi152-e1	# 1	Up	Authenticated	☑	PEAPv0	TLS 1.2

```
Supplicant MAC      Auth Method      State        VLAN Id
--------------      -----------      -----        -------
00:2a:01:00:00:01   EAPOL            SUCCESS      541
```

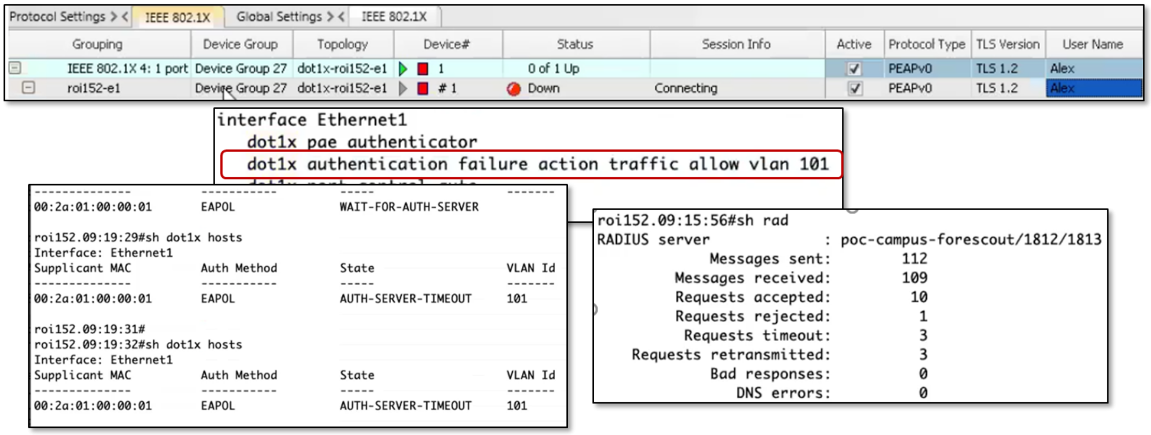
```
Tunnel-Private-Group-ID Attribute (81), length: 9, Value: DYNVLAN
Filter-Id Attribute (11), length: 11, Value: fs-acl541
```

```
roi152.09:12:29#sh vlan 541
VLAN  Name                             Status    Ports
----- -------------------------------- --------- ------------------
541   DYNVLAN                          active    Et1, Et17, Po1

roi152.09:12:36#sh ip access-lists summary
IPV4 ACL default-control-plane-acl [readonly]
        Total rules configured: 22
        Configured on Ingress: control-plane(default VRF)
        Active on     Ingress: control-plane(default VRF)

IPV4 ACL fs-acl541
        Total rules configured: 1
        Configured on Ingress: Et1
        Active on     Ingress: Et1
```

After “roi152” authenticated the simulated device in the Ixia GUI and the CLI, we then checked if the device was assigned a named VLAN and ACL. According to the CLI, the switch would assign an authenticated device to the VLAN named “DYNVLAN” (equivalent to VLAN 541) and the ACL labeled “fs-acl541.” We inputted “sh vlan 541” in the CLI and confirmed the “DYNVLAN” label was associated with VLAN 541. When we inputted “sh ip access-lists-summary.” we found that the switch applied the ACL “fs-acl541 on to Ethernet port 1, on which our device connected to “roi152.”

Finally, ESG observed how the Arista 720XP isolates devices should they not be authenticated. We navigated to the Ixia GUI and changed the owner of the device so that the leaf switch “roi152” would not authenticate it via 802.1X. We accessed “roi152” via the CLI and configured the switch such that any unauthenticated device would be assigned to VLAN 101 (see Figure 5). We verified how “roi152” assigned the device to VLAN 101 after multiple attempts at 802.1X authentication timed out. Also, the RADIUS server indicated that it rejected the device’s request to be authenticated.

Figure 5. Assigning Unauthenticated Devices to VLAN 101



Protocol Settings > < IEEE 802.1X
Global Settings > < IEEE 802.1X

Grouping	Device Group	Topology	Device#	Status	Session Info	Active	Protocol Type	TLS Version	User Name
IEEE 802.1X 4: 1 port	Device Group 27	dot1x-roi152-e1	1	0 of 1 Up		☑	PEAPv0	TLS 1.2	Alex
roi152-e1	Device Group 27	dot1x-roi152-e1	# 1	Down	Connecting	☑	PEAPv0	TLS 1.2	Alex

```
interface Ethernet1
   dot1x pae authenticator
   dot1x authentication failure action traffic allow vlan 101
```

```
--------------      -----------      -----                   -------
00:2a:01:00:00:01   EAPOL            WAIT-FOR-AUTH-SERVER

roi152.09:19:29#sh dot1x hosts
Interface: Ethernet1
Supplicant MAC      Auth Method      State                   VLAN Id
--------------      -----------      -----                   -------
00:2a:01:00:00:01   EAPOL            AUTH-SERVER-TIMEOUT     101

roi152.09:19:31#
roi152.09:19:32#sh dot1x hosts
Interface: Ethernet1
Supplicant MAC      Auth Method      State                   VLAN Id
--------------      -----------      -----                   -------
00:2a:01:00:00:01   EAPOL            AUTH-SERVER-TIMEOUT     101
```

```
roi152.09:15:56#sh rad
RADIUS server            : poc-campus-forescout/1812/1813
             Messages sent:        112
         Messages received:        109
         Requests accepted:         10
         Requests rejected:          1
          Requests timeout:          3
    Requests retransmitted:          3
             Bad responses:          0
                DNS errors:          0
```

Why This Matters

Using a unified software architecture across all network elements in a campus network can simplify an organization's network architecture. By employing this approach, as opposed to using point solutions with disparate software architectures, organizations can achieve consistency in network operations and management.

ESG validated that the software architecture of the Arista 720XP can enable organizations to accomplish tasks that are particularly critical to address in campus networks, such as segmentation and authentication. These tasks can be performed consistently, simplifying network operations and, subsequently, decreasing operational and administration costs.

