Miercom

Cisco Intent-Based Networking

CISCO

Detailed Report DR180830H

Competitive test data for campus architecture solutions from HPE-Aruba and Huawei Technologies

MIERCOM.COM

CONTENTS

EXECUTIVE SUMMARY

1

Enterprise campus networks continue to evolve to meet the business needs of users, devices and things. The architectural design behind these networks becomes the forefront of integrating business demands with effective communication technology. A poor design can have serious consequences on user experience and management.

Cisco Systems, Inc. engaged Miercom to independently assess Cisco's next generation enterprise campus architecture, Cisco Digital Network Architecture (Cisco DNA), alongside the latest competitive offerings of Hewlett Packard Enterprise (HPE-Aruba) and Huawei Technologies for positive impact on end users, applications and administration for three key areas:

Network Automation: How easily can new network devices and services be designed and provisioned?

Network Segmentation: How well can the network be segmented for diverse users and devices, all while maintaining security?

Network Assurance: Can network problems be addressed with automatic features, such as self monitoring, troubleshooting and remediating insight?

Key Findings and Conclusions

- **Unified Resource Management.** Cisco's DNA Center effectively consolidates and manages wired and wireless network resources, far exceeding the capabilities of HPE-Aruba and Huawei.
- **Simplified Operations.** Cisco offers automation for the end-to-end network which saves time, resources and money for IT operations, as opposed to HPE-Aruba and Huawei which involves multiple steps and touchpoints.
- **Granular Policies for Users, Devices & IoT.** Cisco's SD-Access offers security based on group-based policies and virtual networks which delivers multi-level segmentation without compromise.
- **Insightful Resolution.** Cisco DNA Center offers impressive assessments of problems like DHCP issues and RF issues with understandable descriptions, root cause analysis, proactive insight and guided remediation.
- **Intuitive Diagnostic Tools.** Cisco provides proactive, leading-edge visual tools, like Path Trace and Intelligent Capture, to help administrators eliminate issues.

Based on our review and findings, the Cisco Digital Network Architecture (Cisco DNA) far outpaces the competitive solutions from HPE-Aruba and Huawei. We proudly award Cisco DNA the ***Miercom Performance Verified*** certification.

Miercom PERFORMANCE VERIFIED ™

Robert Smithers

CEO

Miercom

About Products Reviewed

2

Networks are defined by the users. The user demands dictate how the network is setup, accessed, secured and optimized. As the complexity of these demands increases, network administrators must rely on well-designed architectures to achieve expected management, protection and quality of communication services.

A campus network architecture transcends traditional pieces of the network, like routers and Access Points (APs). This high-level infrastructure unifies advanced technologies with basic network requirements in real-time for evolving business requirements to avoid piecemeal integration that incurs downtime and cost.

In this study we acquired and assembled the wired and wireless components of three network-equipment competitors—Cisco, HPE-Aruba and Huawei. Each vendor's network consisted of functional layers: the access, core and services layers.

Cisco Digital Network Architecture (Cisco DNA)

All the latest Cisco products have been built for intent-based networking. This adoption of intent-based networking also extends to earlier Cisco devices and, to varying degrees, even non-Cisco equipment.

Cisco uses the term "intent-based" to describe Cisco DNA's goals. This means the software is structured to accept and execute many low-level processes, to address the customer's intent. Examples include: adding a segmented guest network or identifying traffic bottlenecks without requiring hours of rigid commands on multiple touchpoints (applications and platforms). Cisco DNA makes network deployment, management, monitoring and troubleshooting easier and quicker. This directly equates to reduced maintenance, downtime and costs.

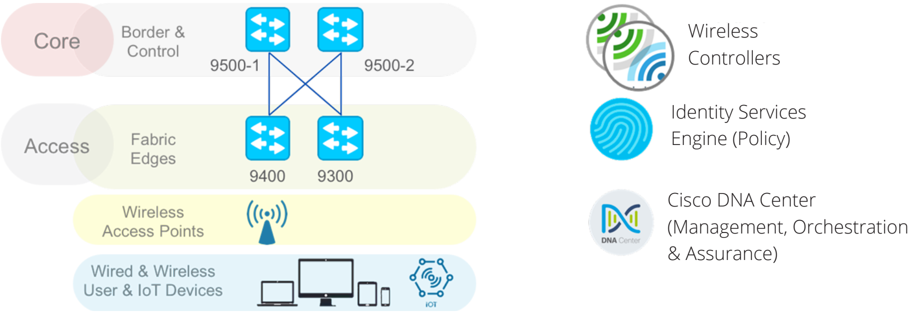
The Cisco DNA test bed featured Cisco DNA-ready equipment, including the Catalyst 9500 at the network core. The access layer consisted of Catalyst 9300 and 9400 switches. Wireless Access was enabled using Cisco 8540/ 5520 Wireless LAN Controller and 4800/3800 Wireless APs. At the heart of the network, was the Cisco DNA Center – a suite of automation and analytics software which includes applications such as design, policy, provisioning and assurance.

Augmenting the Cisco DNA Center at the services level is Cisco Identity Services Engine (ISE), which streamlines security policy management and provides security context information about devices and users. This policy management and security system shares data on users, devices, threats and vulnerabilities. The ISE configurations are abstracted from ISE to Cisco DNA Center, so that the administrator rarely must leave the Cisco DNA Center dashboard.

SD-Access provides policy-based automation from the edge to the cloud with secure segmentation for users and things. The SD-Access architecture is supported by fabric technology implemented for the campus, which enables the use of virtual networks (overlay networks) running on a physical network (underlay network) in order to create alternative topologies to connect devices.

The underlay is comprised of the physical network devices, such as routers, switches, and wireless LAN controllers (WLCs) plus a traditional Layer 3 routing protocol. The overlay is the logical, virtualized topology built on top of the physical underlay.

The SD-Access architecture is implemented via Cisco DNA Center.


Core
Border & Control
9500-1
9500-2
Access
Fabric Edges
9400
9300
Wireless Access Points
Wired & Wireless User & IoT Devices
Wireless Controllers
Identity Services Engine (Policy)
Cisco DNA Center (Management, Orchestration & Assurance)

Source: Cisco

Fabric edge: The SD-Access fabric edge nodes are the equivalent of an access layer switches in a traditional campus design which interface with wired hosts (laptops, IoT devices etc.), wireless access points or other fabric extension switches.

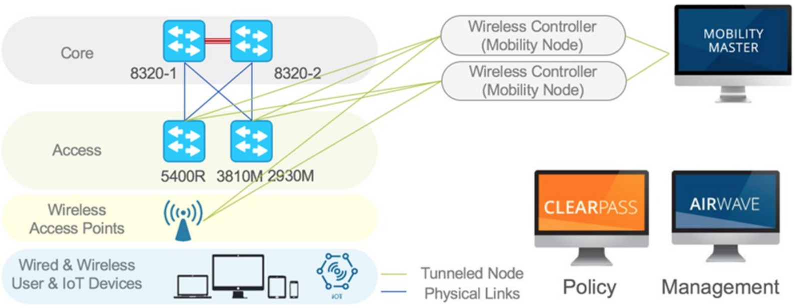
Border node: The fabric border nodes serve as the gateway between the SD-Access fabric domain and the network outside of the fabric. The fabric border node is responsible for encapsulation-decapsulation for network virtualization interworking and SGT propagation from the fabric to the rest of the network.

Control plane node: The SD-Access fabric control plane node is based on the LISP Map-Server (MS) and Map-Resolver (MR) functionality combined on the same node or also distributed on separate nodes. The control plane node enables those functions together to create the Host tracking database.

HPE-Aruba Mobile First Campus Solution

HPE-Aruba expanded into the wireless realm with the 2015 acquisition of Aruba Networks and its impressive repertoire of Wi-Fi equipment, such as APs, controllers and wireless management applications. Additionally, HPE has adopted Aruba's AirWave management, ClearPass policy management and Mobility Master for wireless configuration. HPE-Aruba also offers four distinct assurance platforms: Connectivity Health (part of AirWave), Network Analytics Engine (part of ArubaOS-CX), NetInsight (acquisition Rasa Networks) and Aruba User Experience Insight ('Cape Networks' acquisition, Sensor overlay solution).

HPE-Aruba offers another high-level management package, the Intelligent Management Center (IMC), which is oriented towards campus core and wired data centers, and without wireless support. We selected AirWave as the most appropriate application for this comparative analysis.



Source: Miercom

AirWave is designed with mobility in mind, proactively monitoring devices, users and applications for health and performance.

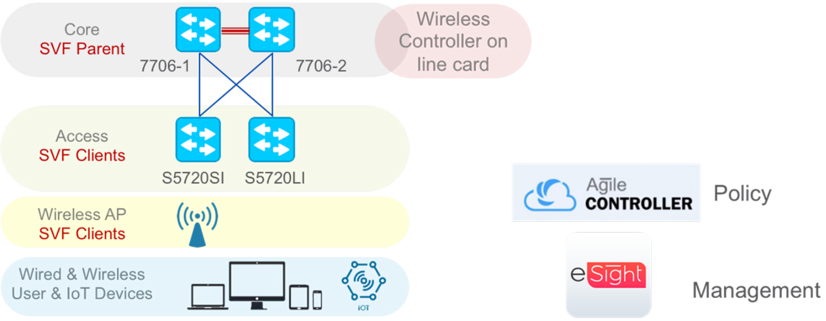
Our HPE-Aruba test bed also included the former Aruba application – ClearPass, a policy manager platform for Network Access Control (NAC), secure device onboarding and guest access. We also deployed Mobility Master, a wireless-oriented package also from Aruba, which addresses configuration and deployment, operations, and Wi-Fi client load balancing.

Huawei Agile Campus Network Solution

Huawei's Agile Campus Network architecture comprises of their Software Defined Campus (SD-Campus), a component of Huawei's Intent Driven Networking (IDN). Huawei's SD-Campus consists of Super Virtual Fabric (SVF) and Unified Virtual Fabric (UVF). Huawei eSight is a software suite for unified enterprise control. This network management package is the centerpiece of the Huawei campus architecture and is used for planning, operating and maintaining the complex infrastructure. Additionally, Huawei offers their Agile Controller-Campus 3.0 for automation of an overlay network. Unfortunately, the Agile Controller 3.0 was unavailable for purchase during testing

Another key ingredient in the Huawei architecture is the Agile Controller-Campus 1.0, which handles AAA, Guest, and policy management.

Huawei's Super Virtual Fabric (SVF) is one of the many components of the Huawei SD-Campus. Huawei requires SVF for Unified Management of wired and wireless networks. SVF uses a Parent switch for management and configuration for the SVF system.



Source: Miercom

SVF Clients (wired and wireless APs) are connected to the parent. Traffic is sent to a Parent Switch for wired and wireless forwarding. When configuring SVF, Huawei recommends configuring parent switches in a CSS pair (Cluster Switching System). Configuring CSS was only available via CLI on the S7706. This was a 9-step operation and consisted of a reboot of the S7706 chassis to form the CSS. Miercom followed Huawei's Recommended SVF configuration via the configuration assistant.

Products and Software Under Test

	Cisco	HPE-Aruba	Huawei
Core Switches	9500 (16.8.1)	8320 (10.01)	7700 (V200R010)
Access Switches (Modular)	9400 (16.8.1)	5400R (16.08)	7700 (V200R010)
Access Switches (Fixed)	9300 / 3850 (16.8.1)	3810M / 2930M (16.08)	S5720SI / S5720LI (V200R011)
Wireless Controller	8540 / 5520 (8.8)	Mobility Master / 7280 / 7210 (8.4)	X2 / AC6605 (V200R010)
Access Point	3802 / 4800	335 / 345	7050DE
Policy	ISE 2.4	ClearPass 6.8	Agile Controller 1.0 (V100R003)
Management	Cisco DNA Center 1.2	AirWave 8.2	eSight V300R008

Network Automation

3

Typical network design and deployment is a very complex and time-consuming process. It becomes increasingly complicated as enterprises include wired and wireless user devices, newly introduced Internet-of-Things (IoT) devices, advanced services (e.g. guest, host mobility), operations and maintenance. Today, network administrators need automation and orchestration platforms to support end-to-end networking devices (e.g. switching, wireless, routing, SD-Access, SD-WAN). To assess how network automation works per each vendor's architecture, we verified following two test cases:

- Part 1: Network Design
- Part 2: Out-of-box Switch and Access Point Deployment

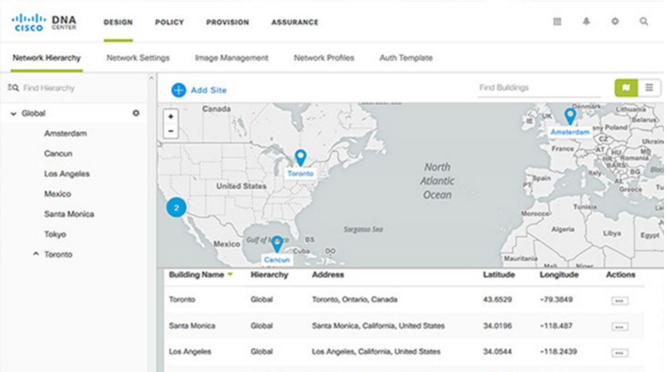
Part 1: Network Design

In this test case, we evaluated how each of the vendor offers the network design capabilities before device deployment. Accurate network design is very crucial, saving lot of time and money by avoiding any future misconfiguration or errors.

Cisco

In our testing, only Cisco offered a single, unified dashboard for designing an entire campus network with switching, wireless and routing using Cisco DNA Center. Network design started with the site creation for multiple locations/branches, and it zoomed into building and floor level, with floor plan maps. All shared network services (e.g. DHCP, AAA, SNMP, device credentials) can be configured globally or per location, which automatically trickled down to hierarchy-based sub-groups. Even common network parameters, like wireless SSID for employees, guest access, authentication methods and configuration templates were defined based on a hierarchy.

