Enterprise Wi-Fi Stress Test

Cloud-managed 802.11ax (Wi-Fi 6) Access Points

MARCH 2021

Rowell Dionicio, CWNE #210
rowell@packet6.com

Executive Summary

The cloud has transformed businesses in more ways than we can count; and Wi-Fi infrastructure is at an inflection point. Network performance is more important than ever as IT copes with increasing demands, in particular for prioritized voice and video traffic. Many organizations are also considering the added benefits of network analytics using artificial intelligence (AI) and machine learning (ML) to gauge the end-user experience and Wi-Fi performance.

This report details the performance attributes of cloud-managed 802.11ax (Wi-Fi 6) access points (APs) in a high-density and high-capacity environment with a mix of video, VoIP, and data traffic. The intent is to test cloud-managed enterprise AP performance under a real-world scenario that is relevant to most enterprise networks today.

According to the Global Economic Value of Wi-Fi report, the Wi-Fi Alliance estimates the global value of Wi-Fi at $3.3 trillion in 2021[1]. Enterprises are leveraging Wi-Fi to support new and innovative use cases while Wi-Fi 6 continues to gain market adoption at a rapid pace.

Video applications and other multimedia services will be the largest consumers of bandwidth on Wi-Fi networks. For example, in a survey conducted by Education Week Research Center, 71% of teachers viewed Wi-Fi as a technological innovation significantly improving teaching and learning[2].

CommScope RUCKUS ("RUCKUS") sponsored this test, procured the equipment, and conducted the tests outlined in this report. The author observed the test, validated the configuration, and ensured a level playing field for each tested vendor. The author performed the troubleshooting and analytics test with RUCKUS personnel observing. RUCKUS maintained a fair and neutral testing environment, as required by the author as a condition for writing this report.

About the author

Rowell Dionicio, CWNE #210, is the Founder and Managing Director of Packet6, a company with a framework for implementing Wi-Fi that is simple, seamless, and reliable. Rowell has 15+ years of experience in IT and specializes in Wi-Fi technologies. Rowell is the co-host of a Wi-Fi focused podcast, Clear To Send, which publishes weekly technical content for the purpose of educating IT operators on Wi-Fi topics.

[1] Wi-Fi Alliance: Global Economic Value of Wi-Fi 2021-2025
[2] Education Week Research Center: Teachers and Ed-Tech Innovation. Results of a National Survey

Test Methodology

Why this test is important

Wi-Fi continues to be the most widely used method of access network connectivity. Enterprises are leveraging mobile devices with real-time, low-latency applications; and mission-critical applications need reliable, high-performing Wi-Fi. In hotels, guests are joining video conferences in their rooms and rely on a stable Wi-Fi network. In the classroom, laptops and tablet devices consume multimedia for instructional purposes.

Video use and video traffic volume is increasing alongside data and VoIP, it is imperative to understand the impact of network loading on end-user experience for all of these applications.

The objective of this test was two-fold: (1) Establish the performance level of each vendor's access point (AP); (2) assess how well the vendor's corresponding cloud solution can help the information technology (IT) team minimize the mean time to identify (MTTI) an issue.

Those objectives are evaluated in a high-density, high-capacity environment in which cloud-managed enterprise APs must provide reliable service to the associated devices. In cases of network failures of any kind, IT operators should be able to quickly and reliably identify root cause.

Many organizations are migrating away from on-premises controller appliances to public cloud-based control and management. This test reveals how each cloud solution stands up to today's requirements.

About the test

The results in this report are drawn from two tests—one measuring AP performance and a second assessing troubleshooting and analytics capabilities of each vendor's enterprise cloud platform. A range of 4x4:4 Wi-Fi 6 APs was selected and tested against a high-density and high-capacity scenario similar to that found in real-world deployments.

Thirty (30) Dell Latitude 5400 laptops with Wi-Fi 6 capability were used to play a high-definition (1080p HD) video in a single room. The Dell laptops include the Intel AX200 Wi-Fi chipset, a configuration available for purchase at the time of this test. Each Dell laptop played a unicast HD video stream before, during, and after the test.

Co-located with the Dell laptops were five (5) Apple iPads running a bi-directional Voice-over-IP (VoIP) test to simulate a VoIP conversation. The iPads ran this test using an IxChariot client configured with the G.711u codec. The G.711u codec is one of the most widely used voice codecs in VoIP deployments and is supported by nearly all VoIP devices and providers. Five additional iPads running an IxChariot client conducted data downloads, as described in the following paragraph.

In an adjacent room, associated to the same access point, were twenty (20) Apple MacBook Pros each running an IxChariot client. A UDP download of varying data sizes was used to simulate random downloads such as web browsing, email, and file transfer.

The signal traversed a false ceiling and two walls consisting of wood framing and ½-inch sheetrock.

Each AP was tested for throughput and other performance metrics using an 80 MHz-wide channel. While the author does not recommend routinely configuring production APs to use 80 MHz-wide channels, in this case it was required in order to realize the maximum performance of each AP. With that said, many network administrators can and will use 80 MHz-wide channels given the opportunity, so this is not an unlikely scenario.

The following table summarizes the traffic types used in the performance portion of this test.

Video	VoIP	Data
High definition	G.711u codec	UDP download
1920x1080	Bi-directional	64/256/512/1460 bytes
30 clients	5 clients	25 clients
QoS - DSCP 40	QoS - DSCP 46	QoS - Best effort

Table 1. Traffic types used

Access points tested

The performance test evaluated cloud-managed 802.11ax (Wi-Fi 6) access points from HPE Aruba (“Aruba”), Extreme Networks (“Extreme”), Juniper Mist (“Mist”), Cisco Meraki (“Meraki”) and RUCKUS. Each Wi-Fi 6 AP selected has similar hardware specifications and is designed to support high-density environments.