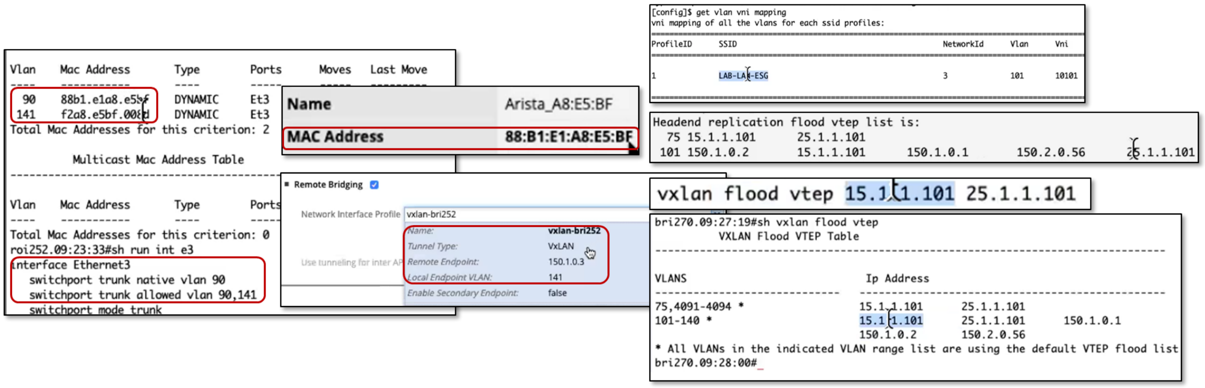
Cognitive WiFi Edge

Organizations contend with a growing amount of WiFi traffic in campus networks as the number of users and endpoint devices increases. The traditional way of building out a controller-based WiFi network cannot scale without adding additional hardware and software, thus incurring additional capital and operational costs. Arista offers a viable model for scaling and managing the WiFi network while enabling user mobility across the campus network without the restrictions posed by traditional controller-based network architectures. To manage this growth and maintain network performance and availability, organizations must also gain a more comprehensive view of WiFi networks so that end-user access is not unnecessarily compromised or prevented.

ESG Testing

ESG first created a VxLAN tunnel between an AP and an Arista 720XP in the same VLAN yet separated by a Layer 3 network. The tunnel would extend from the AP connected to "roi252" to "bri270" via a trunk interface. These switches are separated by the Layer 3 network (see test bed). We first verified the assigned VLANs—VLAN 90 (the AP management network) and VLAN 141 (the VLAN that will transport VxLAN-encapsulated packets from the AP) on "roi252" (see Figure 6). Next, we accessed the AP via CLI and checked that it was associated with the stretched VLAN 101 with 10101 as its VNI (its static configuration). We then checked the switch "bri270" to see that the AP VxLAN tunnel endpoint (VTEP) was mapped to VLAN 101. The VxLAN tunnel thus stretched VLAN 101 from the AP to "bri270."

Figure 6. Creating a VxLAN Tunnel Between an AP and Arista720XP in Different VLANs



```
Vlan    Mac Address       Type        Ports      Moves   Last Move
----    -----------       ----        -----      -----   ---------
  90    88b1.e1a8.e5bf    DYNAMIC     Et3
 141    f2a8.e5bf.008d    DYNAMIC     Et3
Total Mac Addresses for this criterion: 2

          Multicast Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       ----        -----
Total Mac Addresses for this criterion: 0
roi252.09:23:33#sh run int e3
interface Ethernet3
   switchport trunk native vlan 90
   switchport trunk allowed vlan 90,141
   switchport mode trunk
```

Name: Arista_A8:E5:BF
MAC Address: 88:B1:E1:A8:E5:BF

■ Remote Bridging ☑

Network Interface Profile: vxlan-bri252

Use tunneling for inter AP

- Name: vxlan-bri252
- Tunnel Type: VxLAN
- Remote Endpoint: 150.1.0.3
- Local Endpoint VLAN: 141
- Enable Secondary Endpoint: false

```
[config]$ get vlan vni mapping
vni mapping of all the vlans for each ssid profiles:
=====================================================================
ProfileID     SSID                          NetworkId    Vlan    Vni
=====================================================================

1             LAB-LAN-ESG                   3            101     10101

=====================================================================
```

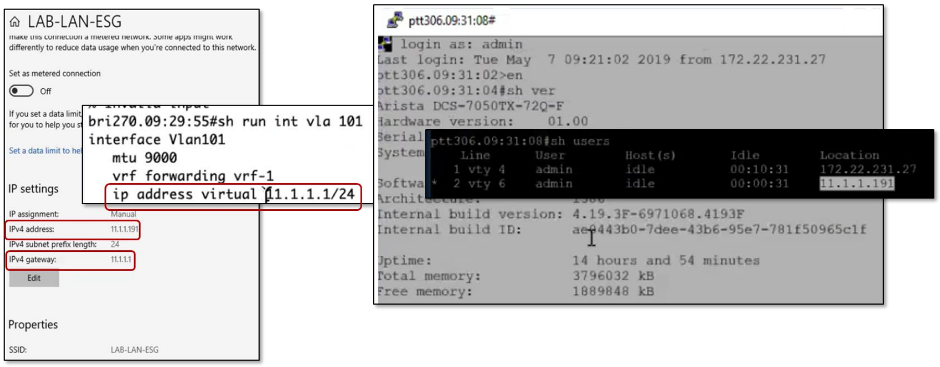
```
Headend replication flood vtep list is:
  75 15.1.1.101       25.1.1.101
 101 150.1.0.2        15.1.1.101       150.1.0.1        150.2.0.56       25.1.1.101
```

```
vxlan flood vtep 15.1.1.101 25.1.1.101
```

```
bri270.09:27:19#sh vxlan flood vtep
          VXLAN Flood VTEP Table
--------------------------------------------------------------------------------

VLANS                            Ip Address
-----------------------------   ----------------------------------------------
75,4091-4094 *                   15.1.1.101      25.1.1.101
101-140 *                        15.1.1.101      25.1.1.101      150.1.0.1
                                 150.1.0.2       150.2.0.56
* All VLANs in the indicated VLAN range list are using the default VTEP flood list
bri270.09:28:00#_
```

ESG then tested whether we could reach the leaf switch "ptt306" via a WiFi LAN configured on the "bri270." In this case, we leveraged the VxLAN tunnel to reach the "bri270," then accessed a gateway on a leaf switch "ptt306"(see test bed). We obtained the IP address of the WiFi network "LAB-LAN-ESG" (11.1.1.191) and verified that this was configured on one port of the "bri270." Using PuTTY, we confirmed that we could reach this IP address (shown in Figure 7).