Cisco showed excellent design automation using Cisco DNA Center workflows and a hierarchical deployment model, which truly turns business intent into the automated network configuration. An automation scenario we verified was deploying wireless SSIDs across multiple sites and multiple wireless controllers, based on a hierarchy, with just few clicks on Cisco DNA Center dashboard. We never touched multiple wireless controllers for configuration changes.



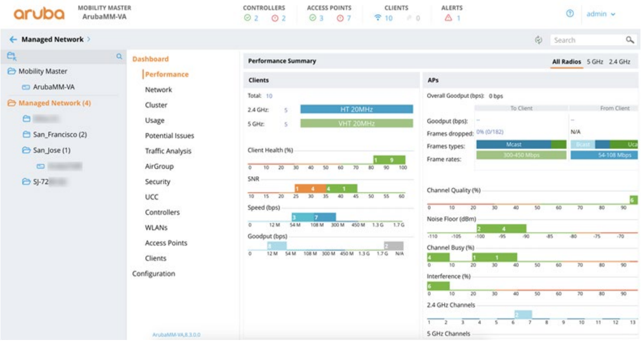
Building Name	Hierarchy	Address	Latitude	Longitude	Actions
Toronto	Global	Toronto, Ontario, Canada	43.6529	-79.3849	···
Santa Monica	Global	Santa Monica, California, United States	34.0196	-118.487	···
Los Angeles	Global	Los Angeles, California, United States	34.0544	-118.2439	···

Source: Miercom

Cisco DNA Center took care of creating various SSIDs, respective interfaces and AP groups automatically, abstracting and automating the configurations behind-the-scenes.

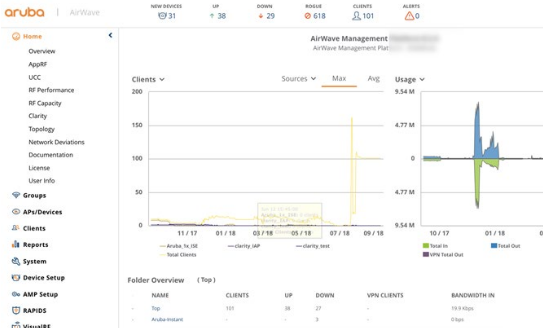
HPE-Aruba

HPE-Aruba offers the hierarchical model of network design using Aruba Mobility Master, but it is only for wireless networks. All switch network designing is done traditionally using configuration templates, for individual or batches of switches using AirWave Management platform. Automation is not supported. This leads to two separate touchpoints for designing wired and wireless networks. Moreover, routing support can be only added using FlexNetwork routers and IMC Management platform, creating another touchpoint.



Aruba Mobility Master

Source: Miercom

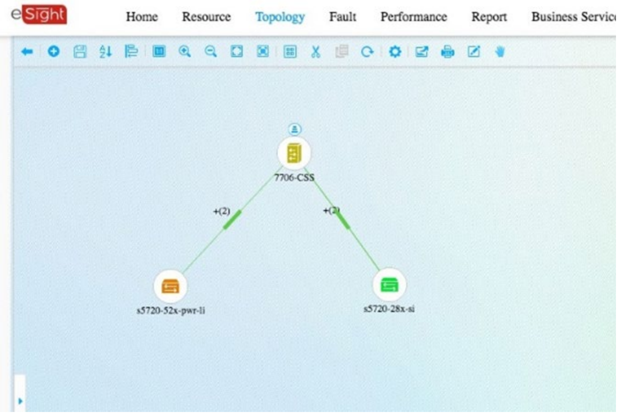


Aruba AirWave

Source: Miercom

Huawei

Huawei's SD-Campus solution does not offer any hierarchical model for network design and deployment. Huawei still relies on the traditional way of network design, which is neither time-saving nor agile. Huawei relies on multiple ways to configure network deployments. For example, SVF (Super Virtual Fabric) can be configured through CLI, Easy Operations (switch dashboard) and eSight NMS. Huawei supports a limited design capability and automation using eSight maps/topology view; it is only for traditional networks and offers no fabric support.



Source: Miercom

Network Design Summary

	Cisco	HPE-Aruba	Huawei
Site Creation/ Hierarchy/ Maps	Yes	Requires both Mobility Master and AirWave	No support for hierarchy, Maps requires eSight
Shared Services Configuration	DHCP, AAA, DNS, SNMP, CLI credentials	AAA, SNMP	DHCP, SNMP, CLI credentials
Image Management	Direct cloud download for images and patches for wireless, switches and routers	Manual upload using AirWave	Manual upload using Easy Operations (SVF parent) or eSight
Network Profile	Wireless, Switches, Routing, Authentication methods	Wireless Only	Wireless and Wired using Easy Operations (SVF parent) or eSight
Guest	Built-in auth. and portal customization	Requires access to ClearPass or any other external server	Requires access to Agile or any other external server

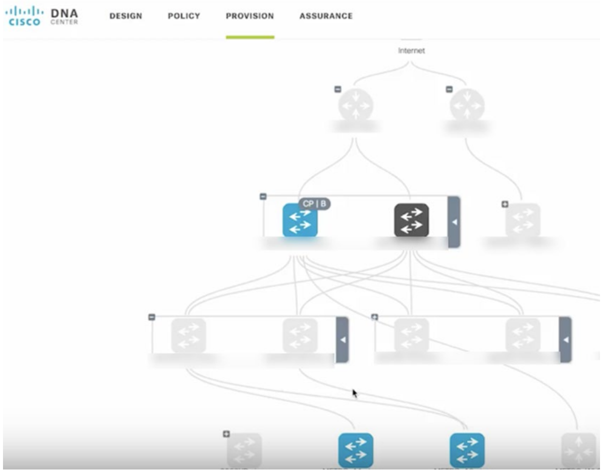
Part 2: Out-of-Box Switch and Access Point Deployment

In this test case, a customer wants to incorporate new network devices and services, and then provision a new area for network access. The following criteria was applied to each vendor:

1. How easy is it to bring up a new switch and AP out-of-the-box?
2. How easy is it to setup the underlay and overlay networks? (An overlay network is a virtual network built on top of an underlying network infrastructure – the underlay network. The underlay provides a service to the overlay.)
3. How simple or difficult is it to provision advanced network services like wireless for employees and guest access?

Cisco

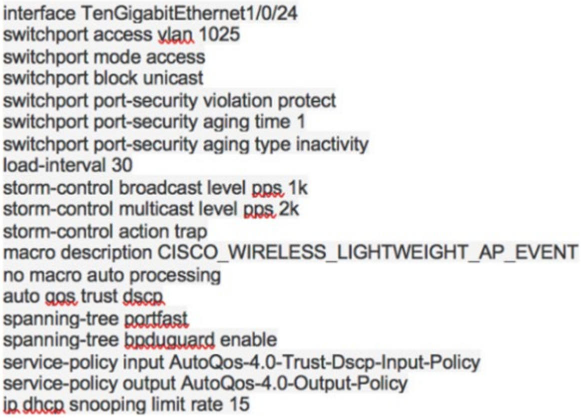
All the above processes are executed completely from the Cisco DNA Center main screen. From the top options (Design, Policy, Provision, Assurance), the Provision Application is selected. Activation and configuration of the new devices, once appropriately connected, is straightforward and quick. Cisco DNA Center used the seed device (switch) to discover all the connected network devices using CDP (Cisco Discovery Protocol), and then onboarded those devices on the network, automatically creating a topology. Adding these devices to Software-Defined Access (SD-Access) fabric was simple two-click operation.



Source: Miercom

Cisco DNA Center onboarded the devices and provided them with prescriptive configuration according to Cisco design best practices. Cicso DNA Center also automatically pulled the required software images and patches directly from Cisco.com and made them available for the joining devices.

Cisco automatically configured switchports, based on the connected device, using switchport macros triggered by Cisco DNA Center in the background, without user intervention. Shown right is an example an automatically pushed configuration by Cisco DNA Center for a connected wireless AP. Cisco DNA Center automation saved a significant amount of time in manual configuration and avoided any syntax or user error while configuring this on potentially hundreds of AP switchports.



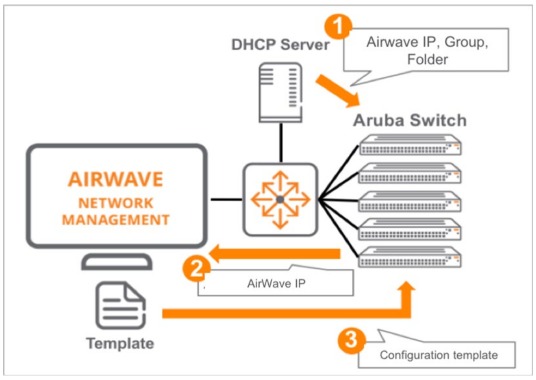
```
interface TenGigabitEthernet1/0/24
switchport access vlan 1025
switchport mode access
switchport block unicast
switchport port-security violation protect
switchport port-security aging time 1
switchport port-security aging type inactivity
load-interval 30
storm-control broadcast level pps 1k
storm-control multicast level pps 2k
storm-control action trap
macro description CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT
no macro auto processing
auto qos trust dscp
spanning-tree portfast
spanning-tree bpduguard enable
service-policy input AutoQos-4.0-Trust-Dscp-Input-Policy
service-policy output AutoQos-4.0-Output-Policy
ip dhcp snooping limit rate 15
```

Source: Miercom

Cisco DNA Center directly communicated with ISE to add devices to ISE network devices database and made them ready for policy implemntation.

HPE-Aruba

HPE-Aruba AirWave network management platform is used for Zero Touch Provisioning (ZTP) to successfully deploy the new switch and AP. ZTP relies on the traditional method of DHCP Option 43 to discover the AirWave server, making the process of adding a switch and AP manual and requiring multiple touchpoints. This also requires pre-loaded configuration templates for every unique device to accomplish complete network provisioning. This old way of provisioning is prone to user errors and consumes significant amount of time and money.



Source: HPE-Aruba

Moreover, HPE-Aruba does not have direct hooks into ClearPass for automatic network device configuration. Unlike Cisco, we had to manually add and configure all the networking devices in the ClearPass to start using ClearPass policy.

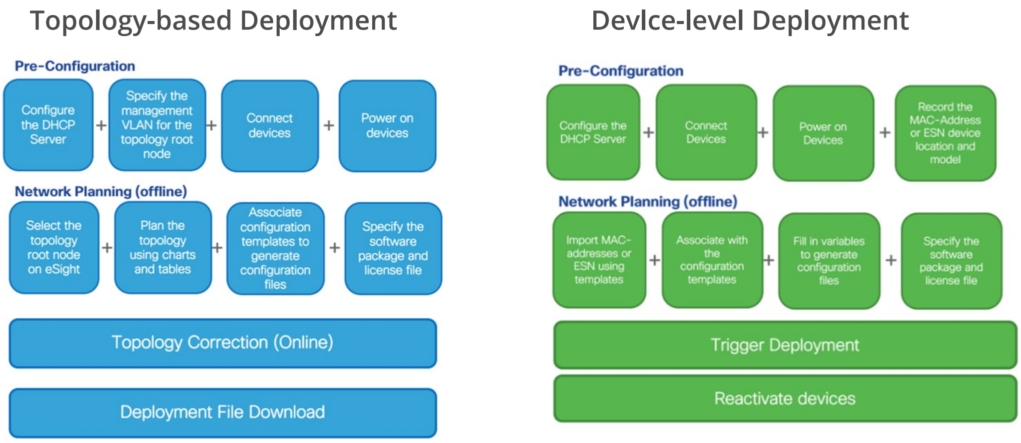
Huawei

Huawei's eSight, like HPE-Aruba's AirWave, is one of several touchpoints the customer uses to manually perform the proper connection and configuration of a new switch and AP.

Huawei's eSight is a management platform with multiple modules which requires different licenses for various features such as MPLS, Wireless, Network Infrastructure, Network Traffic Analytics, Wireless Management and more. Huawei uses a ZTP module within the eSight tool.

Huawei eSight Zero-Touch Provisioning

Huawei offers two modes for ZTP with their eSight NMS: device-level, and topology based.

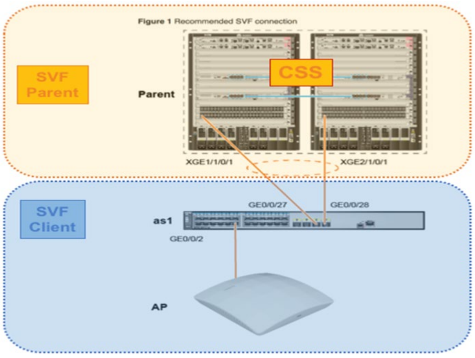

Topology-based Deployment

DevIce-level Deployment

Pre-Configuration
Configure the DHCP Server
+
Specify the management VLAN for the topology root node
+
Connect devices
+
Power on devices
Network Planning (offline)
Select the topology root node on eSight
+
Plan the topology using charts and tables
+
Associate configuration templates to generate configuration files
+
Specify the software package and license file
Topology Correction (Online)
Deployment File Download
Pre-Configuration
Configure the DHCP Server
+
Connect Devices
+
Power on Devices
+
Record the MAC-Address or ESN device location and model
Network Planning (offline)
Import MAC-addresses or ESN using templates
+
Associate with the configuration templates
+
Fill in variables to generate configuration files
+
Specify the software package and license file
Trigger Deployment
Reactivate devices

Source: Huawei

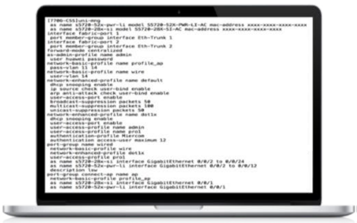
The topology method is used when there are multiple switches for a greenfield or batch deployment. The device level method applies to expanding a brownfield campus where a few wired switches need to be deployed by manually entering MAC addresses or ESN (Electronic Serial Number).