	Aruba	Extreme	Mist	Meraki	RUCKUS
AP Model	AP535	AP650*	AP43	MR46	R750
Cloud Release	2.5.2-922-P	21.1.22.2	0.6.18841	27.5.1	20.11.11
AP Firmware	8.7.1.1_78245	10.3r1 build-254243	0.6.18841	27.5.1	5.2.1.1051
MIMO	4x4:4	4x4:4	4x4:4	4x4:4	4x4:4
Ethernet	5 Gbps	2.5 Gbps	2.5 Gbps	2.5 Gbps	2.5 Gbps

*Note: Also known as AP510C

Table 2. Access points tested

Test environment

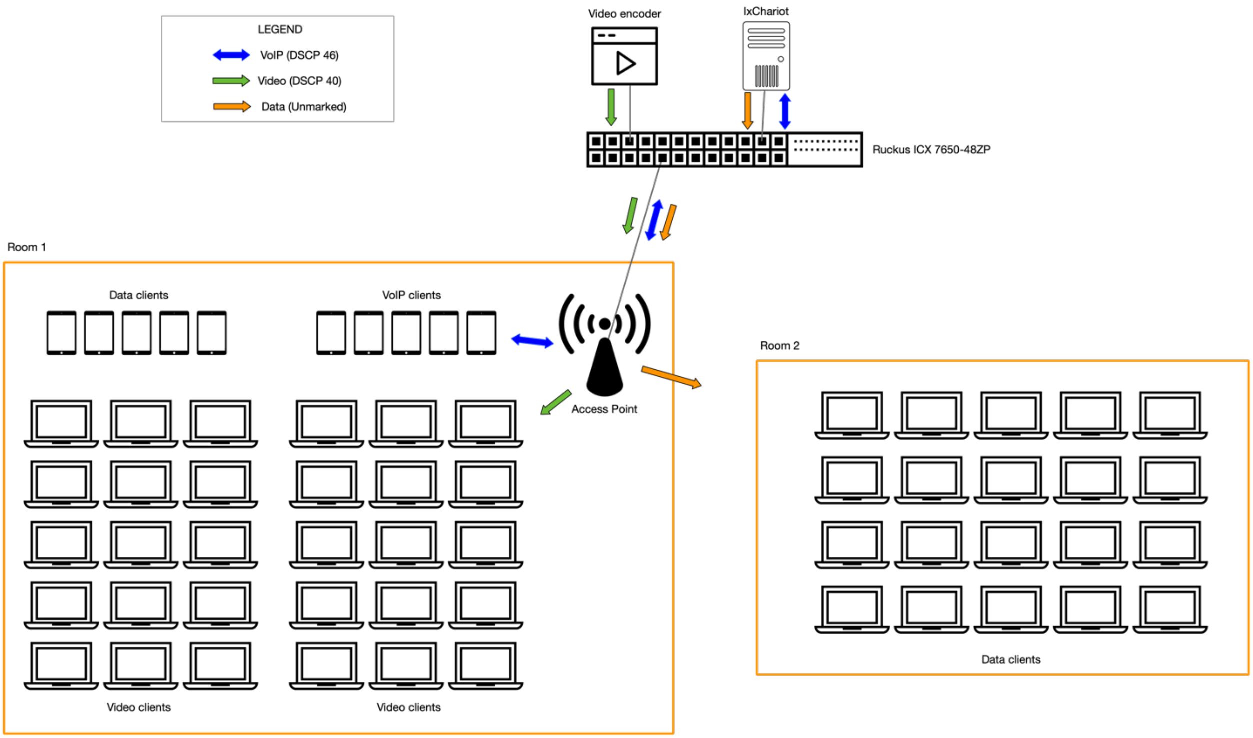

Figure 1. Test network diagram and traffic flows

Client Types

Each test used the clients listed in Table 3. The goal of having a client mix is to simulate a real-world environment comprised of Wi-Fi 6, Wi-Fi 5, and mobile devices. A total of 60 clients was used in this test.

Client	Quantity	Capability	Test
Dell Latitude 5400 (Video client)	30	Intel AX200 (Wi-Fi 6) 2x2	HD Video
Apple MacBook Pro, 2015 model (Data client)	20	Wi-Fi 5 3x3	Data download
Apple iPad (Data client)	5	Wi-Fi 5 2x2	Data download
Apple iPad (VoIP client)	5	Wi-Fi 5 2x2	VoIP