Figure 7. Reachability of 'ptt306' via VxLAN Tunnel



LAB-LAN-ESG

make this connection a metered network. Some apps might work differently to reduce data usage when you're connected to this network.

Set as metered connection

○ Off

If you set a data limit … for you to help you s…

Set a data limit to hel…

IP settings

- IP assignment: Manual
- IPv4 address: 11.1.1.191
- IPv4 subnet prefix length: 24
- IPv4 gateway: 11.1.1.1

Edit

Properties

- SSID: LAB-LAN-ESG

```
% Invalid input
bri270.09:29:55#sh run int vla 101
interface Vlan101
   mtu 9000
   vrf forwarding vrf-1
   ip address virtual 11.1.1.1/24
```

ptt306.09:31:08#

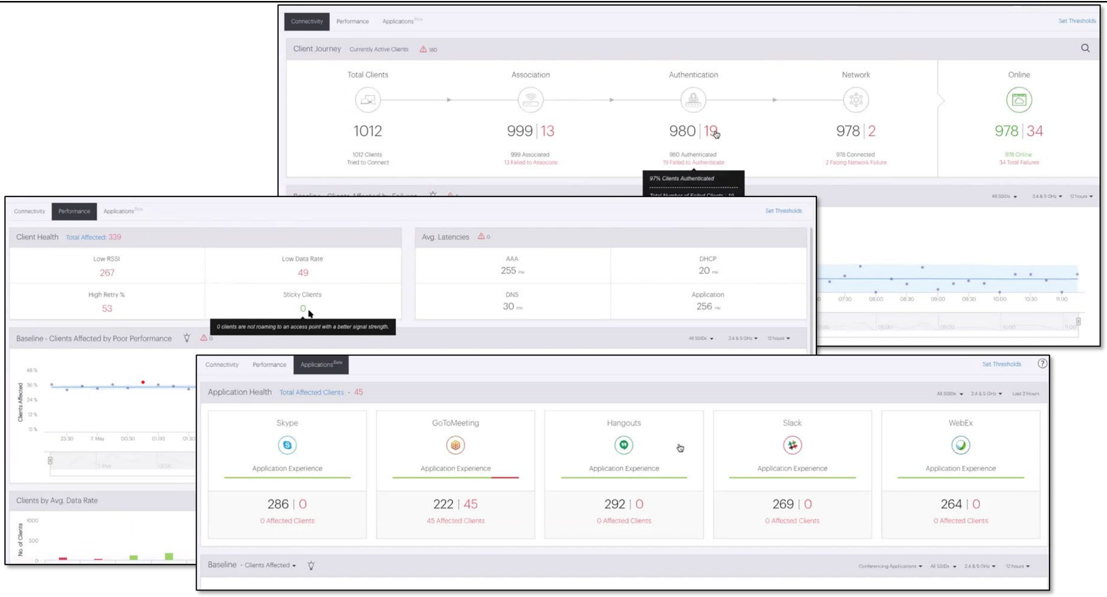
```
login as: admin
Last login: Tue May  7 09:21:02 2019 from 172.22.231.27
ptt306.09:31:02>en
ptt306.09:31:04#sh ver
Arista DCS-7050TX-72Q-F
Hardware version:    01.00
Serial
System

Softwa
Archit
Internal build version: 4.19.3F-6971068.4193F
Internal build ID:      ae0443b0-7dee-43b6-95e7-781f50965c1f

Uptime:                 14 hours and 54 minutes
Total memory:           3796032 kB
Free memory:            1889848 kB
```

```
ptt306.09:31:08#sh users
    Line       User        Host(s)       Idle          Location
   1 vty 4     admin       idle          00:10:31      172.22.231.27
*  2 vty 6     admin       idle          00:00:31      11.1.1.191
```

ESG noted how a network administrator can benefit from using VxLAN tunneling to direct WiFi traffic to anywhere within the campus network on a per SSID basis without any restriction imposed by local VLANs. For example, an administrator can direct guest WiFi traffic to an Internet gateway and send corporate traffic to the connecting leaf switch as a standard 802.3 packet without relying on additional switches, routers, or controllers. An administrator can migrate WiFi traffic to other parts of the campus network when necessary—network upgrades, for example. If the administrator needs to restrict access of specific user groups like contractors on a campus network, traffic can be directed to specific network locations, such as a contractor portal.

ESG then explored how the solution provides both detailed visibility and network intelligence into WiFi networks. We navigated to the portal focused on WiFi network management and observed that we gain insight into a WiFi network via three views—*Connectivity*, *Performance*, and *Applications*. The *Connectivity* tab provides details on a "client journey," a summary of events that occurred while clients attempted to access a specific WiFi network (see Figure 8), including association and authentication. The *Performance* tab illustrated key metrics associated with a WiFi network, such as high retry %, low data rate, and low RSSI. The *Applications* tab displays metrics related to application performance. We also observed that we can drill down for additional detail in each tab, such as if a client failed to associate with an AP. The level of information provided by these tabs showed how an administrator can improve overall network management and monitoring.

Figure 8. CloudVision WiFi Portal – Connectivity, Performance, and Applications Views



Client Journey Currently Active Clients ⚠ 180

Total Clients	Association	Authentication	Network	Online
1012	999 | 13	980 | 19	978 | 2	978 | 34
1012 Clients Tried to Connect	999 Associated 13 Failed to Associate	980 Authenticated 19 Failed to Authenticate	978 Connected 2 Facing Network Failure	978 Online 34 Total Failures

97% Clients Authenticated

Client Health Total Affected: 339

Low RSSI	Low Data Rate
267	49
High Retry %	**Sticky Clients**
53	0

0 clients are not roaming to an access point with a better signal strength.