Source: MIercom

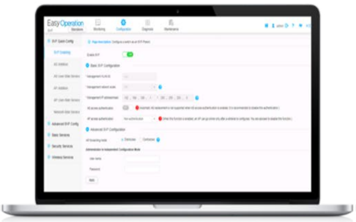
Steps required for building the Huawei Campus Solition

A collection of dashboards such as CLI, Easy Operation, and eSight operations were required to build the Agile Campus 5.0 architecture. ZTP was performed through eSight. Huawei offers three ways to configure the campus into a Super Virtual Fabric. After enabling SVF, STP mode is set to RSTP.

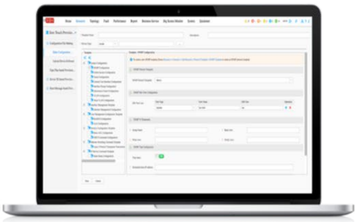


```
[7700-CSS]uni-mng
 as name s5720-52x-pwr-li model S5720-52X-PWR-LI-AC mac-address xxxx-xxxx-xxxx-xxxx
 as name s5720-28x-si model S5720-28X-SI-AC mac-address xxxx-xxxx-xxxx-xxxx
interface fabric-port 1
 port member-group interface Eth-Trunk 1
interface fabric-port 2
 port member-group interface Eth-Trunk 2
forward-mode centralized
as-admin-profile name admin
 user huawei password
network-basic-profile name profile_ap
 pass-vlan 11 14
network-basic-profile name wire
 user-vlan 14
network-enhanced-profile name default
 dhcp snooping enable
 ip source check user-bind enable
 arp anti-attack check user-bind enable
 user-access-port enable
 broadcast-suppression packets 50
 multicast-suppression packets 100
 unicast-suppression packets 50
network-enhanced-profile name dot1x
 dhcp snooping enable
 user-access-port enable
 user-access-profile name admin
 user-access-profile name prol
 authentication-profile Miercom
 authentication access-user maximum 12
port-group name wired
 network-basic-profile wire
 network-enhanced-profile dot1x
 user-access-profile prol
 as name s5720-28x-si interface GigabitEthernet 0/0/2 to 0/0/24
 as name s5720-52x-pwr-li interface GigabitEthernet 0/0/2 to 0/0/12
 description lsw
port-group connect-ap name ap
 network-basic-profile profile_ap
 as name s5720-28x-si interface GigabitEthernet 0/0/1
 as name s5720-52x-pwr-li interface GigabitEthernet 0/0/1
```

CLI



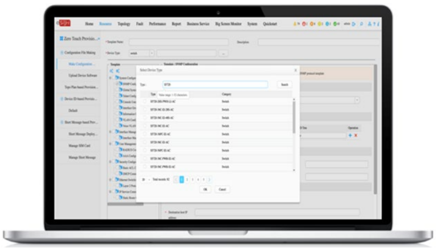
EasyOperation

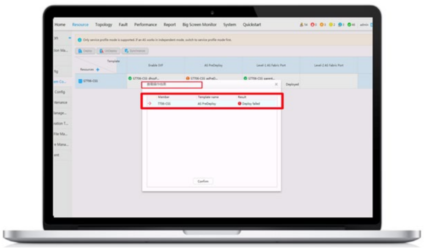


eSight

Source: Huawei

eSight appeared to have an older look and feel, not a current user experience for an Intent-Driven Network. Miercom encountered an error when using the eSights template-based operation for SVF. Operating eSight is sometimes difficult, as these errors may appear in non-English language.





Source: Huawei

Similar to HPE-Aruba, Huawei does not offer any direct hooks into the Agile Controller platform to automatically add network devices for policy; the administrator is forced to go through various dashboards to complete the configuration. This old way of provisioning is prone to user errors and consumes significant amount of time and money.

Steps required to build an Enterprise Network

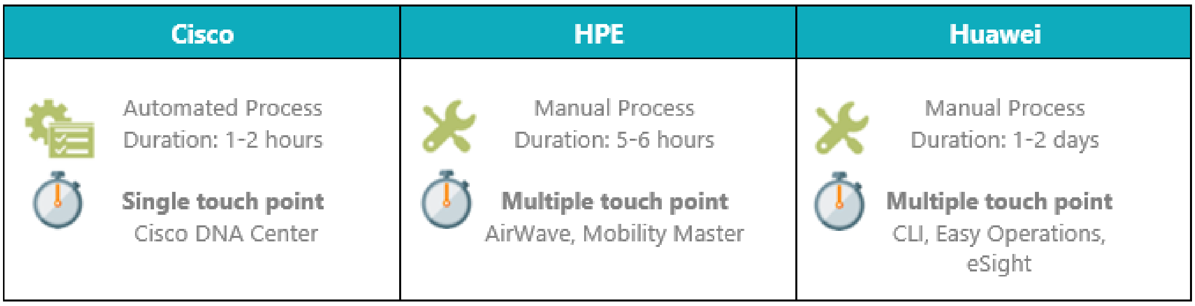
Cisco	HPE	Huawei
• Cisco DNA Center runs the Plug-n-Play service for LAN Automation for all the new devices • Create hierarchy for sites, buildings, etc. • Use the seed device to start network automation to find all the connected devices in your network using Cisco Discovery Protocol (CDP) neighbor discovery • Cisco DNA Center automatically onboards all the connected Cisco devices and configures them with certificates, credentials, basic configurations based on the site-specific network settings and automatically creates topology	• Aruba AirWave runs ZTP feature • Create groups and folders for the onboarding devices (no hierarchy option) • Create configuration template for every device or group of devices • Configure DHCP Option 43 on the DHCP server with AirWave's IP address, Device Group, Folder name, etc. (If you have multiple AirWave servers, take caution to configure the right server) • Connect out-of-box devices (switches, AP, etc.) to network • Accept all the new devices on AirWave • For Wireless, Aruba Mobility Master can be used to create hierarchy-based configuration	• ZTP eSight (Seed Device) Device-level based deployment • Configured S7706 Pair as CSS Cluster (Total of 9 steps) • Create Multi-Action Detection configuration on CSS device • Enable Parent SVF Functionality (This can be done via CLI, Easy Operation, or eSight. If eSight is selected, SNMP, SSH/Telnet Configuration is required on the Parent switch and eSight.) • When using eSight, the network administrator will use templates to enable SVF Parent, VLANs, IP Pools • Configure SVF Template for access layer switches; this requires knowledge of the switch name, switch part number, MAC-address of switch, and adding to whitelist • Configure Fabric Port ID, Fabric Ethernet Trunk ID, Ethernet Trunk Member, Interface selection, Connection type • After the templates are configured, eSight pushes the templates to the Parent Switch • Create Port Groups for Access Switches and APs • Create User interface (VLAN) for Access switch • Deploy SVF Port Config • Create Manage of Access switches and AP parameters • Physically cable the access layer switch to the parent SVF switch, and connect AP(s) to access layer switch • Configure WLAN service on SVF Parent

Network Automation Summary

Cisco DNA Center abstracted the complexities involved in the deployment of networks and offered a single, unified dashboard to design and deploy end-to-end network. DNA Center gracefully handled all the complicated tasks and best practices behind-the-scenes, helping Miercom translating business intent into reliable network automation.

HPE-Aruba and Huawei forced Miercom to use multiple dashboards to design and deploy networks. Sometimes there were different platforms for switching and wireless networks. Their lack of a granular hierarchy-based model made provisioning and configuration time-consuming. HPE-Aruba and Huawei lack network automation and its inherent simplicity. Their traditional way of deploying enterprise networks is prone to user errors, lacks best practices and most importantly costs more money in CAPEX and OPEX.

Cisco DNA Center extends its support to the Cisco-Meraki Cloud Networking solution, Cisco SD-WAN solution and to third parties using SDKs and APIs.

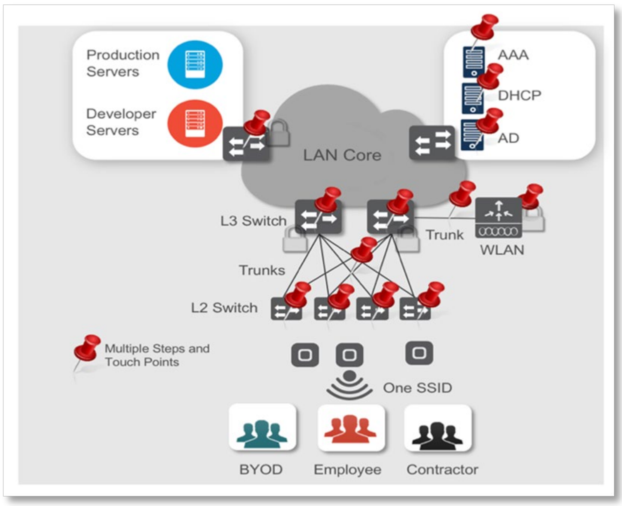


Cisco	HPE	Huawei
Automated Process Duration: 1-2 hours	Manual Process Duration: 5-6 hours	Manual Process Duration: 1-2 days
Single touch point Cisco DNA Center	**Multiple touch point** AirWave, Mobility Master	**Multiple touch point** CLI, Easy Operations, eSight

Network Segmentation

4

Network segmentation refers to the subdividing of a network into logical partitions for reasons such as: to segregate Guest access in a WLAN or to create a highly secure VLAN for a specific set of endpoints to prevent malicious East-West traffic within the network. The figure (shown right) depicts multiple configuration touchpoints to deploy segmentation.



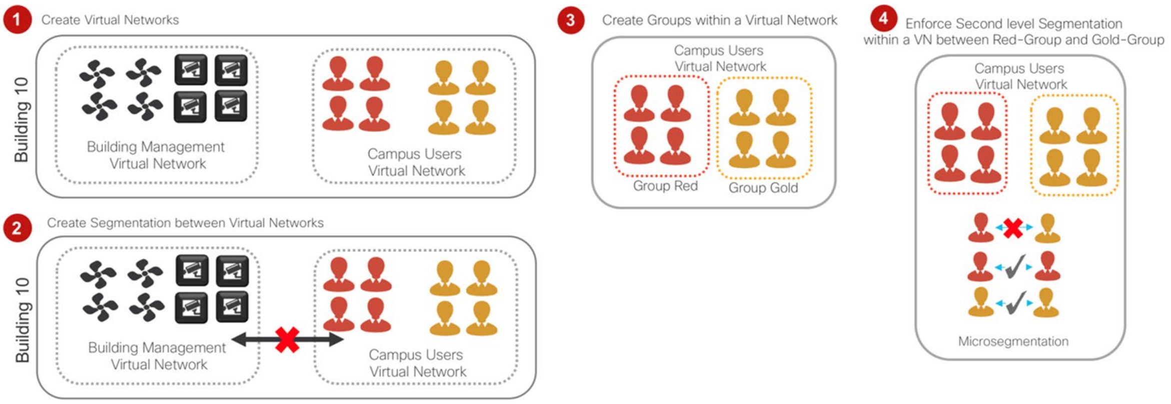
Source: Miercom

Applying Policies

In this test case, Miercom tested the capability to segment at the network level using virtual networks and at the micro segmentation level with group-based policies.

Miercom also compared the network administrator experience using a single dashboard using the following test cases:

1. Create Virtual Networks
2. Create Segmentation between Virtual Networks
3. Create Groups within a Virtual Network
4. Create Intra-Virtual network Segmentation


1
Create Virtual Networks
Building 10
Building Management Virtual Network
Campus Users Virtual Network
2
Create Segmentation between Virtual Networks
Building 10
Building Management Virtual Network
Campus Users Virtual Network
3
Create Groups within a Virtual Network
Campus Users Virtual Network
Group Red
Group Gold
4
Enforce Second level Segmentation within a VN between Red-Group and Gold-Group
Campus Users Virtual Network
Microsegmentation

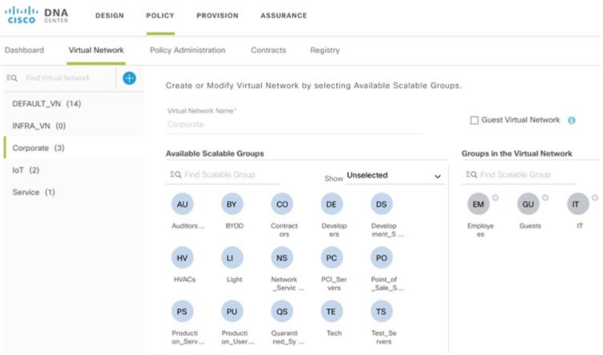
Source: Miercom

Cisco

Miercom used Cisco's DNA Center Policy Application to create virtual networks. Cisco DNA Center is a system for centralized deployment and policy management of devices within a campus network. The DNA Center acts as a software-defined controller pushing down configurations and policy to every node across the enterprise.

Cisco's SD-Access provides embedded multi-level segmentation. Under the covers, SD-Access allows for creation of multiple Virtual Networks using Virtual Routing and Forwarding (VRF) definitions and micro segmentation using Scalable Group Tags. Access policies are enabled in hardware on each individual edge switch to provide an unprecedented level of granularity in routing and access control for wired and wireless users and devices.

Cisco's DNA Center allowed creation of virtual networks and management of scalable groups from a single dashboard.

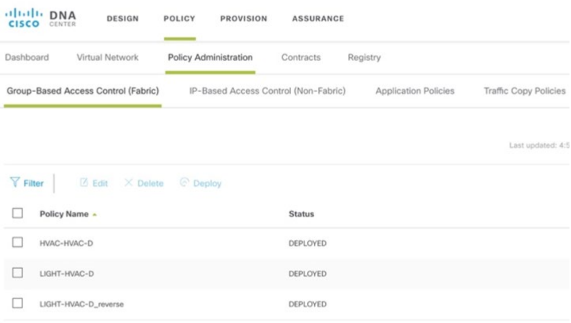


Create or Modify Virtual Network by selecting Available Scalable Groups.

