Arista CloudVision WiFi vs Juniper Networks-Mist Cloud Competitive Performance Assessment

February 2021

DR210125G

Contents

1.0 Executive Summary 3

2.0 Test Summary 5

3.0 Introduction 6

3.1 Arista CloudVision WiFi (CV WiFi) 6

3.2 Mist Cloud 8

4.0 How We Did It 9

5.0 Client Connectivity Issues 11

5.1 DNS Server Invalid Address 11

5.2 DHCP Server Unresponsive 16

5.3 Incorrect PSK (Password) 21

5.4 RADIUS Server Unresponsive 24

6.0 Client / Application / Network Performance Issues 27

6.1 Poor Coverage / Low RSSI 27

6.2 High Channel Congestion / High Retry Rate 29

6.3 Poor Application Performance 32

About Miercom 34

Use of This Report 34

1.0 Executive Summary

Cloud-based networks are always striving for optimized efficiency, provisioning, monitoring and troubleshooting for more cohesive network management. Having a self-driven network allows it to perform automatic root cause analysis and offer remediation for found issues. To accomplish this, vendors began building their platforms using Artificial Intelligence / Machine Learning (AI/ML) implementations. This approach allows for faster, more cost-effective resolution to common, and unique, connectivity and performance issues in WiFi networks.

Arista CloudVision WiFi (CV WiFi) is a software-driven cloud platform built on a programmable, resilient and self-healing structure. It allows for a stateful network view and class-based automation across cloud networks to reduce the need for custom internal development. As a turnkey solution, Arista CV WiFi performs network-wide optimization, orchestration and automation. Its AI/ML, real-time telemetry offers predictive and enhanced root cause analysis for remediation.

Arista engaged Miercom to independently assess the CV WiFi solution in a realistic environment to verify its claimed functionality of root causes analysis, automatic packet capture, and automatic remediation recommendations in comparison to a reputable competitor – the Juniper Networks Mist Cloud platform. We observed the following key findings:

Key Findings

- **AI/ML Auto Root Cause Analysis.** Arista consistently managed to correctly identify root causes for common connectivity and performance issues. Mist failed in multiple tests to correctly identify root causes for the same issues.
- **AI/ML Remediation Recommendations.** Arista Inference Engine managed to offer reasonable remediation recommendations for all performance issues introduced. Mist's Marvis Actions failed, in all test scenarios, to offer automatic remediation recommendations.
- **Application Performance/Awareness/Assurance.** Arista's Network Assurance approach considers L1-L7 and network services (e.g., DNS, DHCP). Mist's Network Assurance mainly focuses on L1-L2 and network services without meaningful attention to application performance. This major architectural limitation will not be remedied until Mist implements a DPI on their APs, train application flow models and other means to accomplish performance optimization.
- **Workflows.** Arista's troubleshooting workflows are efficient and intuitive, requiring fewer clicks to get to root cause and remediation recommendations. Mist has a straightforward interface with quick Insights, but details are not as upfront and are delayed. The Marvis Actions interface was not helpful; it does not register issues that were tested and identified in other parts of the platform. In fact, the only issue identified by Marvis Actions was that APs were offline. The Mist SLE Dashboard requires manual tuning, provides cryptic fault messaging and, at times, incorrect or missing automatic root cause analysis.

- **ML Algorithms.** Arista deploys ML algorithms, such as Support Vector Machines (ML) for the Application Quality of Experience Dashboard and Decision Tree (ML) for the Inference Engine. This comprehensive ML approach proved to be more effective at determining root cause and offering remediation recommendations for issues than those deployed by Mist.

Based on our findings, we found the Arista CloudVision WiFi platform to be proficient in supporting and troubleshooting WiFi network connectivity and performance. We proudly award the Arista CloudVision WiFi solution the ***Miercom Performance Verified*** certification.

Robert Smithers
CEO, Miercom

2.0 Test Summary

Summary of Arista CloudVision vs Juniper Networks-Mist Cloud Connectivity and Performance

Test	Arista		Mist	
Connectivity Issues				
	Auto Root Cause Analysis	Auto Packet Capture	Auto Root Cause Analysis	Auto Packet Capture
DNS Server Incorrect Address	**PASS**	**PASS**	**Limited[1,2]**	**FAIL**
DHCP Server Unresponsive	**PASS**	**PASS**	**Limited[2]**	**FAIL**
Incorrect Password (PSK)	**PASS**	**PASS**	**Limited[2,3]**	**FAIL**
RADIUS Server Unresponsive	**PASS**	**PASS**	**Limited[2]**	**FAIL**
Performance Issues				
	Auto Root Cause Analysis	Auto Remediation Recommendation	Auto Root Cause Analysis	Auto Remediation Recommendation
Poor Coverage/Low RSSI	**PASS**	**PASS**	**Limited[2]**	**FAIL**
Channel Congestion/High Retry Rate	**PASS**	**PASS**	**Limited[2, 4]**	**FAIL**
Poor Application Performance	**PASS**	**PASS**	**Not Supported**	**Not Supported**

[1] No indication of DNS issue in SLE dashboard.

[2] Marvis Actions did not identify the issue.

[3] Did not specify the root cause as incorrect PSK. Lists cause as "WPA 4way handshake timeout(15)".

[4] Incorrectly listed Client Count as the main cause of High Channel Capacity when, in fact, the cause was due to Client Usage for a single client.

3.0 Introduction

Artificial Intelligence (AI) systems use automated algorithms that imitate human intelligence and do not require pre-programming (e.g. Siri). Machine Learning (ML) is a sub-field of AI that focuses on refining the algorithm based on historical data for enhanced predictability (e.g. Google Search).

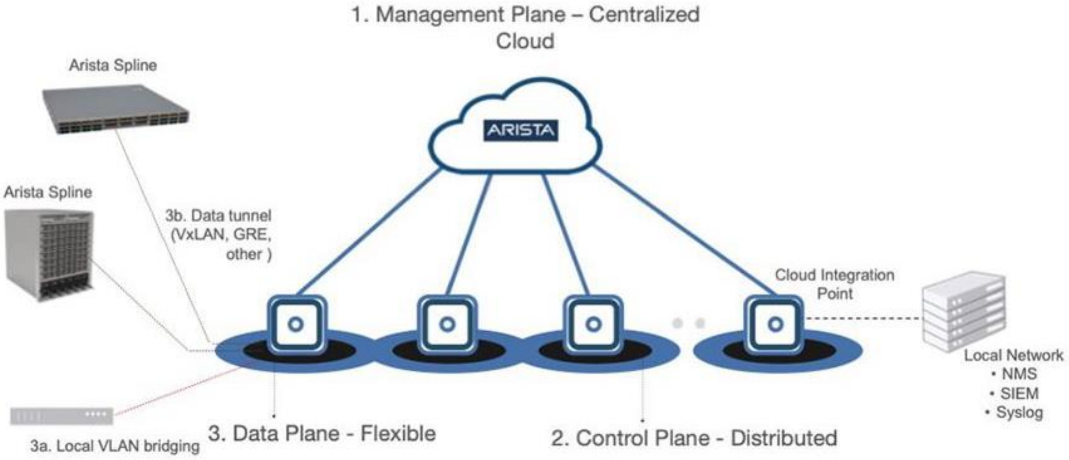
Testing analyzed and compared the detection and remediation capabilities of Arista CloudVision and Mist Cloud – solutions that perform based on AI and ML advancements.

We evaluated Arista and Mist platforms for the following:

- Client Connectivity Issues
    - DNS Server Invalid Address
    - DHCP Server Unresponsive
    - Incorrect PSK (Password)
    - RADIUS Server Unresponsive
- Client / Network / Application Performance Issues
    - Poor coverage / Low RSSI
    - High Channel Congestion / High Retry Rate
    - Poor Application Performance

3.1 Arista CloudVision WiFi (CV WiFi)

CloudVision WiFi (CV WiFi) is an Arista cloud-native approach to enterprise-level wireless networks. Its simplified AP management allows for centralized policy and provisioning functionality at the network edge. By separating management and control planes and having a flexible data plane for AP traffic redirection, Arista provides a robust WiFi network with high availability – making it a seamless and scalable network for up to thousands of APs.



Unlike controller-based WLAN architecture, Arista CV WiFi provides elastic storage and processing using innovative features seen in big data analytics, ML and cognitive computing.

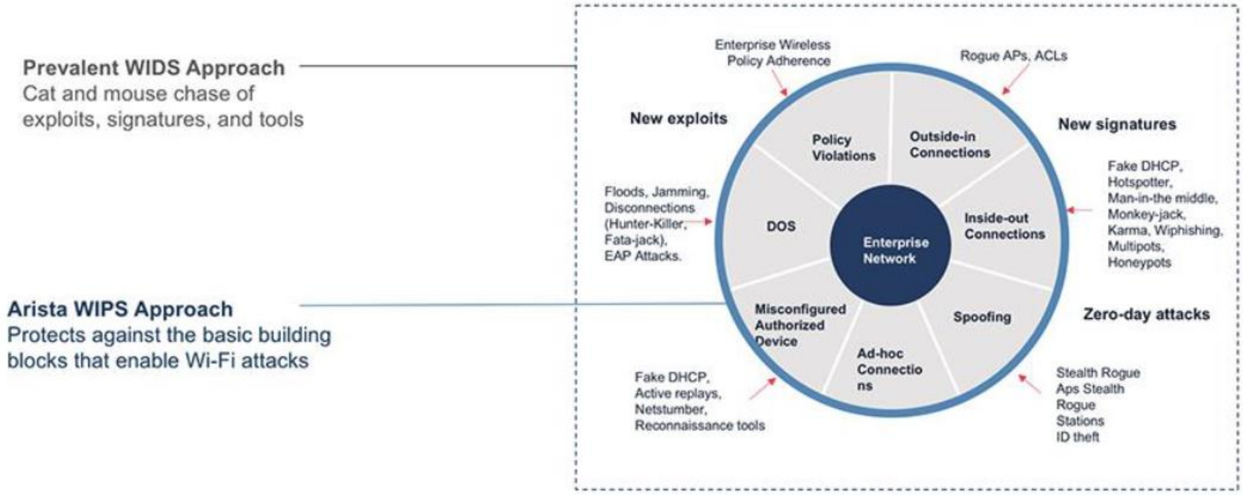
Cognitive Management Plane

The Cognitive Management Plane simplifies configuration and remediation and delivers robust telemetry using AI and ML techniques. The resulting root cause analysis and proactive troubleshooting reduces cost and time to resolve WiFi issues. This plane runs on Arista's NetDB – a state-based and cloud-hosted database that runs in real-time across the network for both wired and wireless devices for cognitive analytic data collection. These capabilities can be enhanced with third-party integrations with applications like OpenConfig and Arista's REST API framework.

Process	Description
Network Baselining	Baselines network behavior and automatically detects and highlights algorithms.
Root Cause Analysis Engine	Automatically detects and classifies WiFi clients' connection failures real-time.
Single Client Inferencing	Identifies clients facing poor QoE, based on RF, network and application cause analysis for specific clients.
Automatic Packet Capture	Proactively captures packet traces to help diagnose problems; traces failures or symptoms to simplify troubleshooting later.
Client Emulation and Network Profiling	Takes advantage of the multi-function radio; is present in most Arista WiFi to run a wide variety of tests and proactively identify problems before users do.

Wireless Intrusion Prevention

CV WiFi uses a multi-function radio for a dedicated Wireless Intrusion Prevention System (WIPS) sensor for detecting and blocking threats in real-time, based on behavioral-based detection for zero-day protection against exploits, tools and their signatures.


Prevalent WIDS Approach
Cat and mouse chase of exploits, signatures, and tools
Arista WIPS Approach
Protects against the basic building blocks that enable Wi-Fi attacks
Enterprise Wireless Policy Adherence
Rogue APs, ACLs
New exploits
New signatures
Policy Violations
Outside-in Connections
Floods, Jamming, Disconnections (Hunter-Killer, Fata-jack), EAP Attacks.
DOS
Enterprise Network
Inside-out Connections
Fake DHCP, Hotspotter, Man-in-the middle, Monkey-jack, Karma, Wiphishing, Multipots, Honeypots
Misconfigured Authorized Device
Ad-hoc Connectio ns
Spoofing
Zero-day attacks
Fake DHCP, Active replays, Netstumber, Reconnaissance tools
Stealth Rogue Aps Stealth Rogue Stations ID theft

Secure Client Access

Clients have flexible access into enterprise WiFi networks using CV WiFi's integration with leading identity management solutions (e.g. Aruba ClearPass, ForeScout NAC, Cisco ISE). Arista's Guest Manager provide multiple ways for enterprise guess access.

Client Journey

The Client Journey dashboard shows a timeline view of events to see which issues affect a particular client for a given time. This contextual view helps administrators quickly find the root of a wireless problem and take steps to mitigate.

3.2 Mist Cloud

Using microservices cloud architecture, Mist Cloud provides a scalable and flexible wired and wireless solution for mission-critical operations involving connectivity, security and performance. Its subscription services include: Wi-Fi Assurance, Wired Assurance, WAN Assurance, AI-Driven Virtual Assistant, Premium Analytics, User Engagement, and Asset Vulnerability.

For troubleshooting, Mist offers its inline AI engine to adapt in real-time to user, device and application behavior and changes for predictable and reliable Wi-Fi. This monitoring tool sends alerts when service levels degrade and offers remediation for proactive mitigation.

Service Level Expectations (SLE)

Mist's SLE dashboard presents results from its Predictive Analytics and Correlation Engine (PACE) – a patent-pending, machine learning technology that performs and correlates dynamic wireless event collection for root cause detection. The SLE dashboard gives an insightful look at each mobile user's RF packets from the cloud, displaying issues and aiding in troubleshooting.

SLE Thresholds

Thresholds can be set for functions that affect performance (e.g. time to connect, coverage, capacity), when exceeded or fall short, helps the administrator determine how this affects the wireless network and its devices.