Table 3. Client types

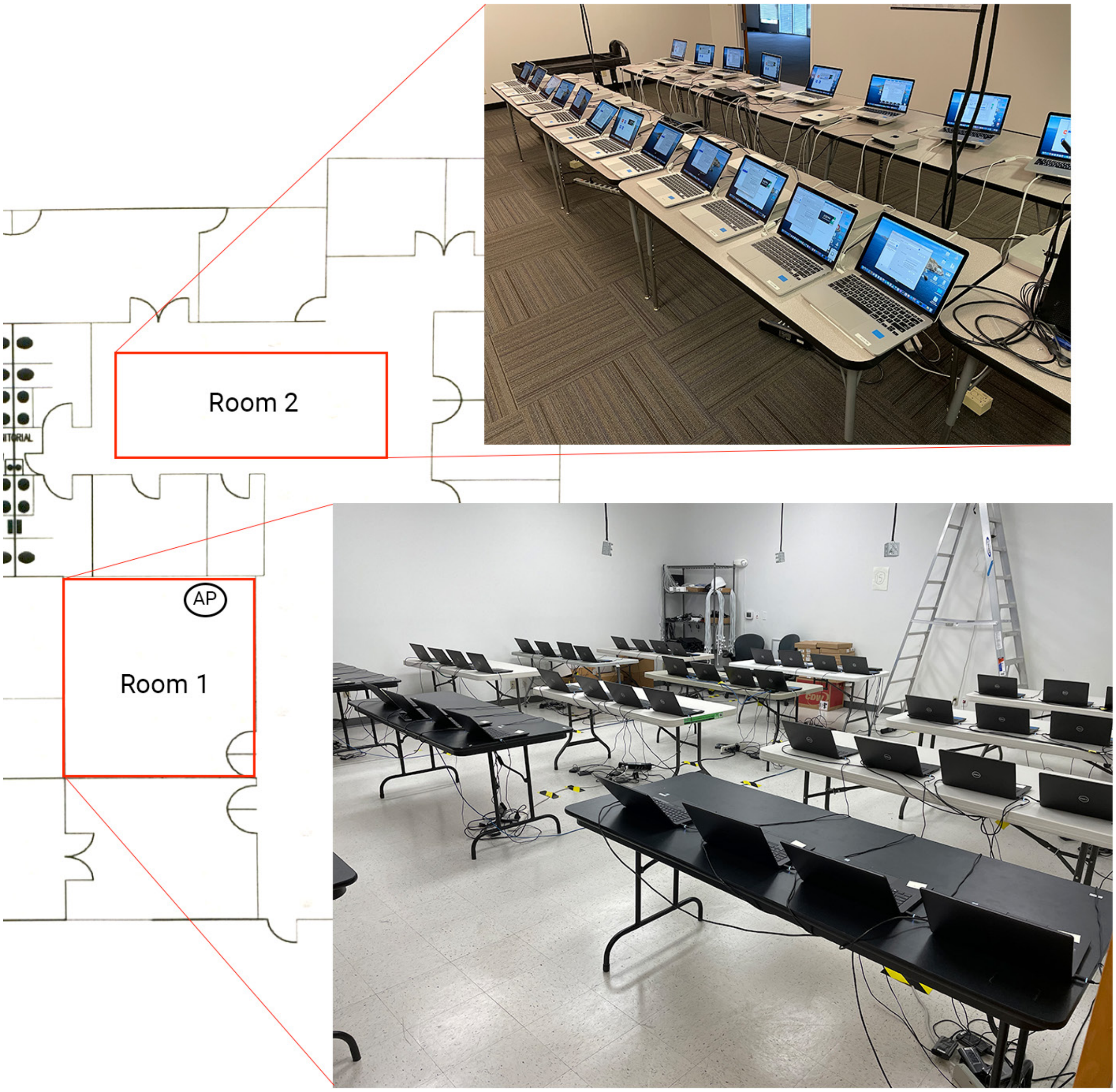

Figure 2. Test environment

WLAN configuration

Each AP used the out-of-the-box default settings, similar to what an IT administrator would see upon deployment. Each test was run on the 5 GHz band in UNII-3 to ensure consistent results. For Test 1, a single SSID was configured using WPA2-PSK encryption. For Test 2, three SSIDs were configured on each AP. Two SSIDs used a pre-shared key and the third SSID was configured for 802.1X.

Each SSID was configured using an 80 MHz-wide channel.

Switch configuration

A RUCKUS ICX 7650-48ZP switch provided Power-over-Ethernet (PoE) to the APs, each of which was connected to a multigigabit Ethernet port and auto-negotiated to full speed. Each AP received full power according to its requirements. The switch was configured to place all devices on the same virtual LAN (VLAN). This eliminated the need for routing.

An IP access list for the video encoder was configured for the VLAN in order to mark the video stream with a Differentiated Services Code Point (DSCP) of 40.

Video stream configuration

To test HD video, a DVD player was connected to a video encoder to provide HTTP Live Stream (HLS) capability for the Dell laptops (video clients). This allowed an individual unicast HD video stream to be downloaded by each video client.

The settings for the video encoder are outlined in Table 4.

Input Size	1920x1080p @ 60 fps
Input Audio Sample Rate	48000
Output Encoding Type	H.264
Output Encoded Size	1920x1080 @ 60 fps
Output Bitrate (kbit)	8000
Output Multicast URL	Disabled

Table 4. Video encoder settings

Test 1 - Multimedia

The purpose of this test was to apply a high-density and high-capacity scenario for each AP. In one room, there were thirty (30) Dell Latitude 5400 laptops playing an HD video and ten (10) iPads, five of which were running a bidirectional VoIP call and five of which were downloading UDP data. The AP was mounted on the ceiling T-Bar in the back of the room to maximize coverage across both rooms. Video streams were initiated on the Dell Latitude laptops before the test began and played non-stop during the test.

In the next room, as outlined in Figure 2, twenty (20) Apple MacBook Pros were running UDP data downloads. These downloads consisted of packets of 64, 256, 512 and1460 bytes to simulate different types of data traffic.

Two (2) test runs were performed with a duration of 3 minutes per run.

Before the Test →

Each video client is playing an HD video. Stalled videos are restarted and if continue to stall, is noted.

During the Test →

While each video client is playing an HD video, data and VoIP test is initiated. The test is run for 3 min.

After the Test →

Once the data and VoIP test is complete, we take note of any stalled video clients.

Maintaining expected Quality of Service (QoS) is an important criterion in this test. Video traffic from the encoder was marked with DSCP 40 on the switch port. VoIP traffic was marked with DSCP 46 from the IxChariot server and the IxChariot clients (iPads). The reason for the DSCP markings is to provide the correct forwarding for special traffic that may require low latency, loss, and jitter. This ensured each vendor had the opportunity to prioritize traffic based on QoS markings. No QoS parameters were configured on the WLAN.

Success Criteria

Each AP must successfully deliver stall-free video streams to all 30 Dell laptops before starting the test. If a stalled video is encountered prior to the test, the stream is refreshed on the video client and documented if it continues to stall. During the test, the AP must deliver high-quality video, data, and VoIP traffic simultaneously to all clients.

The implied user experience associated with the video clients is measured by visually inspecting for videos that stalled for 20 seconds or longer. This is a conservative estimate of implied user experience but one that is easy to accurately assess. Data and VoIP metrics are collected by

IxChariot. Total throughput is collected for the data clients. The voice mean opinion score (MOS) is determined based on jitter, latency, and packet loss collected from the VoIP clients. Airtime utilization is documented using the WiFi Explorer application.

Average throughput, MOS and the number of non-stalled video clients are compared for each AP.

Test 1 - Results

Throughput
Throughput is a common metric used to evaluate the performance of access points. During the test, we measured and averaged the throughput of the data clients, using IxChariot, and the video clients, as measured at the switchport where the video encoder is connected. Two test runs were conducted. Figure 3 indicates the sum of the throughput values associated with the video and data clients, averaged over the two test runs.

In general, a higher throughput number is better as long as data is not favored at the expense of higher priority traffic (voice and video).