Avg. Latencies ⚠ 0

AAA	DHCP
255 ms	20 ms
DNS	**Application**
30 ms	256 ms

Baseline - Clients Affected by Poor Performance ⚠ 0

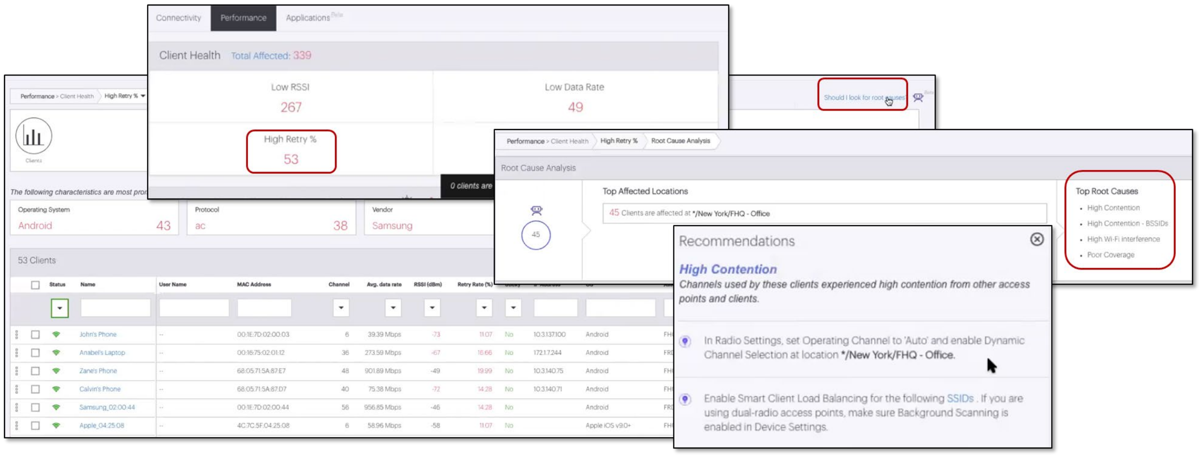
Application Health Total Affected Clients - 45

Skype	GoToMeeting	Hangouts	Slack	WebEx
Application Experience	Application Experience	Application Experience	Application Experience	Application Experience
286 | 0	222 | 45	292 | 0	269 | 0	264 | 0
0 Affected Clients	45 Affected Clients	0 Affected Clients	0 Affected Clients	0 Affected Clients

Baseline - Clients Affected

Once we verified the level of monitoring provided by the CloudVision WiFi portal, we then observed how an administrator can conduct a root cause analysis (see Figure 9). We navigated to the *Performance* tab and clicked on the number under "High Retry %." A screen showing details about the metric appeared. We clicked on the hyperlink in the upper left-hand corner of the window, "Should I look for root causes?" This prompted the underlying inference engine to list out top root causes, such as high contention and poor coverage. We also brought up recommendations to address the root causes.

Figure 9. Root Cause Analysis Using Inference Engine



Client Health Total Affected: 339

Low RSSI	Low Data Rate
267	49
High Retry %	
53	

Performance > Client Health > High Retry %

Should I look for root causes?

The following characteristics are most pro

Operating System	Protocol	Vendor
Android 43	ac 38	Samsung

53 Clients

Status	Name	User Name	MAC Address	Channel	Avg. data rate	RSSI (dBm)	Retry Rate (%)			
	John's Phone	--	00:1E:7D:02:00:03	6	39.39 Mbps	-73	11.07	No	10.3.137.100	Android
	Anabel's Laptop	--	00:16:75:02:01:12	36	273.59 Mbps	-67	16.66	No	172.1.7.244	Android
	Zane's Phone	--	68:05:71:5A:87:E7	48	901.89 Mbps	-49	19.99	No	10.3.140.75	Android
	Calvin's Phone	--	68:05:71:5A:87:D7	40	75.38 Mbps	-72	14.28	No	10.3.140.71	Android
	Samsung_02:00:44	--	00:1E:7D:02:00:44	56	956.85 Mbps	-46	14.28	No		Android
	Apple_04:25:08	--	4C:7C:5F:04:25:08	6	58.96 Mbps	-58	11.07	No		Apple iOS v9.0+

Performance > Client Health > High Retry % > Root Cause Analysis

Root Cause Analysis

Top Affected Locations

45 Clients are affected at */New York/FHQ - Office

Top Root Causes

- High Contention
- High Contention - BSSIDs
- High Wi-Fi interference
- Poor Coverage

Recommendations

High Contention

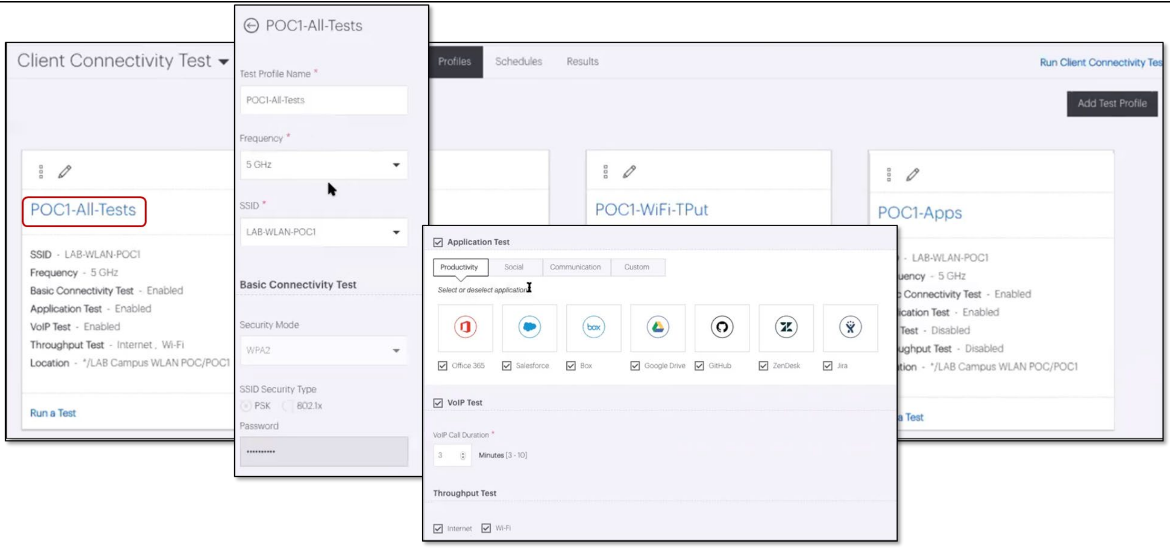
Channels used by these clients experienced high contention from other access points and clients.

In Radio Settings, set Operating Channel to 'Auto' and enable Dynamic Channel Selection at location ***/New York/FHQ - Office.**

Enable Smart Client Load Balancing for the following SSIDs . If you are using dual-radio access points, make sure Background Scanning is enabled in Device Settings.