Dynamic PCAP (dPCAP)

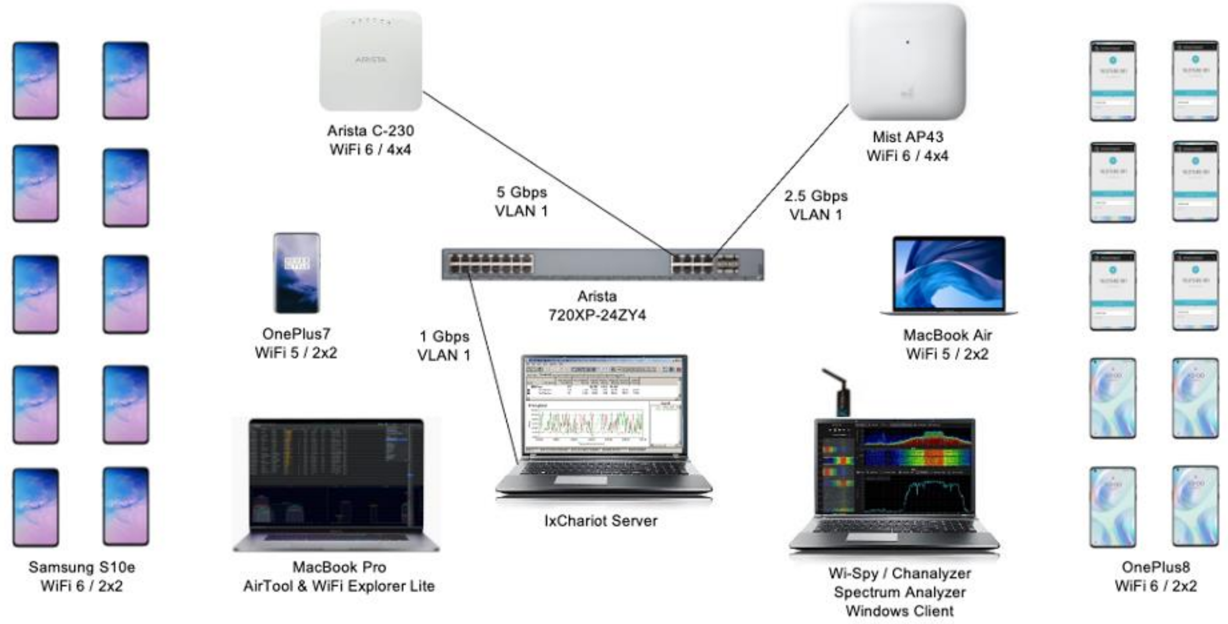
Mist automatically detects and captures network anomalies in real-time packet captures to help remediate issues while saving time and cost of manual involvement.

For more information, visit: https://www.mist.com/learning-wlan/

4.0 How We Did It

Using a realistic network environment, we tested the Arista CloudVision and Mist Cloud platforms. Miercom independently assesses security and performance products for their claimed functionality and compares solutions to determine strengths and unique features.

Test Bed Overview



Source: Arista

The test bed consisted of IEEE 802.11ax clients (10 Samsung S10e, 10 OnePlus8, 1 OnePlus7, 1 MacBook Pro, 1 Windows Client) and an 802.11ac client (1 MacBook Air), the Arista C-230 and Mist AP43 access points. Traffic is generated through an Arista 720XP-24ZY4 switch via an Ixia IxChariot server. Spectrum analysis was performed using a Wi-Spy / Chanalyzer spectrum analyzer. All settings used were set the default (no tagging).

Solution	Version
Arista CloudVision	9.0.0-54
Mist Cloud	0.8.21202

Test Tools

The following tools are a representative list of software tools and exploits we used to carry out our analysis.

Ixia IxChariot (v. 7.30 SP4)

ixia
A Keysight Business

Simulates real-world applications for predicting device and system performance under practical load conditions. It has been used to accurately access the performance characteristics of any application running on wired and wireless networks.

Wi-Spy

Scans and displays all activity in the 2.4-GHz or 5-GHz spectrum to identify interference, find the ideal channel, and analyze signal quality.

Licensing

Arista

Only a single cloud license per AP is required to enable all available features in the Arista WiFi solution: *Cognitive Management Subscription*.

Mist

Multiple licenses are required per AP to enable all available features in the Mist solution. The system used for this test project had all available WiFi licenses installed:

- *Asset Visibility*
- *Premium Analytics*
- *vBLE Engagement*
- *Virtual Network Assistant*
- *WiFi Management and Assurance*

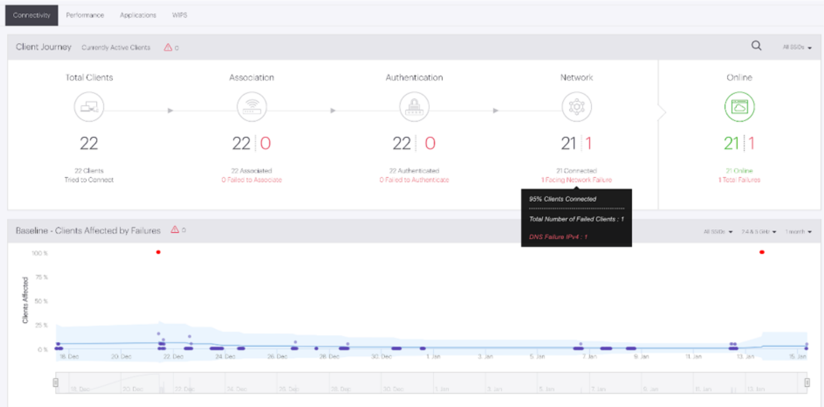
5.0 Client Connectivity Issues

5.1 DNS Server Invalid Address

Using 1 AP and 1 Client, we locally configured an incorrect DNS server address on a client (e.g. MacBook) and attempted to connect it to the test SSID/radio. After several minutes, of the client connecting, we use the tested solution's interface to determine if the issue was automatically detected, analyzed and captured.

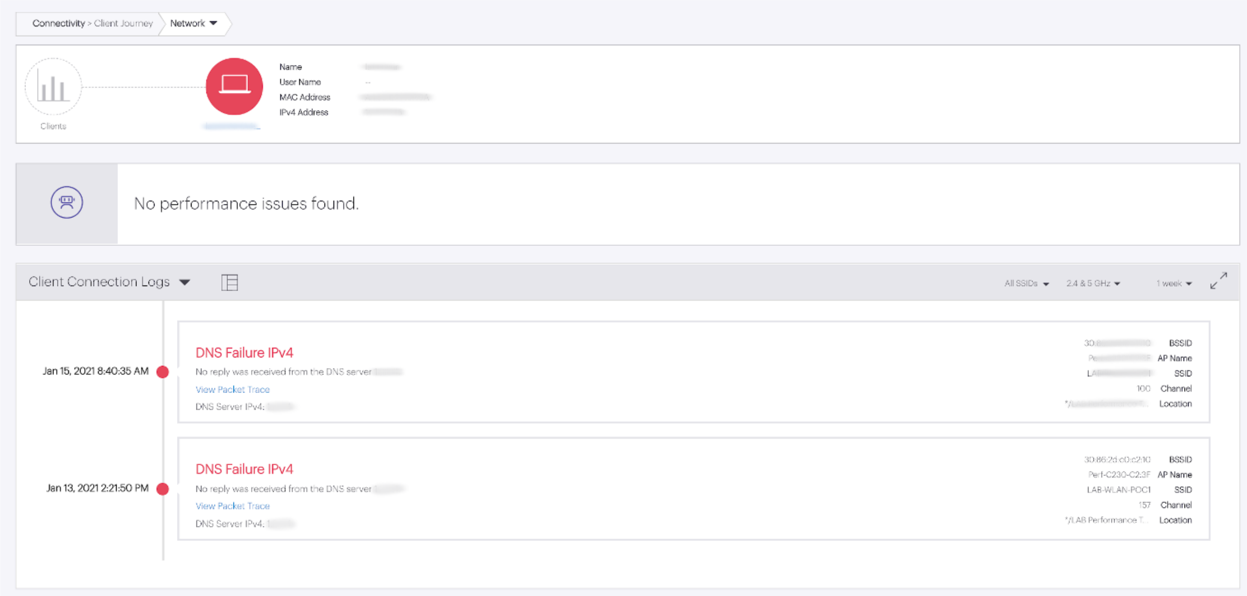
Arista: PASS

About 5 minutes post-event, the Arista Connectivity interface (Dashboard > Network > Connectivity) displayed the "Client Journey", where we could view/click on a client experiencing any DNS issues.



One client had a DNS issue and when clicked showed the "Client Connection Logs".

We view the Client Connection Logs to see the DNS server address used by the client.



Name [redacted]
User Name --
MAC Address [redacted]
IPv4 Address [redacted]

No performance issues found.

Jan 15, 2021 8:40:35 AM

DNS Failure IPv4
No reply was received from the DNS server [redacted]
View Packet Trace
DNS Server IPv4: [redacted]

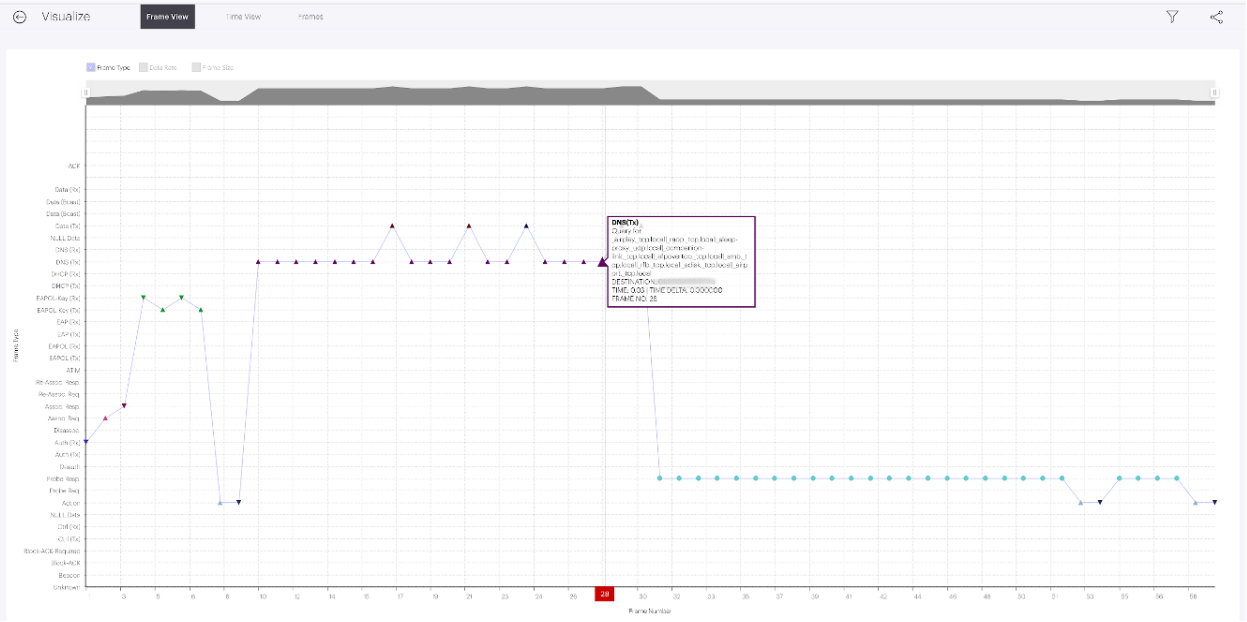
3D:[redacted] BSSID
Pe[redacted] AP Name
LA[redacted] SSID
100 Channel
*/[redacted] Location

Jan 13, 2021 2:21:50 PM

DNS Failure IPv4
No reply was received from the DNS server [redacted]
View Packet Trace
DNS Server IPv4: [redacted]

30:86:2d:c0:c2:10 BSSID
Perf-C230-C2:3F AP Name
LAB-WLAN-POC1 SSID
157 Channel
*/LAB Performance T... Location

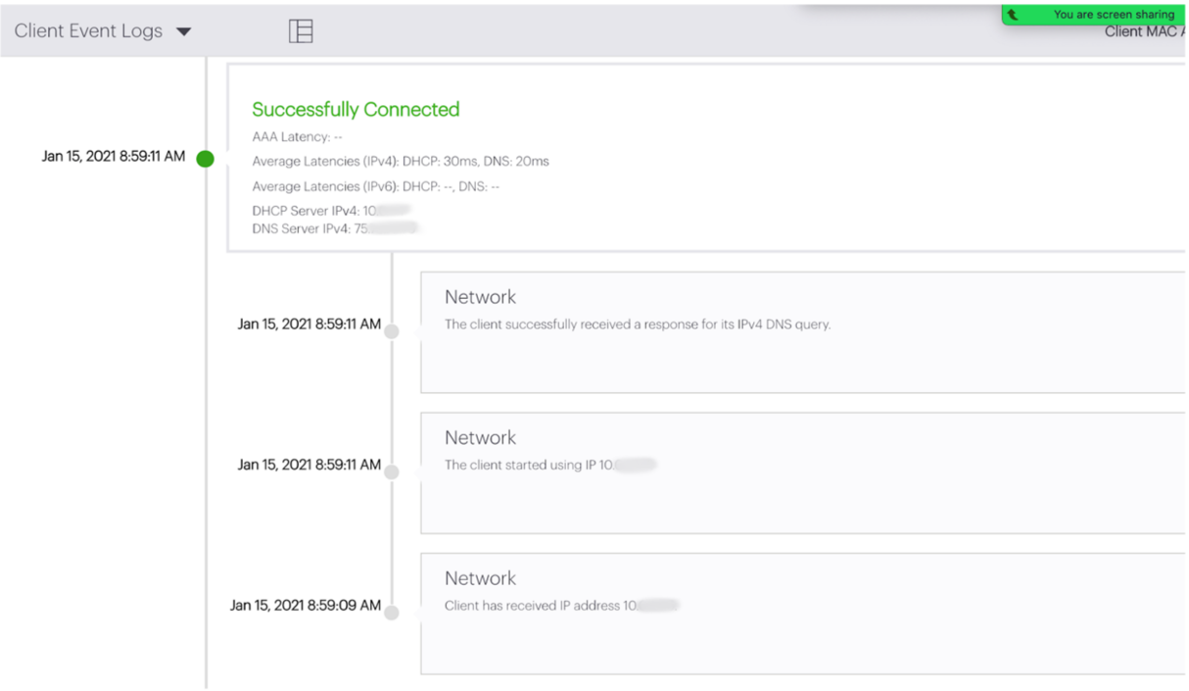
We saw there were two instances of DNS Failure IPv4 associated with this client. We clicked on "View Packet Trace" for further investigation.



DNS(Tx)
Query for
_airplay._tcp.local|_raop._tcp.local|_sleep-proxy._udp.local|_companion-link._tcp.local|_afpovertcp._tcp.local|_smb._tcp.local|_rfb._tcp.local|_adisk._tcp.local|_airport._tcp.local
DESTINATION: [redacted]
TIME: 0.03 | TIME DELTA: 0.000000
FRAME NO: 28

Arista Packets showed frame view of packets. We saw the client sending DNS packets (Tx) but not receiving them (Rx). When clicking on an event, we saw the DNS query.

After resolving the DNS misconfiguration, we saw that there was no longer any failure displayed in the Client Journey.



Jan 15, 2021 8:59:11 AM

Successfully Connected
AAA Latency: --
Average Latencies (IPv4): DHCP: 30ms, DNS: 20ms
Average Latencies (IPv6): DHCP: --, DNS: --
DHCP Server IPv4: 10[redacted]
DNS Server IPv4: 75[redacted]

Jan 15, 2021 8:59:11 AM

Network
The client successfully received a response for its IPv4 DNS query.