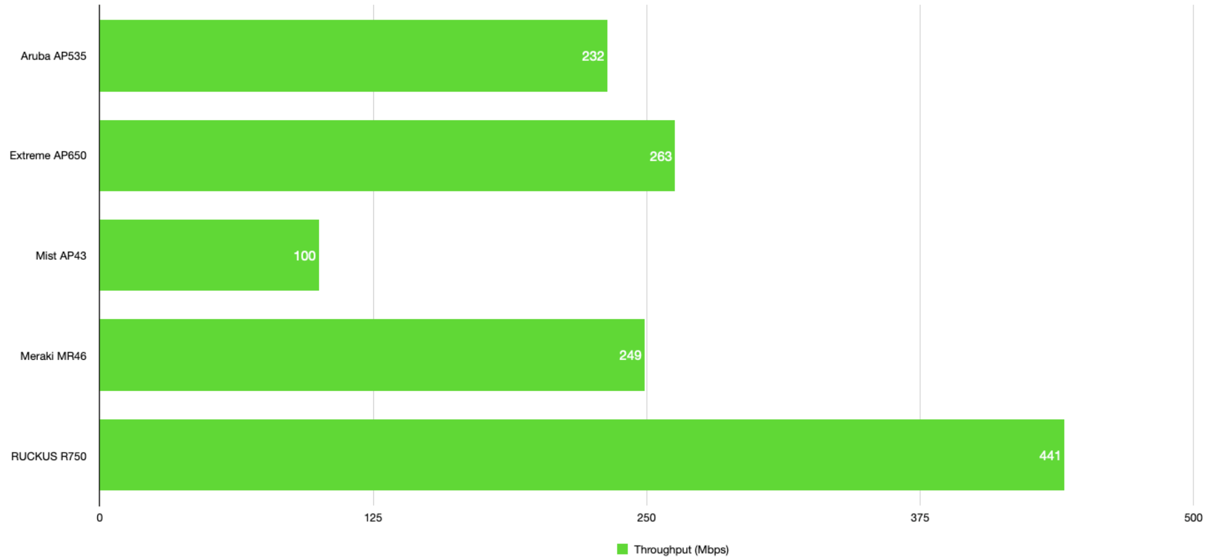

Figure 3. Throughput in Mbps

The RUCKUS R750 significantly outperformed every other AP on the throughput metric.

MOS
MOS is a measure of VoIP call quality. A lower score can mean users will experience poor call quality. An AP with a network load or one that does not correctly prioritize voice traffic may not be able to maintain an adequate MOS, as perceived by users. MOS is a function of jitter, latency, and packet loss. The following table shows how MOS is commonly indexed against user-perceived voice quality.

Mean Opinion Score	Quality
5	Excellent
4	Good
3	Fair
2	Poor
1	Bad

Table 5. MOS and perceived voice quality

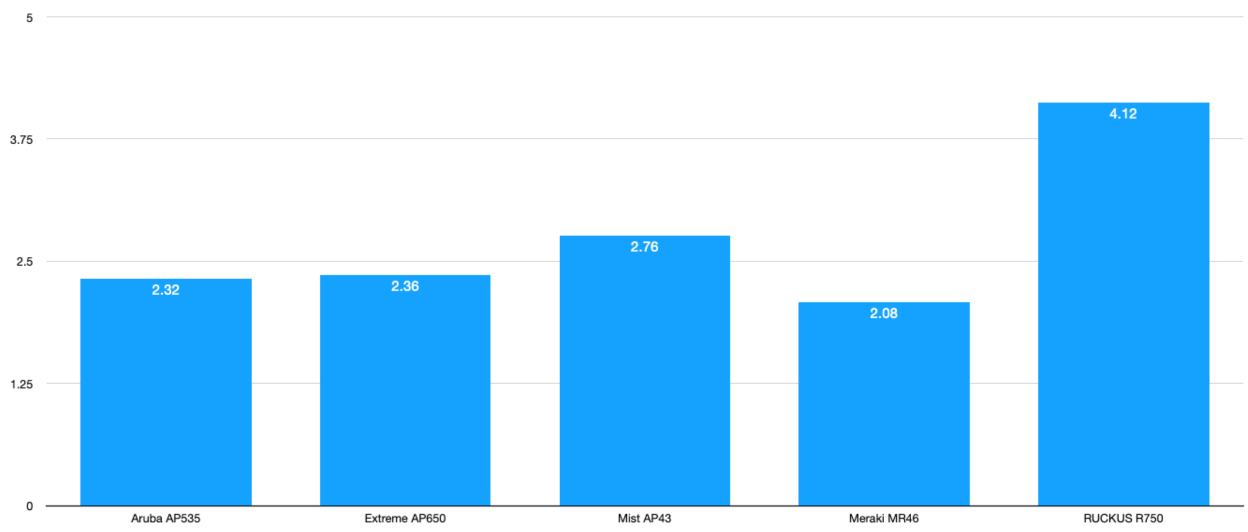

Figure 4. MOS results

The RUCKUS R750 outperformed all other APs on the MOS metric, providing significantly higher call quality under heavy network load. More specifically, no APs other than the RUCKUS R750 supported a MOS value that would meet typical enterprise service level agreements (SLAs) requiring “good” voice quality.

Streaming Video

Video traffic is the most widely used multimedia format over Wi-Fi. An AP can simultaneously serve clients in various multimedia formats. Using HTTP Live Streaming (HLS), video clients can cache up to 10 seconds of data.

In this scenario, HD video clients were playing a unicast HLS video stream prior to starting the test. Testers took note of any video clients with stalled video, refreshed their video stream, and confirmed the video was playing before the test was initiated. This was done to give each vendor an opportunity to get all video streams running simultaneously prior to test initiation, a state that the test conductors were able to achieve for all but one vendor (Mist).

The table below shows the number of non-stalled video streams for each AP before, during, and after the test. A lower number indicates more stalled video streams leading to a poor end user experience.

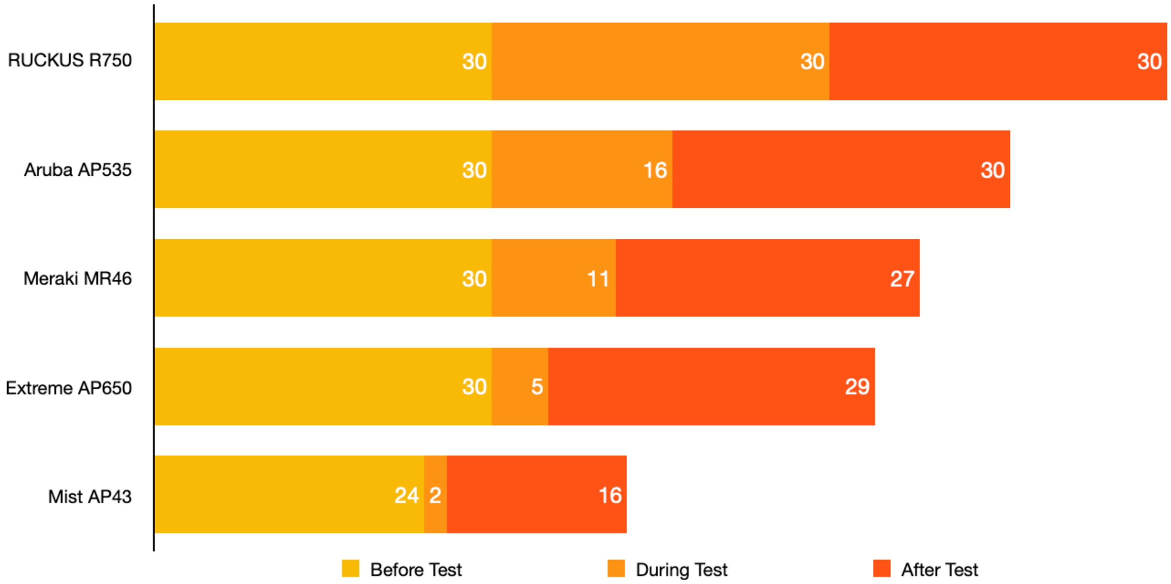

Figure 5. Number of non-stalled videos before, during, and after the test

The RUCKUS R750 outperformed all other APs, providing continuously streaming HD video to each video client before, during and after the test period.