Finally, ESG observed how the third radio on the Arista access point can be used to emulate a client. The emulated client can perform a variety of tests including connectivity and network assurance, throughput between APs, throughput to the WAN, and application availability. Because the client is virtual, these tests can be automated and scheduled, removing the need for manual intervention. Under the *Troubleshooting* menu, we clicked on *Client Connectivity Test* to view various tests created (see Figure 10). We examined the test named "POC1-All Tests," covering aspects such as security protocols (e.g., WPA2), availability of specified cloud applications, quality of VoIP calls (via the MOS score), and WiFi network throughput.

Figure 10. Running Client Connectivity Test Using Emulated Clients



POC1-All-Tests

SSID - LAB-WLAN-POC1
Frequency - 5 GHz
Basic Connectivity Test - Enabled
Application Test - Enabled
VoIP Test - Enabled
Throughput Test - Internet , Wi-Fi
Location - */LAB Campus WLAN POC/POC1

POC1-WiFi-TPut

POC1-Apps

- LAB-WLAN-POC1
uency - 5 GHz
c Connectivity Test - Enabled
lication Test - Enabled
Test - Disabled
ughput Test - Disabled
tion - */LAB Campus WLAN POC/POC1

POC1-All-Tests

Test Profile Name *: POC1-All-Tests
Frequency *: 5 GHz
SSID *: LAB-WLAN-POC1

Basic Connectivity Test

Security Mode: WPA2
SSID Security Type: ● PSK ○ 802.1x
Password: ••••••••••

☑ Application Test

☑ Office 365 ☑ Salesforce ☑ Box ☑ Google Drive ☑ GitHub ☑ ZenDesk ☑ Jira

☑ VoIP Test

VoIP Call Duration *: 3 Minutes [3 - 10]

Throughput Test

☑ Internet ☑ Wi-Fi

As ESG navigated through the CloudVision WiFi portal, we noted that an administrator can obtain detailed network WiFi network information, via the client connectivity tests to quickly identify issues that can adversely impact network performance and availability, such as a low MOS score for VoIP calls. More importantly, the portal can support an administrator in obtaining possible root causes and remediation options easily via the portal's inference engine.

As more users are leveraging WiFi networks in campus networks, ESG can see that an administrator will need to monitor WiFi network performance and availability more frequently and proactively. The CloudVision WiFi portal enables tests to be automated and scheduled, removing that burden from the administrator's daily responsibilities. Emulating clients ensures that the administrator conducts tests that simulate how WiFi networks work in production networks. Issues uncovered using this testing method, if addressed, can potentially save time and resources spent should they occur in a live environment.

Why This Matters

Organizations face dual challenges as WiFi access in campus networks is more prevalent. As more end-users embrace mobility, administrators must provide them with the right level of network access without compromising performance and security. The other challenge is to monitor WiFi networks to proactively identify and resolve issues that may disrupt end-user access, as users within organizations rely more on WiFi networks to access campus network resources to conduct their daily lives and accomplish their work. Organizations need a solution that will enable them to provide appropriate levels of network access to specific user groups, monitor WiFi network performance and availability, and proactively identify issues and troubleshooting options.

ESG validated that the Cognitive WiFi Edge capabilities of the Arista Cognitive Campus solution support organizations in managing WiFi access to campus networks without compromising network performance and security. We verified that the Cognitive WiFi capabilities enable organizations to tunnel WiFi traffic via L3 VxLANs, which support isolation and segmentation of traffic to any part of the network. We then validated that the CloudVision WiFi portal supplies organizations with detailed statistics describing the health of the WiFi network. ESG also verified that the CloudVision WiFi portal provides organizations with the ability to automate test WiFi networks using emulated clients. Using this approach to testing allows organizations to identify and remediate issues before they exacerbate and affect end-user access. Ultimately, ESG saw how the Cognitive WiFi Edge helps organizations to decrease operational costs, increase network uptime, and improve overall network security via managing WiFi network access.

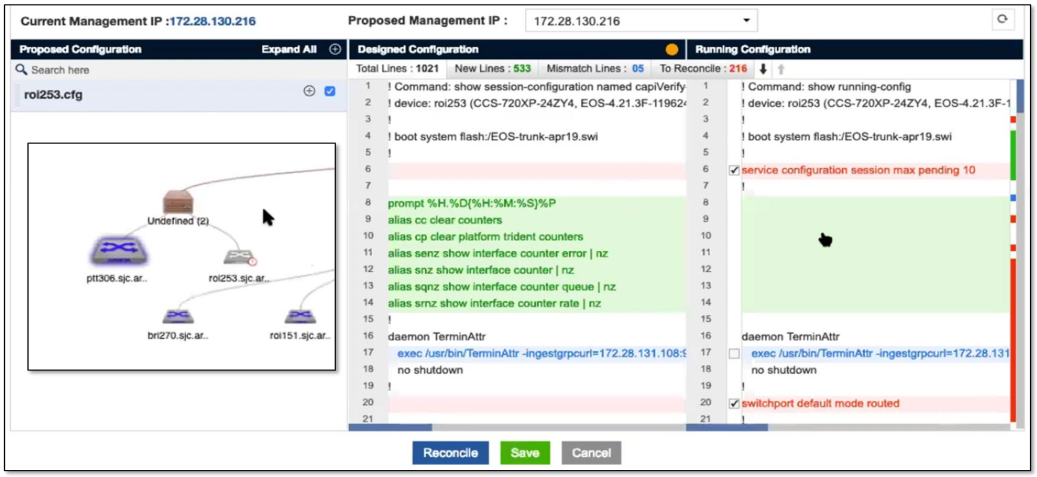
Management and Monitoring

With the growth in the scale and size of campus networks, organizations face the challenge of network monitoring and management that provides the level of visibility required to simplify network operations, isolate network issues proactively, and troubleshoot these issues with little impact to end-users. CloudVision Portal provides visibility of network connections from the datacenter to the cloud and now to the campus network, including endpoint devices. CloudVision is a management platform that uses only state-streaming mechanisms designed for granularity and completeness of data. This provides a level of visibility that far exceeds what is possible with SNMP-polling models. This visibility ultimately helps organizations to improve overall management and control. CloudVision also helps to manage workflows so that organizations can make network changes and updates while minimizing errors and rework.

