Cisco Catalyst 9100 Wi-Fi 6 Access Points & Cisco DNA Center Competitive Assessment

March 2021

DR201007G

Contents

1.0 Executive Summary

Cisco Systems Inc. engaged in performing and conducting competitive analysis and comparative testing of Cisco's Catalyst 9100 Series Wireless Access Points (APs) and Cisco DNA Center offerings. The vendors comparatively tested were: Cisco Systems (Cisco), HPE-Aruba (Aruba), CommScope-Ruckus (Ruckus), Arista and Juniper-Mist (Mist).

Miercom collaborated in creating the test cases in which key features are highlighted and the comparison between the vendor offerings would be assessed.

The test plan and comparative criteria is focused into three parts:

- **Wi-Fi 6 Performance -** How well the Wi-Fi 6 access point provides optimum performance and reliability to devices (legacy and Wi-Fi 6) in a high-density scenario while being power efficient?
- **Network Operations -** How easy is it to run the day-to-day operations, including adding new AP models, fixing bugs, upgrading wireless network infrastructure without impacting mission-critical networks and always maintaining the clients' connectivity?
- **Network Assurance -** Can the network show actionable insights from the network, automatically identify and determine root cause anomalies, and offer intuitive tools to troubleshoot the problems?

Criteria	Key Findings
Wi-Fi 6 Performance	
High-Density Mix Multi-Client	Cisco Access Points consistently performed the best among all the competitors in each access points category (8x8 AP, 4x4 AP, 2x2 AP).
High-Quality Video Streaming	Cisco Catalyst 9130AX can successfully stream a clear 2K video feed consistently to more clients than the competitor APs.
Efficient PoE Power Consumption	The Cisco access points had the least power consumption compared to all the other vendors in each category (8x8 AP, 4x4 AP, 2x2 AP).
Reliable Voice Application	The Wi-Fi 6 networks offer noticeable latency improvements over Wi-Fi 5 networks in a congested wireless network.
Network Operations	
AP Device Pack (APDP)	In Cisco and Mist, new access points model can be added to the wireless network without any downtime, whereas Aruba does not offer this.
AP Refresh	Cisco's AP Refresh saves cost and time by allowing older AP models to be easily replaced with newer ones with integrated Cisco DNA Center workflow which the other vendors do not offer.
ISSU (Rolling AP Upgrade)	Cisco Catalyst 9800 controller ISSU feature enables APs' software upgrade through automation that prevents the tedious process of acquiring downtime. Aruba also offers a similar feature but requires an

	added appliance to perform it. Arista, Mist, Ruckus upgrade APs result in network disruption.
Helpdesk Ticket Management	While all vendors provide some level of integration with the IT Service Management, only Cisco offers a complete bi-directional integration with ITSM platform to simplify ticket management processes.
Network Assurance	
Wi-Fi 6 Insights	Cisco offers a unique Wi-Fi 6 dashboard that provides valuable insights into existing Wi-Fi 6 network and helps the IT team to make informed decisions.
AI Analytics	Cisco DNA Center impressive AI/ML-based Analytics identifies the most important issues in the network and provide root cause for quick issue resolution.
Troubleshooting	Cisco DNA Center Intelligent Capture offers a comprehensive view for troubleshooting a network or client problem. Aruba and Mist also offer a similar tool to troubleshoot a problem but lacks a complete perspective of the network.
Device Ecosystem Partnerships	Cisco exclusive partnership with Apple and Samsung provide analytics right from the end-user device side to locate the exact cause of the issue saving on time and effort.

We proudly award the Cisco Catalyst 9100 Series Access Points, Cisco Catalyst 9800 Series Wireless Controller, and the Cisco DNA Center the **Miercom Performance Verified** certification.

Robert Smithers
CEO, Miercom

2.0 Introduction

2.1 About Wi-Fi 6

Wi-Fi 6 is based on the IEEE 802.11ax standard – the sixth generation of Wi-Fi. Its predecessor, 802.11ac, only operates in the 5-GHz range, but Wi-Fi 6 supports both 2.4 and 5-GHz bands. This expansion of available channels increases capacity and scalability for higher wireless performance.

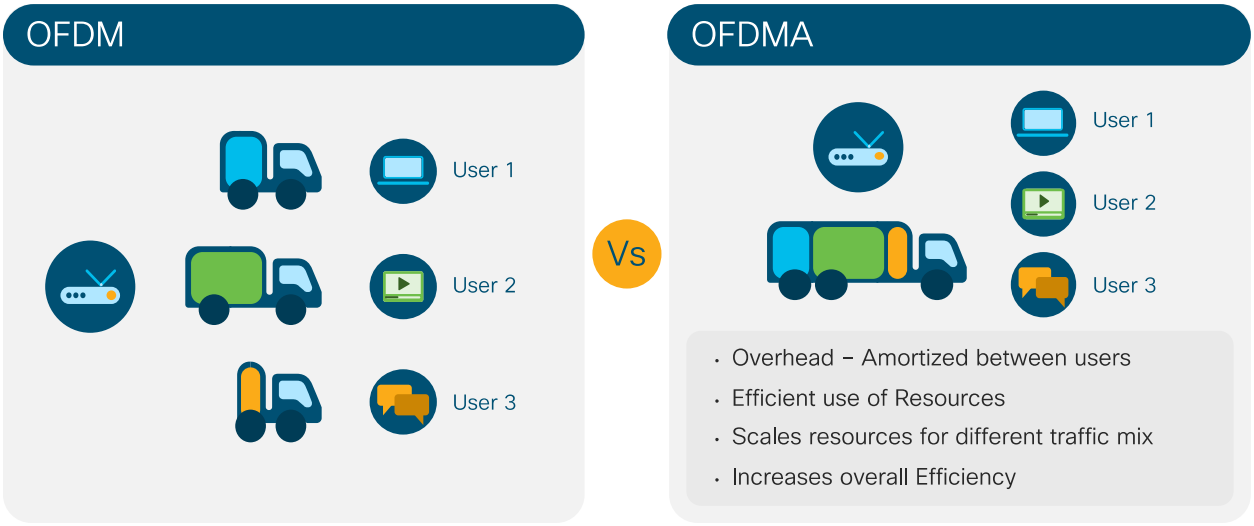
The 802.11ax standard allows an increase in modulation from 256 QAM to 1024 QAM, resulting in higher speeds for Wi-Fi 6 clients compared to Wi-Fi 5 clients.

MU-MIMO (or Multi-User, Multiple-Input, Multiple-Output) technology, increase network speed using simultaneous connections. While 802.11ac Wave 2 supports only downlink MU-MIMO, Wi-Fi 6 supports both uplink and downlink transmissions. More specifically, Wi-Fi 6 supports up to 8 MU-MIMO connections at a time.

Another benefit of Wi-Fi 6 is OFDMA (Orthogonal Frequency-Division Multiple Access), which segments each Wi-Fi channel into multiple Resource Units to simultaneously provide transmission to multiple clients. It significantly improves efficiency, latency, reliability and power.

High-density networks only stand to benefit from the speed, scalability and reliability brought by Wi-Fi 6. Changing network products and their connections from old to new standards is a daunting task that administrators strive to justify since it can incur downtime that lowers productivity.

Using the Enterprise wireless Access Points products in the industry, we aimed to determine the value of Wi-Fi 6 and what it means to modern networks – both on-site and remote.



2.2 Products Tested

We evaluated two aspects of the network-

1) Wi-Fi 6 APs Performance
2) Network Solution platforms

For the Performance section, we tested the following products:

					
5GHz: 8x8 (4x4+4x4) 2.4GHz: 4x4 Tri-Radio: (4x4+4x4+4x4)	Cisco 9130	Aruba AP555	N/A	N/A	N/A
5GHz: 8x8 2.4GHz: 4x4	Cisco 9117*	N/A	Ruckus R850 Ruckus R730*	N/A	Arista C-260** Arista C-250
5GHz: 4x4 2.4GHz: 4x4 Dual-5: (4x4+4x4)	Cisco 9120	N/A	N/A	Mist AP43	N/A
5GHz: 4x4 2.4GHz: 4x4	Cisco 9115	Aruba AP535	Ruckus R750	N/A	N/A
5GHz: 4x4 2.4GHz: 2x2	N/A	Aruba AP515	Ruckus R650	Mist AP33** Mist AP32**	Arista C-230**
5GHz: 2x2 2.4GHz: 2x2	Cisco 9105	Aruba AP505	Ruckus R550	N/A	N/A

N/A – No product with this capability

* Product not part of the performance test

**Product was not shipping at the time of the performance test

For the Solution section of this report, we evaluated capabilities such as Network Operations, Network Assurance and Business Continuity of the Cisco, HPE-Aruba (“Aruba”), and Juniper-Mist (“Mist”) Cloud solutions.

Management/Assurance/Orchestration Platforms

Cisco DNA Center is Cisco’s management and orchestration solution that offers a long-term commitment to deploying, managing, monitoring, and troubleshooting any network environment. Its Assurance module provides insightful tools like AI Analytics, Network 360, Client 360, Device 360, Intelligent Capture and more to give IT teams the context they need to identify and remediate issues. Cisco DNA Assurance automatically collects and organizes device, application, and user data overtime. It helps administrators to correlate and analyze the data to make smarter decisions before users’ services are impacted by the issues in the end-to-end wired and wireless network.

Aruba Central is cloud-based network management and analytics platform that provides deployment and management of wired, wireless and SD-WAN networks. The AI Insights module of Aruba Central offers insights into the network issues based on AI/ML for up to three months. Network administrator can drill into AI Insights dashboard to take actions to resolve network problems such as RF or network connectivity issues.

Mist Cloud is a microservices based cloud management and Assurance platform for Mist Access Points, Juniper SRX Routers and EX Switches. Mist Cloud has a unique feature called MARVIS used for Network Assurance and AI Anomaly Detection. It is a Virtual Network Assistant based on Natural Language Processing engine that helps network administrators find the network issues in their organization and root cause for faster resolution.

3.0 How We Did It

Using hands-on testing in a live business environment, we challenged each device with real-world scenarios to determine performance, automation, assurance and remote worker capabilities.

Performance Test Bed Overview

Source: Cisco

A view of the test setup is shown above. The AP under test was ceiling mounted and clients were spread around the AP from 10ft. (3m) to 45ft. (13.7m).

Test Tools

The following tools are a representative list of tools used to carry out analysis:

Ixia IxChariot

This network tool quantifies and compares wireless access point performance. This tool can support multiple platforms and test automation to simulate real-world applications for device and system performance under specific load conditions. IxChariot can produce and transfer traffic between wireless endpoints in set packet sizes for statistical reporting. The IxChariot endpoint application is installed on each mobile client, and tests are configured via the management console's WebUI to enable the client devices to receive and transmit traffic.

4.0 Performance

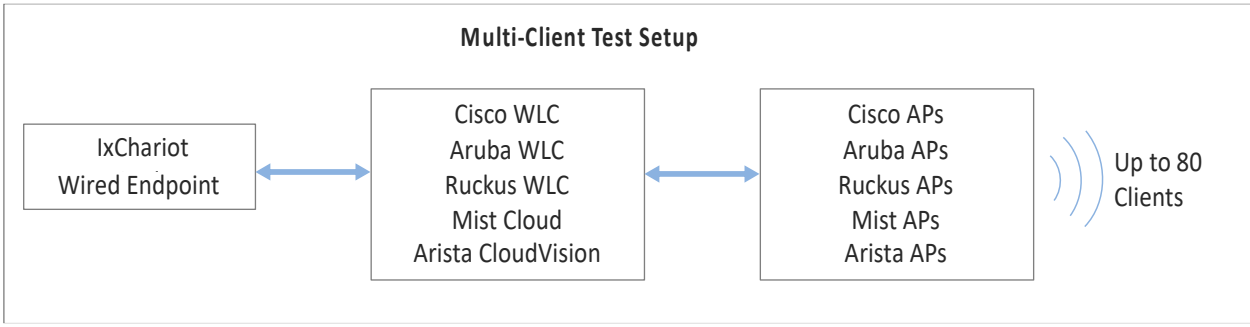
4.1 High Density Test: 80-client Mix 11ax/11ac

How We Did It

This test compared Wireless AP performance from the pool of 14 APs from different vendors with similar radio capabilities, with 802.11ax, OFDMA and MU-MIMO enabled. A real-world, representative mixture of 80 wireless client devices were connected to the AP under test, set to operate on Channel 36 in 80MHz and Channel 1 in 20MHz. 64 clients were connected to 5GHz (80 percent) and 16 clients were connected to 2.4GHz (20 percent). A total of 8 set of clients count were tested, from 10 clients to 80 clients. The table below shows the assortment of wireless client device types used for the test.

Client Device	Total Number	Wi-Fi Protocol	Spatial Streams
MacBook Pro	5	Wi-Fi 4 (802.11n)	3SS
Dell Laptops	20	Wi-Fi 5 (802.11ac)	2SS
MacBook Pro	15	Wi-Fi 5 (802.11ac)	3SS
MacBook Air	20	Wi-Fi 5 (802.11ac)	2SS
Dell Laptops	40	Wi-Fi 6 (802.11ax)	2SS

The Ixia IxChariot test system was configured to deliver TCP traffic from Wired Endpoint with an Ethernet link through the Access point to the wireless client devices.



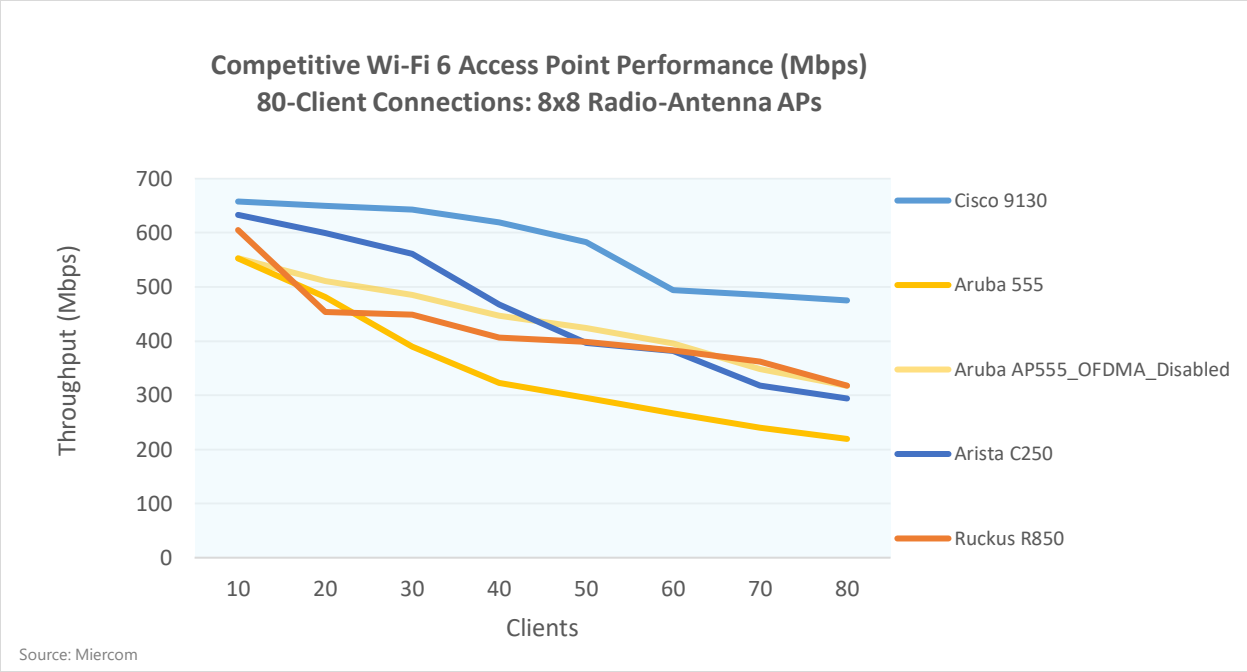
We evaluated all APs from Cisco, HPE-Aruba, Ruckus, Arista and Juniper-Mist. Then we grouped the results by the APs with similar radio-antenna specifications (e.g., 8x8). Refer to AP table in Product Tested section.