The Mist AP43 started with only 24 video streams. Test conductors attempted but, after several tries, were unable to refresh all stalled video streams prior to starting the test.

Airtime Utilization

Establishing airtime utilization performance was not a test objective, however, airtime utilization is a useful metric for better understanding the impact of radio frequency (RF) capacity on the end-user experience. Therefore, a brief discussion is included here. In general, lower airtime utilization is better, assuming an AP is able to successfully handle all traffic (voice, video, data). Lower airtime utilization is desirable because it allows the AP to more easily accommodate additional connected devices and traffic.

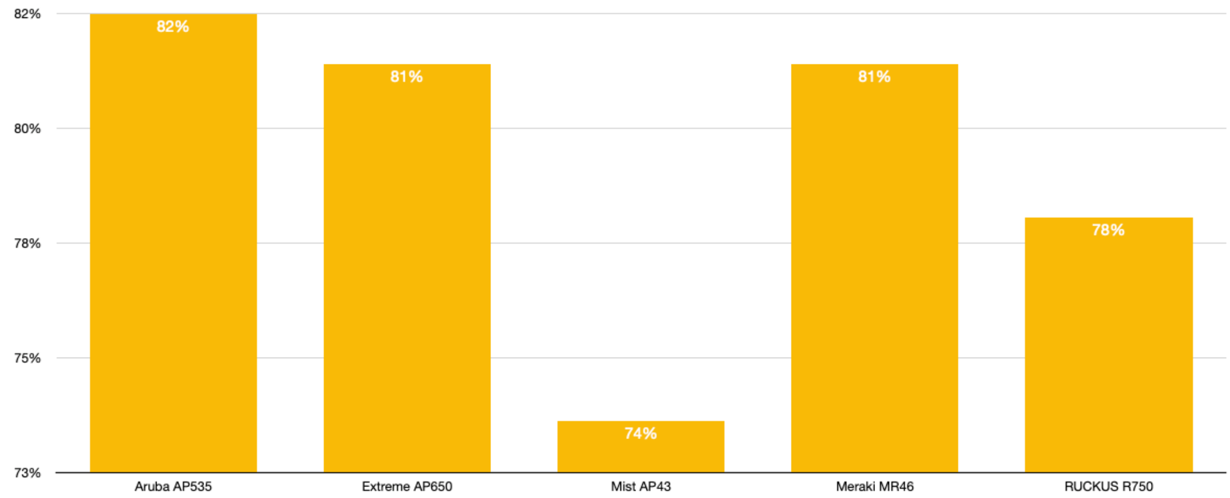

Figure 6. Airtime utilization during test

As was the case with the video stalling results, the demonstrated airtime utilization of Mist AP43 stands out as lower than that of the other APs. The author concludes that the relatively low utilization is due to the high number of stalled video clients during the test. Because the video clients were not playing any video, there was less over-the-air traffic.

We can correlate the number of video clients with stalled video and airtime utilization during the test as shown in Figure 7.

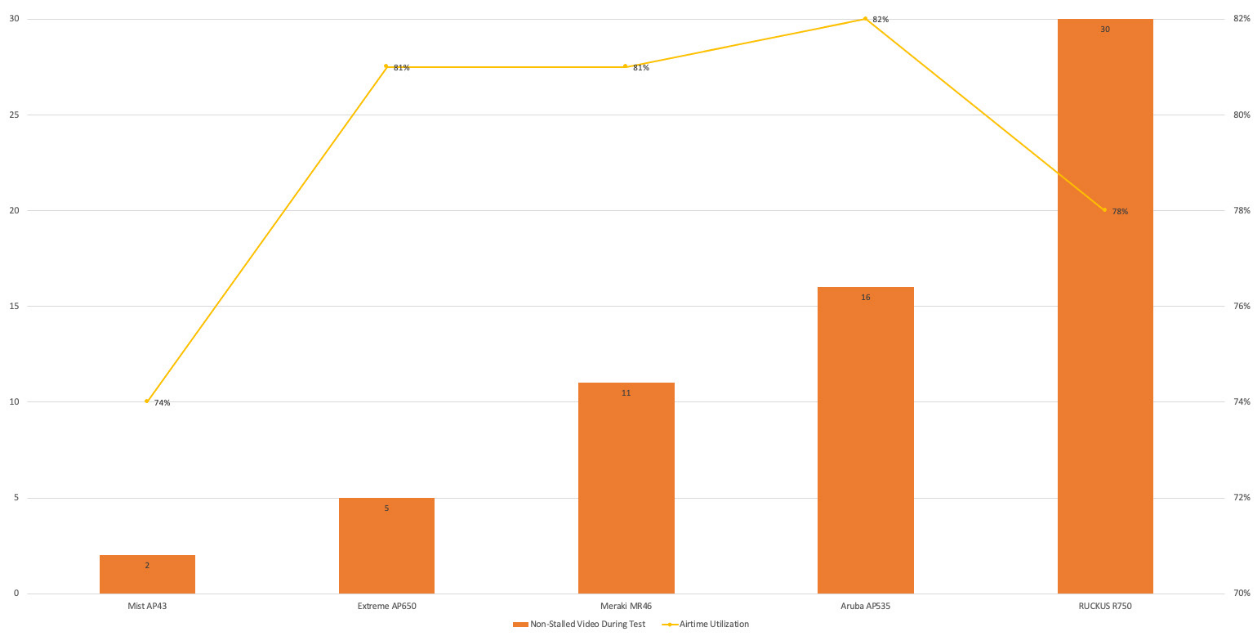

Figure 7. Number of non-stalled videos during the test with airtime utilization

In contrast to the Mist AP43, the RUCKUS R750 exhibited the second lowest airtime utilization value, yet it exhibited no video stalling during the test. Consequently, one would expect its airtime utilization to be the highest of the tested group. Since this is not the case, the author concludes that the RUCKUS R750 makes more efficient use of available airtime than do the other APs.