Jan 15, 2021 8:59:11 AM

Network
The client started using IP 10.[redacted]

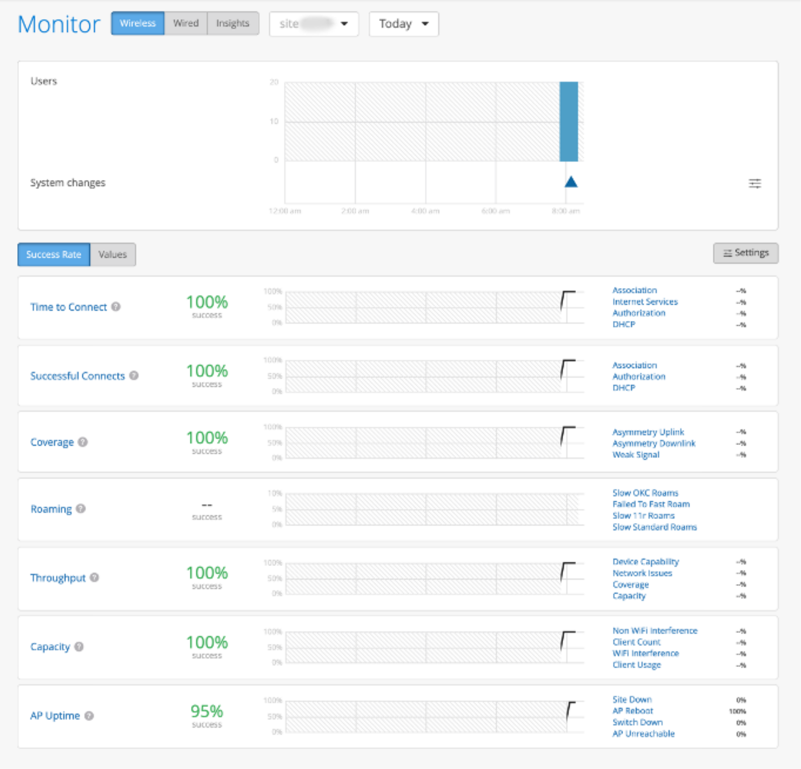
Jan 15, 2021 8:59:09 AM

Network
Client has received IP address 10[redacted]

The client was shown to successfully connect after the DNS misconfiguration was fixed.

Mist: Limited

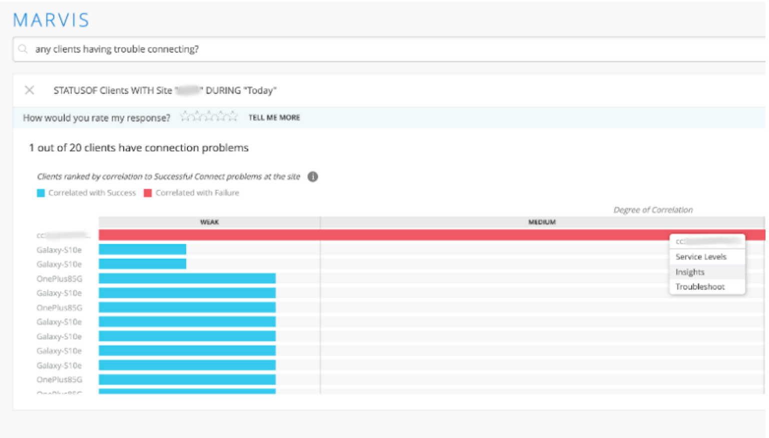
Using the SLE dashboard, we viewed “Successful Connects” to observe any issues. After 5 minutes post-connect, we did not see any indication of a DNS issue or other connectivity issues.



Time to Connect	100% success	Association –% Internet Services –% Authorization –% DHCP –%
Successful Connects	100% success	Association –% Authorization –% DHCP –%
Coverage	100% success	Asymmetry Uplink –% Asymmetry Downlink –% Weak Signal –%
Roaming	-- success	Slow OKC Roams Failed To Fast Roam Slow 11r Roams Slow Standard Roams
Throughput	100% success	Device Capability –% Network Issues –% Coverage –% Capacity –%
Capacity	100% success	Non WiFi Interference –% Client Count –% WiFi Interference –% Client Usage –%
AP Uptime	95% success	Site Down 0% AP Reboot 100% Switch Down 0% AP Unreachable 0%

No events were observed under the Successful Connects view for wireless monitoring in the SLE dashboard.

We asked Marvis, “any clients having trouble connecting?” to find potential connectivity issues, and we saw 1 out of 20 clients had a connection problem.


MARVIS

any clients having trouble connecting?

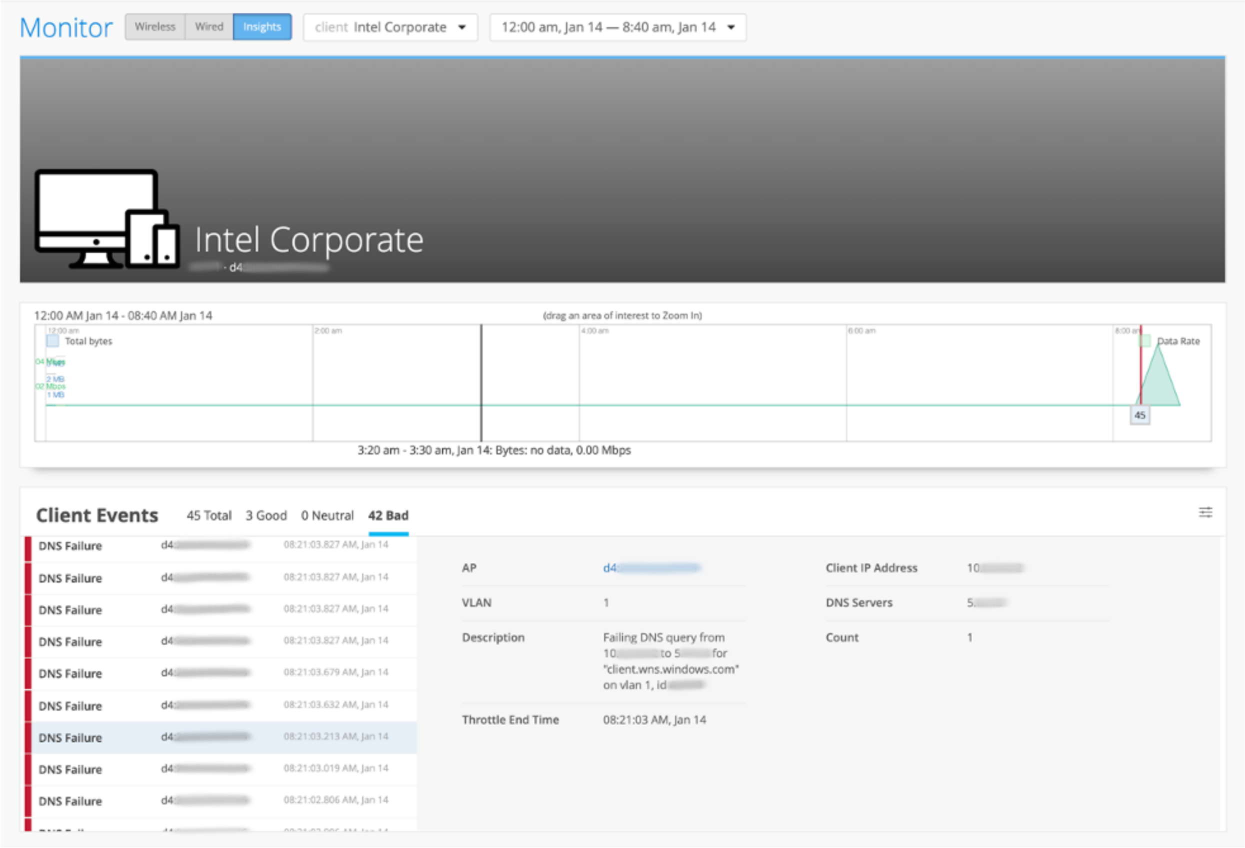
STATUSOF Clients WITH Site "[redacted]" DURING "Today"

How would you rate my response? ☆☆☆☆☆ TELL ME MORE

1 out of 20 clients have connection problems

Clients ranked by correlation to Successful Connect problems at the site

By clicking on the failed client and selecting “Insights”, we were directed to Client Events.


Monitor
Wireless
Wired
Insights
client Intel Corporate
12:00 am, Jan 14 — 8:40 am, Jan 14
Intel Corporate
[redacted] - d4[redacted]
12:00 AM Jan 14 - 08:40 AM Jan 14
(drag an area of interest to Zoom In)
12:00 am
2:00 am
4:00 am
6:00 am
8:00 am
Total bytes
Data Rate
04 Mbps
2 MB
02 Mbps
1 MB
45
3:20 am - 3:30 am, Jan 14: Bytes: no data, 0.00 Mbps

Client Events 45 Total 3 Good 0 Neutral **42 Bad**

DNS Failure	d4[redacted]	08:21:03.827 AM, Jan 14
DNS Failure	d4[redacted]	08:21:03.827 AM, Jan 14
DNS Failure	d4[redacted]	08:21:03.827 AM, Jan 14
DNS Failure	d4[redacted]	08:21:03.827 AM, Jan 14
DNS Failure	d4[redacted]	08:21:03.679 AM, Jan 14
DNS Failure	d4[redacted]	08:21:03.632 AM, Jan 14
DNS Failure	d4[redacted]	08:21:03.213 AM, Jan 14
DNS Failure	d4[redacted]	08:21:03.019 AM, Jan 14
DNS Failure	d4[redacted]	08:21:02.806 AM, Jan 14

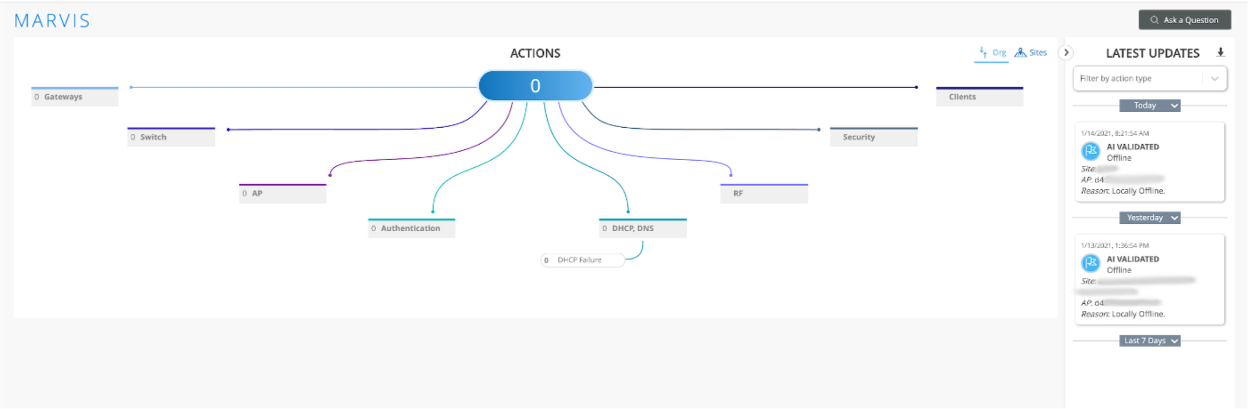
AP	d4[redacted]	Client IP Address	10[redacted]
VLAN	1	DNS Servers	5[redacted]
Description	Failing DNS query from 10[redacted] to 5[redacted] for "client.wns.windows.com" on vlan 1, id[redacted]	Count	1
Throttle End Time	08:21:03 AM, Jan 14		

Under Insights, we saw a list of Client Events where there were 42 instances of DNS failure with the AP used. The error was labeled "Failing DNS query", but there was no packet capture available for this anomaly.

Mist dPCAP failed to performed packet captures for this connectivity issue. According to their documentation, Mist dPCAP is enabled by default, and it should automatically capture network anomalies such as DNS, DHCP, and PSK issues. However, this was not the case.

For more documentation on Mist dPCAP, visit: https://www.mist.com/wireless-packet-captures-troubleshooting-else-fails/

Even when using the Marvis Actions interface, we did not see any automatic root cause analysis or recommended actions given on how to resolve this issue.



1/14/2021, 8:21:54 AM
AI VALIDATED
Offline
Site: [redacted]
AP: d4[redacted]
Reason: Locally Offline.

1/13/2021, 1:36:54 PM
AI VALIDATED
Offline
Site: [redacted]
AP: d4[redacted]
Reason: Locally Offline.

The only issues Marvis Actions showed were that the AP was locally offline earlier from an unrelated reboot event. This proves the updates were working, but that Mist simply was not registering the DNS Failure event from the troubleshooting perspective.

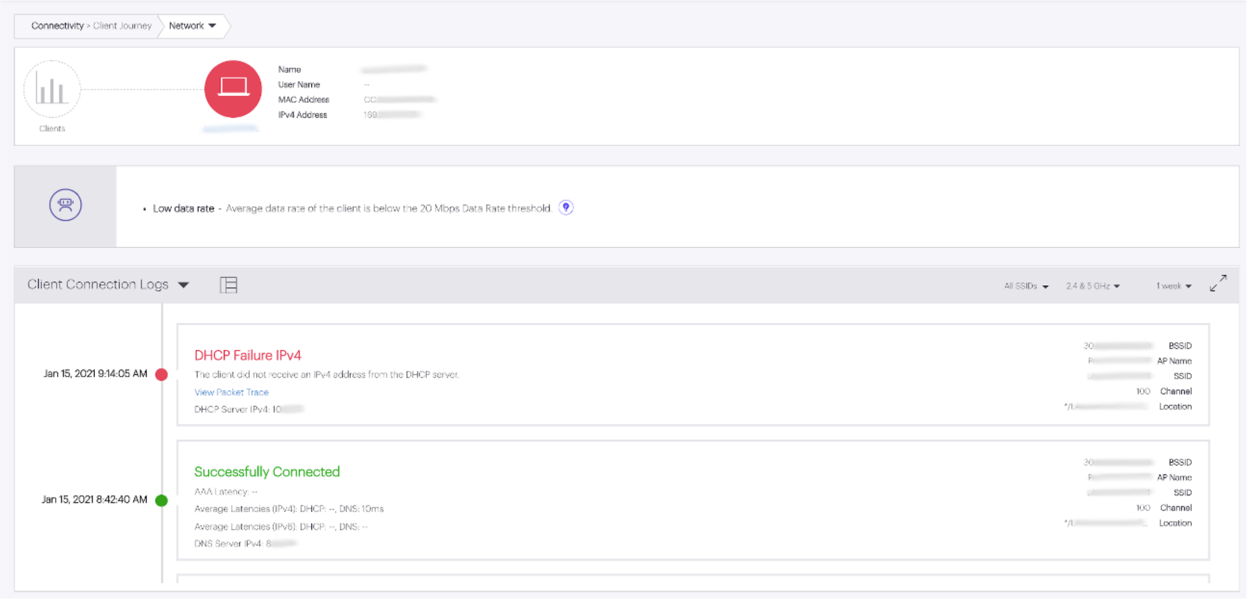
After 25 minutes, there was still no indication of a DNS issue or any other connectivity event in the SLE dashboard or Marvis Actions interface.

5.2 DHCP Server Unresponsive

For this test, we use 1 AP and 1 Client. We disconnected/disabled the DHCP server from the test SSID/radio and attempted to connect the client to the test SSID/radio. After several minutes, of the client connecting, we use the tested solution's interface to determine if the issue was automatically detected, analyzed and captured.

Arista: PASS

After 5 minutes, the Arista Connectivity dashboard registered "DHCP Failure for IPv4". We clicked on the client for its details page and view its Client Connection Logs.