Why is this Important?

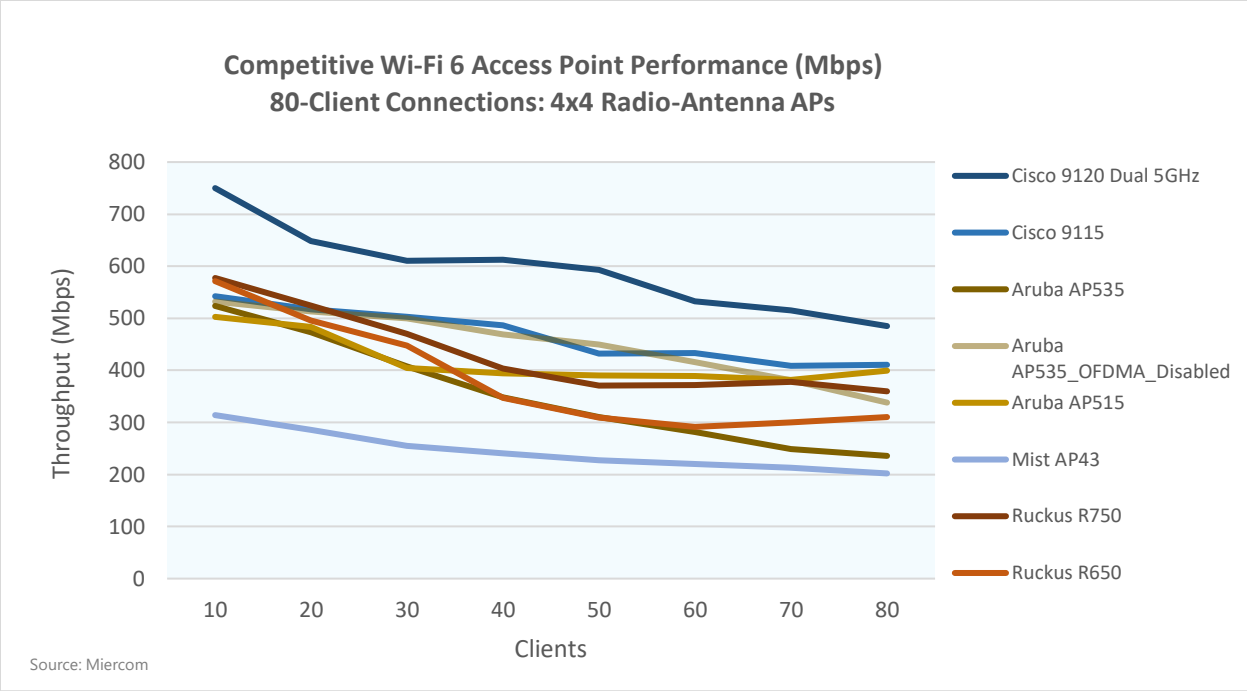
High-density wireless environments are becoming a more common scenario for networks. Bottlenecks can cause packets dropping and latency that affects the end user clients and overall network efficiency.

The Cisco Advantage

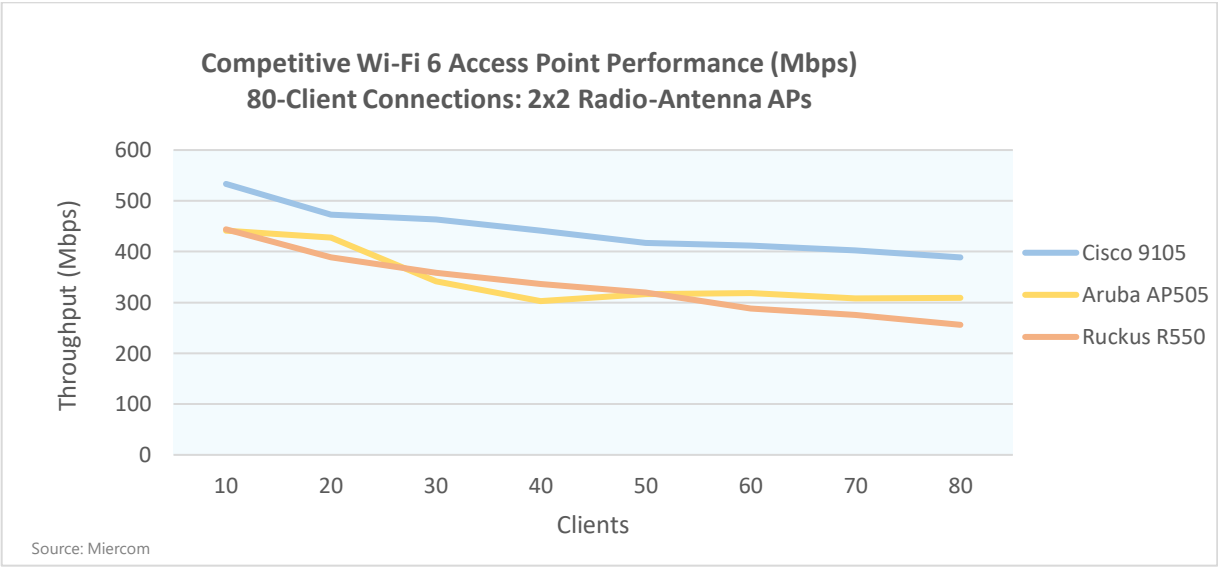
The below graphs show the TCP downstream throughput results for each set of client counts (10 to 80 clients) for the APs tested.



For the performance comparison of all 8x8 radio-antenna APs, the Cisco 9130 showed the highest performance despite the increase in client connections. Its maximum of 658 Mbps at 10 clients. The second highest performer, the Arista C250, showed 21 percent less performance compared to Cisco 9130. Ruckus 850 performed at a 26 percent decrease of Cisco 9130. For Aruba it is important to highlight that Aruba 555 was tested with both OFDMA enabled and disabled. This is because the tested Aruba controller code ArubaOS 8.7.0.0 has performance degradation issue with OFDMA enabled on AP-535 (refer to Aruba release note 8.7.0.0 Bug ID AOS-205666). However, it seems that AP-555 is also affected by the bug since it uses the same platform as AP-535. Aruba 555 declined by 40 percent with OFDMA enabled and 24 percent with OFDMA disabled respectively.



For the performance comparison of all 4x4 radio-antenna APs, the Cisco 9120 and 9115 APs showed the most consistent performance. Both proved the highest performance. Since Cisco 9120 offers dual 5GHz capability, we tested dual 5GHz instead of dual-band to gauge its maximum capacity. Cisco 9120 produced the highest performance starting with 750 Mbps at 10 clients and significantly beating all other competitors throughout client load increase. Cisco 9115 offers the second-best results with client load increase. Ruckus R750 and R650 APs started with a strong performance at lower clients count but quickly declined in performance as clients were added. With the Aruba performance degradation bug, AP535 was tested with both OFDMA enabled and disabled. Aruba AP535 with OFDMA enabled performed at a 40 percent decrease of Cisco 9120 and 24 percent comparing to 9115. Aruba 535 with OFDMA disabled had a decrease of 26 percent and six percent respectively. The Aruba AP515 performance had decrease of 29 percent decline and 10 percent respectively. Mist AP43 also offers Dual 5GHz but at the time of testing the feature was not released. Mist had the lowest performance for all client loads and showed a 58 percent decrease in performance from the highest Cisco 9120 and 47 percent with the second highest Cisco 9115.



In the performance comparison of all 2x2 radio-antenna APs, the Cisco 9105 AP had the highest performance of its competitors for all client loads. From 10 to 80 client connections, Cisco saw a 27 percent decline in throughput. The Aruba AP505 and Ruckus R550 had similar performance for 10 clients, but both declined as the load increased by 30 and 42 percent, respectively.

4.2 Power-over-Ethernet (PoE) Power Draw Comparison

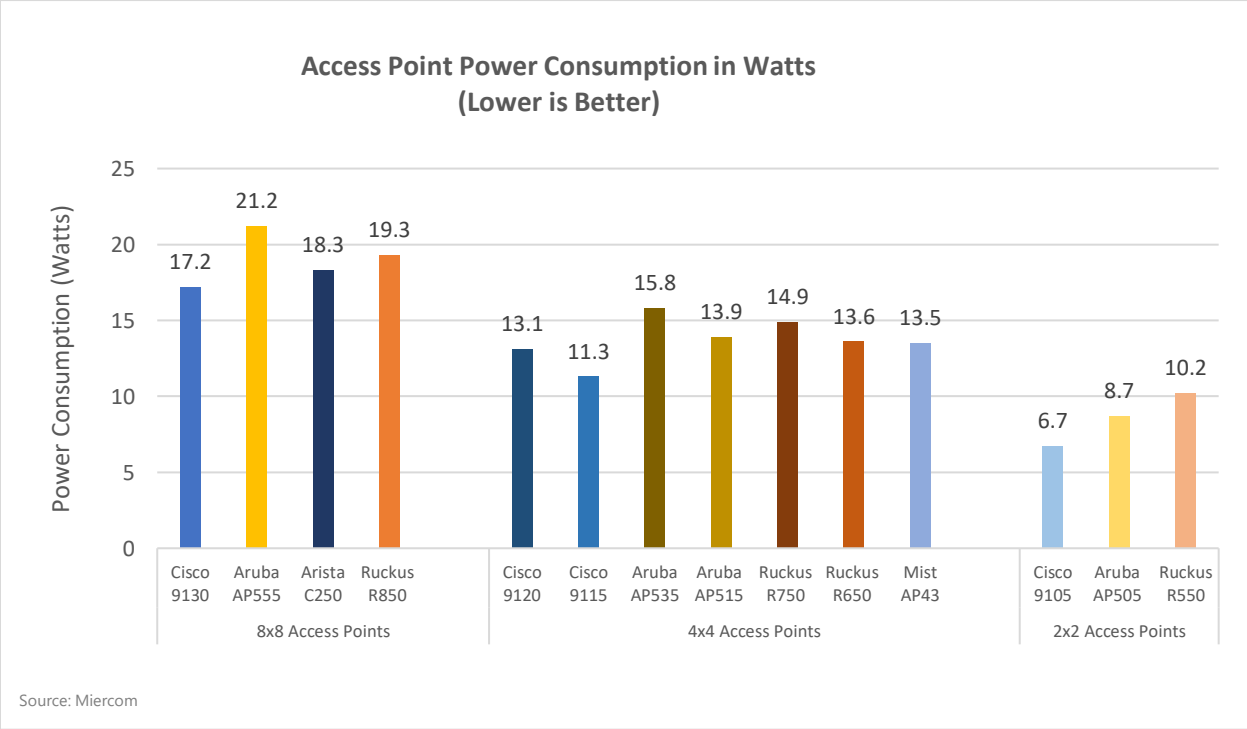
How We Did It

In this test, we evaluated the operating power consumption of the pool of APs under test. The PoE test used the same setup as the High-Density Test: 80-client Mix 11ax/11ac (4.1). The command “show power inline policy” was used to calculate the power consumption on the switch port connected to the AP during the 10-client test run.

Why is this Important?

Enterprises are always looking for ways to save energy for environmental cause and reduce electricity bills generated from multiple sources. When enterprises are using APs in hundreds and thousands, the electricity bill can rapidly increase based on AP power consumption.

The Cisco Advantage



Source: Miercom

For the power consumption in the 8x8 AP category, the Cisco 9130 was the most power efficient, followed by Arista C250, and Ruckus R850. The Aruba AP555 operated on the highest power among all the APs. In the 4x4 category, Cisco 9115 consumed the least power, 28 percent less power than Aruba AP535, which had the highest operating power. Cisco 9120 came at second place, followed by MistAP43, Ruckus R650, Aruba AP515, and Ruckus R750. In the 2x2 category, Cisco 9105 consumed the least power, 23 percent less than Aruba AP505, and 34 percent less than Ruckus R550.

4.3 Voice Calling Application Test

How We Did It

In this test, we wanted to observe the benefits of Wi-Fi 6 over Wi-Fi 5 technology for VoIP calling applications such as a Webex call. For the test, we focused on just comparing Cisco 9130AX Wi-Fi 6 AP with Cisco 3700 Wi-Fi 5 AP. We used 50 Dell Laptops with AX200 chipset running IxChariot G.711u VoIP call script. Simultaneously 5x11ac MacBook laptops were used running "TCP High Performance" IxChariot script to inject contention in the 80MHz channel. The test consisted of 5 sets of clients count starting with 10 x 11ax Dell laptop clients and 1 x 11ac MacBook Pro laptop client up to 50 x 11ax Dell clients and 5 x 11ac MacBook Pro clients.

Why is this Important?

The emergence of new devices and applications pose an ever-growing challenge for Wi-Fi network to provide ample airtime to latency-sensitive traffic. The Wi-Fi 6 solves this problem with OFDMA technology which helps maintain a consistent low delay for small packet applications such as VoIP call even if other applications such as file transfer or a video streaming are running concurrently in the network.

The Wi-Fi 6 Advantage

The below graph displays the one-way delay in milliseconds for both access points. The increase in delay translates to deteriorating VoIP call quality.

Comparing the two access points, the average delay of Cisco 9130 (23.38ms) was two times lower than the Cisco 3700 (46.66ms). Moreover, the increase in delay for Cisco 9130 was consistently low compared to Cisco 3700, of which the delay increased significantly at 40 and 50 clients count.