Test 1 - Conclusion

The RUCKUS R750 significantly outperformed all other access points in every test. It was the only access point capable of meeting real-world success criteria: Maintaining a “good” MOS while simultaneously delivering stall-free HD video streams to 30 clients and maintaining “high” throughput for all data clients.

The Aruba AP535 was the next most capable of managing the applied network load. While half the clients experienced stalled videos, they were able to recover after the test. During the test, however, the AP535 exhibited a “poor” MOS.

The Extreme AP650 maintained the second highest throughput but yielded 25 stalled video clients during the test and a “poor” MOS. The author concludes that the AP650 applied no QoS to the traffic.

The Meraki MR46 maintained 250 Mbps of throughput but had the lowest MOS of the group and was able to support only 11 stall-free video streams. After the test, it recovered all but three video streams.

The Mist AP43 demonstrated the poorest performance of the evaluated APs. It was able to support only 24 video streams in the absence of additional network loading and, during load, supported only two video streams. The AP43 also exhibited the lowest throughput of the evaluated APs but did exhibit the second highest MOS (rising nearly to “fair”). The author concludes that the AP43 prioritized VoIP traffic above other traffic classes.

In summary, the RUCKUS R750 stands out as being the most capable of delivering expected user experience levels and meeting SLAs. Processing various types of multimedia traffic is critical in today’s networks and the R750 appears to have an exceptional method of handling QoS, without the need for additional configuration of QoS parameters. This may be attributable to the SmartCast feature, which prioritizes video traffic over unmarked data traffic.

Test 2 - Troubleshooting/Analytics

The cloud offers increased benefits for network administrators in terms of convenience as well as insights and scale. Cloud-managed APs can leverage cloud resources to deliver network analytics and enhanced troubleshooting tools. Network analytics, in particular those driven by Artificial Intelligence (AI) and Machine Learning (ML), are especially well-suited for cloud delivery due to the high computational resources and data correlation volume that on-premises equipment may require.

Because Wi-Fi is typically a critical network access method, network administrators are often required to triage and troubleshoot various network issues. In this test, we introduce end-user issues for the system to diagnose: Wrong pre-shared key, DHCP unavailability, and an 802.1X issue (unreachable RADIUS server). The goal is to understand how quickly each vendor's product reacts to and reveals to the network administrator the root cause of network incidents.

The author received the three different "tickets", or test cases, along with the device information; and was provided with a cloud dashboard to assess ease of use, establish the accuracy of the information presented, and evaluate the efficacy of the troubleshooting tools available. This scenario is similar to what a typical IT engineer might experience if an end user called the IT help desk with a problem.

Another aspect of this test is to discover how Artificial Intelligence (AI) and Machine Learning (ML) improves the network administrators' mean time to identify (MTTI), also referred to as mean time to detect (MTTD).

Test 2 - Results

Before reviewing the results, it's important to distinguish the type of analytics and troubleshooting capability provided by each vendor.

Each vendor offers network analytics. This data provides insight into statistics such as throughput and AP up/down status. This is expected of any cloud-managed system. Another component of network analytics involves AI and ML, in which the system uses deeper insights to quickly identify issues and present root cause analysis. While each vendor offers network analytics, not every vendor's tested system offered AI/ML insights.

When using each vendor's dashboard, the author focused on a particular set of criteria. IT teams aim for low MTTI through dashboard workflow efficiency and accuracy of the data displayed. The author considered the use of event logs, using dashboard widgets to determine the scope of an issue, and whether a network administrator needs to navigate multiple pages to identify a problem. The author looked for details that clearly identified an issue and provided actionable next steps.

HPE Aruba

Aruba Central is Aruba's cloud management platform. AI Insights is the Aruba feature used to assist in troubleshooting their WLAN.

At first glance, the dashboard did not clearly display end-user experience issues with the Wi-Fi network. It required further analysis of event logs. Finding an event log may require additional research of an error message or additional troubleshooting external to the cloud interface to determine the impact.

Most importantly, information relating to troubleshooting using AI Insights required 3 hours to update and be displayed in the AI Insights dashboard. Once displayed, drilling into a specific device exposed constructive details to help identify the issue. However, there was no easy way to gauge the impact of a particular issue.

The MTTI for the test-case issues was 6.3 minutes, based on the use of tools other than AI Insights. The author scrutinized the event log to find the right timestamp and log for the client to identify there was a PSK mismatch. The DHCP case required filtering of the client device by MAC address to see an error message relating to a DHCP Discover timeout. On the 802.1X test case, the author overlooked small text that pointed to the issue of an authentication server timeout, which added time to identifying the problem. There was no method to test RADIUS server reachability from the dashboard. The AI insights displays these issues more easily but only after waiting up to 3 hours to update.

Extreme Networks

ExtremeCloud^{TM} IQ is Extreme's cloud management platform, which includes AI/ML insights in the IQ Pilot feature. The dashboard displays large amounts of data and analytics, which can be intimidating, in particular for an administrator who is not well-versed in the system or Wi-Fi in general. Fresh data, critical for real-time troubleshooting, is displayed under the client device details which can be challenging to find if you do not have the actual client device details, such as a MAC address or IP address.

The system includes multiple ML scorecards to rate the status of the network, but it wasn't clear why most areas scored well, yet the overall score was low. Client health reporting does not reflect near-real-time data. Once clients are connected, this feature requires about one hour to update. The ML scorecard view provided an overview of how the network is performing, based on an ML score.

By navigating through different views and pages, a network administrator can identify an issue and piece together the impact. Identification of an issue can be found in different views of the dashboard. The overall workflow, however, serves to increase rather than decrease the MTTI. Effective use of AI and ML insights required a deeper understanding of the scoring methodology; this information was unavailable (or not obvious) within the user interface.