ESG Testing

ESG validated specific use cases that an administrator can encounter when managing a campus network. We first looked at how an administrator can add or replace switches using its “zero-touch provisioning” capability. From CloudVision, we navigated to the *Provisioning* menu to view a network topology (see Figure 11).

Figure 11. Provisioning ‘roi253’ via the CloudVision



Current Management IP :172.28.130.216

Proposed Management IP : 172.28.130.216

Total Lines : 1021 | New Lines : 533 | Mismatch Lines : 05 | To Reconcile : 216

Designed Configuration:

```
! Command: show session-configuration named capiVerify
! device: roi253 (CCS-720XP-24ZY4, EOS-4.21.3F-11962
!
! boot system flash:/EOS-trunk-apr19.swi
!


prompt %H.%D{%H:%M:%S}%P
alias cc clear counters
alias cp clear platform trident counters
alias senz show interface counter error | nz
alias snz show interface counter | nz
alias sqnz show interface counter queue | nz
alias srnz show interface counter rate | nz
!
daemon TerminAttr
  exec /usr/bin/TerminAttr -ingestgrpcurl=172.28.131.108:
  no shutdown
!

```

Running Configuration:

```
  ! Command: show running-config
  ! device: roi253 (CCS-720XP-24ZY4, EOS-4.21.3F-1
  !
  ! boot system flash:/EOS-trunk-apr19.swi
  !
☑ service configuration session max pending 10
  !







  daemon TerminAttr
□   exec /usr/bin/TerminAttr -ingestgrpcurl=172.28.131
    no shutdown
  !
☑ switchport default mode routed
  !
```

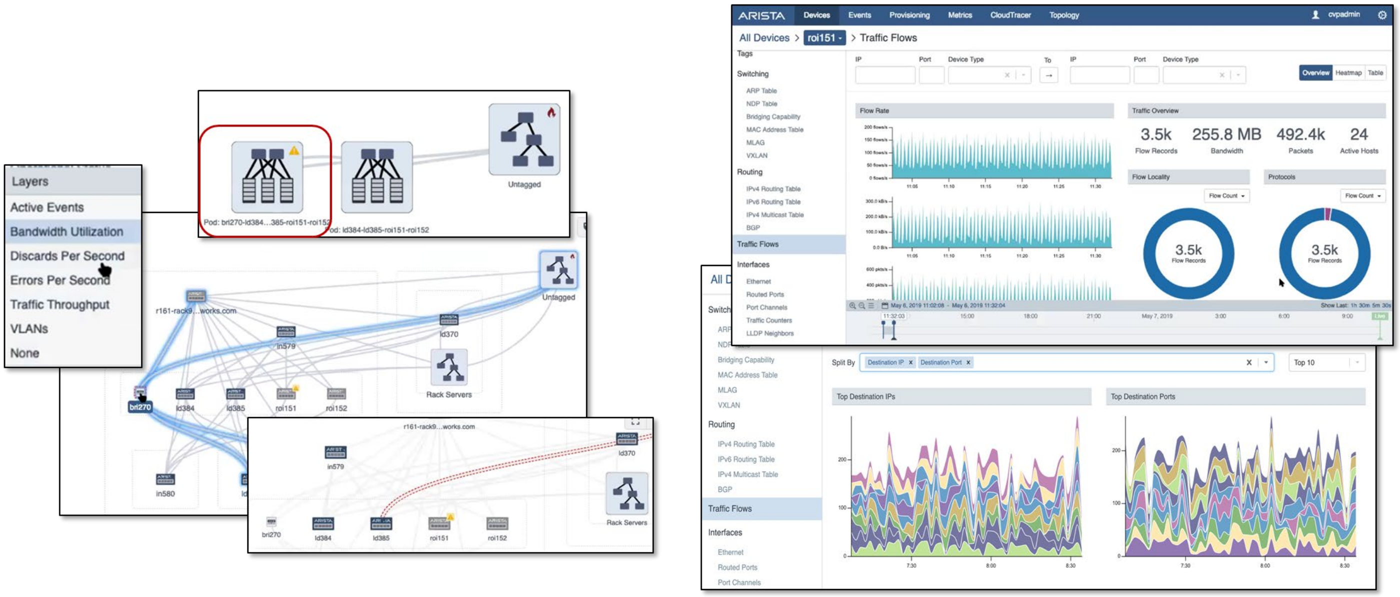
We deleted the device name “roi253” via the portal and removed its configuration via CLI. After rebooting the device via the CLI, its icon appeared again in the network diagram. We then applied its configuration as it existed before the device was deleted (already saved in the CloudVision database). To reconfigure the device, we clicked on the icon “roi253” and selected *Manage*, then *Configlet*, and selected “roi253.cfg.” CloudVision then prompted ESG to ensure that we wanted to apply the “Designed Configuration” as it existed before deleting “roi253.” We chose to reconcile the “Designed Configuration” with the “Running Configuration” (the base configuration for new devices), then apply the configuration to the rebooted switch.

ESG noted that the process for provisioning devices can apply to both new and replaced devices. We also noted how this enables an administrator to easily add new devices, as configurations can be added to the CloudVision without having to physically access the device. Switch configurations can be performed centrally via the CloudVision, then remotely applied to any switch installed in the network. This process also helps to return the network to its operating state faster when replacing devices. Rather than reconfiguring the device, CloudVision can apply the configuration the device had before being replaced. The administrator saves time in having to manually duplicate its configuration without errors, returning the device to its desired state.

ESG then proceeded to examine how CloudVision provides detailed network visibility. CloudVision can provide these views using network telemetry. We examined several screens that provide network detail from device, connectivity, network statistics, and flow monitoring levels. To begin, we saw how the CloudVision provides network views that show device connectivity (see left-hand side of Figure 12). CloudVision revealed device connectivity from the rack server to the device level, along with how the devices were wired to each other. Other aspects that we examined included such characteristics as bandwidth utilization and discards per second, as shown by the color-coded lines.