4.4 Video Performance

How We Did It

The access points evaluated for the test consisted of were Cisco 9130, Aruba 555, Ruckus R850, C250, and the Mist AP43. The access points were all deployed in the exact position in the center of the lab tested one at a time on a client range of 10 to 50 802.11ax (Wi-Fi 6 Chipset) Dell laptops. The open-source multimedia player known as VLC was installed to stream The Transformers Trailer at 2K resolution on loop on each client. While the stream is playing clients are added to the stream to look for three things:

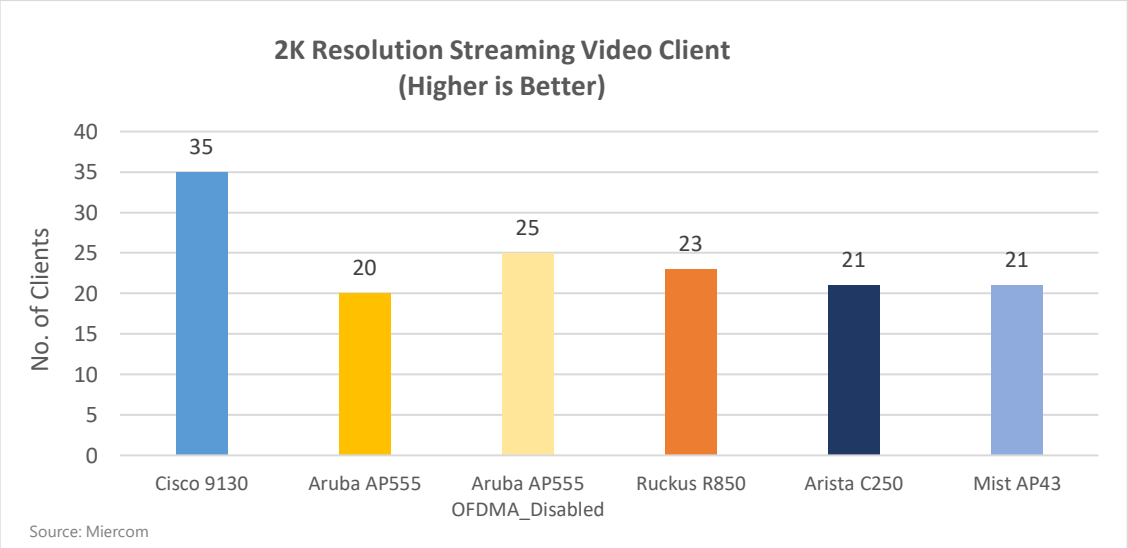
1) "Freezing:" Where the video would pause for more than 3 seconds
2) "Pixel Delay:" Where the original video translates into pixelated squares while playing
3) "Jitter:" Where the video is playing in a consistent breaking manner

The number of clients that exhibited these cases during the test-run was noted and restarted until the maximum number of supported clients were at a viewable state.

Why is this Important?

Video or live streaming is becoming the norm especially as work from home environments are emerging. Active engagement and interaction to spread information has become a demand. With streaming any delay, jitter, pixilation issues would be detrimental to business operations and functionality.

The Cisco Advantage



Cisco 9130 was the most capable AP to maintain the most stable and highest number of clients simultaneously while streaming. Due to the OFDMA performance bug (refer section 4.1) in Aruba AP555, we also included performance number with OFDMA disabled. In OFDMA enabled mode, Aruba AP555 started experiencing light freezes at 15-16 clients but was very noticeable at 20 clients. In OFDMA disabled mode, Aruba AP555 was able to stream up to 25 clients without showing any performance glitches. In Ruckus R850, the clients experienced light freezes at 19-21 clients but noticeable heavy pixel crashes at 23 clients. Ruckus 850 had a decrease of 34 percent in comparison to Cisco 9130. Both Arista C250 and Mist AP43 shared similar results and tied with a 40 percent decrease compared to Cisco 9130.

4.5 Performance Summary

4.1 Highest Wi-Fi 6 AP Performance for 80-Client Connection	
Overall	Cisco 9130
8x8 APs	Cisco 9130
4x4 APs	Cisco 9120 & 9115
2x2 APs	Cisco 9105
4.2 Access Point with the least Power-over-Ethernet (PoE) Power Draw	
8x8 APs	Cisco 9130
4x4 APs	Cisco 9115
2x2 APs	Cisco 9105
4.3 Latency improvement of Wi-Fi 6 over Wi-Fi 5 for Voice Calling Application Test	
	Cisco 9130 offered two times better latency than Cisco 3700 for VoIP call
4.4 Video Performance	
8x8 AP	Cisco 9130

5.0 Solution

5.1 RF Interference Protection

Whether APs use Wi-Fi 5 or Wi-Fi 6, there will be radio frequency (RF) interference occurring. Sources of interference include anything from a microwave to a video surveillance camera.

How We Did It

This test was performed on Cisco 9120, Aruba AP-535, and Mist AP43 by utilizing their respective spectrum-analysis capability to detect non-Wi-Fi interference. We broadcasted various non-Wi-Fi type devices (2.4GHz and 5GHz) on to the network to observe three tasks:

1) Does the vendor's AP detect the presence of the interference?
2) Does the vendor's AP accurately identify the non-Wi-Fi device type?
3) Does the vendor AP alter the broadcasting channel to avoid high interference?

The non-Wi-Fi device interference device types consisted of:

a) Microwave
b) Video Camera (2.4 GHz)
c) Video Camera (5GHz)
d) Cordless Phone
e) Jammer

Why is this important?

The rapid growth of IoT devices makes the use of RF spectrum even more challenging. Often the RF interference from a variety of non-Wi-Fi devices can significantly degrade the performance of a Wi-Fi network. Administrators should work to reduce the noise without having to remove or relocate the sources of interference physically.

The Cisco Advantage

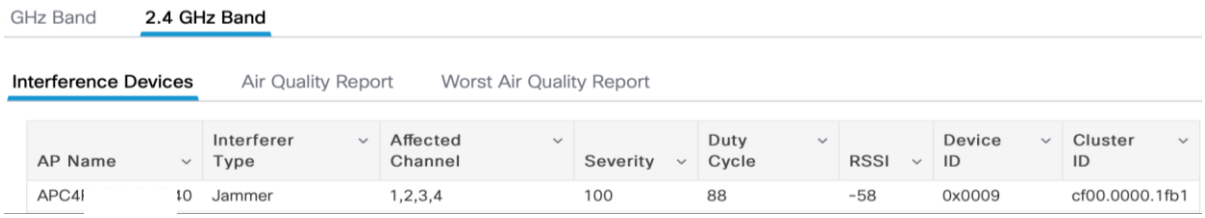
Cisco 9120 and 9130 Access Point has an integrated dedicated radio called Cisco RF ASIC that offload many operations from an AP's client-serving radios. One of the RF ASIC features is CleanAir, which handles the identification of non-Wi-Fi interference sources, which helps Cisco Catalyst 9120 and 9130 APs have secure, resilient and intelligent connections for clients and IoT devices.

	CISCO		ARUBA		MIST	
Interference Device	**Detect and Recognize?**	**What did it report?**	**Detect and Recognize?**	**What did it report?**	**Detect and Recognize?**	**What did it report?**
Video Camera (2.4GHz)	Yes	Video Camera	No	N/A	Yes (after 10 minutes)	N/A
Video Camera (5GHz)	Yes	Video Camera	Yes	Cordless Base	Yes (after 10 minutes)	N/A
Microwave	Yes	MW Oven	Yes	Microwave	Yes (after 10 minutes)	N/A
Cordless Phone	Yes	Cordless Phone	Yes	Cordless Base	No	N/A
Jammer	Yes	Jammer	No	N/A	No	N/A

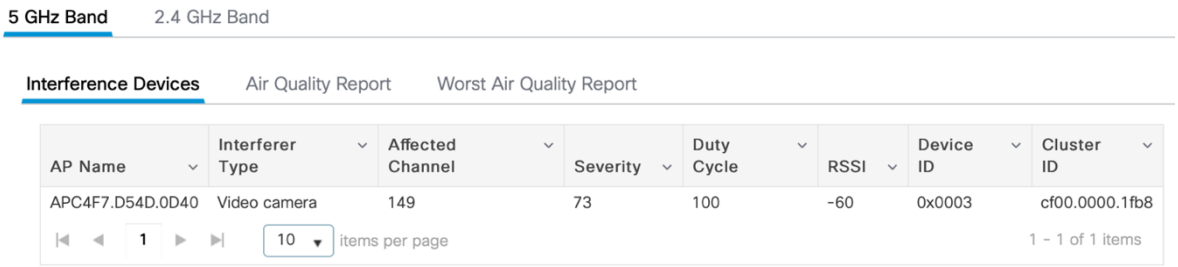
How Cisco Compares?

In all the test cases, every device on the list was detected and identified accurately with the appropriate name. We observed that the Cisco solution reacted to the interference and changed the channel. The below screenshots of Cisco 9800 wireless controller dashboard show the detection of the illegal jammer and a 5GHz video camera interference with additional details.

Device Type: Jammer



Device Type: 5GHz Video Camera



How Aruba Compares?

Aruba has a similar spectrum analysis mechanism for identifying RF interference. Aruba detected the presence of all devices except for the Jammer and 2.4 GHz video camera. During the jammer interference test, Aruba could simply not identify nor list the device or showed an increase in channel utilization. Aruba did detect the presence of 5GHz camera but could not identify it correctly. The access point also changed the channel due to interference from the camera but only one out of three test runs. The other two times, the access point stopped broadcasting the SSID on the affected channel.

Device Type: 5GHz Video Camera

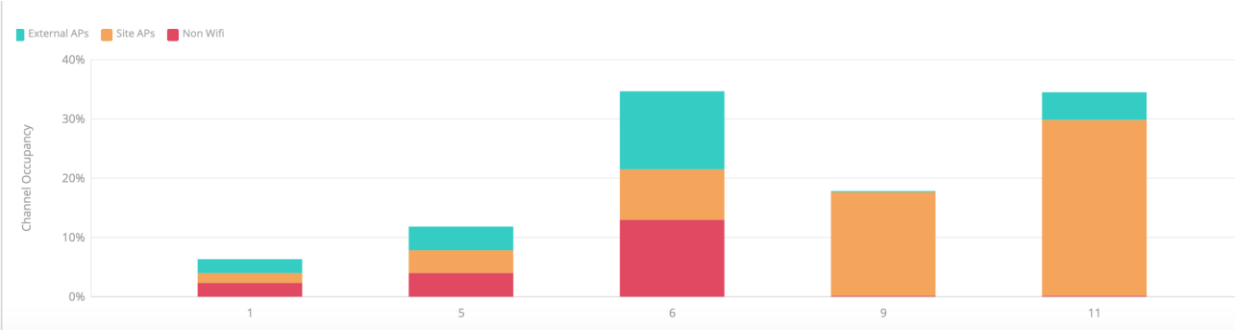
```
(Aruba7210) *#show ap spectrum device-list ap-name AP555-1

Non-WiFi Device List: 5GHz
--------------------------
Type              ID  CFreq(KHz)  Bandwidth(KHz)  Channels-affected     Signal(dBm)  Duty-cycle  Add-time             Last-seen
----              --  ----------  --------------  -----------------     -----------  ----------  --------             ---------
Cordless Base FH  1   5785000     79000           149 153 157 161 165   -22          5           2020-09-09 21:39:48  2020-09-09 21:39:59
```

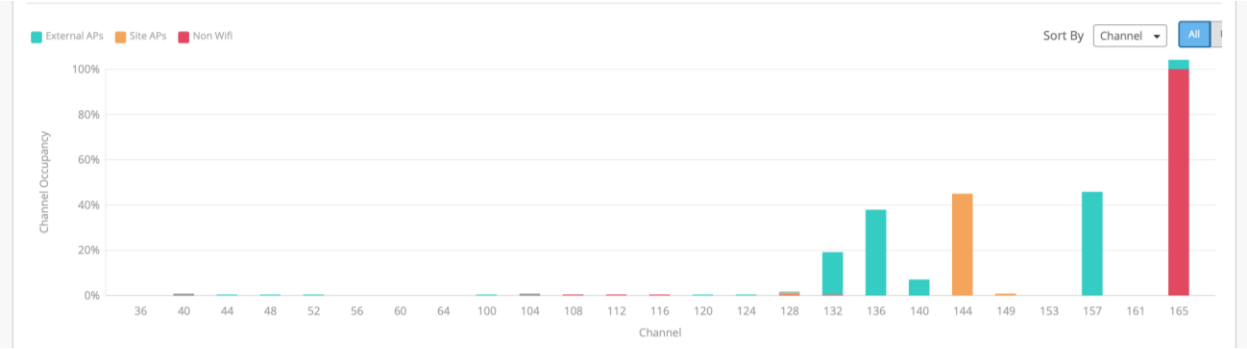
How Mist Compares?

Mist provided the least amount of information when it came to interference. The Mist dashboard only shows the percentage of channel utilization; therefore, Mist could not identify any of the device type names. Mist identified the presence of three devices (Microwave, Cordless Phone, and Video Camera) but required at least 10 minutes of waiting time. Mist also did not perform any channel change with the 5GHz camera but did show 100% non-Wi-Fi interference on the appropriate channel. The SSID would also stop broadcasting on the spectrum. The Mist dashboard could not detect the jammer interference. The jammer should spread across the spectrum and be identified as non-Wi-Fi.

Device Type: Jammer (cannot detect properly)



Device Type: 5GHz Video Camera



5.2 Network Operations

The expense of operating a network is intimidating for most IT teams. If the process takes too long, the network suffers large gaps of downtime that will cost the enterprise in productivity and revenue. The IT team must constantly search for the downtime window to perform wireless network upgrades, which takes time, skill and cost that, with resiliency features, can be resolved to allow more pressing matters to be addressed.

In the following tests, we show how Cisco 9800 and Cisco DNA Center improves, simplifies and hastens the process of planned software upgrades and unplanned events.

5.2.1 Onboarding new APs without Downtime

Once the IT team is ready to upgrade the network to Wi-Fi 6 devices, the administrator can begin adding the new access points to existing network.

Why is this important?

Traditionally in on-prem networks, the network administrator must upgrade wireless controller if they need to add new AP models. It required a downtime maintenance window that was not always realistic – if there even was one. The result was an unacceptable amount of time to upgrade to new hardware. Additionally, software versions are usually standardized, to ensure all user devices are compatible, and all the network devices are without critical bugs (common in healthcare, manufacturing and retail environments). The cost to ensure compatibility and standardization between hardware and software can cost tens of thousands and take weeks to accomplish.

The Cisco Advantage

Cisco can add new APs hardware, without having to upgrade pre-existing software on the wireless controller. With the help of AP Device Pack (APDP) feature the new APs can go online without upgrading the entire wireless controller software or the wireless controller reboot.

Mist can seamlessly add new APs to its cloud dashboard without needing any downtime. Aruba Controller requires a full software upgrade and reboot to support new APs. This operation would require an administrator to plan network downtime and validate controller image interoperability with all the endpoints.

5.2.2 Fixing bugs in the existing APs

AP software can fail or have bugs which require patching.

Why is this important?

Ideally, administrators want to fix the AP software without a complete software upgrade, causing disruption and downtime.

The Cisco Advantage

The AP Service Pack (APSP) ensures if there are any software bugs, the patch can be applied to only the AP in question. This does not require upgrades of the entire wireless controller. No reboot is required.

The APSP can apply patches by distribution of 5, 15, 25 or 100 percent clients – depending on how small you want the maintenance window to be. This is especially useful in healthcare environments. Like APDP, you also have the option to roll back to any point of the update process for a select number of APs.

In Aruba, administrator would need to upgrade and reboot the entire controller in order to fix an AP software bug which will lead to downtime. Since Mist is a cloud solution, they do not have controller upgrade requirements.

5.2.3 AP Refresh from Old to New Generation

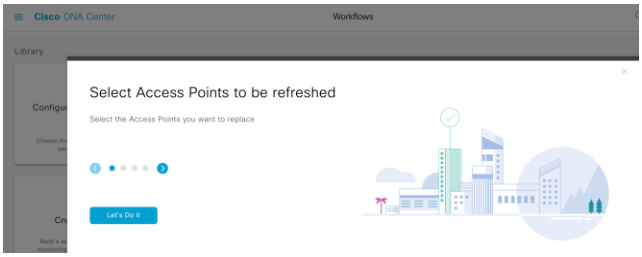
Upgrading APs from, for example, Wi-Fi 5 (802.11ac) to Wi-Fi 6 (802.11ax), can be an intimidating job as it requires hardware replace, software upgrade, naming changes, map update and many more tasks.