Virtual Network Name* Corporate

□ Guest Virtual Network

Show Unselected



□	Policy Name	Status
□	HVAC-HVAC-D	DEPLOYED
□	LIGHT-HVAC-D	DEPLOYED
□	LIGHT-HVAC-D_reverse	DEPLOYED

Source: Miercom

This test case showcased the simplicity of how a customer can leverage Cisco DNA Center to build a complete security policy. With SD-Access we were able to provide macro segmentation using virtual networks and at the micro segmentation level with scalable groups.

Cisco DNA Center was the single dashboard used to build virtual networks, assign groups to virtual networks, define and implement security policy, and define new security contracts.

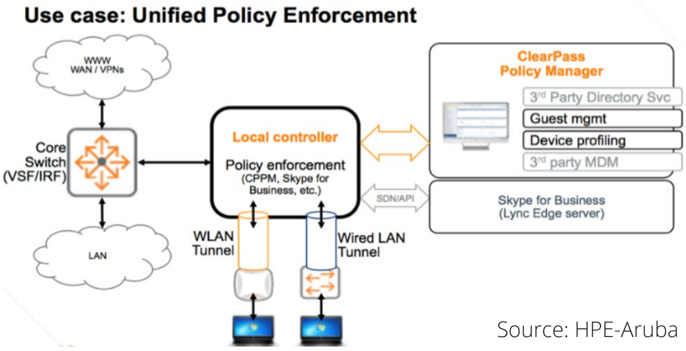
Miercom executed security policies and contracts via simple drag-and-drop method in DNA Center.

Cisco's implementation for policy is not tied to IP address or location, but rather uses identity of users, devices, or things. This provides host mobility with consistent policy without having to reconfigure the various touchpoints for VLANs, subnets, and Access Control Lists (ACLs).

Because of this, Cisco demonstrated the ability to add, remove, and modify virtual networks and group-based policies, independent of network devices or location of user.

HPE-Aruba

For the segmentation test cases, HPE-Aruba requires a feature called Dynamic Segmentation (previously known as Aruba's Tunneled Node). This feature converts an Aruba switch to behave like an AP. User traffic from the switch is redirected to the Aruba Wireless Controller (Mobility Controller) for unified policy enforcement.

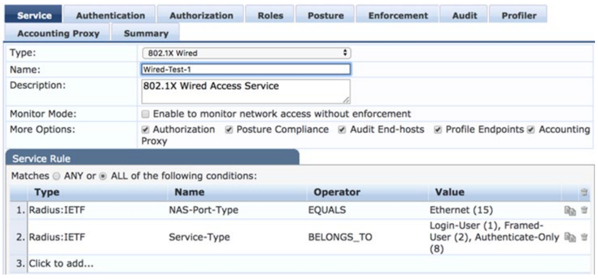


Source: HPE-Aruba

Aruba also recommends Dynamic Segmentation for application visibility and stateful firewall. Tunneling is configured as a per-port or per-user mode, but both are mutually exclusive.

Aruba uses Dynamic Segmentation in conjunction with its ClearPass Policy Manager (CPPM). The switch is manually configured for AAA, VLANs, user policies, port configuration for 802.1x and MAC-Auth, and IP connectivity to the Mobility Controller. The Mobility Controller is configured as the Tunneled Node server. ClearPass is used as the RADIUS policy server. The main purpose of Tunneled Node is to use the controller as a unified policy enforcement point for traffic from both wired and wireless clients.

Under the hood, Aruba uses GRE tunnels from the access switch to the Aruba Mobility Controller to segment traffic. The figure below depicts the ClearPass Configuration and CLI of the ArubaOS Switch required for segmentation. For example:



Type:	802.1X Wired
Name:	Wired-Test-1
Description:	802.1X Wired Access Service
Monitor Mode:	☐ Enable to monitor network access without enforcement
More Options:	☑ Authorization ☑ Posture Compliance ☑ Audit End-hosts ☑ Profile Endpoints ☑ Accounting Proxy

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Click to add...			

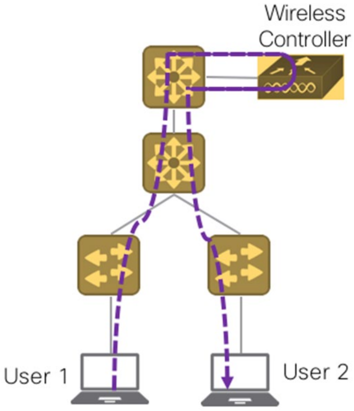
```
class ipv4 "IP-ANY-ANY"
    match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
  exit

policy user "PERMIT-ALL"
    class ipv4 "IP-ANY-ANY" action permit
  exit

aaa authorization user-role name "IoT-Lights"
    policy "PERMIT-ALL"
    reauth-period 28800
    vlan-name "IOT_Lights_vlan1"
    exit
```

Source: Miercom

The HPE-Aruba switches employ traditional segmentation, which uses VLANs and ACLs. The security policy is based on IP addresses and the network topology. Maintaining these policies is complex, time-consuming and prone to error.

Dynamic Segmentation. HPE-Aruba creates an architecture to unify policy for wired and wireless clients, using a common controller, as shown in the graphic. Wired traffic between hosts are not optimized, and all traffic passes to and from the Aruba Mobility controller.

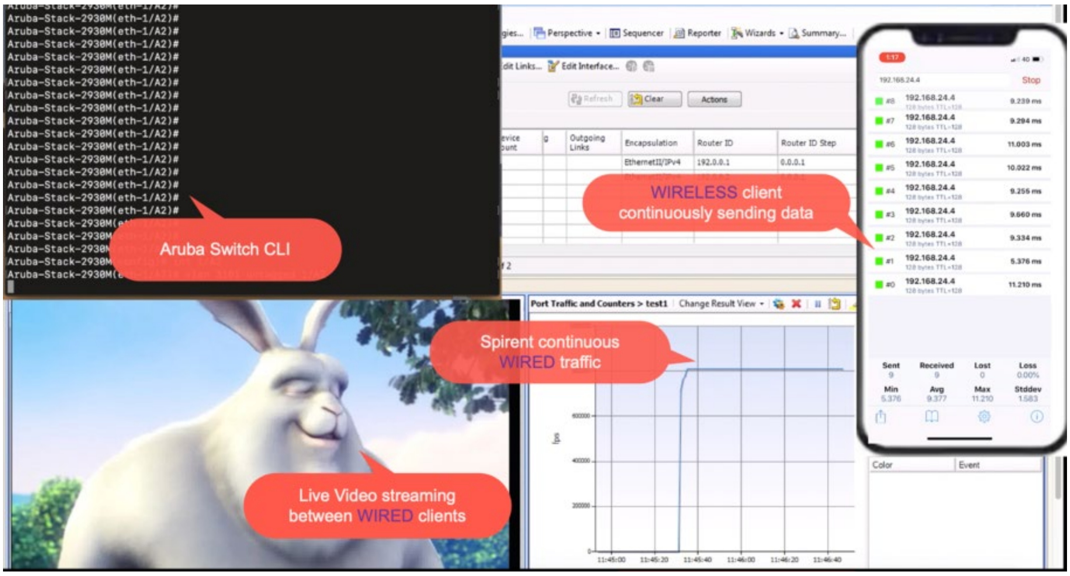
Miercom configured the tunnel-node feature as per Aruba's recommendation using ClearPass, switch configuration, and Mobility controller, allowing only traffic from a specific user/device role is sent to the mobility controller.



Source: Miercom

Validation of client traffic was performed prior to injecting traffic from the Spirent test tool. The following screenshots show figures from the Spirent Test Center and smartphone screen pinging the gateway. The Spirent Test Center was configured to simulate wired clients. Uni-directional traffic streams were configured for IMIX traffic distribution. A pair of wired clients were configured to stream live video. Simultaneously, a smartphone was used as a wireless client associating to the TN-SSID. Pings were generated from the wireless client. Before enabling Aruba's Dynamic Segmentation feature, there was no performance impact, and the phone pinged the gateway.

Before enabling Dynamic Segmentation:



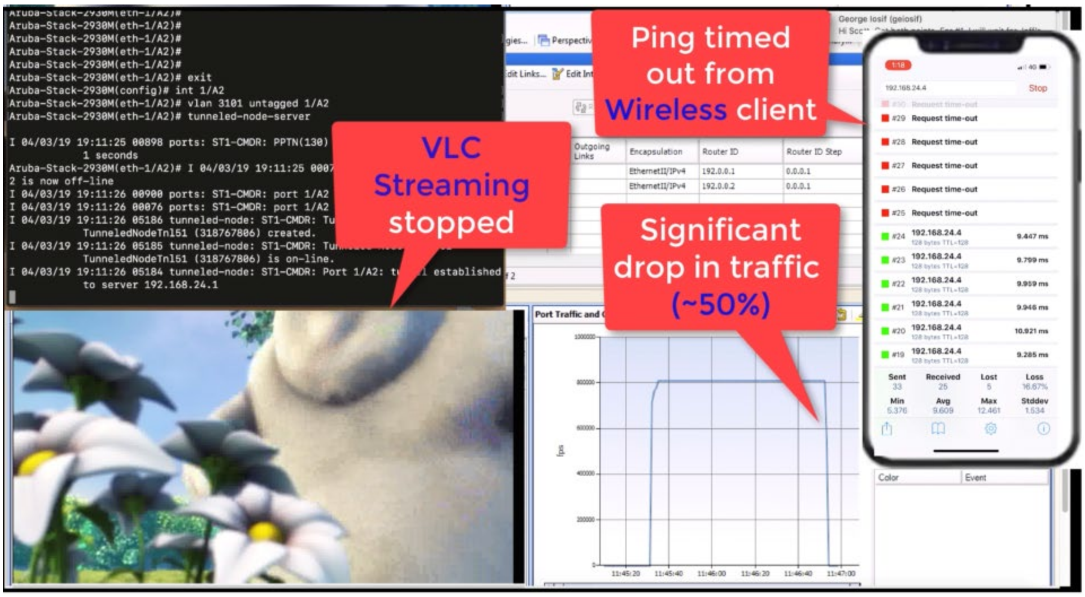
```
Aruba-Stack-2930M(eth-1/A2)#
Aruba-Stack-2930M(eth-1/A2)#
Aruba-Stack-2930M(eth-1/A2)#
Aruba-Stack-2930M(eth-1/A2)#
Aruba-Stack-2930M(eth-1/A2)#
Aruba-Stack-2930M(eth-1/A2)#
Aruba-Stack-2930M(eth-1/A2)#
Aruba-Stack-2930M(eth-1/A2)#
Aruba-Stack-2930M(eth-1/A2)#
Aruba-Stack-2930M(eth-1/A2)#
Aruba-Stack-2930M(eth-1/A2)#
Aruba-Stack-2930M(eth-1/A2)#
Aruba-Stack-2930M(eth-1/A2)#
Aruba-Stack-2930M(eth-1/A2)#
Aruba-Stack-2930M(eth-1/A2)#
Aruba-Stack-2930M(eth-1/A2)#
Aruba-Stack-2930M(e
Aruba-Stack-2930M
Aruba-Stack-2930M
Aruba-Stack-2930M
Aruba-Stack-2930M(e
```

Encapsulation	Router ID	Router ID Step
EthernetII/IPv4	192.0.0.1	0.0.0.1

```
192.168.24.4                              Stop
#8  192.168.24.4  128 bytes TTL=128   9.239 ms
#7  192.168.24.4  128 bytes TTL=128   9.294 ms
#6  192.168.24.4  128 bytes TTL=128  11.003 ms
#5  192.168.24.4  128 bytes TTL=128  10.022 ms
#4  192.168.24.4  128 bytes TTL=128   9.255 ms
#3  192.168.24.4  128 bytes TTL=128   9.660 ms
#2  192.168.24.4  128 bytes TTL=128   9.334 ms
#1  192.168.24.4  128 bytes TTL=128   5.376 ms
#0  192.168.24.4  128 bytes TTL=128  11.210 ms

Sent   Received   Lost    Loss
9      9          0       0.00%
Min    Avg        Max     Stddev
5.376  9.377      11.210  1.583
```

Source: Miercom

After enabling Dynamic Segmentation: The figure below highlights the performance impact to the wired and wireless clients. The Aruba Mobility Controller was impacted by the volume of traffic and was unable to respond to the pings sent by the wireless client. Traffic was severely impacted, and the live video stream froze between the wired clients.



```
Aruba-Stack-2930M(eth-1/A2)#
Aruba-Stack-2930M(eth-1/A2)#
Aruba-Stack-2930M(eth-1/A2)#
Aruba-Stack-2930M(eth-1/A2)#
Aruba-Stack-2930M(eth-1/A2)#
Aruba-Stack-2930M(eth-1/A2)# exit
Aruba-Stack-2930M(config)# int 1/A2
Aruba-Stack-2930M(eth-1/A2)# vlan 3101 untagged 1/A2
Aruba-Stack-2930M(eth-1/A2)# tunneled-node-server

I 04/03/19 19:11:25 00898 ports: ST1-CMDR: PPTN(130)
        1 seconds
Aruba-Stack-2930M(eth-1/A2)# I 04/03/19 19:11:25 0007
2 is now off-line
I 04/03/19 19:11:26 00900 ports: ST1-CMDR: port 1/A2
I 04/03/19 19:11:26 00076 ports: ST1-CMDR: port 1/A2
I 04/03/19 19:11:26 05186 tunneled-node: ST1-CMDR: Tu
        TunneledNodeTnl51 (318767806) created.
I 04/03/19 19:11:26 05185 tunneled-node: ST1-CMDR: Tu
        TunneledNodeTnl51 (318767806) is on-line.
I 04/03/19 19:11:26 05184 tunneled-node: ST1-CMDR: Port 1/A2: t    l established
        to server 192.168.24.1
```

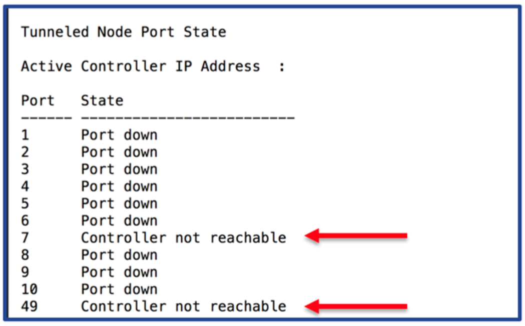
Encapsulation	Router ID	Router ID Step
EthernetII/IPv4	192.0.0.1	0.0.0.1
EthernetII/IPv4	192.0.0.2	0.0.0.1

```
192.168.24.4                              Stop
#30 Request time-out
#29 Request time-out
#28 Request time-out
#27 Request time-out
#26 Request time-out
#25 Request time-out
#24 192.168.24.4  128 bytes TTL=128   9.447 ms
#23 192.168.24.4  128 bytes TTL=128   9.799 ms
#22 192.168.24.4  128 bytes TTL=128   9.959 ms
#21 192.168.24.4  128 bytes TTL=128   9.946 ms
#20 192.168.24.4  128 bytes TTL=128  10.921 ms
#19 192.168.24.4  128 bytes TTL=128   9.285 ms

Sent   Received   Lost    Loss
33     25         5       16.67%
Min    Avg        Max     Stddev
5.376  9.609      12.461  1.534
```

Source: Miercom

Additional wireless clients were unable to associate to the TN-SSID, and the ArubaOS-Switch reported the controller as unreachable via the [show tunneled-node-server state] output.