Name [redacted]
User Name --
MAC Address [redacted]
IPv4 Address [redacted]

- Low data rate - Average data rate of the client is below the 20 Mbps Data Rate threshold

Jan 15, 2021 9:14:05 AM

DHCP Failure IPv4
The client did not receive an IPv4 address from the DHCP server.
View Packet Trace
DHCP Server IPv4: [redacted]

[redacted] BSSID
[redacted] AP Name
[redacted] SSID
100 Channel
[redacted] Location

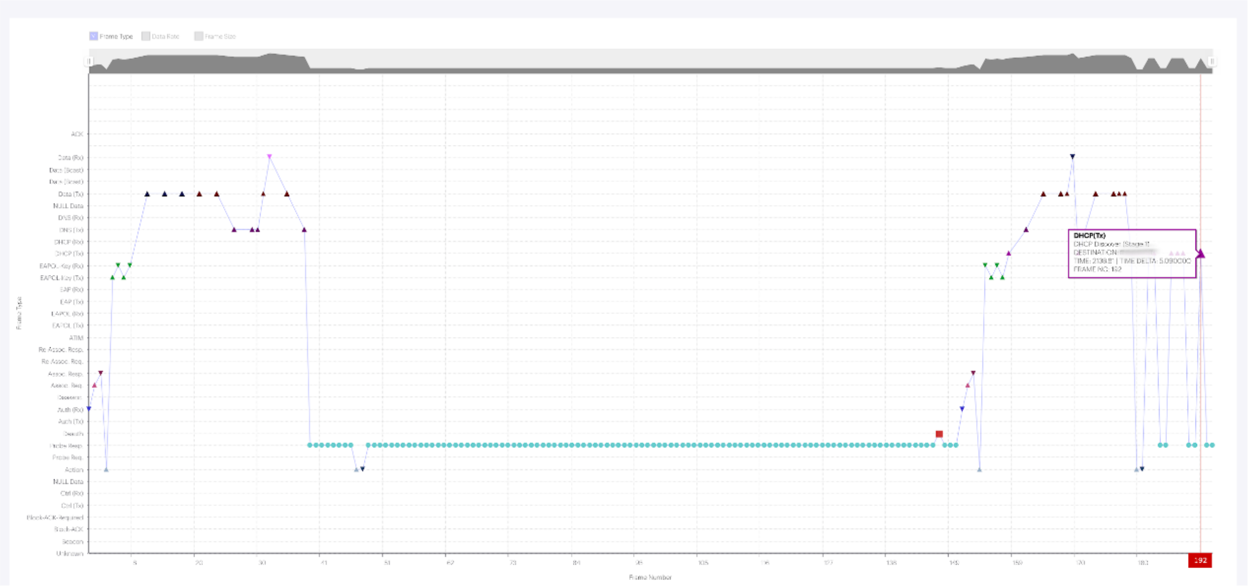
Jan 15, 2021 8:42:40 AM

Successfully Connected
AAA Latency: --
Average Latencies (IPv4): DHCP: --, DNS: 10ms
Average Latencies (IPv6): DHCP: --, DNS: --
DNS Server IPv4: [redacted]

[redacted] BSSID
[redacted] AP Name
[redacted] SSID
100 Channel
[redacted] Location

In the Client Connections Logs, we observed that the client did not receive an IPv4 address from the DHCP server. An auto packet capture was generated, which when clicking on its link, brought us to a packet trace in Arista Packets for further analysis.

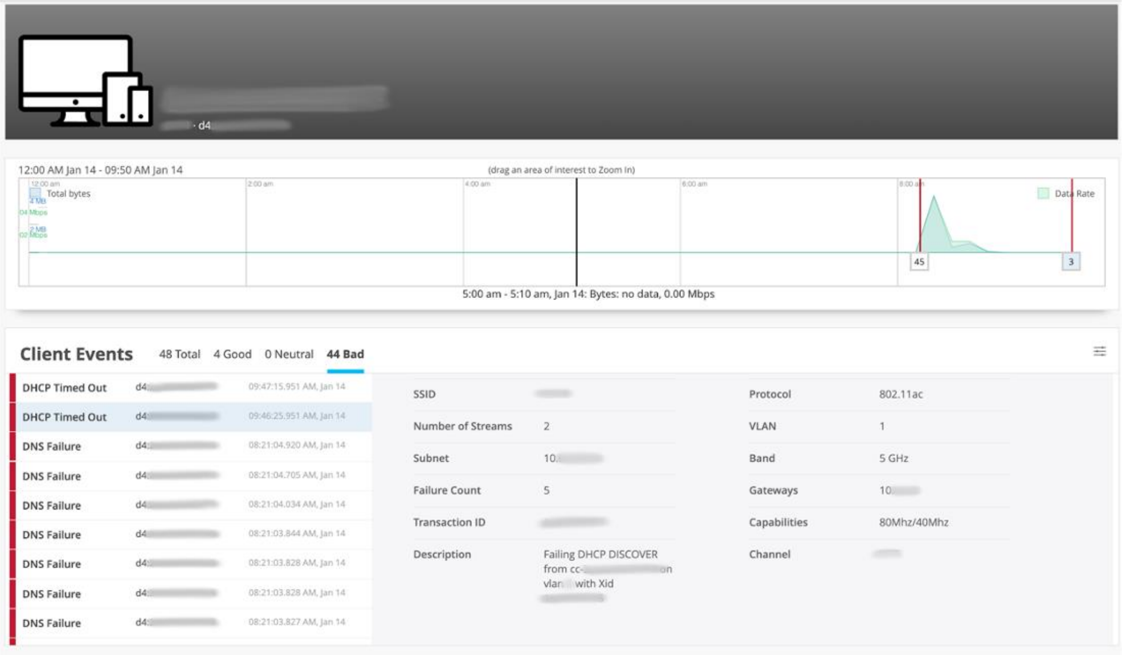
As with the DNS misconfiguration in Section 5.1, we saw successful connection in the Arista Connectivity dashboard once the issue was resolved.



In the Frame View of Arista Packets we saw the client sending DHCP packets (Tx) but not receiving them (Rx).

Mist: Limited

After several minutes post-event, we did not observe any indication of a DHCP issue or other connectivity issue in the SLE dashboard. This is relatively expected, as the algorithm for event detection results in issues not being displayed in real-time. This is also true for Arista and other leading vendors. We navigated to Client Insights for any details.


[redacted]
[redacted] · d4[redacted]

12:00 AM Jan 14 - 09:50 AM Jan 14

(drag an area of interest to Zoom In)

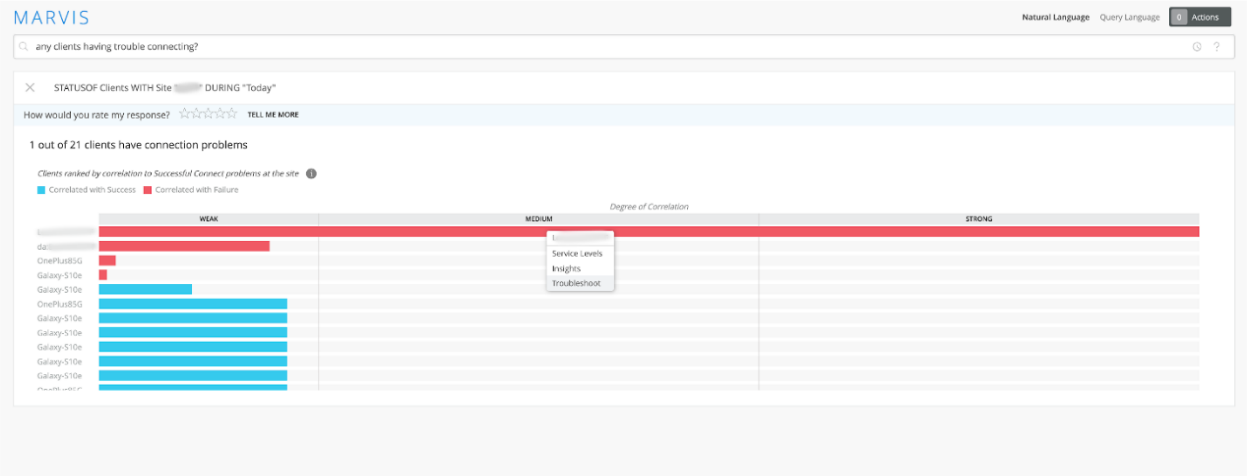
5:00 am - 5:10 am, Jan 14: Bytes: no data, 0.00 Mbps

Client Events 48 Total 4 Good 0 Neutral **44 Bad**

DHCP Timed Out	d4[redacted]	09:47:15.951 AM, Jan 14
DHCP Timed Out	d4[redacted]	09:46:25.951 AM, Jan 14
DNS Failure	d4[redacted]	08:21:04.920 AM, Jan 14
DNS Failure	d4[redacted]	08:21:04.705 AM, Jan 14
DNS Failure	d4[redacted]	08:21:04.034 AM, Jan 14
DNS Failure	d4[redacted]	08:21:03.844 AM, Jan 14
DNS Failure	d4[redacted]	08:21:03.828 AM, Jan 14
DNS Failure	d4[redacted]	08:21:03.828 AM, Jan 14
DNS Failure	d4[redacted]	08:21:03.827 AM, Jan 14

SSID	[redacted]	Protocol	802.11ac
Number of Streams	2	VLAN	1
Subnet	10.[redacted]	Band	5 GHz
Failure Count	5	Gateways	10[redacted]
Transaction ID	[redacted]	Capabilities	80Mhz/40Mhz
Description	Failing DHCP DISCOVER from cc-[redacted]on vlan[redacted] with Xid [redacted]	Channel	[redacted]

In Client Events, we observed 2 instances of "DHCP Timed Out" described as "Failing DHCP DISCOVER". Like the DNS Failure issue, there was no automatic packet capture available as advertised.



any clients having trouble connecting?

STATUSOF Clients WITH Site "[redacted]" DURING "Today"

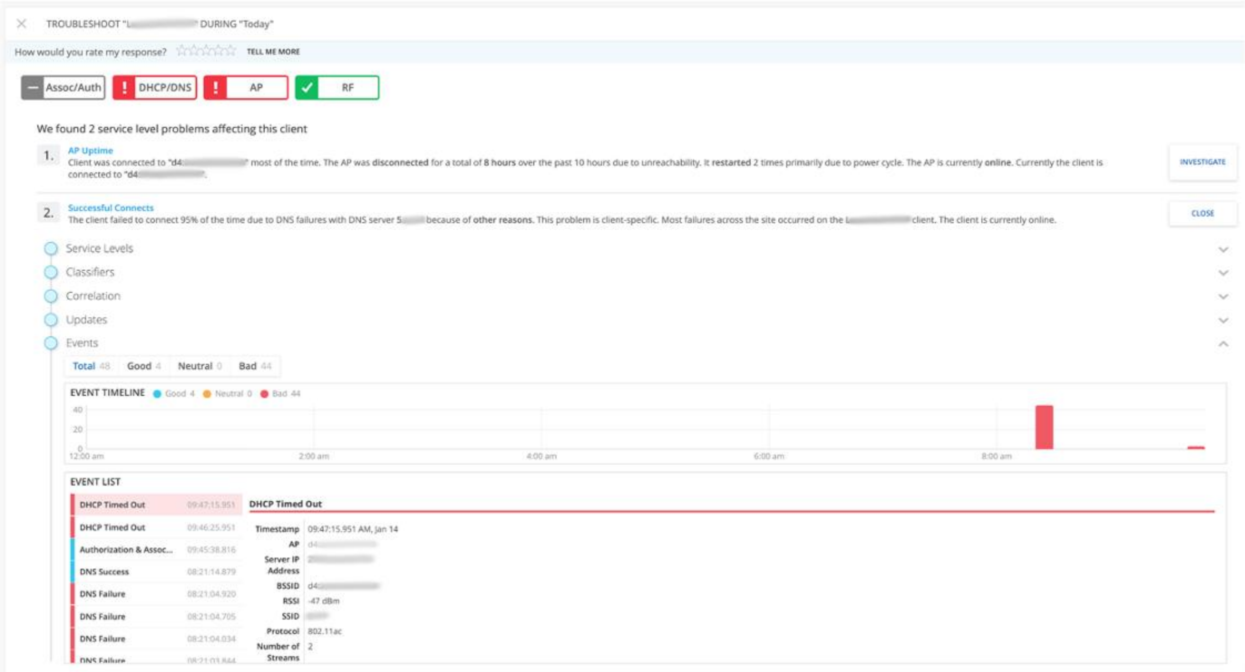
How would you rate my response? ☆☆☆☆☆ TELL ME MORE

1 out of 21 clients have connection problems

Clients ranked by correlation to Successful Connect problems at the site

🟦 Correlated with Success 🟥 Correlated with Failure

By selecting "Troubleshoot" for the AP with the DHCP issue, we were brought to the Marvis Troubleshooting interface for more details.



TROUBLESHOOT "[redacted]" DURING "Today"

How would you rate my response? ☆☆☆☆☆ TELL ME MORE

We found 2 service level problems affecting this client

1. AP Uptime
Client was connected to "d4[redacted]" most of the time. The AP was **disconnected** for a total of **8 hours** over the past 10 hours due to unreachability. It **restarted** 2 times primarily due to power cycle. The AP is currently **online**. Currently the client is connected to "d4[redacted]".

2. Successful Connects
The client failed to connect 95% of the time due to DNS failures with DNS server 5[redacted] because of **other reasons**. This problem is client-specific. Most failures across the site occurred on the [redacted] client. The client is currently online.

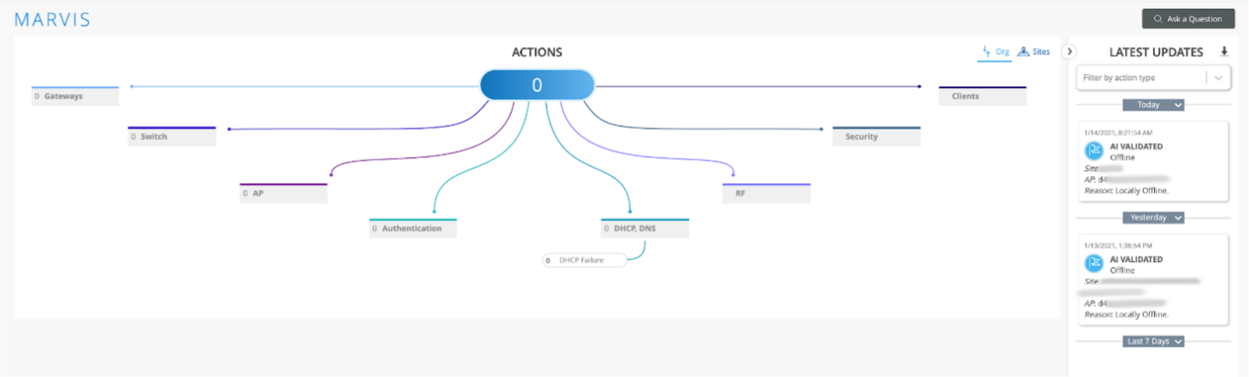
EVENT LIST

DHCP Timed Out	09:47:15.951
DHCP Timed Out	09:46:25.951
Authorization & Assoc...	09:45:38.816
DNS Success	08:21:14.879
DNS Failure	08:21:04.920
DNS Failure	08:21:04.705
DNS Failure	08:21:04.034
DNS Failure	08:21:03.844

DHCP Timed Out

Timestamp	09:47:15.951 AM, Jan 14
AP	d4[redacted]
Server IP Address	[redacted]
BSSID	d4[redacted]
RSSI	-47 dBm
SSID	[redacted]
Protocol	802.11ac
Number of Streams	2

Under Marvis Troubleshooting, we saw 2 service level problems affecting the client. This was listed as AP Uptime and Successful Connects. This allows you to Investigate for further details. We selected Successful Connects and observed an event list for the DHCP Timed Out events.