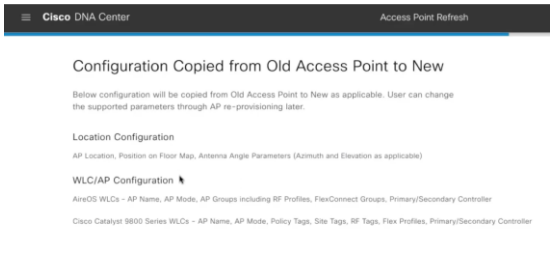
Why is this important?

Older APs are typically scattered across sites, buildings and floors. Also, when migrating to new hardware, you must consider the time-consuming process of adding the naming and mapping the APs.

The Cisco Advantage

Cisco DNA Center provides an AP Refresh Workflow for easy device swapping, decommissioning older devices and then adding the new ones with correct names and mapped location.





The administrator refreshes APs by selecting globally or from the site/building/floor. This process is done behind-the-scenes and does not require the typically manual task of re-applying software, patches, or map locations to each AP. After the AP Refresh, AP 360 dashboard shows the event with the replaced MAC and serial number.

Aruba and Mist do not offer any workflow to seamlessly add new APs and replacing the existing APs in the network and require many operation cycles to deploy and configure the new APs.

5.2.4 ISSU (Rolling AP Upgrade)

Software upgrades are crucial for high availability among devices, such as APs. Upgrading software is ideally done automatically, not manually, and should not incur complete network downtime as a result.

Why is this important?

Always on network is particularly crucial in the healthcare environments or during high-volume remote work scenarios, where it is extremely difficult to find a maintenance window to upgrade software.

The Cisco Advantage

Cisco uses its In-Service Software Upgrade (ISSU) feature to upgrade an image to another device – without requiring total network downtime, and the automated process allows the administrator to keep their focus on other network activities.

This seamless process, also known as the Rolling AP upgrade, avoids outages during upgrades. Rolling AP Upgrades intelligently selects the group of APs based on their neighbors, such that they do not upgrade simultaneously, avoiding downtime. The administrator can choose a percentage of APs to upgrade at once (5%, 15%, 25%) with more iterations for lower percentages – making it less risky. Administrators are offered the flexibility to choose the right balance for their network from the faster upgrade (with more iterations) or less invasive upgrade (with more iterations). Mission-critical network like healthcare will choose 5% to minimize disruption.

How Aruba Compares?

Like Cisco, Aruba allows for upgrades to be performed on groups of APs, but to enable this feature, Aruba requires another platform called Mobility Master which adds additional touchpoint. Also, Aruba requires the software package to be downloaded to the wireless controller manually.

How Mist, Arista, Ruckus Compares?

In the case of Mist, Arista and Ruckus, all APs upgrade together and reboots together, creating downtime. Other option is manually upgrade AP which requires constant admin attention adding OPEX and longer upgrade time.

5.2.5 Simplified RMA Process

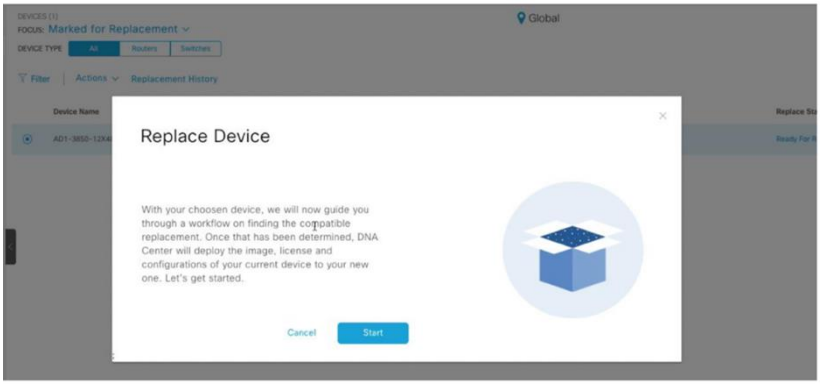
Hardware can be at fault or a failing component, requiring the administrator to replace the device.

Why is this important?

As with installing, refreshing, or software patching, the downtime incurred by replacing devices can be time-consuming and costly. The process requires identifying the faulty device and ensuring that the replacement device has the correct software version and configuration.

The Cisco Advantage

Cisco DNA Center provides a guided workflow for decommissioning the faulty devices and installing new devices.



The faulty device is marked for the replacement, and a new unclaimed device is selected as a replacement. With few clicks, the Cisco DNA Center runs the replacement process in the background without requiring manual configuration transfer from the old device to the new device.

After the replacement process is started the administrator can also monitor replacement process's status indicated by grey, red, green and orange color.

Aruba and Mist does not offer any workflow to replace the faulty hardware. However, Mist does offer a process to send the faulty access point for replacement to Mist TAC.

5.2.6 Closed-Loop ServiceNow Integration

Enterprise systems are often leveraging IT Service Management tools like ServiceNow for help desk ticket management.

Why is this important?

Integration with ITSM tools simplifies the ticket management across the network management platform and ITSM platforms.

The Cisco Advantage

Cisco DNA Center provides a closed-loop integration with the ServiceNow platform to help in simplified and fast resolution of the network issue. When Cisco DNA Center detects a network issue, it automatically creates a ticket with appropriate severity in ServiceNow. It then sends additional details to ServiceNow such as device information, network topology, RCA, and recommended remediations for auto submission of change request on the open tickets.

Once the Cisco DNA Center detects that the resolution of network issue, it verifies ITSM ticket number and automatically informs the ITSM platform to close the open ticket in the system. Cisco DNA Center also displays the ticket status change of the ServiceNow platform in Cisco DNA Center dashboard.

Aruba Central and Mist provide webhook integration with ServiceNow platform that enables automatic ticket creation but lacks the closed-loop ticket resolution. They do not support auto ticket change management and ticket change status on their respective dashboards.

5.3 Network Assurance

When a network problem occurs, the IT administrator must manually analyze a complex environment to find the current issue, and its source. Problems (e.g., client density, AP coverage, RF interference) can even co-occur, making it difficult to troubleshoot.

The following series of tests dives into the unique ways that Cisco Assurance helps remove the burden from IT teams for root-cause analysis and troubleshooting by automatically finding problem areas and providing contextual reports that save time and cost.

We compare Cisco DNA Center to Aruba Central and Mist Dashboard to highlight ways Cisco holds the advantage for typical use cases seen in real-world networks.

Why is this important?

Problems may require prioritization and can often cause outages or unnecessary maintenance downtime. When an IT team can quickly identify the problem source, the network can resume a reliable end-user experience. Assurance differs from traditional monitoring in that it streams multiple sources of data to provide a contextual picture of the network to better address issues.

5.3.1 Wi-Fi 6 Insights

Customers want to setup the latest Wi-Fi standard on the network. The first step is to figure out whether the network is prepared for Wi-Fi 6. After the Wi-Fi 6 APs are upgraded, the next step is to determine the benefits of the Wi-Fi 6 resources.

Getting information on Wi-Fi 6 should be straightforward and contextual. The more information is given, the more the administrator can work with to solve any issues. For this use case, we analyzed three dashboards: Cisco DNA Center, Aruba Central and Mist Marvis.

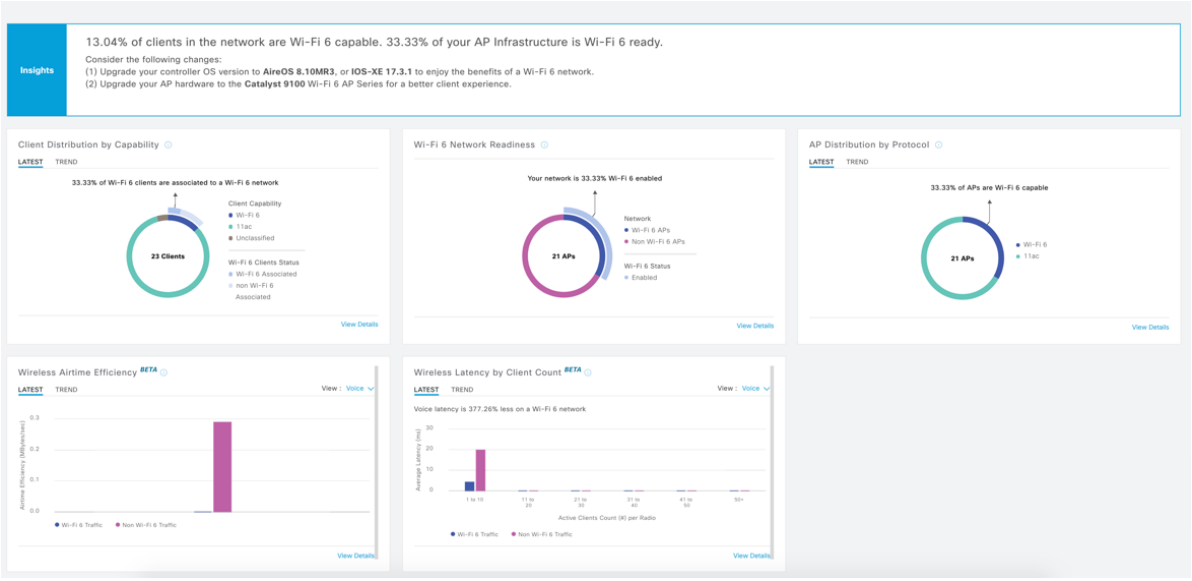
Why is this important?

A Wi-Fi 6 dashboard should not only help upgrade Wi-Fi 6 ready devices but give the administrator a way to justify the upgrade for an informed decision.

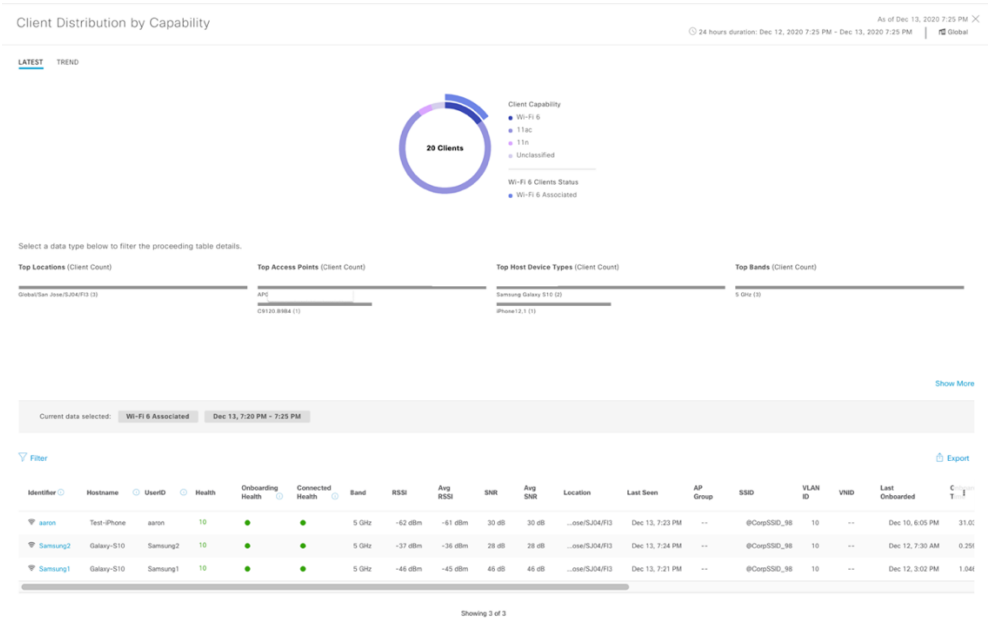
The Cisco Advantage

Cisco Assurance is available using the Cisco Digital Network Architecture Center (Cisco DNA Center) Analytics and Assurance interface. This platform combines network telemetry, contextual data, big data processing, health scores, insights, and proactive troubleshooting for a holistic approach to network reliability.

The Cisco DNA Center Wi-Fi 6 Dashboard gives a contextual, visual insight of Wi-Fi 6 clients, readiness, distribution, efficiency, and latency. The administrator can look at the Wi-Fi network from a global or local perspective. The Wi-Fi 6 dashboard eliminates the IT administrator's need to search each client to determine if they are Wi-Fi 6 capable.



Inside Cisco DNA Center, you can view how many clients and devices are connected, their health and the overall network health. All data can be retrieved retrospectively from 3 hours to 1 day, to 1 week. The Cisco DNA Center Wi-Fi 6 dashboard consists of multiple dashlets that visually represent the latest or trending Wi-Fi 6 characteristics. Each dashlet comes with an explanation of the visual display, its contents, and its legend. It shows the percentage of the Wi-Fi 6 clients associated with the Wi-Fi 6 network. By increasing this percentage, the administrator can expect increased efficiency and decreased latency in other dashlets.

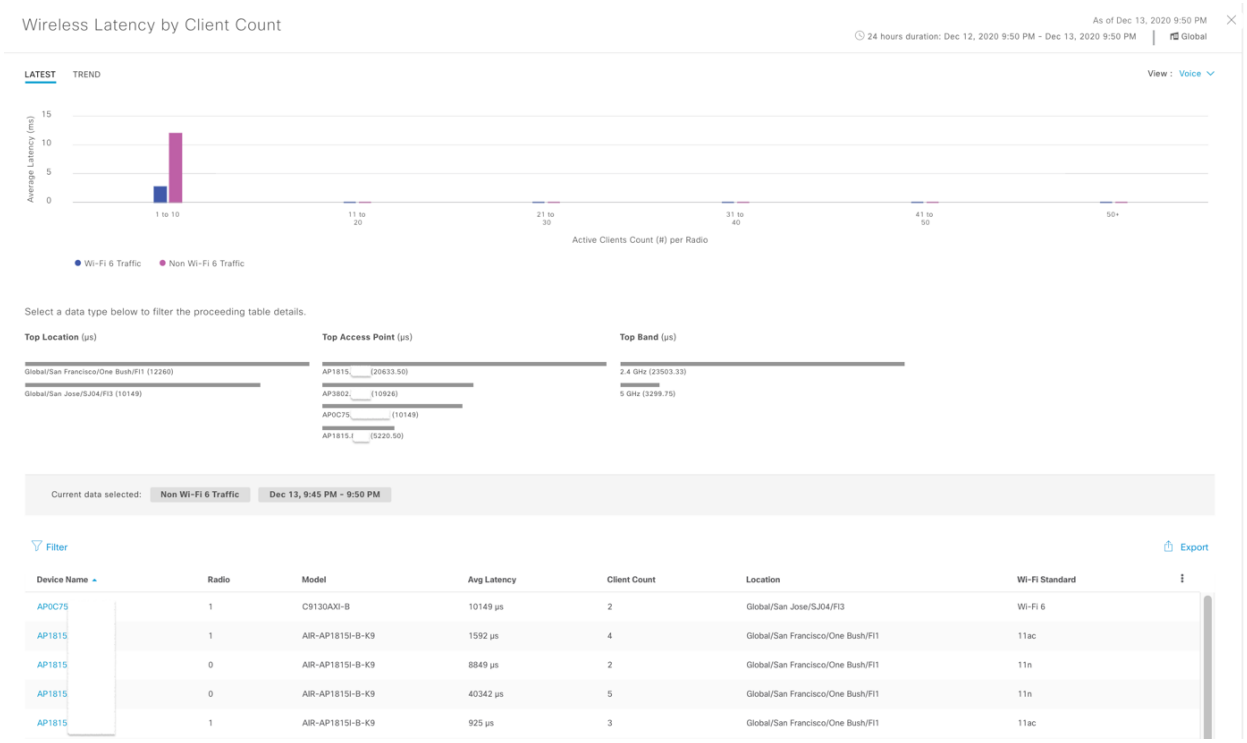


By selecting the dashlet by timeframe, we observed the Client Distribution by Capability trend over the course of 24 hours. The legend shows which Wi-Fi standard is used and is represented in the client count on the vertical axis. At any point, the administrator can hover over to see the amount of Wi-Fi 6, 11ac, 11n, 11abg and unclassified client counts. Details of the datatype are available, showing the Top locations, Top APs, Top Host Device Types, and Top Bands (2.4 and 5 GHz).