The MTTI was 10.3 minutes. For the PSK test case, a single red flag for an incident—visible after restricting the timeframe—pointed to an incorrect PSK. The DHCP case required investigation on two different pages. Initially, the author couldn't determine based on the amount of data presented on screen whether or not there was a DHCP issue. But, after investigating on a separate page, Client Monitor, there was real-time data (that that did not require waiting for data) pointing to a DHCP server issue. The 802.1X test case required navigating to different pages that pointed to an underlying authentication problem.

Cisco Meraki

Meraki offers only cloud-managed control and management of its APs. It does not offer AI/ML-enabled analytics. The main dashboard homepage provides an overall view of network health but does not include the view of the Health feature which is of most interest when troubleshooting a Wi-Fi problem. The Health view of the network is accessible from the Wireless section of the dashboard under Monitor.

Event logs included in Health can be cryptic and require additional research. In some cases, Health was able to determine the exact cause of an issue, though getting to that point required multiple clicks through different sections of the dashboard. Rather than making use of AI or ML, Meraki follows a heuristic approach that specifies the percentage of clients affected by a particular issue.

The MTTI for the issues was 3 minutes. Using Health, there is an overall view of issues but after viewing the specific client on another page, a history of client connectivity listed Association failures stating the PSK was incorrect. For the DHCP test case, the History view of the specific client pointed to an exact reason: The authentication server did not respond. The History view was used again to identify the cause of 802.1X test case indicating the authentication server did not respond to the affected client.

Juniper Mist

Mist offers only cloud-managed control and management of its APs. The main dashboard provides a monitor view of how Wi-Fi is performing throughout a site, including whether Service Levels are being met, and site-level Wi-Fi insights.

Service Levels are a key component of the dashboard and offer a look into how the Wi-Fi network is performing. When a service level is below a threshold, a network operator can dive into a particular threshold to identify the impact. Mist feeds ML data into an AI algorithm and virtual assistant, Marvis (an additional subscription), located at the top-level navigation menu. Mist uses ML to learn from all collected events to improve their predictive capabilities for attributes such as device throughput. Network administrators can ask Marvis about issues with devices or sites and are then presented with identified issues.

The MTTI for the test cases was 5.3 minutes. The author used Service Levels to investigate the PSK case but found insufficient data for a specific client having the issue. But using Marvis (an additional subscription), the PSK test case was clearly identified as an authentication issue. Using Service Levels, the DHCP case was directed to a specific issue of DHCP Discover unresponsive. The scope of the 802.1X test case was identified as being a widespread authentication issue but required viewing another page to establish a RADIUS server failed communication. Then, viewing a dynamic packet capture file showed an authorization failure.

CommScope RUCKUS

RUCKUS offers network analytics as well as AI and ML insights via its RUCKUS Analytics product, which is integrated into its RUCKUS Cloud management platform and is also available on a stand-alone basis for use with RUCKUS on-premises deployments. As is the case with other vendors, an event log is available to view any potential issues. While the impact of an issue may not be easily identified, it can be correlated to a specific SSID. In addition to event logs, pre-defined and customizable reports can be generated and reused to help identify Wi-Fi issues.

RUCKUS offers premium analytics (an additional subscription) which displays the impact of Wi-Fi issues in clear detail, along with potential resolutions to those issues informed by root cause analysis. The RUCKUS virtual assistant, Melissa, aims to help identify Wi-Fi issues by using a natural language chat interface. Wi-Fi issues are displayed clearly with no room for interpretation and with no requirement for additional research. Data visualization included with the analysis serves to shorten the MTTI.

The MTTI for the test-case issues was 2.3 minutes. An incident detail provided a root cause of a passphrase mismatch for the PSK test case. A DHCP incident provided a reason—DHCP timeout— along with a visualization of where in the DHCP process the failure occurred. For the 802.1X case, the author used the Client Troubleshoot feature and viewed the incident for the specific device. The reason for the incident was clear and another visualization revealed where in the 802.1X process the failure occurred.

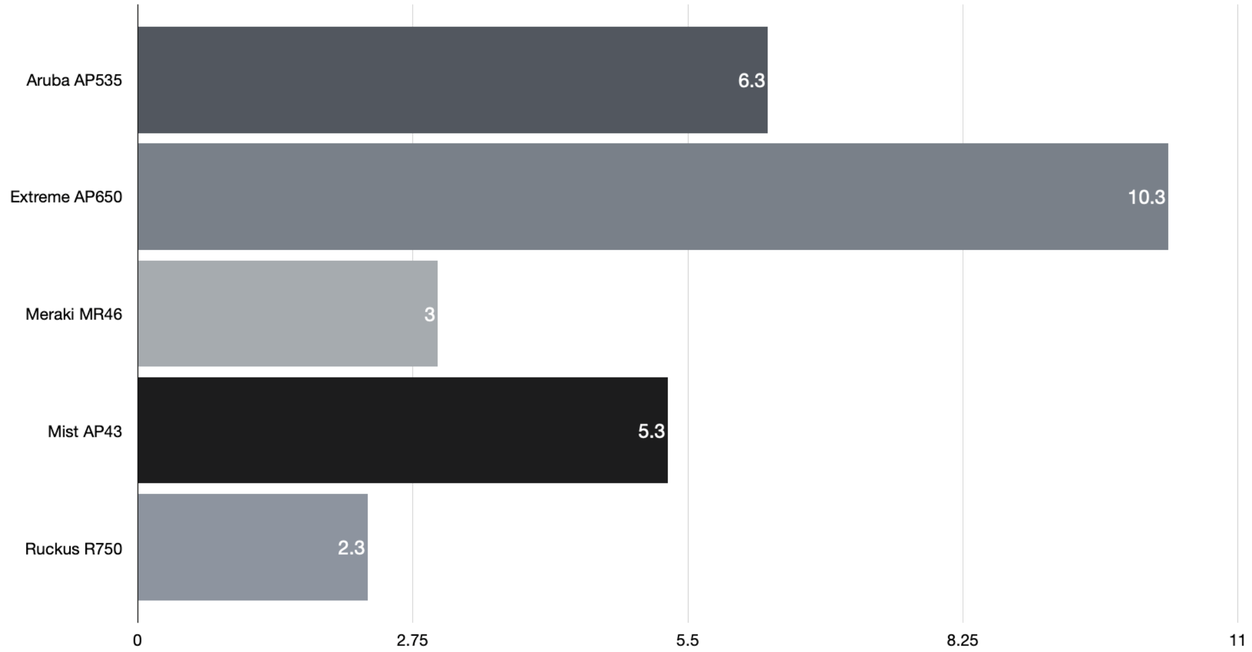

Figure 8. Mean time to identify (MTTI) by vendor in minutes

Test 2 - Conclusion

RUCKUS premium analytics provided detailed, visual insights into user experience, leading to the lowest MTTI in the evaluated group. The AI and ML assistance provided further insight into the impact of Wi-Fi issues than simple event log-driven analysis. The author viewed RUCKUS as the best solution for speed of MTTI and clarity in the reasons for the Wi-Fi issues, leaving no room for assumptions nor requiring further troubleshooting. An example is shown in the figure below.