LATEST UPDATES

Filter by action type

Today

1/14/2021, 8:21:54 AM
AI VALIDATED
Offline
Site: [redacted]
AP: d4[redacted]
Reason: Locally Offline.

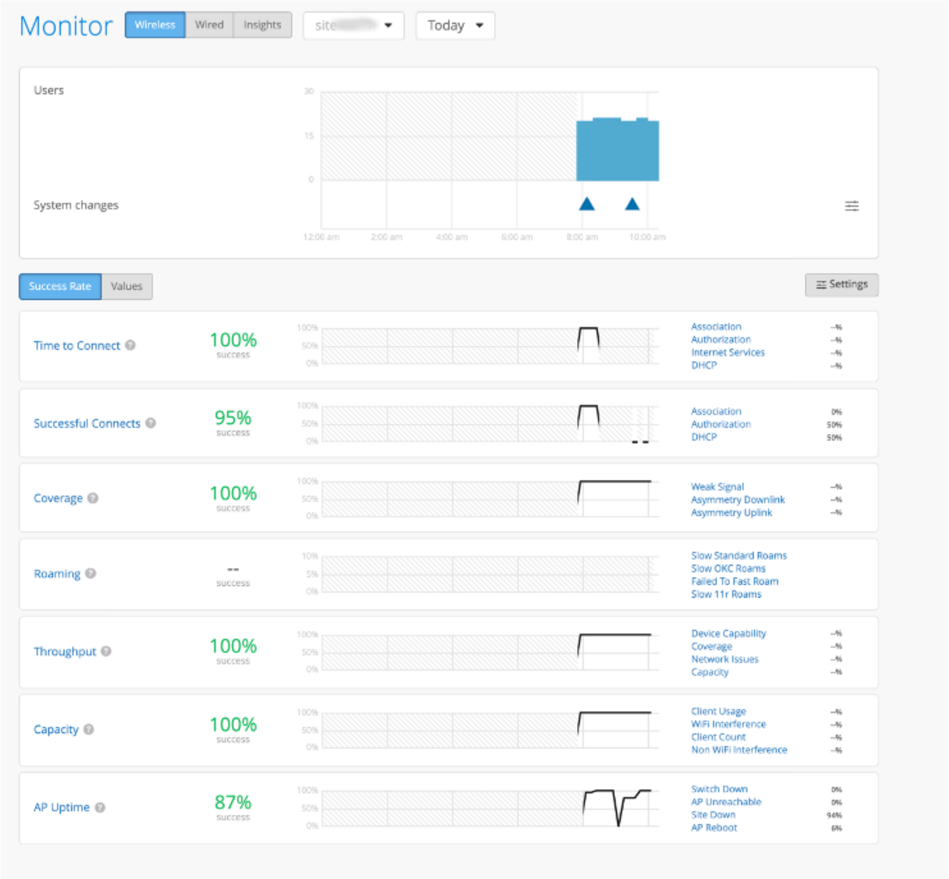
Yesterday

1/13/2021, 1:36:54 PM
AI VALIDATED
Offline
Site: [redacted]
AP: d4[redacted]
Reason: Locally Offline.

Last 7 Days

Under Marvis Actions, there was no DHCP Failure event recorded.

We followed up with this event after 30 minutes to see if it was detected in the SLE dashboard.



Time to Connect 100% success
Association –%
Authorization –%
Internet Services –%
DHCP –%

Successful Connects 95% success
Association 0%
Authorization 50%
DHCP 50%

Coverage 100% success
Weak Signal –%
Asymmetry Downlink –%
Asymmetry Uplink –%

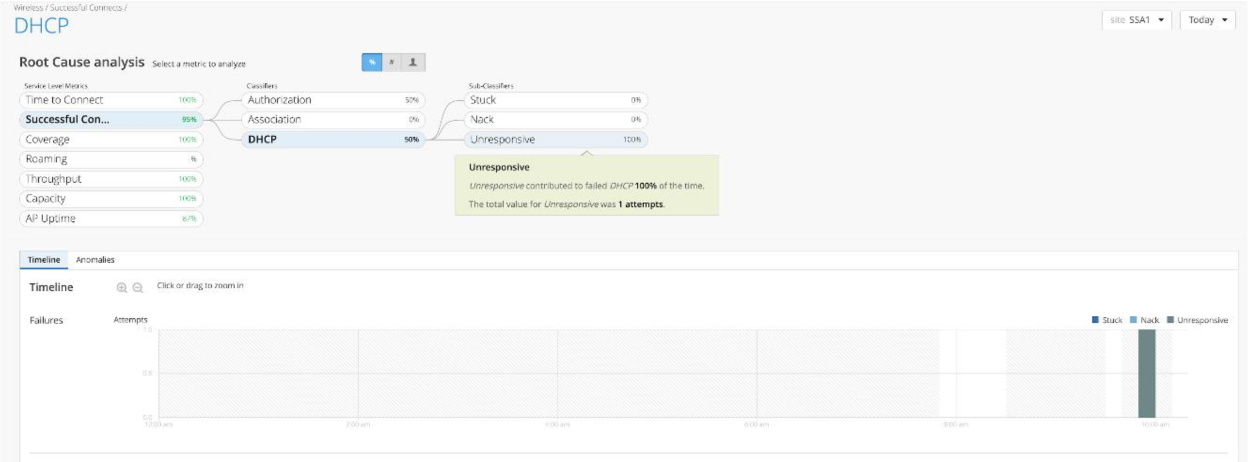
Roaming -- success
Slow Standard Roams
Slow OKC Roams
Failed To Fast Roam
Slow 11r Roams

Throughput 100% success
Device Capability –%
Coverage –%
Network Issues –%
Capacity –%

Capacity 100% success
Client Usage –%
WiFi Interference –%
Client Count –%
Non WiFi Interference –%

AP Uptime 87% success
Switch Down 0%
AP Unreachable 0%
Site Down 94%
AP Reboot 6%

After 30 minutes, and the Mist SLE dashboard registered the DHCP issue. Successful Connects reduced from 100% to 95%. We clicked on DHCP to investigate the root cause analysis.



Unresponsive

Unresponsive contributed to failed *DHCP* **100%** of the time.

The total value for *Unresponsive* was **1 attempts**.

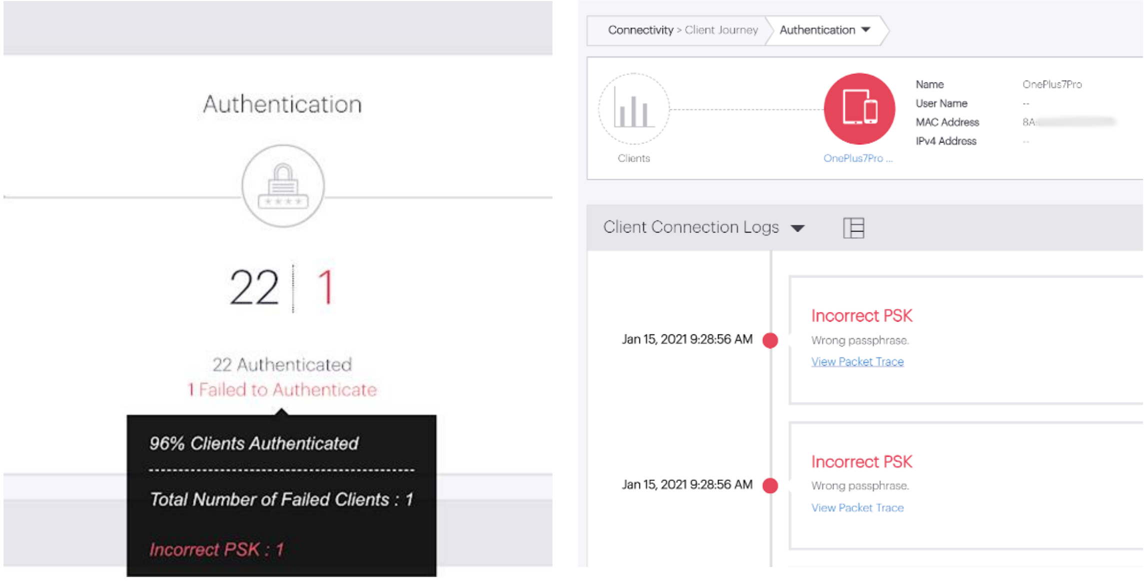
Mist's Root Cause Analysis for the DHCP event showed that a server was unresponsive and failed to this DHCP event for 1 client connection attempt.

5.3 Incorrect PSK (Password)

Using 1 AP and 1 to 4 different clients, we attempted to connect a client to the test SSID/radio with an incorrect Pre-Shared Key (PSK), or password. Clients used were a OnePlus7, MacBook Air, S10e and OnePlus8. After several minutes, of the client connection attempts, we use the tested solution's interface to determine if the issue was automatically detected, analyzed and captured.

Arista: PASS

After 5 minutes, we saw an Authentication Failure for 1 client in the Client Journey dashboard. We used only 1 client for Arista (i.e. OnePlus7) as Arista's Client Journey was able to immediately identify the PSK issue.



96% Clients Authenticated

Total Number of Failed Clients : 1

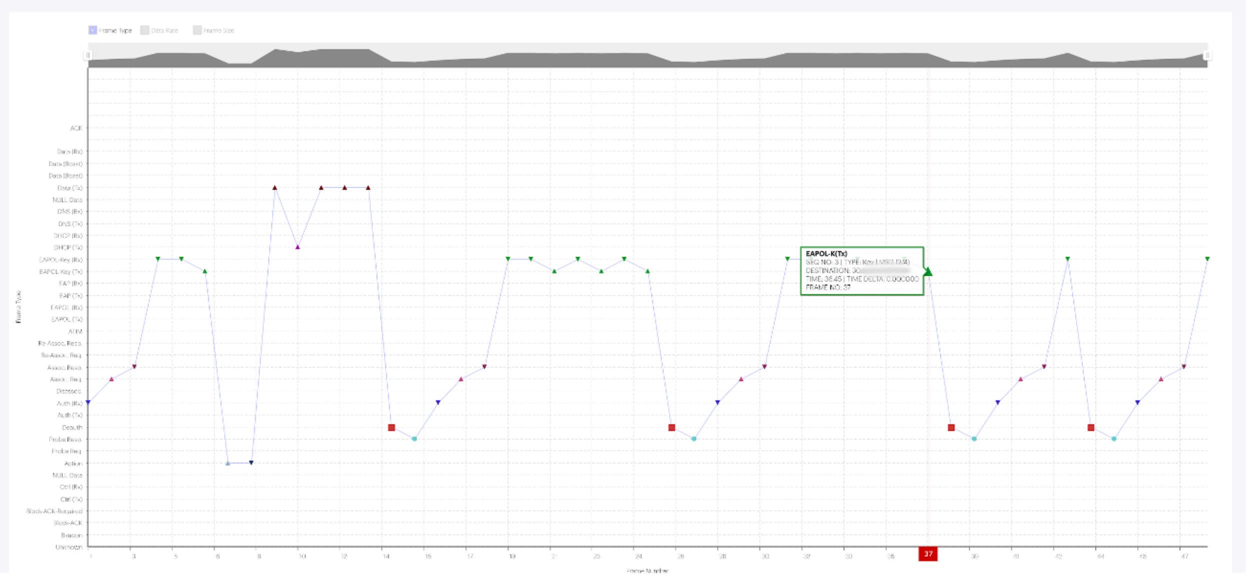
Incorrect PSK : 1

Name	OnePlus7Pro
User Name	--
MAC Address	8A[redacted]
IPv4 Address	--

Jan 15, 2021 9:28:56 AM — Incorrect PSK — Wrong passphrase. — View Packet Trace

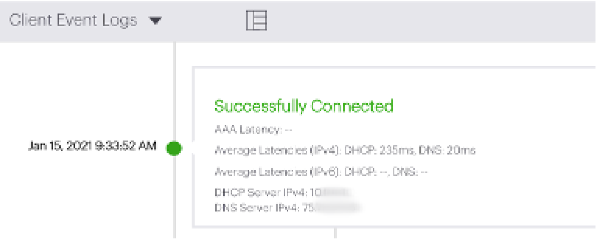
Jan 15, 2021 9:28:56 AM — Incorrect PSK — Wrong passphrase. — View Packet Trace

The Client Connection Logs showed that the wrong passphrase was used by the OnePlus7 device. We saw an auto packet capture was generated for this event, and its link brought us to the packet trace in Arista Packets (or gave the option to download to a local host) for further analysis.



Arista Packets showed us a Frame View of Packets where the EAPOL 4-Way Handshake does not make it to the third part of the sequence. This pattern indicated an incorrect PSK.

After using a correct PSK, we saw the client failure was resolved.