Other dashlets include: Wi-Fi 6 Network Readiness, AP Distribution by Protocol, Wireless Airtime Efficiency, and Wireless Latency by Client Count.

The Wi-Fi 6 Network Readiness dashlet shows how many APs have Wi-Fi 6 enabled and how many are not in a visual graph. This dashlet has the same option for details and trends as the Client Distribution by Capability dashlet. Likewise, the same can be seen for the AP Distribution dashlet.

For a mixed environment of Wi-Fi 6 and non-Wi-Fi 6 traffic, the major benefits come from the Wireless Airtime Efficiency and Wireless Latency by Client Count dashlets.

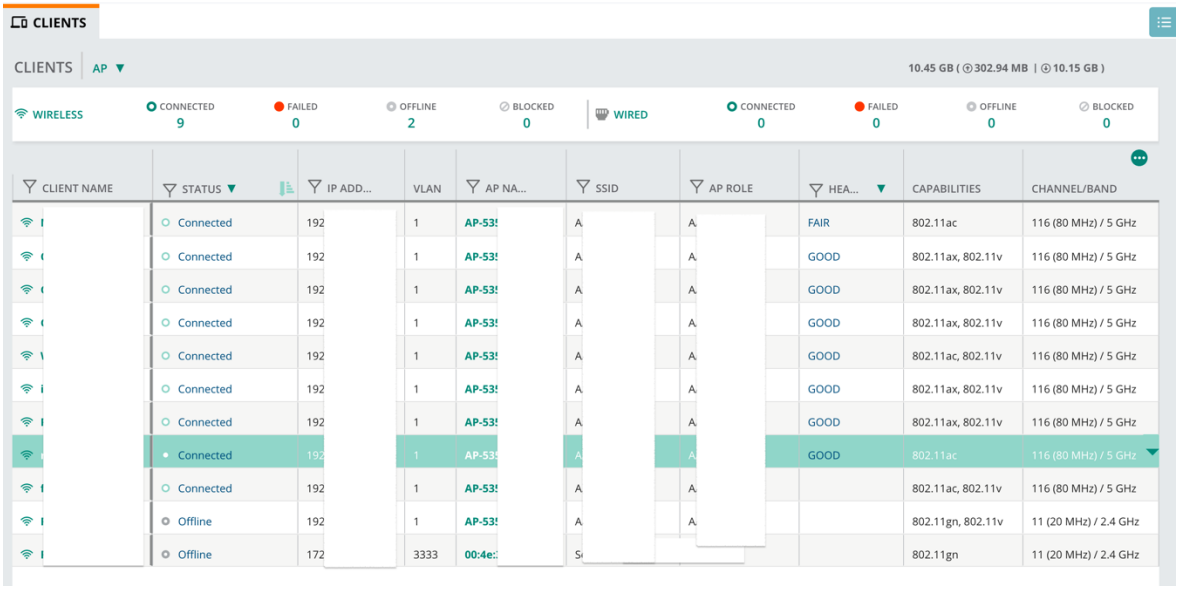


These dashlets help show the percentage of gained efficiency or latency loss from the Wi-Fi 6 environment, compared to the environment without the upgrade. It can be viewed for Voice, Video, Best Effort, Background scenarios. For Airtime Efficiency, the benefit is given in a percentage based on the increased megabytes per second (MB/sec). In the Wireless Latency dashlet, the percentage of average latency loss is displayed, and the average latency is compared for Wi-Fi 6 and non-Wi-Fi 6 clients per radio in the graphic, measured in milliseconds (ms). The administrator gets a clear indication of the direct benefits from upgrading to Wi-Fi 6.

How Aruba Compares?

Unlike Cisco DNA Center, there is no dedicated Wi-Fi 6 dashboard. There are other overview dashboards available that can help give context to the wireless network environment.

Using the Aruba Central interface, under AI Insights, there are items listed that flag the administrator of any issues. For example, “Excessive Access Point Reboots (2 reboots)” was a warning we observed, which indicates APs have rebooted more than usual and require investigation. A timeline chart is available to display trends by the date of occurrence.



While information can be provided in a global view, if you want to investigate the number of Wi-Fi 6 and non-Wi-Fi 6 clients, you can go to a different dashboard – the Clients dashboard. This lists the clients along with different stats including Wi-Fi capabilities, which you can click on to get client details (e.g., data path, health, signal-to-noise ratio, transmission rate, AI Insights, connectivity).

Also available in a global view is Devices/Access Points, which allows the user to see a list of connected or disconnected APs on the network. By clicking on a specific AP, the user can see an overview of all associated information with the device (e.g., AP model, MAC, group), network information, radio modes and status, AI Insights, and more, like the client view.

How Mist Compares?

The Mist dashboard, like Aruba, also does not have a dedicated Wi-Fi 6 dashboard the way Cisco does. It offers many other views of the network and features to help understand the environment's issues. The MARVIS interface allows you to ask a question, like a search engine, to access information. It is one way to try and access information about clients. As an example, we tried to search "how many clients". It serves us with a clients list; however, there is no provision to see the Wi-Fi capability of the listed clients. It also gives the user the option to rate Marvis' response to refine this tool.

The other way to see the clients' list is the Clients tab where you can see a list of connected clients per-site with client count, band, and client count per IEEE Wi-Fi standard (e.g., 802.11ax, 802.11ac, 802.11n). However, when monitoring clients, there is no global view. The user can only access clients list per-site basis.

5.3.2 Artificial Intelligence (AI)/Machine Learning (ML): Client Fails to Connect

Assurance is unlike typical monitoring; it gives a contextual look at the problem from multiple perspectives within the network. Being able to do this in real-time helps but analyzing and troubleshooting the number of alerts is time-consuming because a network is large and challenging to convey. Having an automated, intelligent way to find the issues based on what is normal in your network is key to solving problems quickly.

This test looks at clients failing to connect to a network. We evaluated the following dashboards: Cisco DNA Center AI Network Analytics, Aruba Central AI Insight, and Mist Insight/SLE/Marvis.

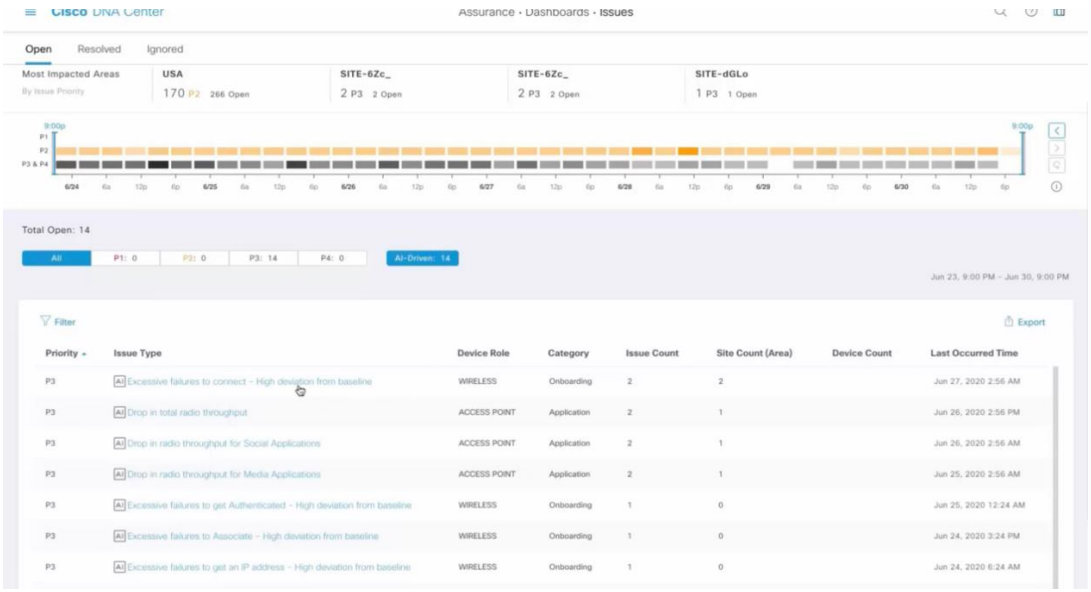
Why is this Important?

Administrators can quickly become inundated with insignificant alerts that IT teams will begin to ignore until a complaint is made to make it a priority. This means that small fires, which seem unimportant at the time, can become large fires to put out later. By that time, more devices and users may be affected – resulting in an overwhelming task of backtracking, troubleshooting and maintenance that can take days or weeks to fix when it can be resolved in minutes.

The Cisco Advantage

Cisco AI Network Analytics is the machine learning and machine reasoning aspect of Cisco DNA Center Assurance. It does not require manual thresholds to be set. Instead, it provides an AI-Driven automated model for baselining, anomaly detection for connectivity and applications issues, proactive insights, comparative benchmarking, and predictive analytics. Its intelligent analysis identifies false positives, and therefore, gives higher accuracy detection for accelerated remediation and suggested options for IT teams to act on.

AI-Driven issues are triggered when anomalies occur with respect to the environment baseline. To view these issues, the administrator can click the AI-Driven button. AI-Driven issues are listed the same way as any other issue in the Assurance dashboard.



The Cisco DNA Center Assurance dashboard displays all open issues for up to 2 weeks. This timeline view correlates to the issue list below, which indicates the priority, type, device role, category, issue count, site count, device count, and timestamp. This gives the why, what, where, when, who and how of every issue that occurs. The timeline windows that are also available are 3 hours, 1 day, and 1 week.

Cisco AI/ML collects multiple layers of information which provide a rich, contextual picture of the network to hasten troubleshooting and remediation. The intuitive, clean view of issues and how they correlate to other issues throughout the network helps relieve the burden of an overloaded IT team that would otherwise need to perform manual investigations.

By clicking on the issue type, you can see the open issue count, affected location (building/floor) count, the issue detail, impacted site and site count, impacted client count, issue count, last occurred timestamp and updated timestamp. By clicking on the open issue, the administrator can drill down into the problem. The window as shown in above screenshot displays the summary of the issue with the number of impacted sites and the impacted clients. It also provides multiple tabs to help remediate the issue quickly. The problem detail tab explains the problem and visualize the deviation from the normal baseline (green band), e.g., DHCP timeouts. Impact tab gives the distribution of the impacted clients per floor, client counts and additional details (e.g., RSSI, SNR). The Root Cause Analysis tab shows the potential root causes for the issue along with Failure Type Breakout, Radios with high onboarding failures. The Suggested actions tab helps the administrator to take step by step actions to remediate the issue. The administrator can also give feedback, by clicking on a thumbs up or down, to tell Cisco if this was helpful – making Cisco AI and machine learning smarter.

On top of the AI-Driven issues, Cisco DNA Center has multiple other AI-based features that help proactively find the problems and optimize the overall network.

Network Insights window shows the deviations outside of the normal behavior in the network for various key performance indicators such as client count, SNR, radio throughput etc. The deviation is shown in a bee-swarm chart format for a period of 4 weeks. This feature helps remediates a deviation before it becomes a network disrupting event in the network impacting many clients.

The Peer Comparison window helps in benchmarking the network's performance compared to the peers for the selected KPIs (Interference, Radio throughput, Cloud App throughput, RSSI, Radio Reset, Packet Failure Rate). The Site Comparison window shows a comparison of the performance within the organization of two different sites. The Comparative Benchmarking feature helps in determining if the optimization of the network or a site is required. Network Heatmap feature is unique to Cisco, which collects up to 1 year of data, allowing the administrator to see and compare 1-month time capsules for various KPIs. For example, when channel change KPI is selected, it will show which APs in the organization or site have more channel changes compared to the rest of the access points. This further expands the context to support faster remediation.

How Aruba Compares?

For this same test, Aruba AI Insights was used to determine the cause of client connection failure. Aruba AI Insight tab lists the issues (e.g., DHCP Server Connection Problems) with option to choose the time range from three hours up to one month. Expanding on the selected issue will show additional information

such as the failure reason, and failure chart with baseline comparison with peer networks or within the company. It also displays the affected APs and clients, server, and affected sites. However, there is no provision to add more KPIs to the issue page, which gives a contextual story that Cisco tells.

There is no Network Heatmap dashboard like Cisco's, but the Aruba Reports are based on data collected for up to 3 months. However, this simply lists APs with associated attributes that require manual investigation for identifying issues.

How Mist Compares?

There are multiple ways to troubleshoot in Mist. One way is through the Monitor dashboard using Wireless SLE metrics with AI Anomaly Detection. It shows a baseline deviation for only connectivity failures. Here the administrator can set manual thresholds, and a red mark is displayed when abnormal behavior has occurred. There is root-cause analysis that provides statistics, a timeline, distribution, affected items, and anomalies. These details are effective but not as intuitive or contextual as Cisco.

The other ways to identify behavioral anomalies is by using Marvis. By asking Marvis, "How is my site doing today?" the administrator is given a list of issues to investigate. The administrator can also go to the Actions dashboards to view anomalies based on connectivity issues. It shows an anomaly timeline and the number of impacted clients, a description of the issue, and the root cause of the problem. Mist, like Cisco, gives the option for rating-based feedback.

Unlike Cisco, Mist lacks proactive troubleshooting. Additionally, like Cisco, there is no Network Heatmap dashboard. The only similar aspect feature is the ability to create an Ad-Hoc Analysis to view trends for up to 3 months in a per-month view. All insight must be gained manually, adding to the IT workload.

5.3.3 Troubleshooting Client Failure

Customers assess and fix client wireless issues, for example, failure to connect to the Wi-Fi network due to association failure. We assessed the following features: Cisco DNA Center Client 360 and Intelligent Capture, Aruba Central Client detail, and Mist Client Insight Events and Dynamic Packet Capture.

Why is this important?