This test proved Aruba's Dynamic Segmentation incurs a severe impact to the client performance. The Aruba Mobility controller was a critical chokepoint and ultimately a bottleneck due to its limited data plane, and once overloaded, became non-operational.



```
Tunneled Node Port State

Active Controller IP Address  :

Port   State
------ -------------------------
1      Port down
2      Port down
3      Port down
4      Port down
5      Port down
6      Port down
7      Controller not reachable
8      Port down
9      Port down
10     Port down
49     Controller not reachable
```

Source: Miercom

To remediate the issue, additional uplinks were added, however the performance did not improve, and clients were still unable to associate to the Mobility controller.

Dynamic Segmentation consumes and wastes bandwidth across the backbone network, resulting in overprovisioning of uplinks. The wireless controller becomes a bottleneck due to its limited data plane, and once overloaded, it becomes non-operational.

To prevent this from occurring, the Aruba solution would require a customer to purchase and deploy additional Aruba Mobility controllers to support unified policy for wired and wireless clients.

Aruba's implementation for segmentation is tied to an IP address. Traditional ACLs and VLANs are still required for configuration. For converged wired and wireless, Dynamic Segmentation is the only offering from Aruba. Dynamic Segmentation exhibits the following limitations:

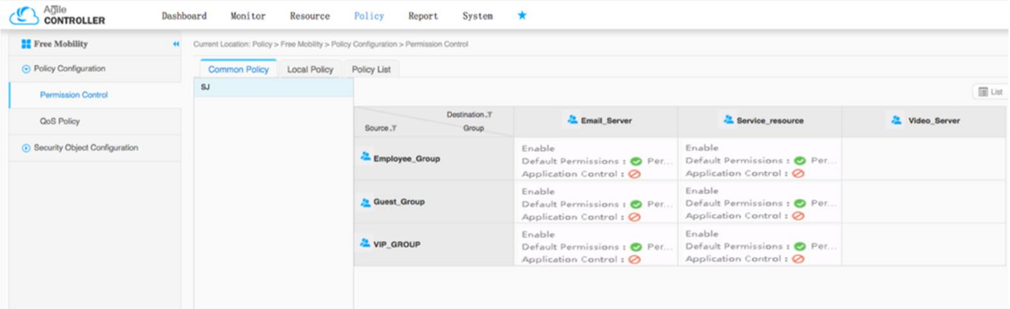
- Performance bottleneck
- Higher number of Aruba Mobiity controller appliances required for wired and wireless, along with additional device licenses
- Requires high-capacity uplinks to carry wired traffic to the Aruba Mobility controller

Huawei

The Agile Controller functions as the authentication server and uses RADIUS interfaces to authenticate users by interacting with Huawei devices. It also functions as the policy server and delivers Free Mobility policies to the switches and firewalls through XMPP interfaces.

Huawei uses the Free Mobility function to provide and obtain group-based policies regardless of user location and IP address but requires multiple touchpoints for all campus network layers. Huawei's Group-based policy was complex to enable. It took Miercom twelve steps to configure a single Security Group and sixteen steps to configure a single policy.

The figure below depicts the matrix when configuring a Free-Mobility policy.



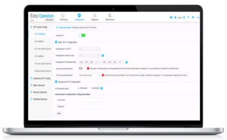
Current Location: Policy > Free Mobility > Policy Configuration > Permission Control

Destination.T Group / Source.T	Email_Server	Service_resource	Video_Server
Employee_Group	Enable Default Permissions : ✓ Per... Application Control : ⊘	Enable Default Permissions : ✓ Per... Application Control : ⊘	
Guest_Group	Enable Default Permissions : ✓ Per... Application Control : ⊘	Enable Default Permissions : ✓ Per... Application Control : ⊘	
VIP_GROUP	Enable Default Permissions : ✓ Per... Application Control : ⊘	Enable Default Permissions : ✓ Per... Application Control : ⊘	

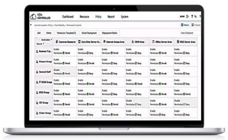
Source: Miercom

Huawei Dashboards required for Network Segmentation:

CLI



EasyOperation



Agile Controller

Source: Huawei

Huawei offers group-based policies by maintaining a database of users and their current IP addresses, coupled with location. Policies configured on the Agile controller are implemented using traditional means of configuration through VLANs and ACLs. This adds complexity when configuring segmentation on the network.

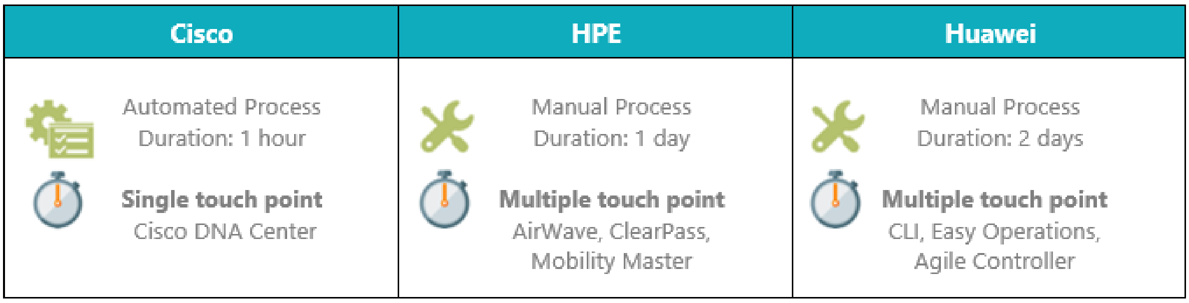
Huawei's policy enforcement using Free Mobility is only supported on their high-end Ethernet Networking Processor-based (ENP-based) switches.

If there is a customer requirement for user-to-user access control, Layer 2 isolation must be deployed on Huawei's access switches to divert all traffic to authentication point switches. User isolation for wireless services needs to be configured in the Virtual AP profile. These are manual configuration steps performed by the network administrator.

Cisco SDA	HPE	Huawei
Ensure ISE and DNA Center are communicating over pxGrid. • Assign Scalable Groups (SGTs) to Virtual Networks (VNs) • Define access policies between SGTs based on either source, destination or application	• Switch (12 steps) • Configure RADIUS-SERVER (ClearPass) to download CA certificate • Configure RADIUS "Dynamic Authorization" • Configure Crypto Certificate Authority from ClearPass • Configure Tunneled-Node Controller IP address • Configure Tunnel Mode Role-based/User Based Tunneling and reserve VLAN for Control-Plane communication to Mobility Controller • Configure AAA Authorization for Downloadable User Roles • Configure 802.1X on the Access Switch port, Client limit • Enable 802.1X Globally ...and many more • ClearPass (12 steps) • Create Profile for Downloadable Role Enforcement • Select Product to ArubaOS Switch • Create VLAN ID • Add ACL (optional) • Create Policy to assign Profile to and Enforcement Type • Create Rule via Rule Editor • Assign Profile to Policy • Configure service (802.1X Wired) ...and many more • Mobility Master (7 steps) • Configure VLAN Name/ID • Assign IP address (Static • Configured NAT inside (NAT VLAN to MC Network) • Configure the Secondary Role (configured on CPMM & pushed to the switch) • Assign policy (new or predefined) to the role • Configure Role User-VLAN (terminating) ...and many more	Manually configured on each Access and Aggregation Layer Switch: • Configure L2 VLAN (Global, Interface), L2 Protocol Transparent Transmission Core Layer • Configure IP Address for VLAN and IP Pool of Gateway • Configure DHCP/DNS, RADIUS Server, Authentication Templates, Domain, accounting scheme, authentication profiles for 802.1 + MAC-Auth • Configure XMPP and connection to Agile Controller for Group-Based Policy • Configure Wired 802.1x, MAC-Auth, Web-Auth and Wireless Portal Authentication • Configure CAPWAP Source interface, WLAN Controller/AP Agile Controller Server • Configure authentication Device (Switch), MAC Account of AP, account for 802.1x and Portal Authentication • Configure authentication and authorization process • Configure Security Groups (Static) and Security Groups (Dynamic) • Configure policy of Free Mobility

Network Segmentation Summary

- HPE-Aruba and Huawei did not pass all test cases. Aruba does not offer a unified method of virtualization services for wired and wireless beyond VLANs. Both HPE-Aruba and Huawei required multiple dashboards and manual operations during each of the test cases.
- Cisco DNA Center is a system for centralized deployment and policy management of devices within a campus network. It reduces security operations while increasing the organization's security footprint.
- With Cisco, policy enforcement was immediately applied at the edge switch where unknown devices connect. Both HPE-Aruba and Huawei push the policy enforcement up the stack, such as the wireless controller (HPE-Aruba) or the SVF parent (Huawei). The policy enforcement point for Cisco is distributed, hence scalable, while HPE-Aruba and Huawei are centralized.



Cisco	HPE	Huawei
Automated Process Duration: 1 hour	Manual Process Duration: 1 day	Manual Process Duration: 2 days
Single touch point Cisco DNA Center	**Multiple touch point** AirWave, ClearPass, Mobility Master	**Multiple touch point** CLI, Easy Operations, Agile Controller

Network Assurance

5

Cisco offers wired and wireless Network Assurance as a part Cisco DNA Center. Aruba, on the other hand, has four separate solutions that offer network assurance. For this analysis, we decided to focus on on-premises solutions only. Aruba NetInsight is a cloud-based solution that provides network assurance such as baselines, root causes and suggestions. Aruba User Experience Insight offers network assurance through their hardware sensors. The Network Analytics Engine provides the network health for the ArubaOS-CX switches. Aruba Connectivity Health comes with Aruba Airwave as an optional module and is free of cost. Since Connectivity Health is Aruba's most popular network assurance solution and readily available, we decided to test it. Huawei recently launched their network assurance solution called CampusInsight 2.0. Huawei eSight also offers basic network and client statistics for network troubleshooting. We decided to test Huawei eSight since CampusInsight 2.0 was not available during the period of testing.

To determine how well each architecture isolates, analyzes and resolves network issues, we applied test cases which reveal what insight, if any, is offered by each vendor's software for reporting wired and wireless client experience.

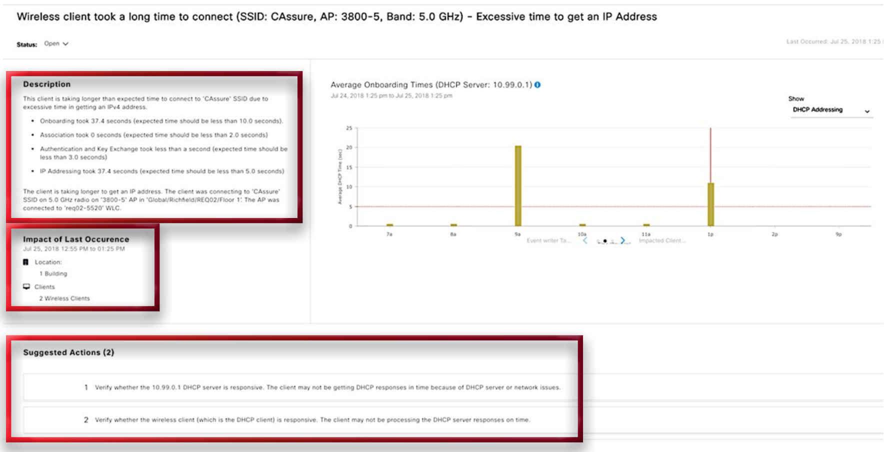
We created an assortment of failure scenarios to assess the individual vendor's software's ability to respond effectively. These included: DHCP server exhausts its IP-address pool exhaustion; Radio Frequency (RF) issues; proactive tests; and troubleshooting with Path Trace.

DHCP Issues

We created conditions so that the wireless clients connecting to the AP could not get the IP address due to an exhausted DHCP IP addresses pool. The client, IP address issue, was confirmed by checking the client's association on the wireless controller showing that the client was connected to the wireless network although could not acquire an IP address through DHCP. Then the IP address pool was restored on the DHCP server and the clients received an IP address from the server.

Cisco

The Cisco DNA Center information gives a description of the problem, details what parts of the network are impacted and provides additional information and possible solutions to the problem. It also shows in the graph the excessive onboarding times of the clients.