Jan 15, 2021 9:33:52 AM

Successfully Connected

AAA Latency: --

Average Latencies (IPv4): DHCP: 235ms, DNS: 20ms

Average Latencies (IPv6): DHCP: --, DNS: --

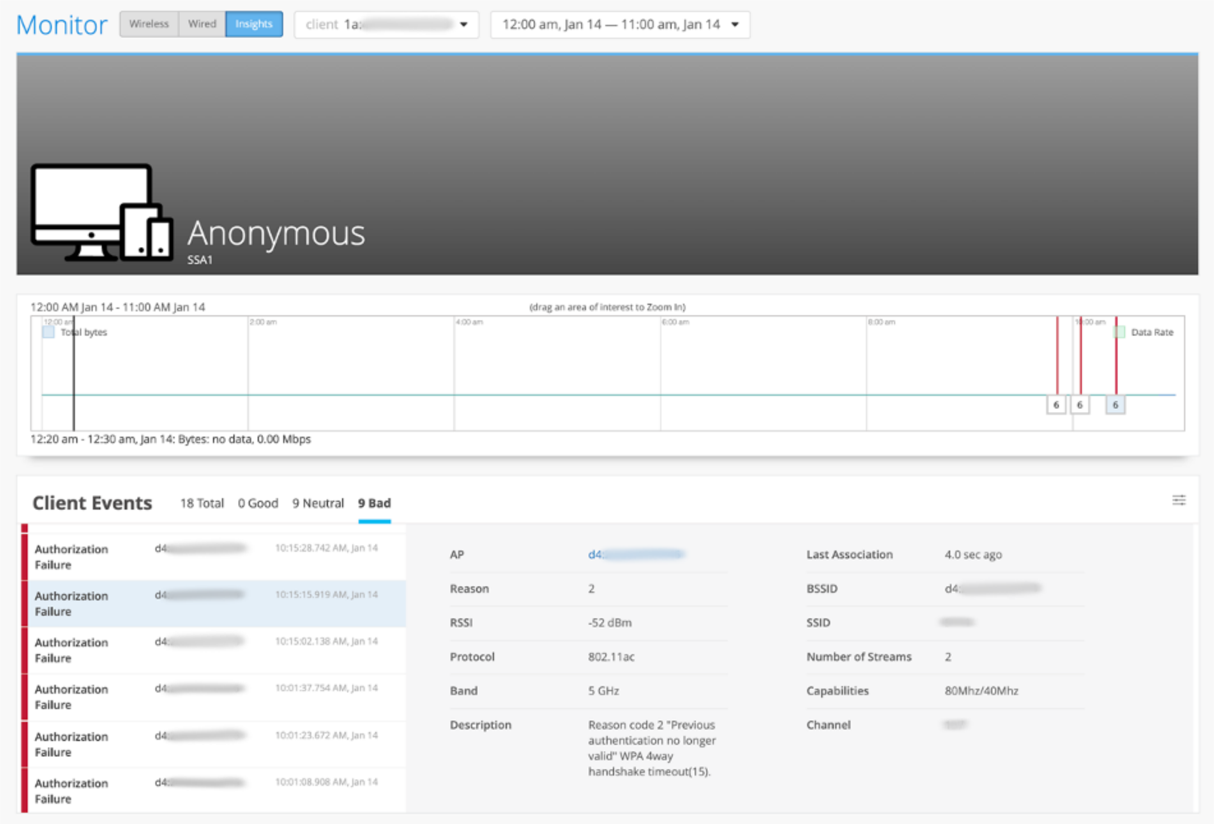
DHCP Server IPv4: 10[redacted]

DNS Server IPv4: 75[redacted]

Mist: **Limited**

Using the SLE dashboard, we observed whether the percentage of "Successful Connects" had reduced as a result of this incorrect PSK issue but saw no indication of a detected event related to the PSK issue or any other connectivity problem.

We then asked the Marvis search bar about potential connectivity issues. Initially, by searching for "any clients having trouble connecting?" was saw a list of failure correlations, but there were no clients related to the incorrect PSK issue. This was when we tried connecting with bad PSKs from additional clients. After more time, we eventually observed a new client registering a connectivity issue.



12:20 am - 12:30 am, Jan 14: Bytes: no data, 0.00 Mbps

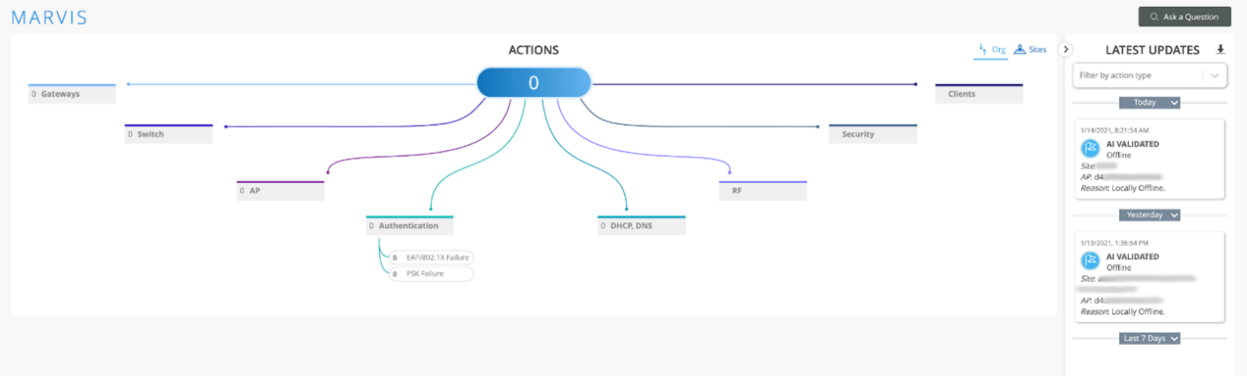
Client Events 18 Total 0 Good 9 Neutral **9 Bad**

Authorization Failure	d4[redacted]	10:15:28.742 AM, Jan 14
Authorization Failure	d4[redacted]	10:15:15.919 AM, Jan 14
Authorization Failure	d4[redacted]	10:15:02.138 AM, Jan 14
Authorization Failure	d4[redacted]	10:01:37.754 AM, Jan 14
Authorization Failure	d4[redacted]	10:01:23.672 AM, Jan 14
Authorization Failure	d4[redacted]	10:01:08.908 AM, Jan 14

AP	d4[redacted]	Last Association	4.0 sec ago
Reason	2	BSSID	d4[redacted]
RSSI	-52 dBm	SSID	[redacted]
Protocol	802.11ac	Number of Streams	2
Band	5 GHz	Capabilities	80Mhz/40Mhz
Description	Reason code 2 "Previous authentication no longer valid" WPA 4way handshake timeout(15).	Channel	[redacted]

The error was listed as an "Authentication Failure", identifying the issue as a "WPA 4way handshake timeout(15)" instead of a more precise PSK failure.

There was no automatic packet capture provided for this event for further investigation.



1/14/2021, 8:21:54 AM
AI VALIDATED
Offline
Site: [redacted]
AP: d4[redacted]
Reason: Locally Offline.

1/13/2021, 1:36:54 PM
AI VALIDATED
Offline
Site: a[redacted]
AP: d4[redacted]
Reason: Locally Offline.

In the Marvis Actions interface, we saw no registered event related to the PSK Failure.

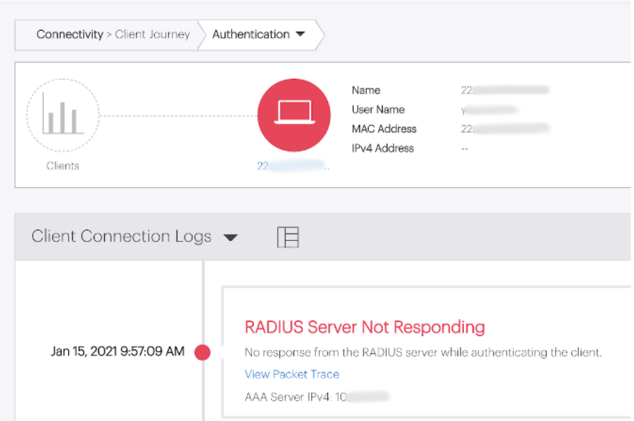
There was no automatic root cause analysis provided by Marvis for this PSK failure issue.

5.4 RADIUS Server Unresponsive

Using 1 AP and 1 client, we misconfigured a RADIUS server using a bad IP address for the test SSID/radio and attempted to connect a client (e.g. smartphone) to the test SSID/radio. After several minutes, of the client connecting, we use the tested solution's interface to determine if the issue was automatically detected, analyzed and captured.

Arista: PASS

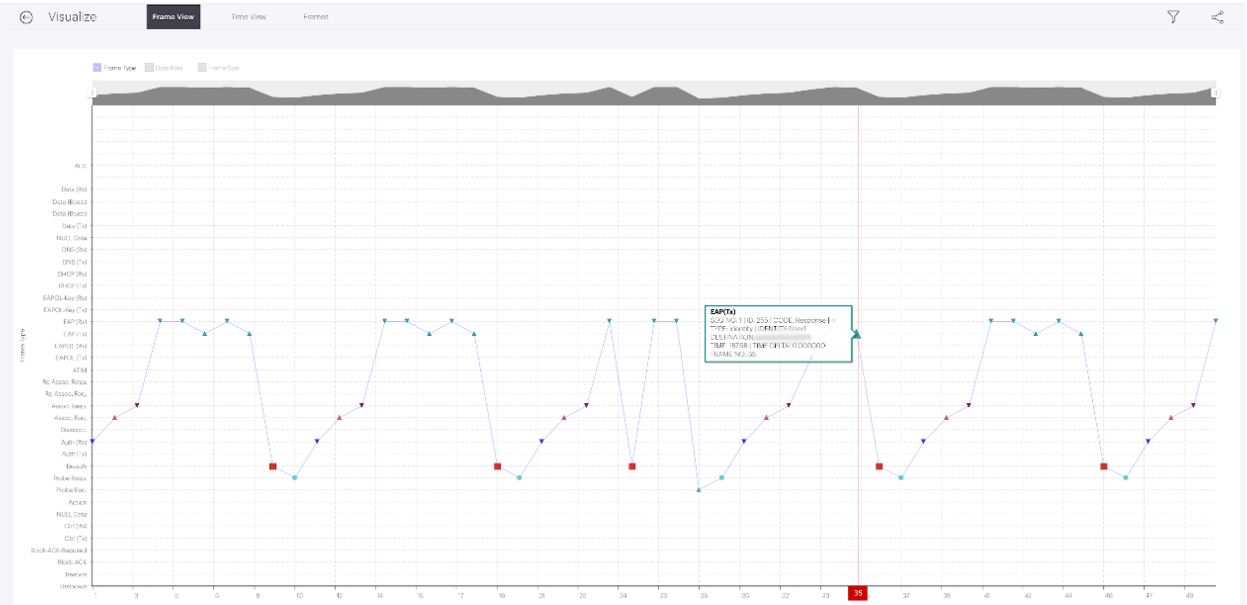
After 5 minutes, we observed an Authentication Failure in the Client Journey dashboard. When clicking on the client experiencing failure, we saw in the Client Connection Logs that this was a RADIUS Server Not Responding. We could also view the auto packet capture that was generated.



Name [redacted]
User Name [redacted]
MAC Address [redacted]
IPv4 Address --

Jan 15, 2021 9:57:09 AM

RADIUS Server Not Responding
No response from the RADIUS server while authenticating the client.
View Packet Trace
AAA Server IPv4: 10[redacted]



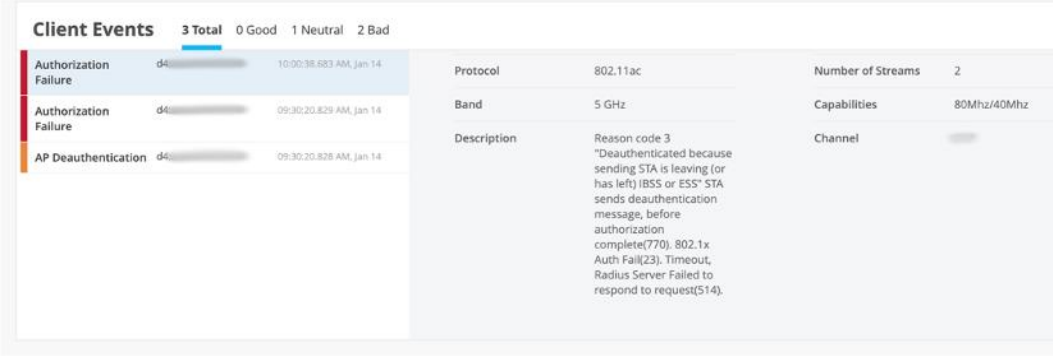
EAP(Tx)
SEQ NO: 1 | ID: 255 | CODE: Response |
TYPE: Identity | IDENTITY: [redacted]
DESTINATION: [redacted]
TIME: 187.68 | TIME DELTA: 0.000000
FRAME NO: 35

In the Frame View of Arista Packets, we saw the client and AP exchange "IDENTITY" requests and responses, but we never observed a response from the RADIUS server.

Mist: Limited

Several minutes after the event, we used the SLE dashboard to see if the RADIUS server was detected as being unresponsive but did not observe a related event.

By using the Marvis search, we asked if there were any client connectivity issues. We saw there were 2 bad instances that occurred regarding “Authorization Failure”.



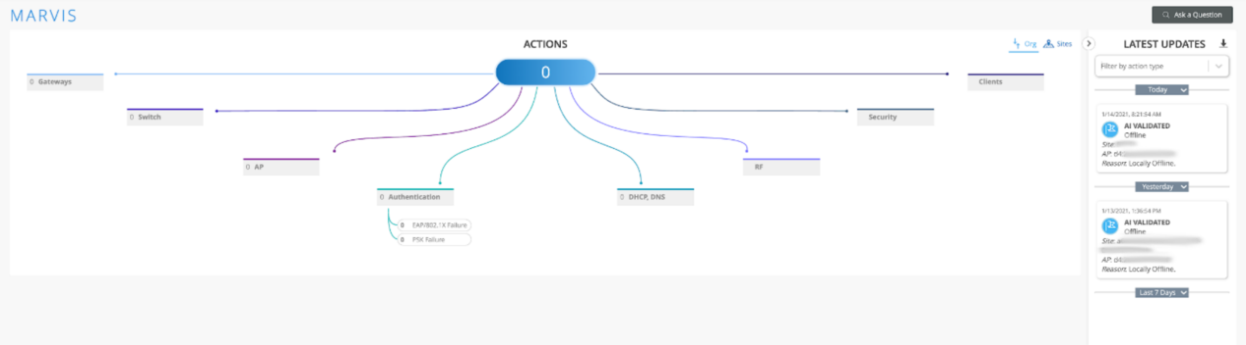
Client Events 3 Total 0 Good 1 Neutral 2 Bad

Authorization Failure	d4[redacted]	10:00:38.683 AM, Jan 14
Authorization Failure	d4[redacted]	09:30:20.829 AM, Jan 14
AP Deauthentication	d4[redacted]	09:30:20.828 AM, Jan 14

Protocol	802.11ac	Number of Streams	2
Band	5 GHz	Capabilities	80Mhz/40Mhz
Description	Reason code 3 "Deauthenticated because sending STA is leaving (or has left) IBSS or ESS" STA sends deauthentication message, before authorization complete(770). 802.1x Auth Fail(23). Timeout, Radius Server Failed to respond to request(514).	Channel	[redacted]

The error associated with the RADIUS server event was described as an authorization failure (timeout) where the “RADIUS server failed to respond to request”.

There was no automatic packet capture provided for this event.