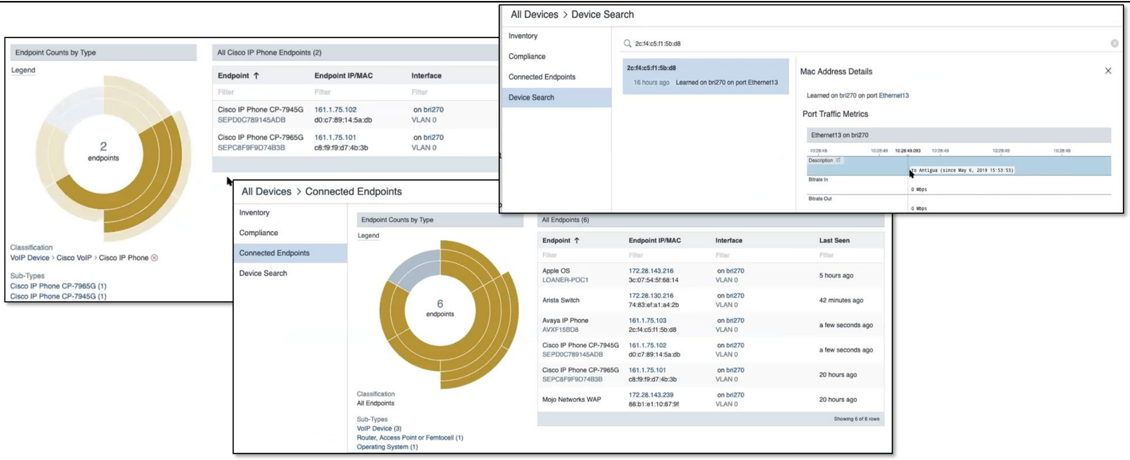
CloudVision also offers views from a flow monitoring perspective. We navigated to the Devices menu and chose "roi151" to view its flow statistics (see right-hand side of Figure 12). We found that we could keep track of traffic flows from the entire device or track specific flows. During our testing, we learned that we can track flows between source and destination ports on this device, specifically tracing bandwidth usage totals. CloudVision allowed us to define specific timeframes to view these stats, shown by the timeline at the bottom of these screens. This timeline allows the user to go back in time to view the state of the network for historic troubleshooting purposes.

Figure 12. Network Visibility via the CloudVision from Device and Flow Monitoring Level



We then examined how CloudVision, via the Device Analyzer, provides views into the endpoints within campus networks (see Figure 13). Not only did CloudVision identify endpoints—IP phones, mobile phones, APs, laptops—but it also provided additional detail such as MAC addresses, connectivity to specific switches, and elapsed time since the device was in use. As we navigated through the concentric circles, specific devices were displayed, such as the Cisco IP Phones. This view also enabled us to search for a specific device and provided additional detail such as port level metrics.

Figure 13. Endpoint Identification in CloudVision



All Cisco IP Phone Endpoints (2)

Endpoint ↑	Endpoint IP/MAC	Interface
Filter	Filter	Filter
Cisco IP Phone CP-7945G SEPD0C789145ADB	161.1.75.102 d0:c7:89:14:5a:db	on bri270 VLAN 0
Cisco IP Phone CP-7965G SEPC8F9F9D74B3B	161.1.75.101 c8:f9:f9:d7:4b:3b	on bri270 VLAN 0

2c:f4:c5:f1:5b:d8
16 hours ago Learned on bri270 on port Ethernet13

Learned on bri270 on port Ethernet13

to Antigua (since May 6, 2019 15:53:53)

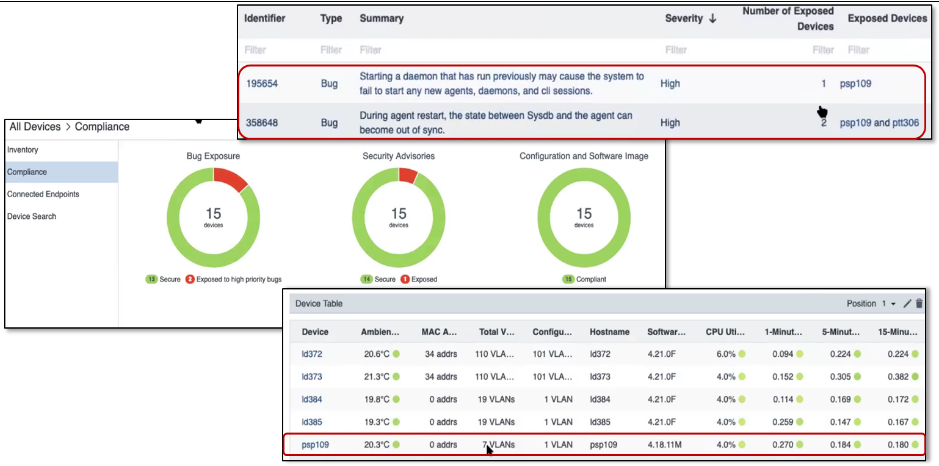
All Endpoints (6)

Endpoint ↑	Endpoint IP/MAC	Interface	Last Seen
Filter	Filter	Filter	Filter
Apple OS LOANER-POC1	172.28.143.216 3c:07:54:5f:68:14	on bri270 VLAN 0	5 hours ago
Arista Switch	172.28.130.216 74:83:ef:a1:a4:2b	on bri270 VLAN 0	42 minutes ago
Avaya IP Phone AVXF15BD8	161.1.75.103 2c:f4:c5:f1:5b:d8	on bri270 VLAN 0	a few seconds ago
Cisco IP Phone CP-7945G SEPD0C789145ADB	161.1.75.102 d0:c7:89:14:5a:db	on bri270 VLAN 0	a few seconds ago
Cisco IP Phone CP-7965G SEPC8F9F9D74B3B	161.1.75.101 c8:f9:f9:d7:4b:3b	on bri270 VLAN 0	20 hours ago
Mojo Networks WAP	172.28.143.239 88:b1:e1:10:87:9f	on bri270 VLAN 0	20 hours ago

ESG finally examined how CloudVision can support compliance management. We navigated to the ***Compliance*** option under the ***Devices*** menu to view the current state of how known bugs and security advisories affect the inventory (see Figure 14). According to the list of identified bugs (under the graphs), bugs associated with "ptt306" and "psp109" exist. Upon further investigation, we also found that the switch "psp109" is configured with an old EOS version. We were able to obtain this information through two sources. The network telemetry enabled the devices, specifically "psp109," to collect information showing why the device is out of compliance. (In this case, CloudVision detected and recorded that the device had an old software image.) CloudVision has automated access to arista.com where a machine-readable alert base is maintained. This alert base is regularly updated with the latest known defects and security advisories, and CloudVision continually checks for impact to the devices under management.