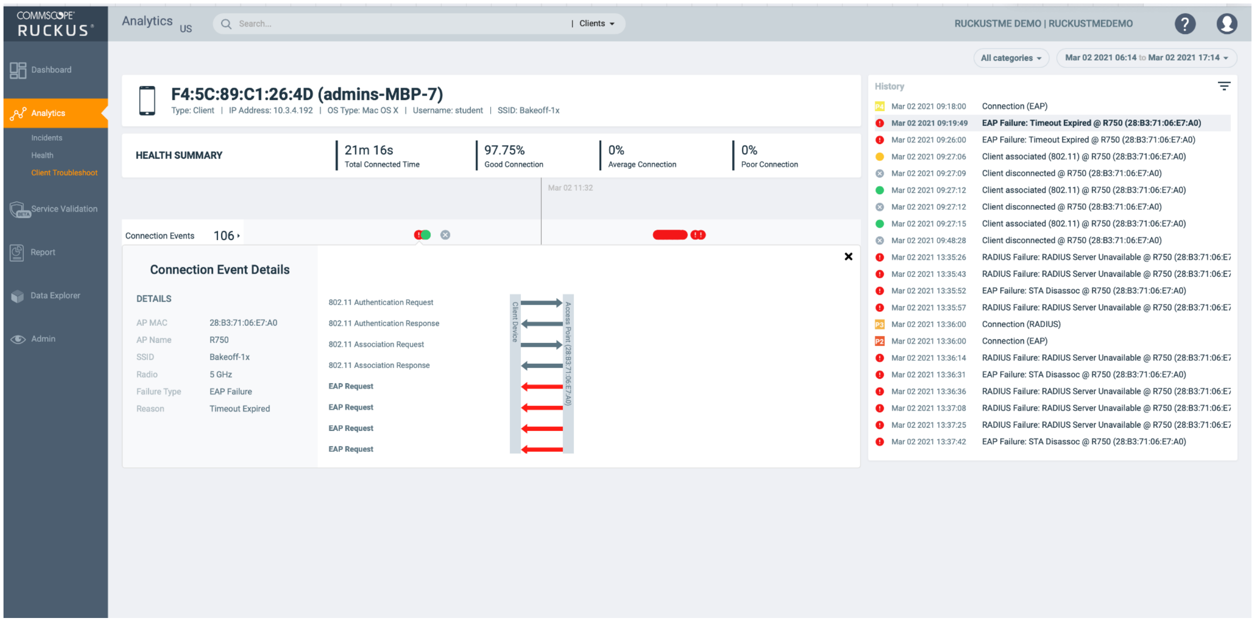

Figure 9. Example of RUCKUS premium analytics and troubleshooting

Meraki offered useful insights without AI/ML or premium analytics, differing from the other vendors in this respect.

The Mist AI assistant, Marvis, effectively narrowed down Wi-Fi issues to their root causes, a helpful feature for IT operators.

In the author’s opinion, Aruba’s AI Insights requires further development to be as effective as comparable features from some of the other vendors, with the requirement for repeated event log queries standing out as an area for improvement.

Extreme’s dashboard offered useful insights into Wi-Fi issues but required the author to first identify and locate the affected client on the dashboard. This requirement significantly increased observed MTTI.

The author acknowledges this assessment is based upon the author's preferred troubleshooting methodology. Others may follow a different approach.

Summary

The author observed and verified the legitimacy of all tests conducted. RUCKUS provided the author with open access to validate configurations, to ensure each configuration was similar, and to make sure that no vendor had an unfair advantage. The author is confident that testing was fairly conducted for each vendor.

The test suite was designed to represent a typical enterprise or campus environment, including a mix of device types and device capabilities. The device and traffic mix simulated a real-world setting that many network administrators will find familiar. For example, devices themselves will be a mix of both new and previous Wi-Fi generations (802.11n, 802.11ac). Additionally, administrators (the author included) do not typically observe just one type of traffic traversing an AP, thus, a mix of HD video, VoIP, and data download traffic was used.

Although each new Wi-Fi generation implements improvements in protocol efficiency, data rate selection, and throughput, a mixed client environment will serve to somewhat constrain the full benefit of Wi-Fi 6 infrastructure. However, it is clear from this testing that both aggregate and individual device performance within a mixed client environment can vary dramatically from one Wi-Fi 6 vendor to the next. The results displayed in this report are likely to provide network administrators with insight into how each AP will perform in a similar environment.

While the author is unable to ascertain the basis for each AP's QoS queuing decisions, the author observed that video and VoIP traffic displayed significant quality variation from vendor to vendor. Only the RUCKUS R750 AP was able to handle all traffic consistently and well.

Network IT teams are increasingly focused on end-user experience and workforce productivity. Therefore, the report includes an analysis of comparative mean-time-to-identify (MTTI) for a set of incident test cases, using each vendor's dashboard. The MTTI results observed can reasonably be extended to mean-time-to-resolution (MTTR) performance. The author acknowledges that the qualitative assessment of each dashboard is inherently subjective and dependent on the network administrator's experience. The author has endeavored to undertake a neutral and fair approach.

Author Commentary

As a Wi-Fi professional and consultant, the author undertook this testing with a set of pre-conceived notions regarding the relative performance of vendor Wi-Fi 6 equipment. Presented with similar offerings and a level playing field, the author expected comparable results, given common underlying silicon.

The author was, thus, surprised to observe the performance variation between different vendors' Wi-Fi 6 APs.

This test made clear that vendors do have the ability to differentiate seemingly equivalent hardware through software, firmware and hardware innovation, even as they seek to differentiate their management tools via user interface and AI/ML investment. The test demonstrated that AI and ML can, indeed, help rapidly identify the source of a network issue, however these technologies cannot resolve an AP's inability to delivery traffic to each client at the service level required.

The author recommends conducting a proof of concept to isolate and establish a baseline network performance level before considering other attributes.