Wireless client took a long time to connect (SSID: CAssure, AP: 3800-5, Band: 5.0 GHz) - Excessive time to get an IP Address

Status: Open

Last Occurred: Jul 25, 2018 1:25

Description

This client is taking longer than expected time to connect to 'CAssure' SSID due to excessive time in getting an IPv4 address.

- Onboarding took 37.4 seconds (expected time should be less than 10.0 seconds).
- Association took 0 seconds (expected time should be less than 2.0 seconds)
- Authentication and Key Exchange took less than a second (expected time should be less than 3.0 seconds)
- IP Addressing took 37.4 seconds (expected time should be less than 5.0 seconds)

The client is taking longer to get an IP address. The client was connecting to 'CAssure' SSID on 5.0 GHz radio on '3800-5' AP in 'Global/Richfield/REQ02/Floor 1'. The AP was connected to 'req02-5520' WLC.

Impact of Last Occurence

Jul 25, 2018 12:55 PM to 01:25 PM

Location:
1 Building

Clients
2 Wireless Clients

Average Onboarding Times (DHCP Server: 10.99.0.1)

Jul 24, 2018 1:25 pm to Jul 25, 2018 1:25 pm

Show: DHCP Addressing

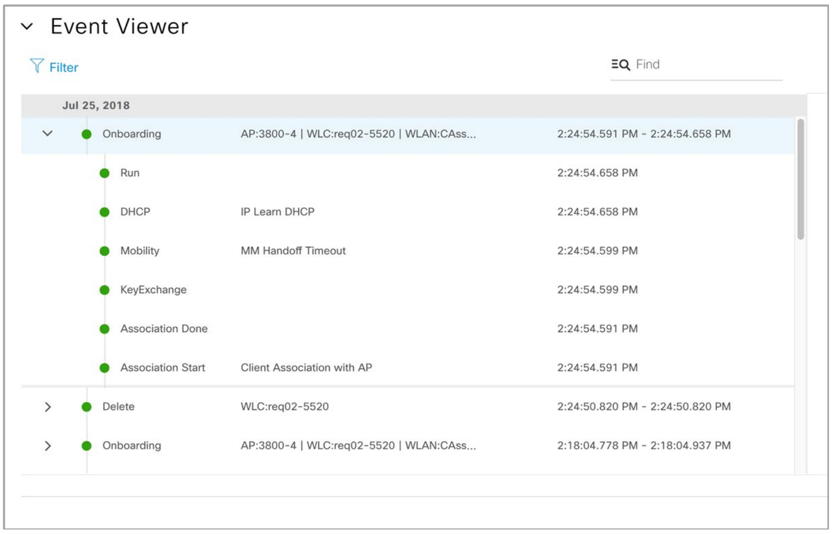
Suggested Actions (2)

1 Verify whether the 10.99.0.1 DHCP server is responsive. The client may not be getting DHCP responses in time because of DHCP server or network issues.

2 Verify whether the wireless client (which is the DHCP client) is responsive. The client may not be processing the DHCP server responses on time.

Source: Miercom

The Cisco DNA Center event viewer shows the chronology of the successful client onboarding process.



Event Viewer

Filter | Find

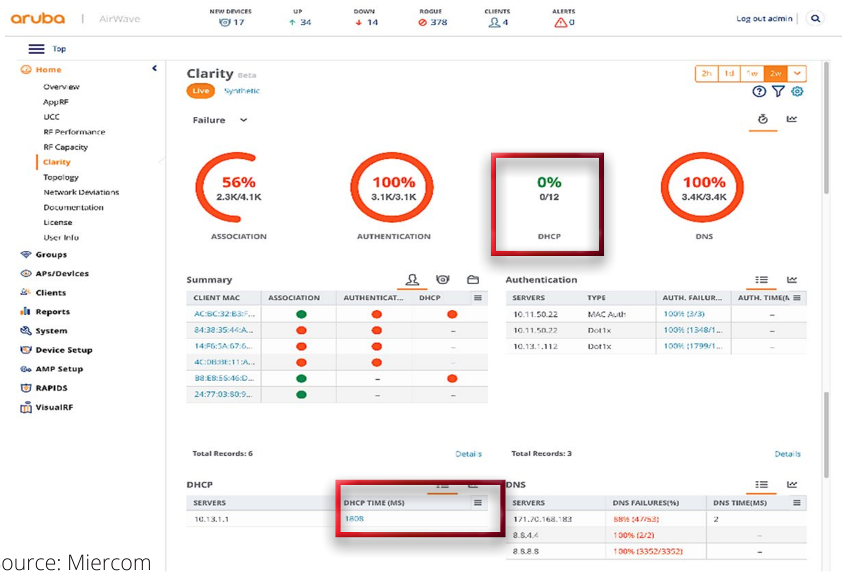
Jul 25, 2018

Event	Details	Time
Onboarding	AP:3800-4 | WLC:req02-5520 | WLAN:CAss...	2:24:54.591 PM - 2:24:54.658 PM
Run		2:24:54.658 PM
DHCP	IP Learn DHCP	2:24:54.658 PM
Mobility	MM Handoff Timeout	2:24:54.599 PM
KeyExchange		2:24:54.599 PM
Association Done		2:24:54.591 PM
Association Start	Client Association with AP	2:24:54.591 PM
Delete	WLC:req02-5520	2:24:50.820 PM - 2:24:50.820 PM
Onboarding	AP:3800-4 | WLC:req02-5520 | WLAN:CAss...	2:18:04.778 PM - 2:18:04.937 PM

Source: Miercom

HPE-Aruba

The Aruba AirWave Connectivity Health dashboard shows the failure percentage of basic network metrics such as association, authentication, DHCP and DNS. It also shows the average time for a client to get an IP address from the DHCP server. A threshold of each metric can be set to show pass/fail. The dashboard depicts the network summary from the client and access point perspective.



Summary

CLIENT MAC	ASSOCIATION	AUTHENTICAT...	DHCP
AC:BC:32:B3:F...	🟢	🔴	🔴
84:38:35:44:A...	🔴	🔴	–
14:F6:5A:67:6...	🔴	🔴	–
4C:0B:BE:11:A...	🔴	🔴	–
B8:E8:56:46:D...	🟢	–	🔴
24:77:03:80:9...	🟢	–	–

Total Records: 6 Details

Authentication

SERVERS	TYPE	AUTH. FAILUR...	AUTH. TIME(N
10.11.50.22	MAC Auth	100% (3/3)	–
10.11.50.22	Dot1x	100% (1348/1...	–
10.13.1.112	Dot1x	100% (1799/1...	–

Total Records: 3 Details

DHCP

SERVERS	DHCP TIME (MS)
10.13.1.1	1808

DNS

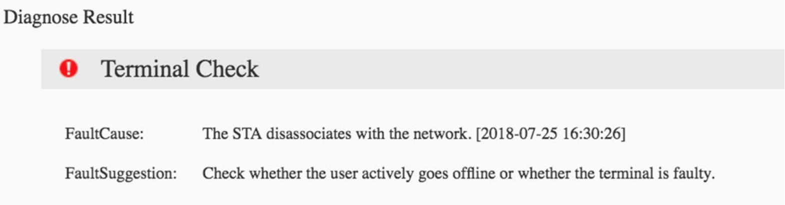
SERVERS	DNS FAILURES(%)	DNS TIME(MS)
171.70.168.183	88% (47/53)	2
8.8.4.4	100% (2/2)	–
8.8.8.8	100% (3352/3352)	–

Source: Miercom

The client details window does show some added information such as timeline of the duration for the client to get an IP address once DHCP is restored to full operation. However, it lacks information on the impacted location, the number of clients affected, and guided remediations.

Huawei

The Huawei eSight doesn't provide any dashboard to show network assurance statistics such as association, authentication DHCP, DNS failure rate or average time. However, the Huawei eSight WLAN Fault Diagnosis screen, in the Terminal Check section, can be used to make fault diagnosis on the client to see the cause of the fault and the suggestion to fix it. It does not go any deeper into the cause of this disassociation.



Diagnose Result

Terminal Check

FaultCause: The STA disassociates with the network. [2018-07-25 16:30:26]

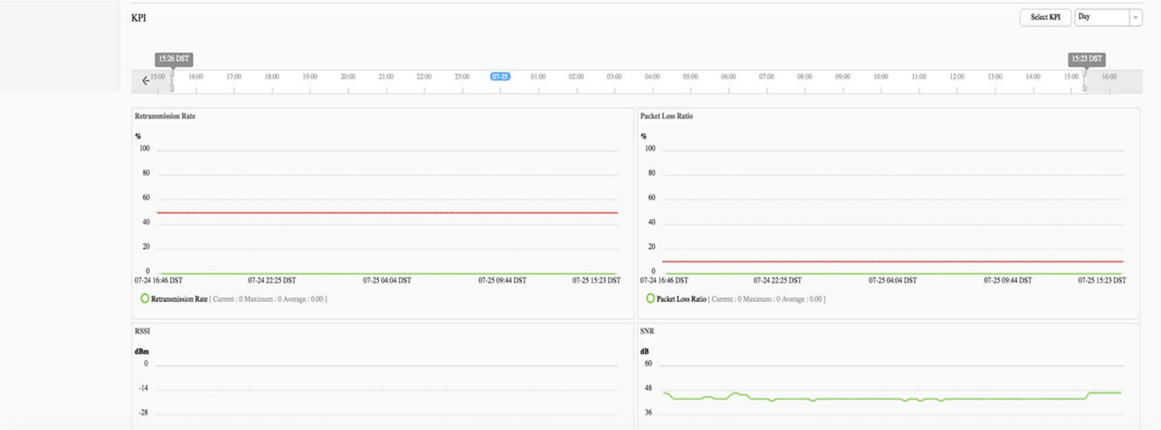
FaultSuggestion: Check whether the user actively goes offline or whether the terminal is faulty.

Source: Miercom

Huawei eSight does offer several additional windows of information, but these collectively provide little additional information that helps in troubleshooting. One such window is the "Client Detail". Client Detail provides additional detail including:

- Topology of the last path accessed from the client, through to the AP controller
- Basic client information such as naming and addressing, various access times and performance information
- Retransmission rate and packet loss information

The screenshot below shows the client traffic information portion of the client page.



Retransmission Rate [Current : 0 Maximum : 0 Average : 0.00]

Packet Loss Ratio [Current : 0 Maximum : 0 Average : 0.00]

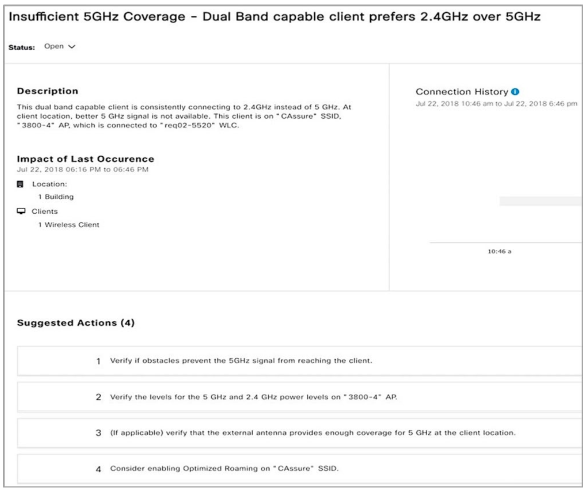
Source: Miercom

RF (Radio Frequency) Issues

In this test case, we created a scenario where a client is forced to join the 2.4-GHz radio instead of 5-GHz radio in a dual-band WLAN. We artificially reduced the transmit power on the 5-GHz radio of the AP and then positioned the client away from the AP. This is a typical scenario in a wireless network where a client joins 2.4-GHz band due to the lack of a 5-GHz signal and suffers from performance issues.

Cisco

As shown below, Cisco DNA Center identifies the cause of the client running on the 2.4-GHz radio rather than the greater bandwidth of 5-GHz. Cisco DNA Center describes the problem in detail, including identifying the AP that is providing the poorer connection. In addition, Cisco DNA Center offers four suggestions for resolving and remedying the situation.



Insufficient 5GHz Coverage – Dual Band capable client prefers 2.4GHz over 5GHz

Status: Open

Description

This dual band capable client is consistently connecting to 2.4GHz instead of 5 GHz. At client location, better 5 GHz signal is not available. This client is on "CAssure" SSID, "3800-4" AP, which is connected to "req02-5520" WLC.

Impact of Last Occurence
Jul 22, 2018 06:16 PM to 06:46 PM

Location:
1 Building

Clients
1 Wireless Client

Connection History
Jul 22, 2018 10:46 am to Jul 22, 2018 6:46 pm

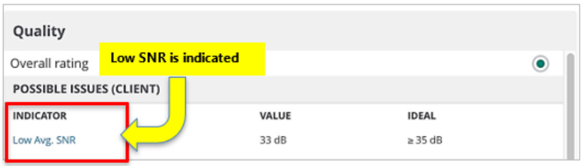
Suggested Actions (4)

1. Verify if obstacles prevent the 5GHz signal from reaching the client.
2. Verify the levels for the 5 GHz and 2.4 GHz power levels on "3800-4" AP.
3. (If applicable) verify that the external antenna provides enough coverage for 5 GHz at the client location.
4. Consider enabling Optimized Roaming on "CAssure" SSID.

Source: Miercom

HPE-Aruba

The HPE-Aruba package notices that the Signal to Noise Ratio (SNR) is low and presents an alert that identifies the low average SNR. This is accompanied by a graph that separately plots the signal to noise levels.