To bring both devices back into compliance, ESG rebooted the "psp109" to install an updated EOS version. In parallel, we updated the software image on "ptt106." Once both devices were installed with the latest software release, the doughnut charts in Figure 14 no longer showed any bugs.

Figure 14. Compliance Management in CloudVision



Identifier	Type	Summary	Severity ↓	Number of Exposed Devices	Exposed Devices
Filter	Filter	Filter	Filter	Filter	Filter
195654	Bug	Starting a daemon that has run previously may cause the system to fail to start any new agents, daemons, and cli sessions.	High	1	psp109
358648	Bug	During agent restart, the state between Sysdb and the agent can become out of sync.	High	2	psp109 and ptt306

Device Table

Device	Ambien...	MAC A...	Total V...	Configu...	Hostname	Softwar...	CPU Uti...	1-Minut...	5-Minut...	15-Minu...
ld372	20.6°C ●	34 addrs	110 VLA...	101 VLA...	ld372	4.21.0F	6.0% ●	0.094 ●	0.224 ●	0.224 ●
ld373	21.3°C ●	34 addrs	110 VLA...	101 VLA...	ld373	4.21.0F	4.0% ●	0.152 ●	0.305 ●	0.382 ●
ld384	19.8°C ●	0 addrs	19 VLANs	1 VLAN	ld384	4.21.0F	4.0% ●	0.114 ●	0.169 ●	0.172 ●
ld385	19.3°C ●	0 addrs	19 VLANs	1 VLAN	ld385	4.21.0F	4.0% ●	0.259 ●	0.147 ●	0.167 ●
psp109	20.3°C ●	0 addrs	7 VLANs	1 VLAN	psp109	4.18.11M	4.0% ●	0.270 ●	0.184 ●	0.180 ●

As ESG examined the various views and capabilities within CloudVision, we noted how they can simplify network operations and management and increase overall network security. Because CloudVision provides access to granular real-time and historical state information, the administrator's ability to proactively monitor traffic, identify issues, and resolve them quickly improves, helping to increase the operator's ability to find root cause. The CloudVision's flow monitoring capability helps an administrator to baseline end-user behavior and point out malicious or unusual actions, as ports can be mapped to applications. Endpoint identification helps an administrator to determine current usage and access levels of various devices and form segmentation and security policies, if necessary. An administrator can also leverage the compliance management capabilities not only to decrease the time to identify and resolve bugs and PSIRTs, but also to decrease the campus network's exposure to security risk.

Why This Matters

Complex campus IT networks presents organizations with the daunting tasks of maintaining a level of visibility so as to stay ahead of network-impacting issues. While organizations traditionally have maintained the operation of a campus network with disjointed device and network management systems, these consume unnecessary time and resources to access and cross-reference information. Organizations have faced no other choice but to piece together information from these disparate systems to obtain some level of network visibility and control. What organizations need is a solution that provides real-time visibility that is continuously updated. The solution should support visibility and control from multiple perspectives so that organizations can manage networks holistically.

ESG validated that the CloudVision portal provides organizations with the capabilities needed to manage and control campus networks. We found the process for adding and replacing devices to be simple, as organizations can configure switches to the correct network state without wasting time and resources in manual configuration. The portal provides organizations with detailed and comprehensive views of campus networks so as to maintain overall network health and security. The portal enables organization to potentially identify network issues related to connectivity, traffic flows, endpoint devices, and compliance. We confirmed that the portal supplies real-time views of network behavior, providing insight into potential network issues that can be contained quickly. The level of network visibility and control that organizations can obtain with CloudVision can help to decrease operations and administration expenses while increasing network uptime and, conversely, lowering the network's exposure to security risk.

The Bigger Truth

As organizations tackle greater levels of complexity in their network, it will be imperative to deploy campus solutions capable of addressing current and future needs, including the growth in the number and variety of endpoint devices, the number of applications that enable users to leverage these devices, and the resulting higher data volumes that are generated. As campus networks continue to play a larger role in connecting IoT and mobile devices to applications, organizations need to focus on network operations and management efficiency, and significantly improve their security and network segmentation capabilities to protect the network against breaches and attacks. Organizations also need to ensure a granular level of network visibility to identify and address issues quickly prior to any impact on network performance and security. Deploying a solution with a common architecture and management system that can extend from the datacenter to the campus core to the access layer and its endpoint devices is key for organizations to improve network visibility, management, monitoring, and security.

Arista applied its networking experience from its datacenter and hybrid cloud solutions to develop its Cognitive Campus Network solution. The solution uses a common hardware and software architecture across the campus core, distribution, and access layers. With the underlying software architecture based on the Arista EOS, organizations can benefit from its consistent operations, workflow automation, and high availability. EOS also lends the benefit of a single database for aggregating and accessing state and configuration of all switches and connected endpoint devices within the campus network. Organizations can access the database via the CloudVision portal to obtain network and device state, illustrate network topology, monitor traffic flows between devices, and determine network connectivity from the campus core to the endpoint device level, using real-time and continuous data collection. CloudVision provides that single point of network management and visibility to maintain overall performance and security with wired and wireless networks.

ESG validated that Arista's Cognitive Campus solution provides organizations with the capabilities to simplify network architecture, operations, and management. We saw how the common software architecture of the Arista switch platforms allows organizations to perform typical network administration activities, such as segmentation and authentication, without resorting to piecing together approaches using disparate platforms. We observed how the solution's Cognitive WiFi Edge capabilities support organizations in managing WiFi access to campus networks and provide detailed visibility into WiFi networks to ease troubleshooting and monitoring. ESG also verified that the CloudVision portal can enable organizations to achieve a comprehensive understanding of the entire campus network, from the spine to the endpoint device in real time. This holistic network view—from a device, configuration, traffic flow, and compliance perspective—can facilitate how organizations identify and remediate issues that can impact network behavior and security. Overall, we validated that the Arista Cognitive Campus solution can empower organizations to effectively architect, manage and control their increasingly complex campus networks.

If your organization is looking to simplify and optimize the behavior, visibility, and management of your campus network, it is worth taking a closer look at the Arista Cognitive Campus solution.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com P. 508.482.0188