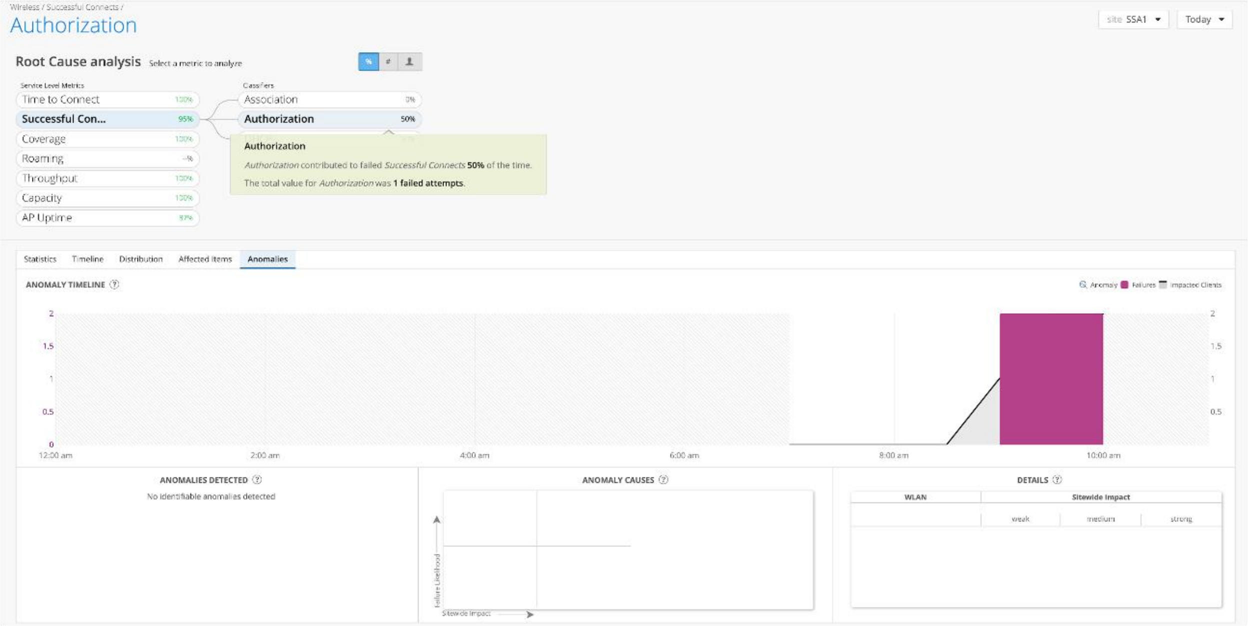


1/14/2021, 8:21:54 AM
AI VALIDATED
Offline
Site: [redacted]
AP: d4[redacted]
Reason: Locally Offline.

1/13/2021, 1:36:54 PM
AI VALIDATED
Offline
Site: a[redacted]
AP: d4[redacted]
Reason: Locally Offline.

In Marvis Actions, there was no Authentication Failure event listed, as it was in the Client Insights interface. And therefore no offered automatic root cause analysis or remediation.

After about 10 minutes post-event, this issue was successfully observed in the SLE dashboard. This proves the interface does eventually display an event, but there is a delay.



Authorization

Authorization contributed to failed *Successful Connects* **50%** of the time.

The total value for *Authorization* was **1 failed attempts**.

No identifiable anomalies detected

When looking at the root cause analysis for this event, we saw the Authorization failure was listed as contributing to 1 of the failed client connection attempts.

6.0 Client / Application / Network Performance Issues

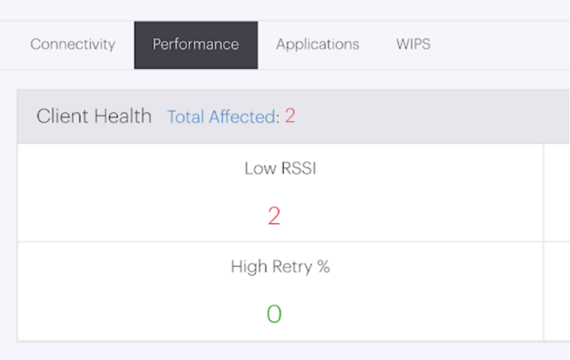
6.1 Poor Coverage / Low RSSI

Using one AP and 1 to 3 clients, we moved clients to the edge of the cell coverage (e.g. -70dBm to -80dBm) to test the SSID/radio.

Arista: PASS

Before moving the clients, the RSSI for the MacBook Air and OnePlus7 devices were -48 dBm and -52 dBm, respectively. Once we move the clients to the edge the cell coverage, this dropped to -80 dBm and -76 dBm, respectively. The goal was to be -65 dBm or better.

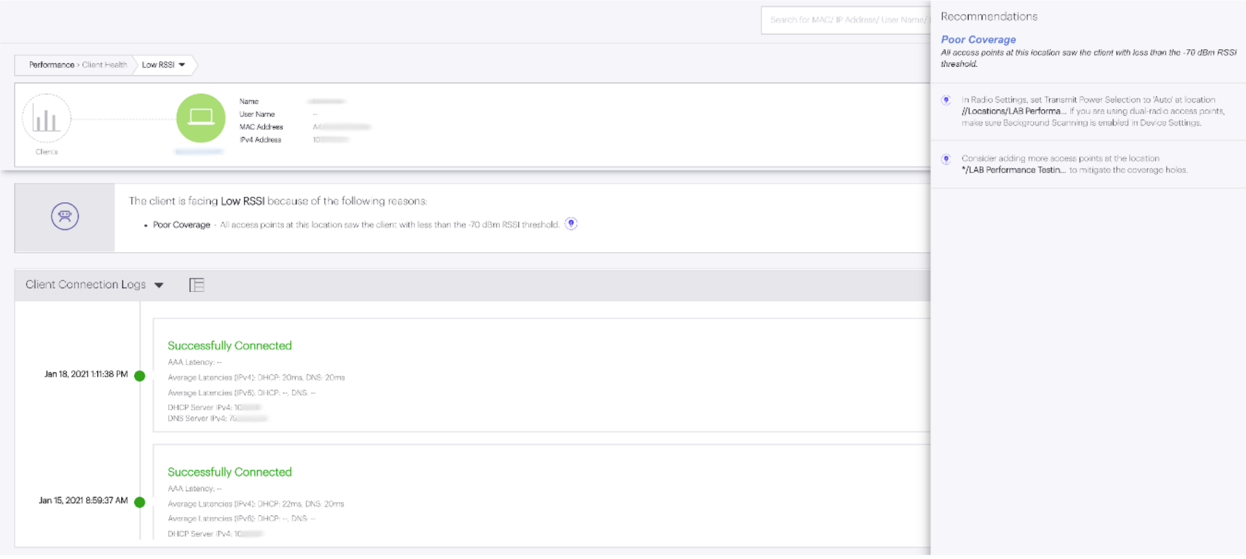
We saw that 2 clients were found to have Low RSSI, with signal strength below the threshold of -70 dBm – a manually set threshold.



Client Health Total Affected: 2

Low RSSI 2

High Retry % 0


Search for MAC/ IP Address/ User Name/
Performance > Client Health
Low RSSI
Clients
Client Connection Logs

Name [redacted]
User Name --
MAC Address [redacted]
IPv4 Address [redacted]

The client is facing Low RSSI because of the following reasons:

- Poor Coverage - All access points at this location saw the client with less than the -70 dBm RSSI threshold.

Jan 18, 2021 1:11:38 PM
Successfully Connected
AAA Latency: --
Average Latencies (IPv4): DHCP: 20ms, DNS: 20ms
Average Latencies (IPv6): DHCP: --, DNS: --
DHCP Server IPv4: [redacted]
DNS Server IPv4: [redacted]

Jan 15, 2021 8:59:37 AM
Successfully Connected
AAA Latency: --
Average Latencies (IPv4): DHCP: 22ms, DNS: 20ms
Average Latencies (IPv6): DHCP: --, DNS: --
DHCP Server IPv4: [redacted]

Recommendations

Poor Coverage
All access points at this location saw the client with less than the -70 dBm RSSI threshold.

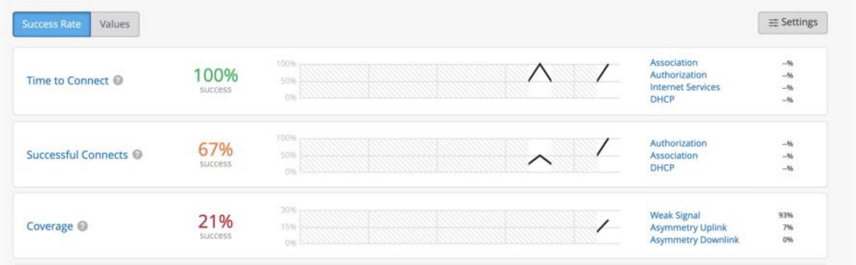
In Radio Settings, set Transmit Power Selection to 'Auto' at location //Locations/LAB Performa... If you are using dual-radio access points, make sure Background Scanning is enabled in Device Settings.

Consider adding more access points at the location */LAB Performance Testin... to mitigate the coverage holes.

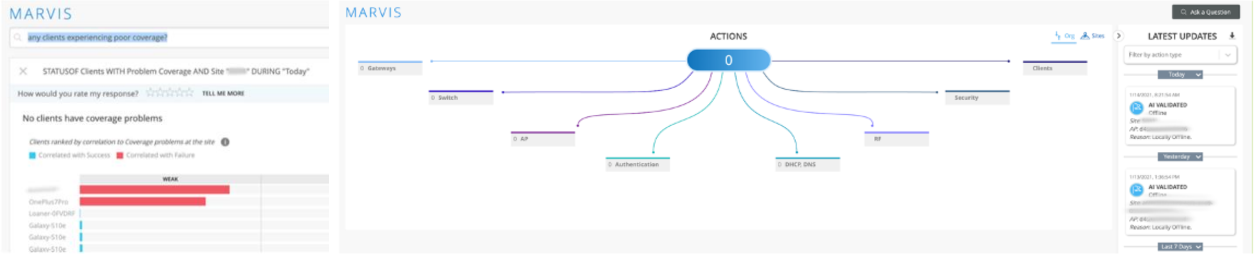
We saw the Inference Engine suggested the root cause for the client's Low RSSI operation was Poor Coverage. By clicking on the lightbulb icon beside it, we saw a panel of remediation recommendations offered by the Inference Engine. One recommendation was to move more APs to the location to mitigate coverage holes. The other recommendation was to enable automatic AP Tx power, which was disabled at the time of testing.

Mist: LIMITED

We observed no coverage related issues in the SLE dashboard at first, but eventually saw there was only 21 percent success due mostly to a weak signal.



Time to Connect	100% success	Association Authorization Internet Services DHCP	--% --% --% --%
Successful Connects	67% success	Authorization Association DHCP	--% --% --%
Coverage	21% success	Weak Signal Asymmetry Uplink Asymmetry Downlink	93% 7% 0%



any clients experiencing poor coverage?

STATUSOF Clients WITH Problem Coverage AND Site "[redacted]" DURING "Today"

How would you rate my response? ☆☆☆☆☆ TELL ME MORE

No clients have coverage problems

Clients ranked by correlation to Coverage problems at the site

🟦 Correlated with Success 🟥 Correlated with Failure

[redacted]
OnePlus7Pro
Loaner-0FVDRF
Galaxy-S10e
Galaxy-S10e
Galaxy-S10e

1/14/2021, 8:21:54 AM
AI VALIDATED
Offline
Site: [redacted]
AP: d4[redacted]
Reason: Locally Offline.

1/13/2021, 1:36:54 PM
AI VALIDATED
Offline
Site: [redacted]
AP: d4[redacted]
Reason: Locally Offline.

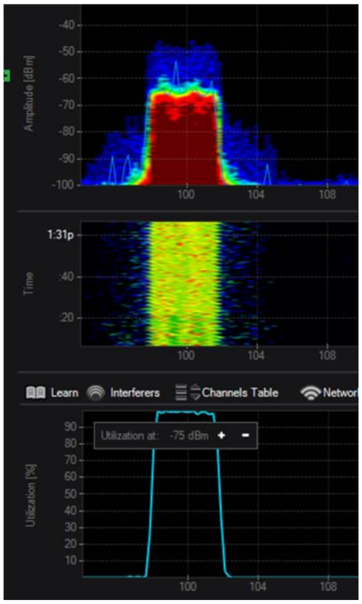
Both the MacBook Air and OnePlus7 Pro devices showed poor coverage when using the Marvis search feature. When using Marvis Actions, we saw no indication of this weak signal error. No recommended remediation was provided.

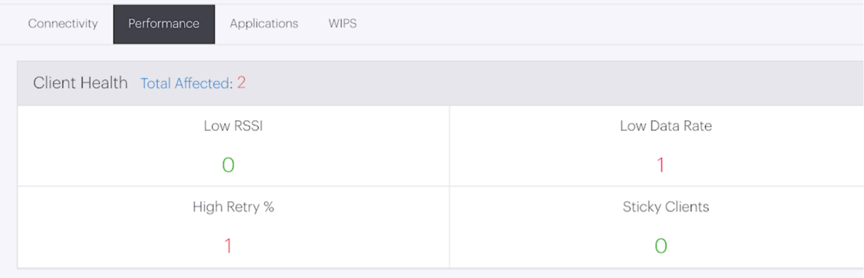
6.2 High Channel Congestion / High Retry Rate

Using 1 AP and 3 Clients, we sent unlimited TCP traffic generated by Ixia IxChariot to the clients connected to the test SSID/radio.

Arista: PASS

For the 3 clients on Channel 100, we saw high utilization in the Wi-Spy spectrum analyzer. In IxChariot, we saw an average throughput of 163 Mbps, with relatively even distribution of bandwidth among clients.



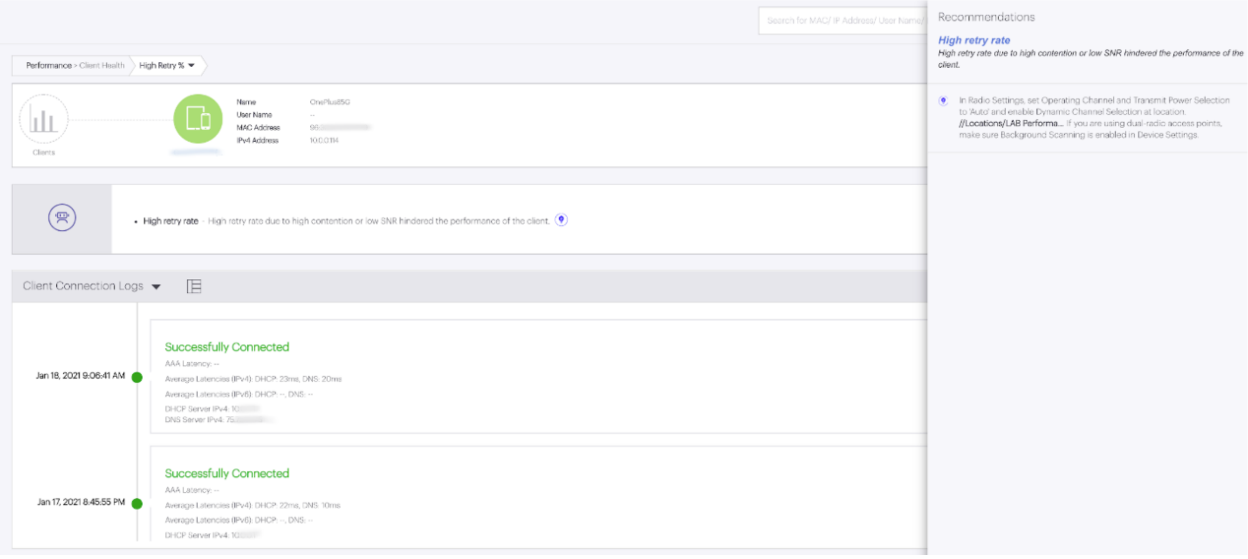


Client Health Total Affected: 2

Low RSSI	Low Data Rate
0	1
High Retry %	**Sticky Clients**
1	0

In the Client Health dashboard, we observed 1 client experiencing a High Retry rate. When clicking on this client, we saw details for this client (e.g. associated AP, SSID, 802.11ax capability, 5-GHz frequency band and location). While the client was successfully connected, we saw the message: "High retry due to high contention or low SNR hindered the performance of the client."