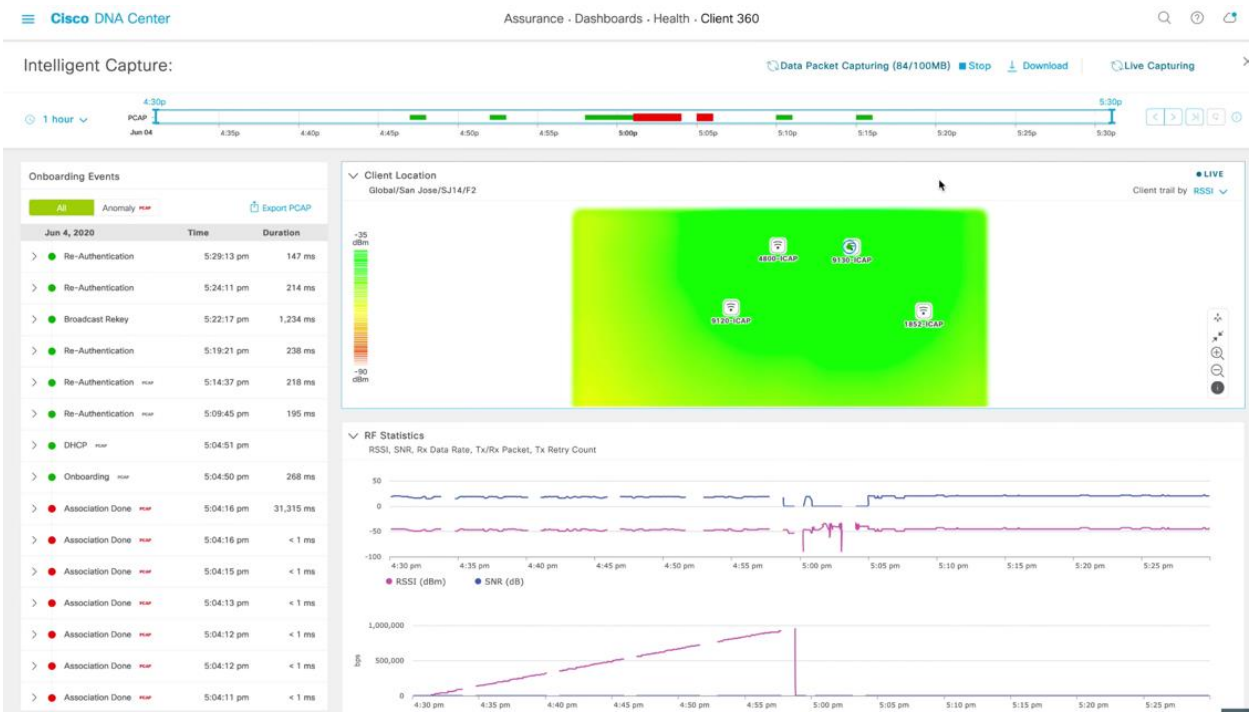
Usually, when an issue is reported, it had already occurred hours ago. In a typical scenario, an admin would try to replicate the issue and capture the packets by physically visiting its location. It gets even more challenging if the problematic site is remote. Having the ability to go back to the exact time when the issue occurred and analyze the packet capture of the event can help diagnose and resolve the matter faster, allowing users to experience less downtime and more productivity. The more time it takes to troubleshoot a client issue, the less attention an IT administrator gives to other high severity network problems.

The Cisco Advantage

The Cisco DNA Center Intelligent Packet Capture provides an Event Viewer for troubleshooting onboarding and roaming issues, real-time client troubleshooting with client tracing, anomaly detection with automated anomaly packet capture, scheduled packet capture, and full packet capture for a set time period. This packet capture feature is also available for APs (specific or all).

Anomaly Packet Capture is accomplished by correlating data from the AP, wireless controller and Cisco DNA Center. The client onboarding state is in the controller, generating a Client Event. The AP uses the Client Onboarding Policy to generate a Client Anomaly event. All event data is forwarded to the Cisco DNA Center. This happens behind-the-scenes, allowing the user to just look at the erroneous event and analyze the corresponding packet capture information needed to help troubleshoot.

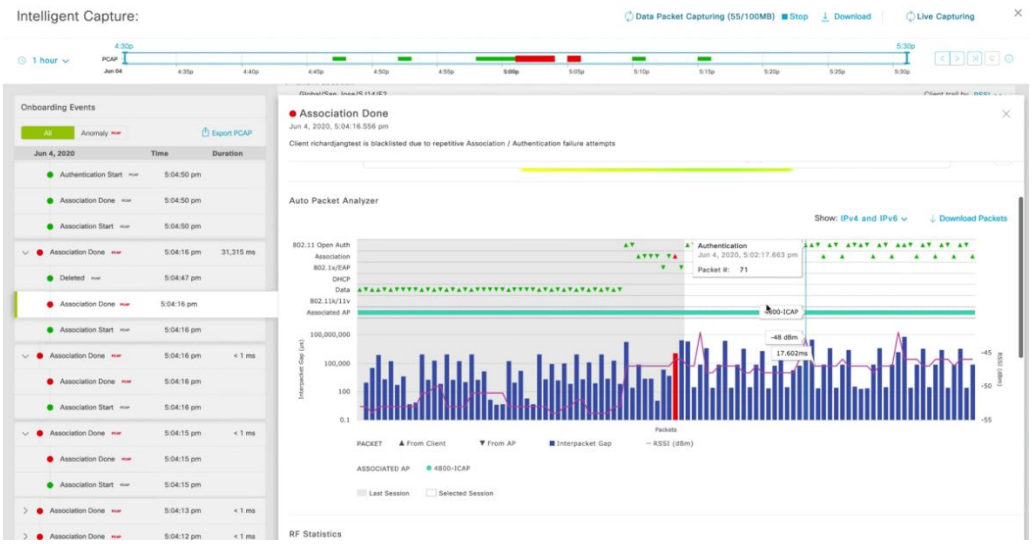
To troubleshoot a client, a direct way is by searching the username or mac address of the client. Clicking on the client will open the Client 360 dashboard, showing a timeline of events, issues, onboarding processes and data path. To the upper-right of the timeline chart is a button called Intelligent Capture.



Intelligent Capture is completely correlated to all live events and issues in the Client 360 dashboard, giving a real-time view of the network. You can go back to 5 hours to check the recent events for the selected client. It also gives the ability to run, download, and capture all events related to the client for information and visual graphics on client location, RF statistics, and wireless packet application analysis. Red dots in the Onboarding Events panel signify an issue that the administrator can investigate and troubleshoot. To see a particular time period of events, you can select and drag the start/stop pointers on the timeline to do so. Additionally, the location map can show if the client is connected to an AP that is too far, which could degrade service quality.

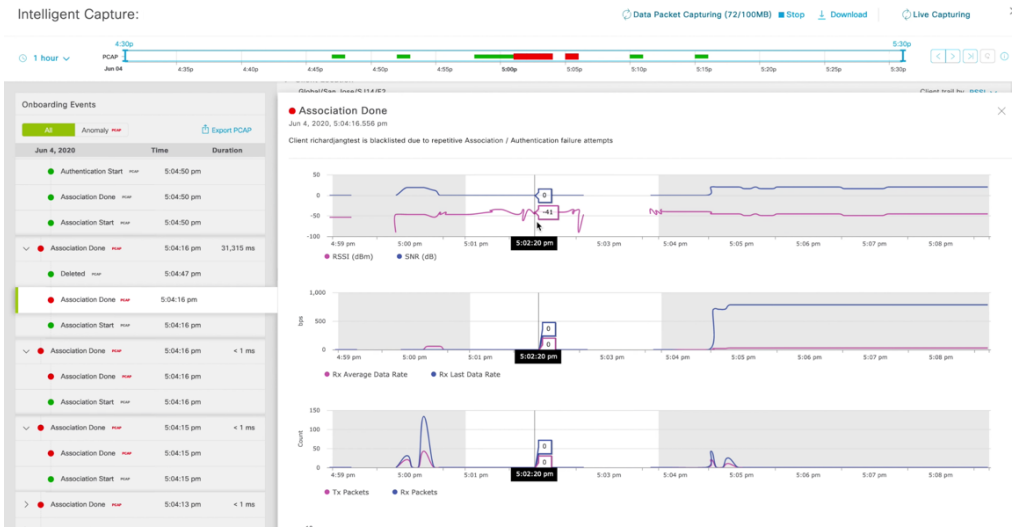
When diving into a specific event issue, a packet capture is indicated by “PCAP”. By clicking on this, the administrator can see the cause of the issue. For example, for a failed client association event the cause was “the client is blacklisted due to repetitive Association/Authentication failure attempts”. The administrator can also see a recorded replay view of location trail of the client with respect to nearby APs.

Cisco has a feature called the Auto Packet Analyzer. This allows the administrator to view all packet captures directly in the dashboard in a visual view. There is no need to export PCAPs to Wireshark, or other packet capture software, to view unless you choose to.



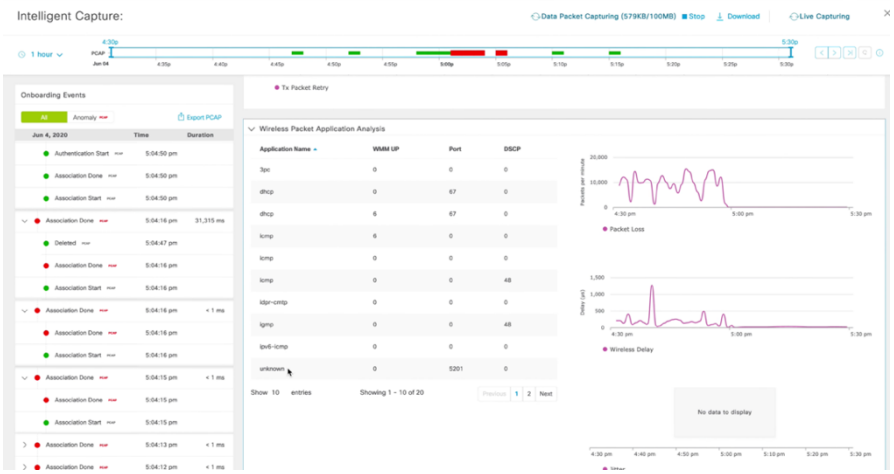
This view correlates and overlays multiple sets of data to pinpoint not just where, but how, the error occurred. The arrows indicate whether data came from the client (face up) or from the AP (face down). Any anomalies are highlighted in red. The green bar depicts the AP to which the client is connected. If the client roamed to another AP, a different colored bar will be shown to represent what packets are sent by which AP. This can correlate with another layer of data, and by clicking on it the administrator can see the issue and any associated AP.

Other data that can be correlated within Intelligent Capture are RF Statistics.



The white portion indicates when the issue took place. It correlates RSSI, SNR, data rates, Tx/Rx packets and Tx packet retry to help the administrator narrow down the problem. From the charts, it can be deduced that the client's poor SNR is the root cause of the client not able to associate to the Wi-Fi network. The client RF stats are captured for five-hour period but can also be captured live for real-time stats.

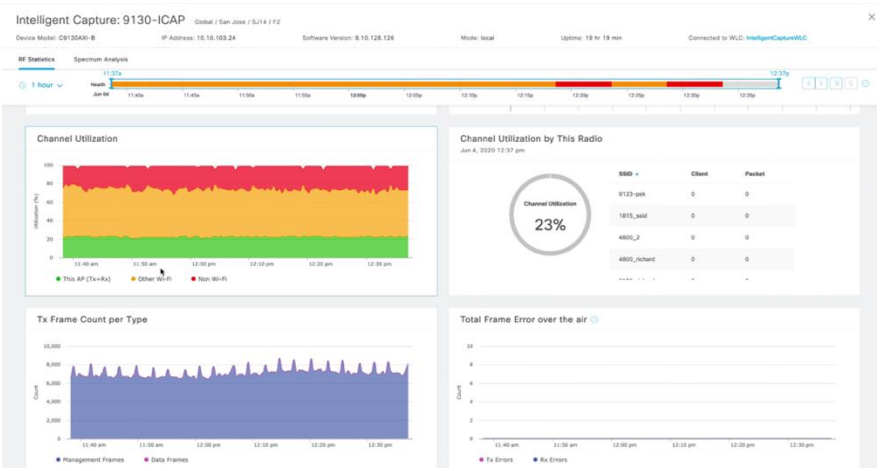
Integration with Cisco vNAM (Network Analyzer Module) gives an Intelligent Capture dashboard capability to list the client's applications and corresponding timeline charts (e.g., QoS settings, packet loss, wireless delay, and jitter).



Intelligent Capture is designed to provide real-time data and live packet capture for light troubleshooting that helps the administrator narrow down the root-cause of a client problem.

This same feature is available for AP devices in the Device 360 dashboard, as it was for clients in Client 360 interface. Like with a client, you can select a particular time period and see all contextual information corresponding to that timeline.

Details for the following are available: Client Count, Top Clients with Tx Failed Packets by SSID, Channel Utilization, Channel Utilization by This Radio, Tx Frame Count per Type, Total Frame Error over the air, Tx Power and Noise Floor, Multicast/Broadcast Counter.



In the Device 360 dashboard, next to RF Statistics, is the dashboard for Spectrum Analysis.

Without affecting the connected clients, the AP collects data to populate the Spectrum Analysis charts for Amplitude and Time per channel. This is shared with the Cisco DNA Center for advanced troubleshooting, as opposed to when this was only possible with separate software. Spectrum analysis can be viewed for 2.4 and 5-GHz bands.

Also included is the Interference and Duty Cycle Severity chart.

Combined with the Spectrum Analysis charts, this correlation can help minimize issues between AP and client.

How Aruba Compares?

Aruba uses on-premise as well as cloud-based Aruba Central tools for assurance. In this evaluation, we focused on the cloud-based Aruba Central AI Connectivity and AI Insight. In addition to the network assurance side, Aruba offers its User Experience Insight (Cape Networks) with sensor-based assurance for the user side. There is a basic level of integration between Aruba Central and User Experience Insight, but for advance troubleshooting, the administrator must go to the User Experience Insight dashboard.

The Aruba Central offers global, site, device and client views for assurance. Under the Global View, the AI Insights dashboard provides a look into any current issues (e.g., DHCP timeout failure) by giving a summary, event timeline, list of impacted devices.

Aruba Central offers client troubleshooting functionality, but it is scattered in different windows. There is a feature like Cisco's Intelligent Capture called Live Events in the site or client window. After selecting the client mac address, you can click Start Troubleshooting to see live events to be resolved. Unlike Cisco, it is real-time only; no previous events shown (e.g., last 3 hours). The Live Event also has provision of enabling the packet capture for a 15-minute window, but it does not do dynamic packet capture for failure events. Aruba Central also does not provide any pcap visualization tool.

The Go Live button in client detail page displays a real-time chart of received and sent throughput (bits/second) through the client device for 15 minutes, or until you manually click Stop Live. Under the Connectivity tab, Aruba displays a live view of throughput, roaming events and latency. The Location tab gives a map of the client, but there is no playback of client location tracing as Cisco does.

The Access Point page RF tab shows RF statistics in real-time or historical view, but there is no live spectrum analysis available.

How Mist Compares?

Under the Site, Client or Device, there is a live view of Insights, just like Cisco and Aruba. The Site Insights tab shows Total bytes graph, site events, details on connections (DHCP Latency, DNS Latency, Associated Clients, Tx/Rx Bytes) and other properties.