Quality

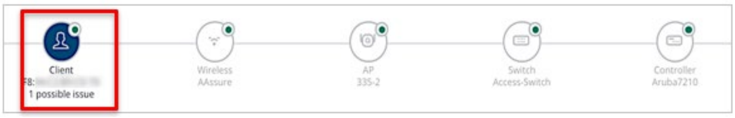
Overall rating

POSSIBLE ISSUES (CLIENT)

INDICATOR	VALUE	IDEAL
Low Avg. SNR	33 dB	≥ 35 dB

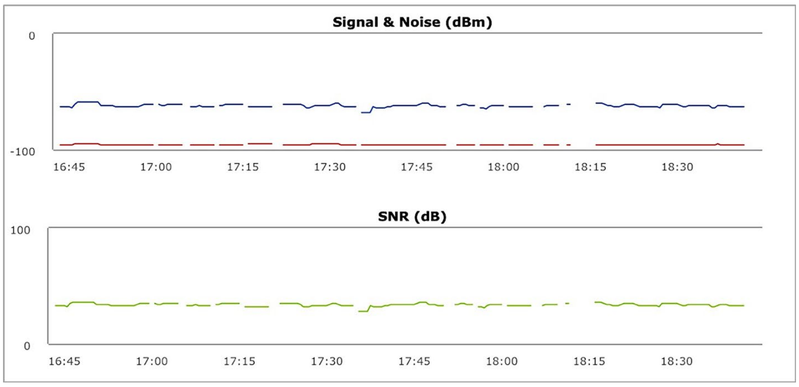
Source: Miercom

While HPE-Aruba provides client alerts based on average SNR, there are no suggested actions and the extent of the impact is not indicated.



Source: Miercom

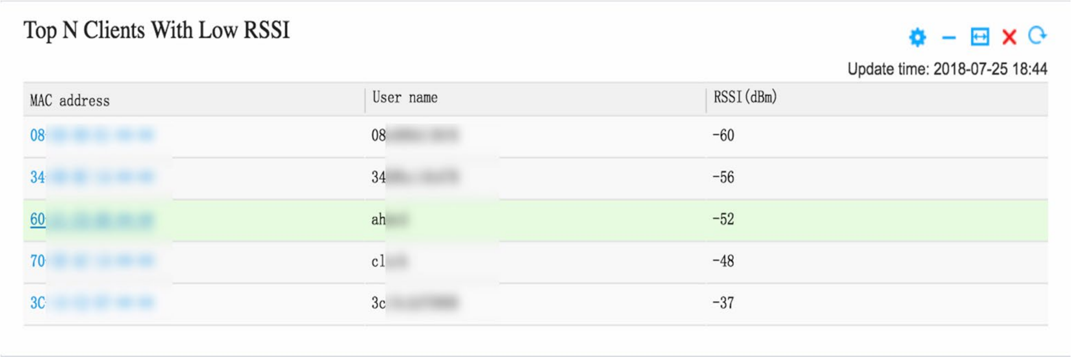
The HPE-Aruba configuration of the SNR threshold, as well as authorization errors and overall station health, for alerts, is straightforward.



Source: Miercom

Huawei

Huawei doesn't have a view that identifies this RF issue (a client and an AP underperforming at 2.4-GHz). But the Huawei package can single out clients with low RSSI (Received Signal Strength Indication) – which could then be researched, using other tools, to eventually find the AP with a bad 5-GHz radio. The Huawei "Low-RSSI" screen is shown below.



Top N Clients With Low RSSI

Update time: 2018-07-25 18:44

MAC address	User name	RSSI(dBm)
08[redacted]	08[redacted]	-60
34[redacted]	34[redacted]	-56
60[redacted]	ah[redacted]	-52
70[redacted]	cl[redacted]	-48
3C[redacted]	3c[redacted]	-37

Source: Miercom

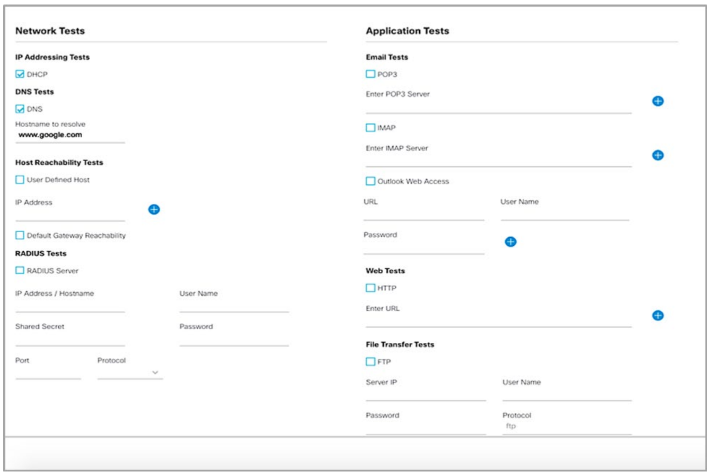
Proactive Testing

A sensor is a network device, such as an AP, which conducts synthetic tests, driven by configurable parameters, rather than based on actual traffic.

Cisco

Cisco has over fifteen available proactive tests, accessible under the Cisco DNA Center "Assurance" tab and under "Manage," via the "Sensor Driven Tests" window. This allows network administrators to select from the various test types to be run manually or automatically on a selected schedule.

Test results are compiled over time to yield a historical view of network stability. The Test Summary window tracks the failure percentage and which tests failed.



Network Tests

IP Addressing Tests

☑ DHCP

DNS Tests

☑ DNS

Hostname to resolve: www.google.com

Host Reachability Tests

□ User Defined Host

IP Address

□ Default Gateway Reachability

RADIUS Tests

□ RADIUS Server

IP Address / Hostname

User Name

Shared Secret

Password

Port

Protocol

Application Tests

Email Tests

□ POP3

Enter POP3 Server

□ IMAP

Enter IMAP Server

□ Outlook Web Access

URL

User Name

Password

Web Tests

□ HTTP

Enter URL

File Transfer Tests

□ FTP

Server IP

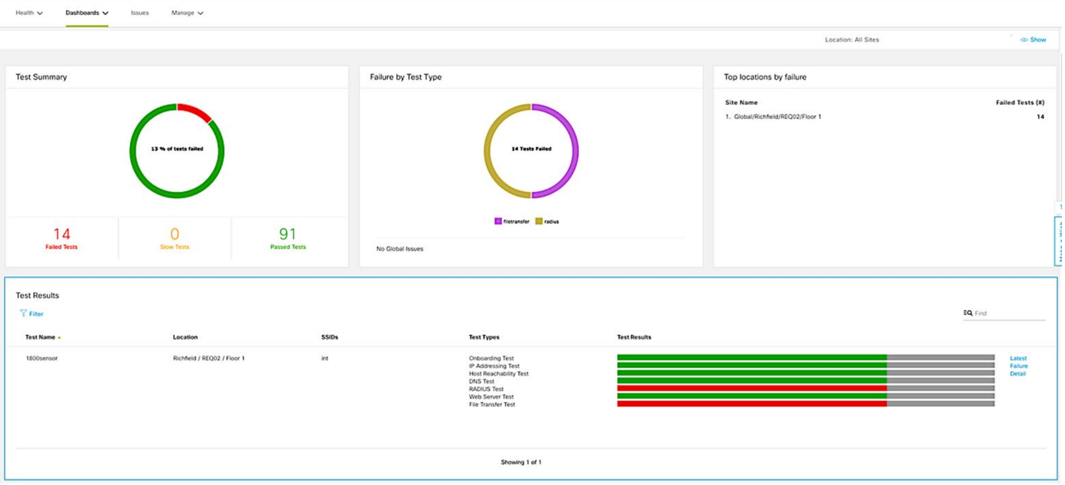
User Name

Password

Protocol: ftp

Source: Miercom

In this case, seven tests were run and two failed as shown by two red lines. This summary is also capable of recording sets of tests run together repeatedly over time.



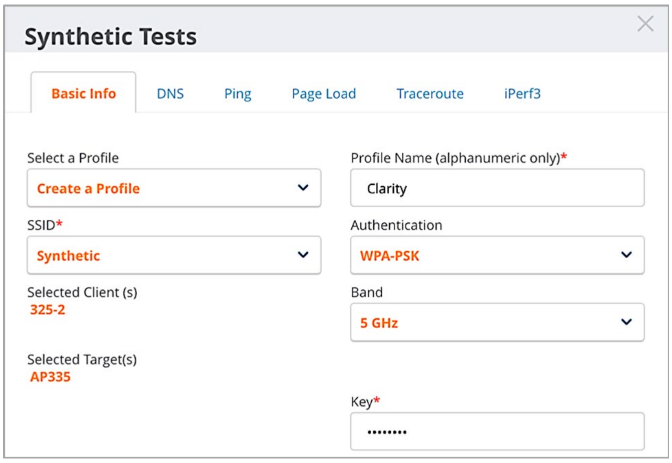
Site Name	Failed Tests (#)
1. Global/Richfield/REQ02/Floor 1	14

Test Name	Location	SSIDs	Test Types
1800sensor	Richfield / REQ02 / Floor 1	int	Onboarding Test IP Addressing Test Host Reachability Test DNS Test RADIUS Test Web Server Test File Transfer Test

Source: Miercom

HPE-Aruba

HPE-Aruba Connectivity Health only offers a battery of seven sensor, or synthetic tests – executable tests of various network functions. This window is offered to configure the synthetic tests.



Select a Profile: Create a Profile

Profile Name (alphanumeric only)*: Clarity

SSID*: Synthetic

Authentication: WPA-PSK

Selected Client (s): 325-2

Band: 5 GHz

Selected Target(s): AP335

Key*: ••••••••

Source: Miercom

Huawei

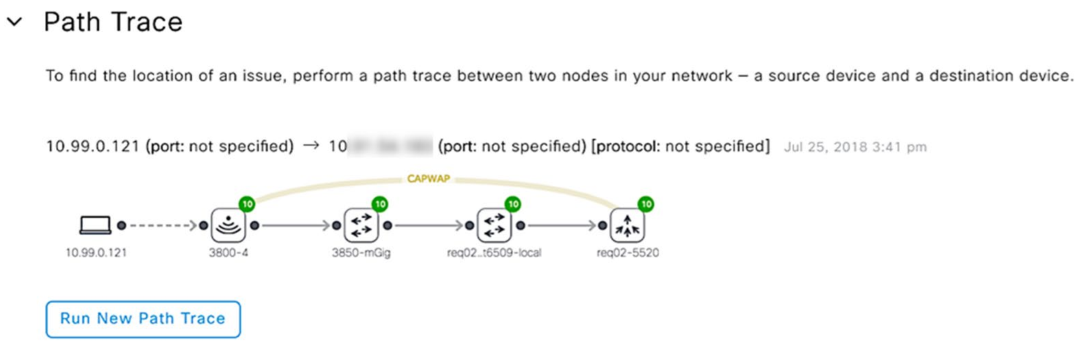
Huawei has no proactively run set of tests.

Troubleshooting via Path Trace

Path Trace is a software diagnostic tool similar to traceroute, a standardized process that has long been used for uncovering network problems. Traceroute has traditionally been launched via CLI. Path Trace, and traceroute, perform a connectivity test between specified network nodes and show all intermediate nodes along the path in the result.

Cisco

Cisco's Path Trace tool shows the topology between any two nodes in the network, wired and wireless. It doesn't generate packet like traceroute/ping. Instead, it depends on device inventory database and models to trace the actual path. The resulting display shows each node along the physical path, as well as the logical network path such as a CAPWAP (Control and Provisioning of Wireless Access Points) tunnel between two nodes, and the connection across a wireless AP.



Path Trace

To find the location of an issue, perform a path trace between two nodes in your network – a source device and a destination device.

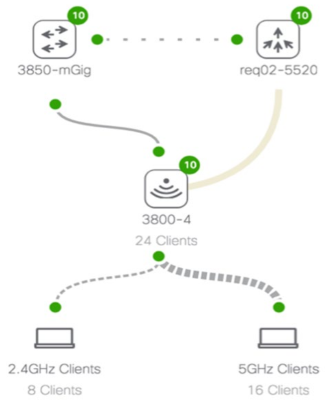
10.99.0.121 (port: not specified) → 10[redacted] (port: not specified) [protocol: not specified] Jul 25, 2018 3:41 pm

Source: Miercom

The Cisco Path Trace utility allows for full visibility of the wired network, logically as well as physically. We found the Cisco topology view, as part of its Path Trace, to show comprehensive detail which proved useful in pinpointing network issues such as bottlenecks and delays.

Path trace also shows health of each device and ACLs applied on the switch.

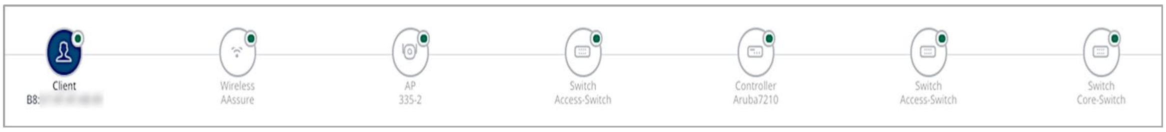
The Cisco DNA Center also shows the network view from the device perspective. The physical neighbor topology in the Device 360 window displays the neighbors connected to the devices. The screenshot, shown right, shows the physical and logical connection of the AP, switch, controller, and the clients connected on both radios.



Source: Miercom

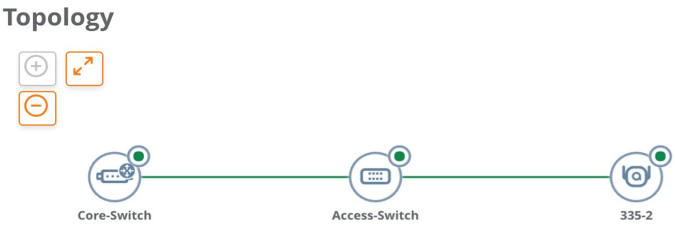
HPE-Aruba

HPE-Aruba doesn't offer an option to run a patch trace. However, it gives a view of the physical connection but not the logical connection in the client detail window. The HPE display is basic but nevertheless informative and useful.