In the case of troubleshooting a client, the Client dashboard gives a bird's eye view of multiple metrics including location, a network time travel chart, RSSI chart, DHCP Latency, Tx/Rx Bytes, and a list of client events (e.g., authorization failure). Events are listed as green (good), orange (neutral), or red (bad) with corresponding and PCAP download button. An auto-PCAP recording feature is available for up to a week for failure events. Mist dashboard also has a separate packet capture tab to do a live packet capture. There is no ability to see a live view of PCAPs in the dashboard like Cisco, but it provides integration with CloudShark, an external PCAP analysis tool.

While there is no spectrum analysis available, Mist can show band utilization in the AP Insight tab. However, it does not provide a granular and real-time view of the RF environment. The other metrics shown in the AP Insight dashboard are network time travel chart, location, RF statistics, Associated Clients and AP properties.

5.3.4 Ecosystem Partnership

The customer is attempting to find the root-cause of a wireless client issue. They want to be sure that this problem is client-related, not network-related. There is a benefit to having partnerships with mobile manufacturers; integration can help make the troubleshooting process seamless. We look at three dashboards for this use case: Cisco DNA Center Client 360, Aruba Central Client Insight, Mist Marvis Client Insight.

Why is this important?

Being able to distinguish between a client and network related issue can save time troubleshooting – time that can be spent fixing other issues, reducing cost and downtime for maintenance as well as increasing business productivity.

The Cisco Advantage

Cisco is the only vendor that has a partnership with both Apple and Samsung, the two top-selling mobile manufacturers in the world.

Apple iOS Analytics

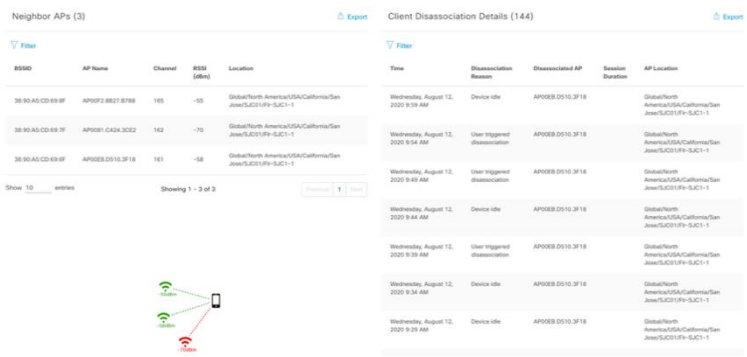
Among many other features that Apple and Cisco partnership offers, one of them is iOS Analytics. The data needed to accomplish this is provided by Apple – a company notorious for not easily sharing data, and there are no other current vendors besides Cisco given access to this information.

Apple Insights provides the client view of the network by providing the following for iPhone models 7 and newer, the iPad Pro and iOS 11:

1. **Device Profile:** Client details and support per-device/group policies and analytics
2. **Wi-Fi Analytics:** BSSID, RSSI, Channel # for insights into client view
3. **Assurance:** Error codes for clarity into connectivity reliability

If there is an issue with an Apple device, there are many ways to identify it. The administrator can find a device using the Assurance dashboard's list of client devices or by typing the device name in the search bar (e.g., by username). Both lead to the Client 360 dashboard, where all the user's clients are shown with a holistic view.

Apple iOS Analytics combines its data with Client 360 for a contextual analysis and detailed direction on how to identify and troubleshoot one or more problems. There you can see the Apple client view of the network such as Neighbor APs, Client Disassociation Details and more. This data comes exclusively from Apple device that gives the client perspective on the device issues that can be quickly resolved.



Samsung Analytics

Starting with IEEE 802.11ax, Cisco DNA Center Assurance works with Samsung for the client perspective of the network. Devices include the Samsung S10 and Note 9/10 and newer. Cisco provides adaptive IEEE 802.11r support, client-side error codes, Samsung Device AP Neighbor list support, Client 360 integration, and Client Event Viewer integration.

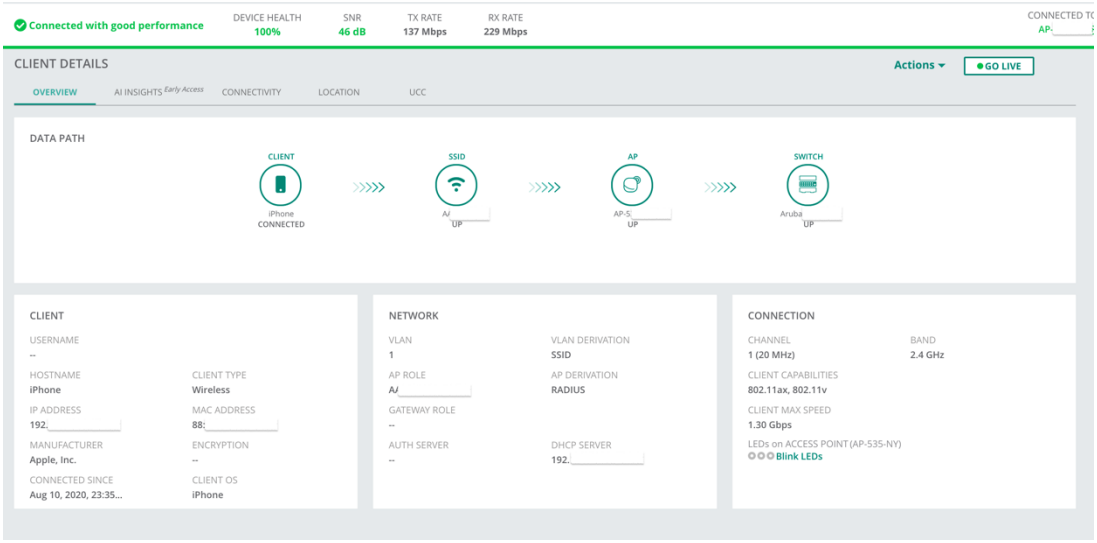
Samsung Analytics include:

1. **Client Classification:** device type, software OS, firmware version, transmission power
2. **Client Roaming:** Adaptive 11r (leverage authentication failures while roaming to root cause)
3. **Client Onboarding:** Client-side forensics (leverage client onboarding failures to root cause)
4. **Wi-Fi Coverage:** Client RF View (uses client's RF to draw coverage view)

Aruba Central Client Insight

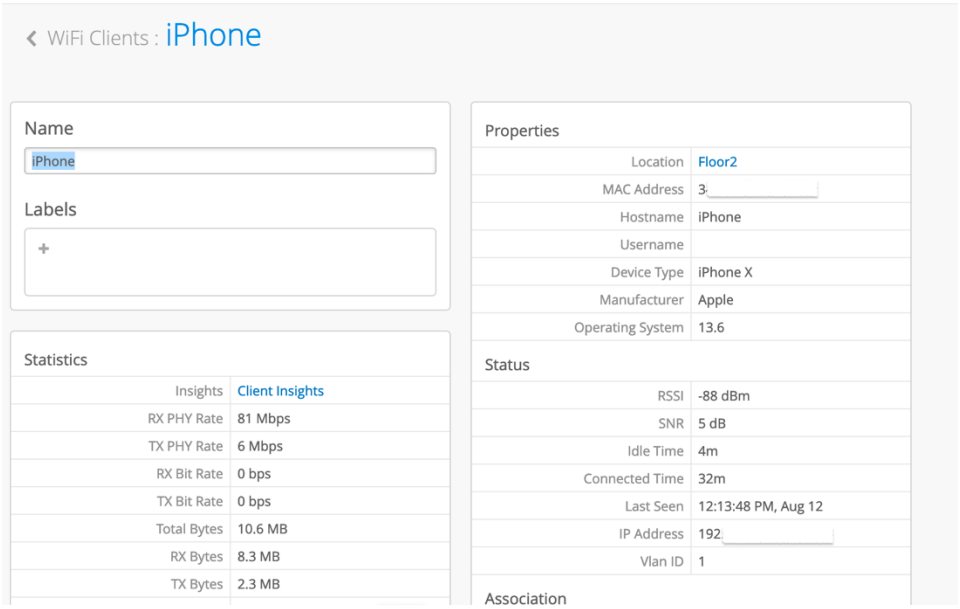
In the Client Dashboard, we selected an iPhone from the client list. The Client Details are listed for this device, but without the client side of view. Details are the same as in Section 5.3.1. This dashboard shows the data path, AI Insights, Connectivity, Location, client details, network and connection properties (e.g., channel, client Wi-Fi capabilities, band, maximum speed).

For Apple iPhone we saw the following properties:



Mist Marvis Client Insight

In the Client View, we selected an iPhone X client. It lists the Statistics (e.g., Client Insights, bit rate, total bytes), Properties (e.g., location, device type, OS), Status (e.g., RSSI, SNR, IP address), and Association (e.g., AP name, WLAN name, channel number, band). In this case, we saw the following:



While there is no client perspective as there was with Cisco, you can click on Client Insights to reveal information for a specific client. This has a timeline and list of events, list of application properties, and pre-connection/post-connection details as seen earlier in Section 5.3.1. Mist also offers Marvis Client SDK for android devices that sends additional client specific information to the Mist Cloud such as client RSSI value, roaming details (RSSI value of nearby APs), radio hardware, and radio firmware.

5.3.5 Power-over-Ethernet (PoE) Analytics

Traditionally, devices used power supplies or outlets to operate. With Power-over-Ethernet (PoE), these same devices can use Ethernet cabling for added benefits of a more flexible environment. Coupling power and data over the same cabling improves safety, simplifies installation and broadens the ability to power more device types.

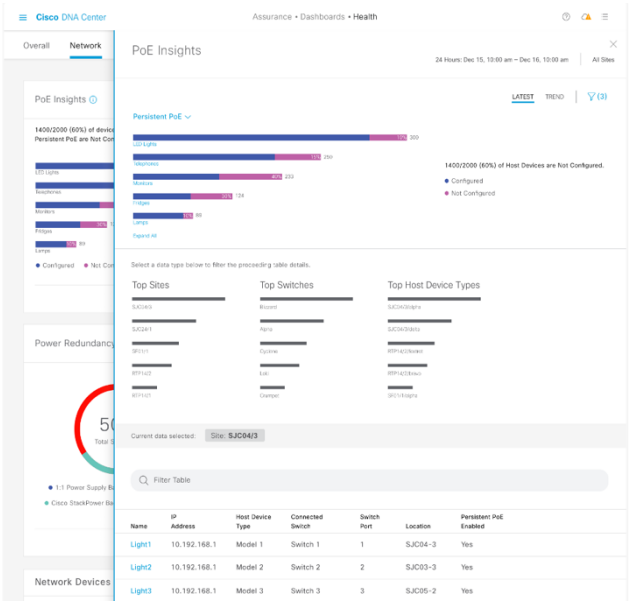
Using PoE is not enough; failures still occur. Administrators need to be able to automatically acquire PoE related data to troubleshoot devices. For this test, we evaluated the Cisco DNA Center Assurance dashboard, Aruba Central Switch Dashboard, and the Mist Switch Dashboard.

Why is this important?

Endpoint devices have PoE requirements such that if they fail to get power, PoE Analytics shows why they are not getting enough power. It helps plan the AP or IoT devices deployment on the switches for the best power distribution.

The Cisco Advantage

The Cisco DNA Center Assurance module has dedicated PoE Analytics dashlets, found under the Network Health tab. The PoE perspective shows operation state distribution, powered device distribution, PoE insights, and power load distribution. These properties are accompanied by visuals of the latest trends: pie charts (e.g., top locations, switch types, clients in faulty states), bar charts (e.g., clients in power range), PoE classification – Universal PoE (UPoE), PoE+, Perpetual PoE (PPoE) – and bar charts of switches on power load range with device list that takes you to Device 360 for troubleshooting.



How Aruba Compares?

There is no dedicated PoE dashboard available. To see the PoE status, power used, power remaining and denied ports, the administrator must go into the switch details. There are no issues displayed, so the root cause must be investigated manually.

How Mist Compares?

The switches dashboard shows few PoE stats: PoE Compliance, Total AP Power, Total Power Draw per switch PoE only for the AP devices. Unlike Cisco, it lacks advance statistic such as PoE endpoint power distribution, switches count distribution based on power budget, etc. However, its Switch Insight dashboard shows power draw per-port, switch port information, and power utility budget. Like Aruba, Mist requires manual investigation of PoE issues.

5.4 Business Continuity

5.4.1 Location Services for Back to Business

Location Services based on Wi-Fi and BLE technologies help customers to achieve many goals in their business. For example, the retail business can identify the customers' behavior visiting their store and increase their visits. Healthcare can track critical assets in their facility to save on time and work resources. Lastly, businesses can leverage insights and engagement toolkits in Cisco DNA Spaces to help the business to open their facilities for people.

Why is this important?

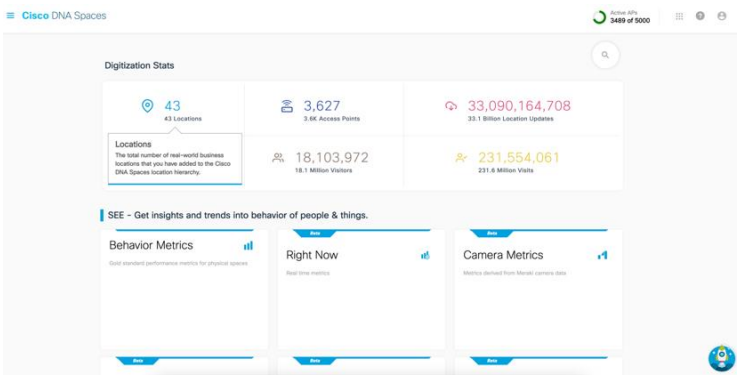
Location-based services are more relevant than ever in COVID-19 era. Many businesses are continually seeking ways to bring back employees or customers while following social distancing best practices. Contact tracing is one way that is used for healthcare, marketing, and quality of service analysis to help businesses better serve their customers and communities. It would be useful to set a threshold in Cisco DNA Spaces to know how many people are in the building and send alerts when a maximum number of allowed individuals has been reached.

The Cisco Advantage

Cisco DNA Spaces is a cloud-based location service platform that enables businesses to generate valuable insights extracted from users' location data and devices in a physical space. Based on these insights, Cisco DNA Spaces can deliver many use cases across various industry verticals.

Cisco DNA Spaces collects data globally – over 1 million live APs, more than 1 billion mobile devices, and over 2 trillion location updates. There are currently more than 140,000 locations worldwide that stream information that help DNA Spaces map the latest location-based trends.

Cisco DNA Spaces allows you to see your network and location, number of location/APs/updates, square footage, visitor count and visit count. The administrator can use Cisco DNA Spaces for performance metrics based on user data: visit duration, average visit frequency charts, repeat visitors, visitor distribution, and time/day/week of visits. These metrics are then benchmarked with the organization average and industry average to analyze the performance of the selected location.



Cisco DNA Spaces is paramount for business decisions across any industry and particularly useful for a pandemic, even like COVID-19. It has in-built applications with intuitive, helpful and aesthetically pleasing visuals for such a large amount of data. Cisco DNA Spaces provides specialized tools to cover all facets of back to business from monitoring to controlling the user density in a building. The real-time snapshot of users is beneficial for all organization departments – IT, sales, and marketing.

- **Right Now:** The Right Now App in Cisco DNA Spaces enables organization to monitor the number of Wi-Fi users entering the building and track them when they move from one area to another. Then density threshold can be set, and density rules can be applied per building, floor, or zone to maintain the appropriate number of people occupying the area.

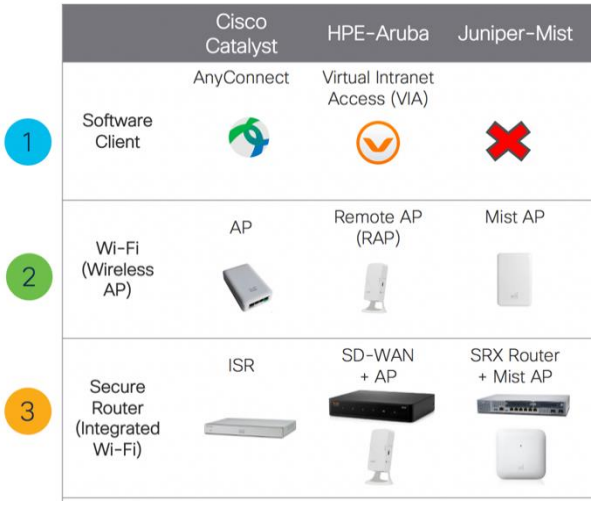
- **Proximity Reporting:** When an individual report positive for COVID-19, a Proximity Report can be generated to help trace the past movement of the user. The report includes the areas (building, floor, or zone) user had visited, the time individual had spent in each location, and the devices which shared the space with the contracted individual. It enables businesses to sanitize the locations and inform the individuals in proximity to the COVID-19 contracted individual.
- **Impact Analysis:** The Impact Analysis app offers an interactive tool to measure the impact of an event or a campaign on a business. An event can be created by selecting the location and the duration of the event to be measured. The selected duration can be compared with the average of the last 365 days or with the identical period before the selected event duration. The graphs are then generated, showing the increase or decrease in visit duration and visit count percentage compared to the selected options.

  Impact Analysis can be leveraged by business to evaluate the back to business policies by observing the visit and dwell time duration of the employees or customers at their locations.
- **Captive Portal:** The pre-built COVID-19 templates in Cisco DNA Spaces helps businesses to onboard the guest, employees and customers in their network. Administrator can design it to inform the users about the compliance rules placed in the building. Cisco DNA Spaces provides an intuitive step-by-step guide to set up the Captive Portal within 10 minutes.
- **Engagement Rules:** The Administrator can set the engagement rules to notify the users through SMS, email or chat. For example, a person entering a building can be notified if it is safe to enter the building or if the building has exceeded its maximum occupancy threshold.

5.4.2 Remote Worker

Work from home is one of the essential requirements that emerged in COVID-19 era. Since WFH has become a new normal, many companies have started embracing it and looking for ways to provide enterprise connectivity to employees at home keeping security and simplicity in mind. Remote connectivity is not a new concept and networking vendors have been offering it via various solutions such as VPN client, Remote Access Point, and WAN router for more than a decade.

In our evaluation, we compared the Cisco Catalyst 9800 Wireless Controller, Aruba Mobility Master Controller and the Mist Cloud to determine which is superior for remote office AP support.



5.4.2.1 Onboarding of Office Extend AP

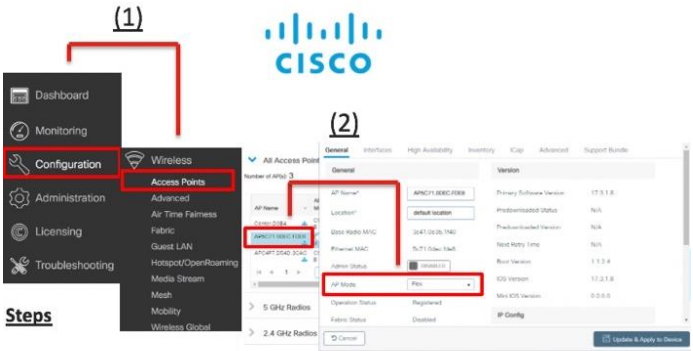
Why is this important?

In the current case of COVID-19, workers need to be able to work from home as easily as they would from the office. The easier it is to add a teleworker access point to the network, the quicker users can continue working – reducing downtime and cost.

The Cisco Advantage

In the Cisco Catalyst 9800 wireless controller dashboard, we simply navigate to Wireless Setup page. The page presents a guided workflow to configure the wireless network. To configure teleworker AP, we selected Flex Profile tab and checked Office Extend AP (OEAP) radio button in 'default-flex-profile' profile. Next, we selected site tag called 'default-site-tag' and assigned default-flex-profile under its Flex Profile drop menu.

Once the new AP joins the controller, we went to Configuration/Wireless/Access Points the final one-step deployment phase. We selected Flex under the AP Mode drop menu and switched Admin Status to enabled. With a single click this was applied, and the RAP was set up. No AP reboot was required.



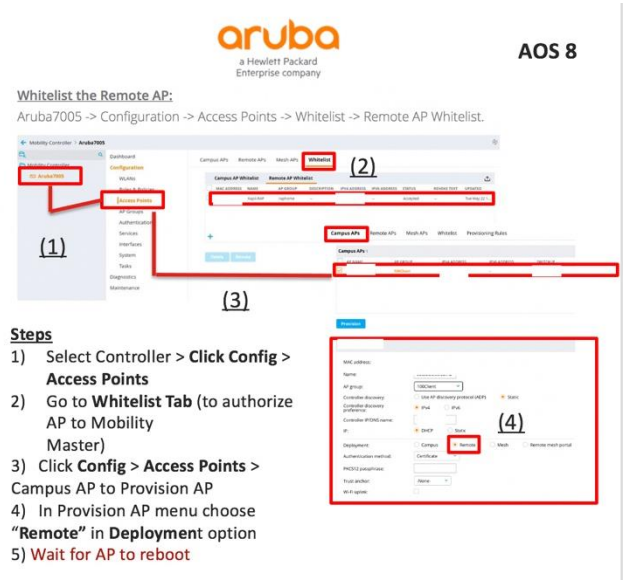
1) Once AP joins controller go to **Configuration > Access Points**
2) Select AP from list and under General select AP mode to "Flex"

How Aruba Compares?

A Controller Cluster RAP Pool must be created in the Mobility Master Interface, which populates in the Mobility Master/Configuration/Services section. Next, you create an AP Group or choose default AP group to assign the RAP via the per-site controller configuration. Then, you create an SSID for the AP Group under the site controller's WLAN configuration tab.

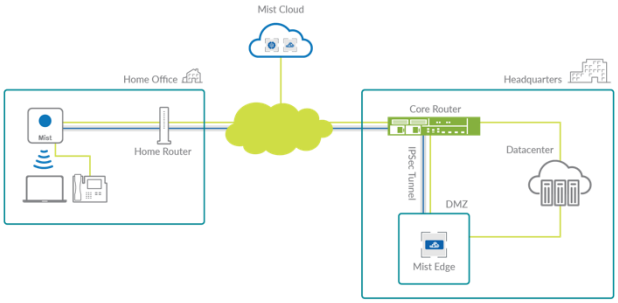
To provision the AP, you must find the AP under the site controller configuration's AP whitelist. Most APs are in standard campus mode by default. It must be ensured that the Campus AP is approved in the whitelist. The AP must be assigned to the appropriate Remote AP group under the AP Group drop menu, and Remote must be selected under the Deployment option section. Applying this configuration reboots the AP and takes time to reboot from Campus to Remote mode.

Each step requires time and a learning curve to accomplish, especially for those who are not technologically strong. There are many steps that must be followed in Mobility Master to onboard a RAP, which becomes confusing. This is not user-friendly for the typical employee attempting to set up an AP to use from home.



How Mist Compares?

Mist is cloud-based only, so the setup is different as Mist APs does not required to be converted into Remote AP mode. Mist Cloud uses its "Enterprise at Home" Wi-Fi Teleworker Solution through the Mist AP and Mist Edge appliance for scalable, distributable services. Network administrator can extend the enterprise Wi-Fi to home by creating IP Sec tunnel from Mist AP at home office to Mist Edge appliance at main office.



Source: Mist

5.4.2.2 Creating and Managing Personal SSID

When working at home office, the Teleworker AP can also be used to broadcast both the enterprise SSID and personal SSID at home or personal office.

Why is this important?

The enterprise user working from home should get the same enterprise-level connectivity, security and Quality of Service (QoS) as they get in their office. Meanwhile, the employee's personal devices can connect to the internet using the same teleworker AP but on a separate network.

The Cisco Advantage

The home user can configure Cisco OEAP to broadcast personal SSID that allows multiple devices to connect to the office network or personal network via the same OEAP. No additional home router required. For example, a user can connect a VoIP phone with the same QoS as a user in-office. Any other users (e.g., spouse, roommate) can join the network and enjoy the benefit. This feature comes out-of-box for a Plug-n-Play enterprise network experience from home. Neither Aruba nor Mist offers this functionality.

5.5 Solution Summary

5.1 RF Interference Protection	
Non-Wi-Fi Detection and Mitigation	Cisco Access Point and Wireless Controller detected the most non-Wi-Fi interferers.
5.2 Network Operations	
Onboarding new access points without downtime	Cisco AP Device Pack can be applied to the controller to add new access points model without requiring reboot. Mist can also add new APs without network disruption. Aruba Controller requires full software upgrade and a reboot.
Fixing bugs in the existing APs	Cisco AP Service Pack ensures software patches are only applied to APs with bugs to avoid downtime. No wireless controller upgrades or reboot is needed. Aruba controller requires full upgrade and reboot.
AP Refresh from old to new generation	Cisco DNA Center's AP Refresh Workflow makes device swapping easy. Mist and Aruba does not offer any such workflow.
ISSU	Cisco's rolling AP upgrade avoids outages by using intelligent channel allocation and percentage-based selections. Aruba and Mist require network downtime, but Cisco does not.
AP RMA	Cisco DNA Center makes faulty AP replacement with the new AP user-friendly through guided workflow. Mist and Aruba offers no such workflow.
5.3 Network Assurance	
Wi-Fi 6 Dashboard	Cisco DNA Center has a dedicated Wi-Fi 6 Dashboard for contextual and visual insight of Wi-Fi 6 clients, readiness, distribution, efficiency, and latency for global or local perspectives. Enterprises can decide to add Wi-Fi 6 Access points and visualize benefits of Wi-Fi 6 network. Neither Aruba nor Mist have a dedicated Wi-Fi 6 Dashboard, but other dashboards available to find the information Cisco displays in a single-pane-of-glass view.
Artificial Intelligence/Machine Learning	Cisco AI Network Analytics is an AI-driven, automated model for baselining, anomaly detection, proactive insights, comparative benchmarking, and network heatmap with high-accuracy detection and accelerated remediation options. Aruba Central AI Insight shows AI-driven issues with baseline visual but lacks proactive insights, AP comparison, dedicated peer and site comparison dashboard for predictive analysis of the network. Mist provides AI-driven baselines for specific properties, but only for connectivity issues. Insight for Mist must be acquired manually, adding time and cost to the troubleshooting process.
Troubleshooting Client Failure	Cisco DNA Center's Intelligent Packet Capture has a live, visual Event Viewer for client tracing, automated anomaly and full packet capture (PCAP) capabilities using data correlated from the AP, wireless controller and Cisco DNA Center. PCAPS can be viewed live or downloaded. The Client 360 Dashboard shows client health scores, properties, statistics and trends. Cisco's Device 360 Dashboard has Spectrum Analysis for advanced troubleshooting on 2.4 and 5-GHz bands. Aruba offers dedicated dashboard for client failure troubleshooting with live events, but it does not offer a dynamic PCAP file. While offering consolidate PCAP capabilities, there is no visual view in the dashboard and is for a specific window only, with no historical view like Cisco. Mist offers a live view of Insights with graphs, details and dynamic PCAP. However, it lacks real-time view of the RF environment.
Ecosystem Partnership	Cisco has partnerships with Apple and Samsung for a client-based, contextual view of the network. Aruba and Mist provide details on Apple and Samsung products, but not to the level of detail that Cisco does or through the client-side view.

PoE Analytics	Cisco's DNA Center Assurance module has a dedicated dashboard for the PoE perspective – showing visuals of the latest trends that help troubleshoot power-related issues. There is no dedicated PoE dashboard for Aruba or Mist; root causes must be investigated manually.
5.4 Business Continuity	
Back to Business with Cisco DNA Spaces	Cisco DNA Spaces is paramount for business decisions regarding pandemic situations like COVID-19, where a real-time snapshot of client locations is beneficial for IT, sales and marketing. It offers a slew of native and custom-build applications for the businesses to bring employees or customers to the physical space safely. Cisco DNA Spaces collects data from over 1 million APs, one billion mobile devices and 2 trillion location updates for the latest location-based trends.
Remote Worker	Cisco's Office Extend AP (OEAP) feature enables APs to work in remote mode – perfect for today's current remote-work situations. Aruba requires to touch many tabs for remote AP configuration; it is not user-friendly. Mist is cloud-based. It is "Enterprise at Home" Teleworker Solution uses a Mist AP and Mist Edge appliance. Unlike Cisco, both Aruba and Mist do not provide creation and control of personal SSID by the employee.

6.0 Conclusion

Cisco emerged as the best the vendor in all the areas of the network evaluation: Wi-Fi 6 Performance, Network Operations, and Network Assurance.

In Wi-Fi 6 Performance, Cisco consistently outperformed the other vendors. In high-density mix-client environment, Cisco 9100 series access points displayed the best performance in each access point category. The Cisco Access Points also proved to be the most power-efficient by consuming the least POE power. Cisco 9130 AP was able to simultaneously stream video successfully to more clients than any other vendor. One of the most significant benefits of Wi-Fi 6 technology is the improvement in reliability of latency-sensitive applications which was clearly demonstrated in the test comparing the voice call performance of Wi-Fi 6 with Wi-Fi 5.

Network Operations refers to the activities required to deploy, maintain and optimize the network. Cisco Catalyst 9800 controller provides a suite of features such as AP Service Pack, AP Device Packs, Rolling AP Upgrade to efficiently fix the device bugs or upgrade the wireless network with minimum disruption. Cisco DNA Center's intuitive workflows make it easy for an administrator to deploy new access points in the network. Aruba lacks in many of these features. Mist supports adding new APs or fixing bugs without disruption but upgrading new access points require network downtime.

To monitor and troubleshoot network, Cisco offers an array of intuitive tools. Cisco unique Wi-Fi 6 dashboard helps in planning upgrade to Wi-Fi 6 Network and realizing the benefits of Wi-Fi 6 technology. Cisco AI Network Analytics displays network issues derived from an abnormality in the network from normal baseline using AI and Machine Learning. While Aruba and Mist also provide AI/ML-based issues, they lack proactive insights to prevent future issues. Cisco Intelligent Capture gives a single pane view for troubleshooting client problems by displaying past and real-time events with PCAP visualization for detailed but straightforward analysis. Aruba and Mist offer client troubleshooting but requires touching multiple points to get to the root of the problem.

7.0 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.

8.0 Use of This Report

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

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

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.

By downloading, circulating or using this report this report in any way you agree to Miercom's Terms of Use. For full disclosure of Miercom's terms, visit: https://miercom.com/tou.