Source: Miercom

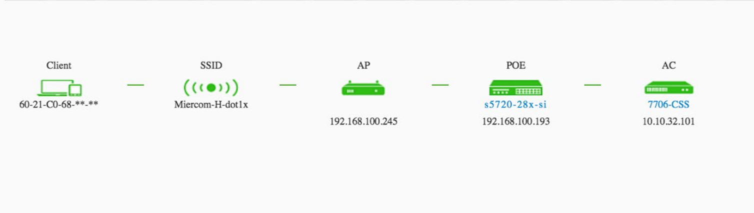
The Aruba Airwave topology window shows the topology of the network devices. It also shows the health of the network devices but doesn't give information on the clients connected the devices. The screenshot below shows the topology view of Aruba Airwave.



Source: Miercom

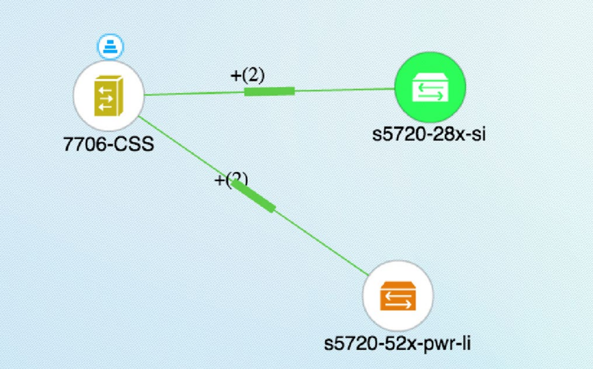
Huawei

Huawei has the path trace capability, but it only shows the physical connection layout. It also displays the IP addresses of the nodes in the physical connection.



Source: Miercom

The Huawei topology tab shows the physical connection of the network devices with CPU usage and memory usage.



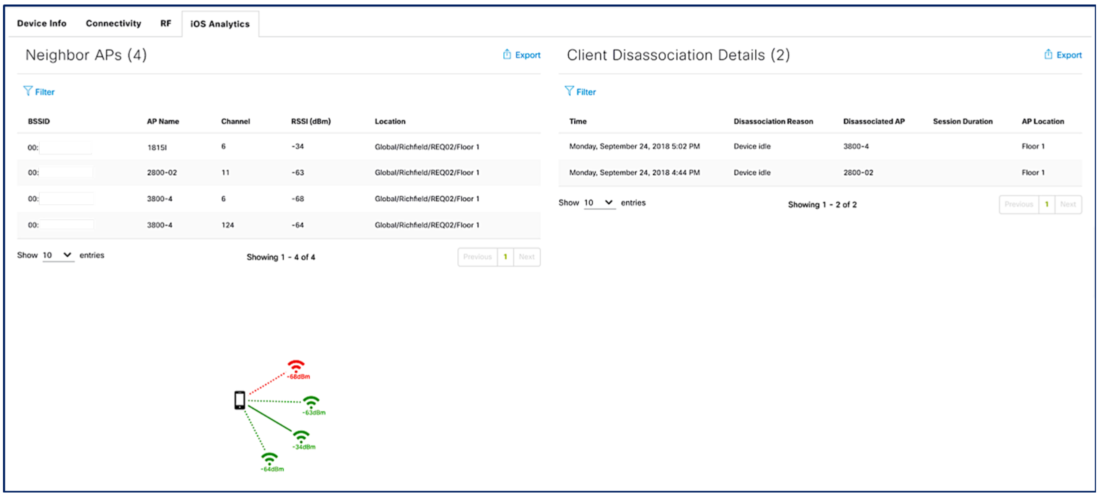
Source: Miercom

Cisco DNA Center Assurance - Additional Features

There are other Cisco DNA Center Assurance features that were not part of the testing because the equivalent features from the competitor solutions were missing. Nevertheless, we summarize these features for the remainder of this section since they play a prominent role in assisting network administrators to proactively monitor and troubleshoot the network.

iOS Wi-Fi Analytics

The Cisco and Apple partnership brings iOS Wi-Fi Analytics feature to Cisco DNA Center Assurance. The feature allows Apple clients to report the client view of the network that includes the list of the APs it can see along with the signal value and channel. It also shows the reasons for the client disconnection to make troubleshooting easier for the network administrator. For example, if a client got disconnected from the network due to its software-related reason, the network administrator can deduce that it is not a network-related problem but a client-related problem. The Cisco DNA Center gathers the client-related information and displays in the client 360 view shown in the figure below.



Neighbor APs (4)

BSSID	AP Name	Channel	RSSI (dBm)	Location
00:	1815I	6	-34	Global/Richfield/REQ02/Floor 1
00:	2800-02	11	-63	Global/Richfield/REQ02/Floor 1
00:	3800-4	6	-68	Global/Richfield/REQ02/Floor 1
00:	3800-4	124	-64	Global/Richfield/REQ02/Floor 1

Show 10 entries

Showing 1 - 4 of 4

Client Disassociation Details (2)

Time	Disassociation Reason	Disassociated AP	Session Duration	AP Location
Monday, September 24, 2018 5:02 PM	Device idle	3800-4		Floor 1
Monday, September 24, 2018 4:44 PM	Device idle	2800-02		Floor 1

Show 10 entries

Showing 1 - 2 of 2

Source: Miercom

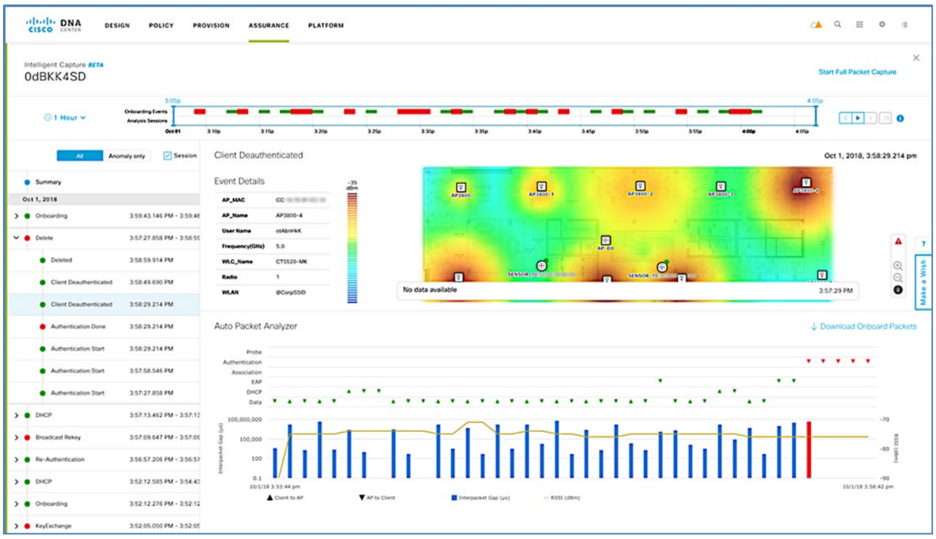
Application Experience

The Cisco DNA Center Application Experience feature allows the network administrator to monitor the health of the applications running on the client devices. A health score is given to the applications based on packet loss and latency metrics. Furthermore, it also segregates the application from business relevant with business irrelevant so that a network administrator can focus on the critical application for diagnosing. The application health can be monitored globally from the main dashboard or per-client basis in the Client 360 view window.

Intelligent Capture

The Intelligent Capture in Cisco DNA Center Assurance provides the network administrator an easier way to diagnose the network and client issues. Packet Captures has been an integral part of network troubleshooting. However, it requires a manual process of visiting the location of impact, recreating the problem and capturing packets. The Intelligent Capture capability in Cisco APs in conjunction with Cisco DNA Center Assurance automates the process without the need of an on-site technician. The packet capture can be scheduled, triggered by error events, or started on-demand.

Moreover, if a client is roaming between the APs, the capture can be run on multiple APs to generate a consolidate decrypted packet capture that can be analyzed and viewed in the Cisco DNA Center Assurance. Intelligent Capture monitors 240+ onboarding anomalies and can automatically remediate specific issues. The Cisco DNA Center also integrates with Cisco CMX engine to provide real-time client location in a building. The below screenshot shows the Intelligent Capture window of a client with the network time travel, event viewer, client details, Auto Packet Analyzer and a floor map with sensors and access points.



Intelligent Capture BETA

0dBKK4SD

● Summary

Oct 1, 2018

> ● Onboarding	3:59:43.146 PM - 3:59:48
⌄ ● Delete	3:57:27.858 PM - 3:58:59
● Deleted	3:58:59.914 PM
● Client Deauthenticated	3:58:49.690 PM
● Client Deauthenticated	3:58:29.214 PM
● Authentication Done	3:58:29.214 PM
● Authentication Start	3:58:29.214 PM
● Authentication Start	3:57:58.546 PM
● Authentication Start	3:57:27.858 PM
> ● DHCP	3:57:13.462 PM - 3:57:13
> ● Broadcast Rekey	3:57:09.647 PM - 3:57:09
> ● Re-Authentication	3:56:57.206 PM - 3:56:57
> ● DHCP	3:52:12.585 PM - 3:54:43
> ● Onboarding	3:52:12.276 PM - 3:52:12
> ● KeyExchange	3:52:05.050 PM - 3:52:05

Client Deauthenticated

Oct 1, 2018, 3:58:29.214 pm

Event Details

AP_MAC	CC:[redacted]
AP_Name	AP3800-4
User Name	otAbnHkK
Frequency(GHz)	5.0
WLC_Name	CT5520-MK
Radio	1
WLAN	@CorpSSID

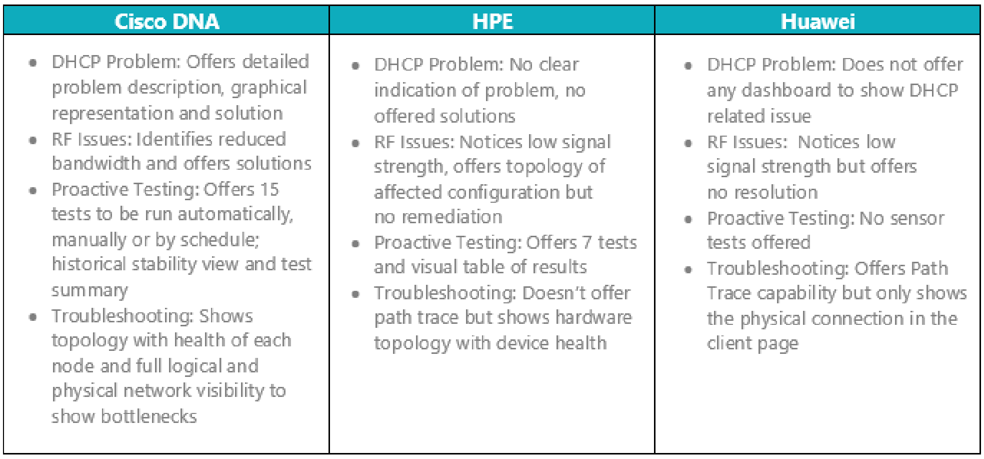
No data available 3:57:29 PM

Auto Packet Analyzer

Source: Miercom

Network Assurance Summary

- Aruba Connectivity Health offers some fundamental assurance capabilities but lacks in providing a multitude of client-based analytics including iOS analytics, wired and wireless client analytics, and patch trace. Huawei eSight also offers some client statistics and can also do a traceroute, but unlike Cisco DNA Assurance it only shows the physical topology with no useful metrics such as ACL, device health.
- Cisco DNA Center Assurance can continuously monitor the health of the network by running comprehensive synthetic tests. Aruba Connectivity Health has the same capability but only offers half of the synthetic test compared to Cisco. Huawei eSight only relies on health diagnostic of the client and doesn't offer any synthetic tests. Cisco DNA Center Intelligent Capture can detect the issues in real-time by providing automatic packet captures and displaying the captures on the Cisco DNA Center. Aruba and Huawei don't have any native packet capture capability.
- Aruba Connectivity Health displays the issues created in the DHCP and RF issue tests but doesn't provide any suggestion to mitigate the issue. Huawei eSight could only detect the client's RF issue, but like Aruba, there are no suggested actions. Cisco DNA Center offers a Client 360 view that shows the client issues over a timeline and provides guided remediations to resolve the issue.



Cisco DNA	HPE	Huawei
• DHCP Problem: Offers detailed problem description, graphical representation and solution • RF Issues: Identifies reduced bandwidth and offers solutions • Proactive Testing: Offers 15 tests to be run automatically, manually or by schedule; historical stability view and test summary • Troubleshooting: Shows topology with health of each node and full logical and physical network visibility to show bottlenecks	• DHCP Problem: No clear indication of problem, no offered solutions • RF Issues: Notices low signal strength, offers topology of affected configuration but no remediation • Proactive Testing: Offers 7 tests and visual table of results • Troubleshooting: Doesn't offer path trace but shows hardware topology with device health	• DHCP Problem: Does not offer any dashboard to show DHCP related issue • RF Issues: Notices low signal strength but offers no resolution • Proactive Testing: No sensor tests offered • Troubleshooting: Offers Path Trace capability but only shows the physical connection in the client page

Cisco automation offers comprehensive network automation capabilities, extending beyond basic day-zero configuration and helps the administrator convert business intent to an automated network configuration. This saves customers a huge amount of time, resources and money. HPE-Aruba and Huawei continue to use manual and rigid, template-based provisioning for wired and wireless networks.

Cisco SD-Access offers ease of policy creation and deployment with micro and macro segmentation using a simple drag-and-drop mechanism. HPE-Aruba and Huawei fail to offer multi-level segmentation and still rely on traditional ACL-based network segmentation – adding complexity and additional operational cost.

Cisco provides a unified assurance platform for wired, wireless and routing with predictive troubleshooting, faster remediation and unique features, like Intelligent Capture. HPE-Aruba and Huawei offer various assurance platforms for different places in the network.

Cisco DNA Center offers a single-pane-of-glass dashboard. HPE-Aruba and Huawei's lack of integration forces the network administrator to use multiple dashboards and tools for network deployment, management, monitoring and troubleshooting.

About Miercom Performance Verified

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

About Miercom

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

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

Use of This Report

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

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

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.