By clicking on the lightbulb icon, we were able to see how the Inference Engine offers to remediate this congestion issue.



Search for MAC/ IP Address/ User Name/
Performance > Client Health
High Retry %
Clients
Client Connection Logs

Name OnePlus8 5G
User Name --
MAC Address 96:[redacted]
IPv4 Address 10.0.0.114

- High retry rate - High retry rate due to high contention or low SNR hindered the performance of the client.

Jan 18, 2021 9:06:41 AM
Successfully Connected
AAA Latency: --
Average Latencies (IPv4): DHCP: 23ms, DNS: 20ms
Average Latencies (IPv6): DHCP: --, DNS: --
DHCP Server IPv4: 10[redacted]
DNS Server IPv4: 75.[redacted]

Jan 17, 2021 8:45:55 PM
Successfully Connected
AAA Latency: --
Average Latencies (IPv4): DHCP: 22ms, DNS: 10ms
Average Latencies (IPv6): DHCP: --, DNS: --
DHCP Server IPv4: 10[redacted]

Recommendations

High retry rate
High retry rate due to high contention or low SNR hindered the performance of the client.

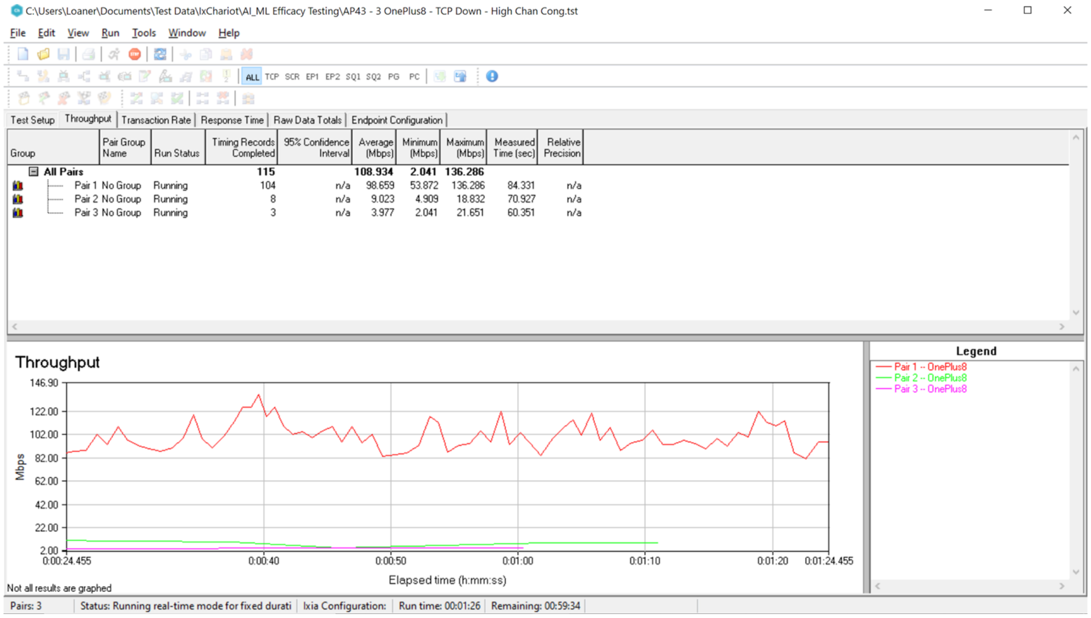
In Radio Settings, set Operating Channel and Transmit Power Selection to 'Auto' and enable Dynamic Channel Selection at location. //Locations/LAB Performa... If you are using dual-radio access points, make sure Background Scanning is enabled in Device Settings.

The Inference Engine shows the high retry rate was a result of high contention or low SNR and suggests setting the Operating Channel and Transmit Power Selection to 'Auto' and enabling Dynamic Channel Selection at the location. Additionally, if using dual APs, the Background Scanning feature should be enabled in the device settings.

The Remediation Recommendation offered was to consider enabling Auto Channel, Auto AP Tx Power, and Dynamic Channel Selection. It is important to note that the Inference Engine knew that these features were disabled. Had these features been enabled, the Inference Engine would not have made this remediation recommendation.

Mist: LIMITED

With congestion, Mist displayed indications of capacity issues. We had set a threshold for the customizable service levels – similar to Arista's Automatic Baselining, but this required manual tuning.



C:\Users\Loaner\Documents\Test Data\IxChariot\AI_ML Efficacy Testing\AP43 - 3 OnePlus8 - TCP Down - High Chan Cong.tst

Group	Pair Group Name	Run Status	Timing Records Completed	95% Confidence Interval	Average (Mbps)	Minimum (Mbps)	Maximum (Mbps)	Measured Time (sec)	Relative Precision
All Pairs			**115**		**108.934**	**2.041**	**136.286**		
Pair 1	No Group	Running	104	n/a	98.659	53.872	136.286	84.331	n/a
Pair 2	No Group	Running	8	n/a	9.023	4.909	18.832	70.927	n/a
Pair 3	No Group	Running	3	n/a	3.977	2.041	21.651	60.351	n/a

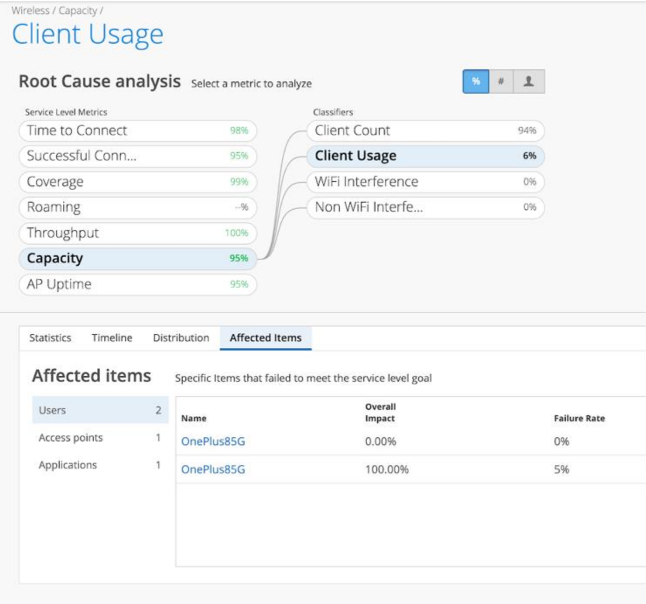
Pairs: 3 | Status: Running real-time mode for fixed durati | Ixia Configuration: | Run time: 00:01:26 | Remaining: 00:59:34

For the 3 clients, we saw an average of 109 Mbps throughput. However, 2 of 3 clients received less than 10 percent of the data rate of the first client. This showed that bandwidth was very unbalanced.

We saw high bandwidth utilization on Channel 100, where the 3 clients were connected, when using the Wi-Spy Spectrum Analyzer.

When looking at Capacity in the SLE dashboard, we saw a drop to 96 percent. This indicated issues that could be investigated with the Root Cause Analysis interface, where we saw a list of affected clients.

We found that "Client Count contributed to failed Capacity 94% of the time", which is a misdiagnosis as it was High Client Usage rather than Client Count that was the cause of the high channel capacity.



Wireless / Capacity /

Client Usage

Root Cause analysis Select a metric to analyze

% #

Service Level Metrics	
Time to Connect	98%
Successful Conn...	95%
Coverage	99%
Roaming	--%
Throughput	100%
Capacity	**95%**
AP Uptime	95%

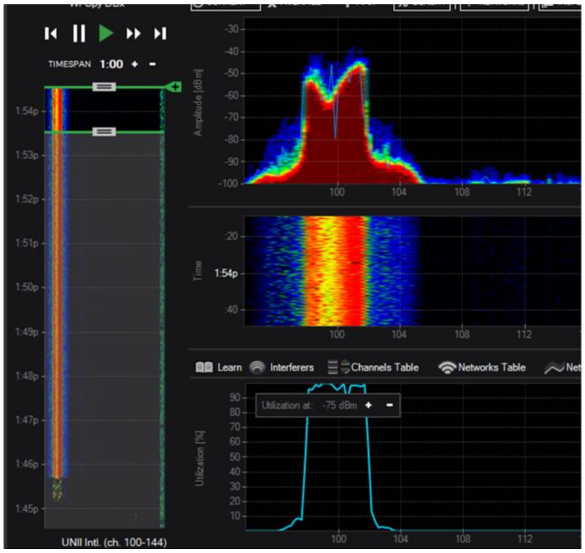
Classifiers	
Client Count	94%
Client Usage	**6%**
WiFi Interference	0%
Non WiFi Interfe...	0%

Statistics | Timeline | Distribution | **Affected Items**

Affected items Specific Items that failed to meet the service level goal

Users	2
Access points	1
Applications	1

Name	Overall Impact	Failure Rate
OnePlus85G	0.00%	0%
OnePlus85G	100.00%	5%



When using the Marvis search feature, and asked "any capacity issues?", we saw that 9 percent of users were below the service level goal set earlier, as a result of Capacity Client Usage issues. The two clients affected were two OnePlus8 devices.

However, the Marvis Actions dashboard did not show any instance of capacity related issues. We did not observe any remediation recommendations when troubleshooting.

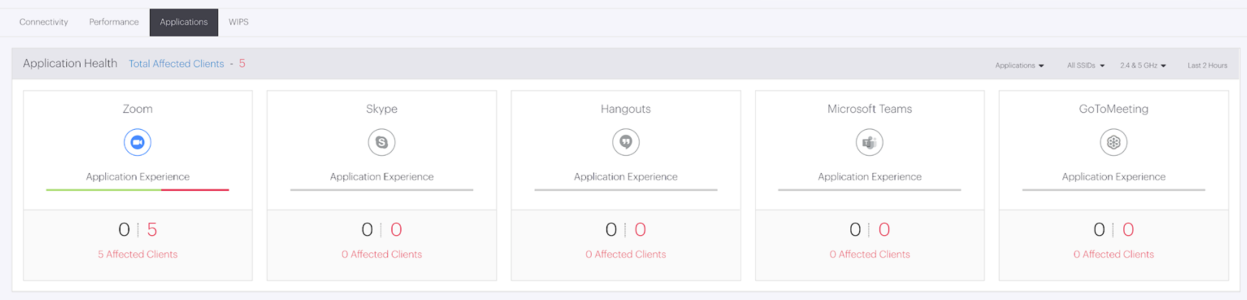
6.3 Poor Application Performance

This test used 1 AP and 10 clients. The following steps were performed:

1. Configure the test SSID/radio to a static channel (i.e. no auto channel).
2. Connect 10 clients to the test SSID/radio.
3. Start a Zoom video call between 4 clients connected to the test SSID/radio.
4. Move 4 of the Zoom clients to the edge of the cell coverage (e.g. -70 dBm to -80 dBm).
5. Use IxChariot to send a mix of voice, video and data traffic (all AC_BE) to remaining 6 clients.

Arista: PASS

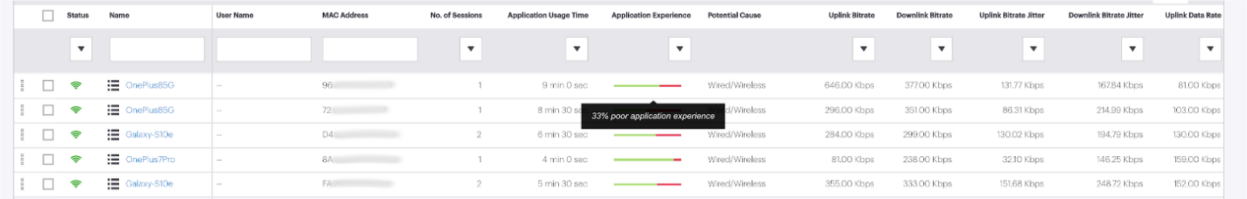
We saw a list of 1,976 applications used under WiFi > Application Visibility. Under Application Health, we observed 5 clients experiencing poor application performance with Zoom.



Application Health Total Affected Clients - 5

Zoom	Skype	Hangouts	Microsoft Teams	GoToMeeting
Application Experience	Application Experience	Application Experience	Application Experience	Application Experience
0 | 5	0 | 0	0 | 0	0 | 0	0 | 0
5 Affected Clients	0 Affected Clients	0 Affected Clients	0 Affected Clients	0 Affected Clients

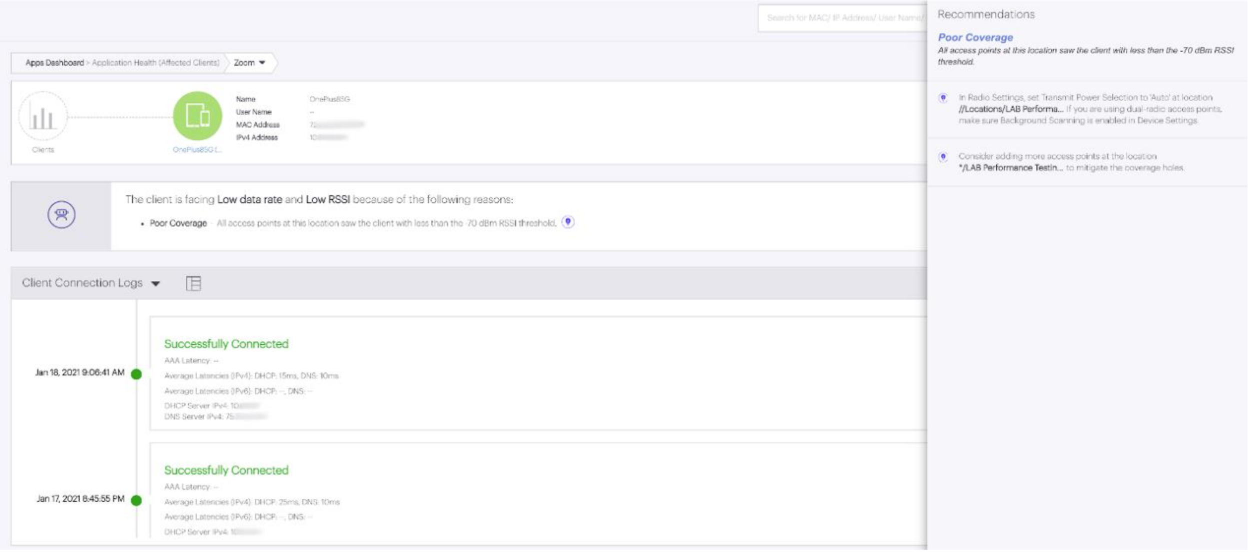
We clicked the red "5" to see the list of affected clients with details regarding this issue.



□	Status	Name	User Name	MAC Address	No. of Sessions	Application Usage Time	Application Experience	Potential Cause	Uplink Bitrate	Downlink Bitrate	Uplink Bitrate Jitter	Downlink Bitrate Jitter	Uplink Data Rate
□		OnePlus85G	--	96[redacted]	1	9 min 0 sec		Wired/Wireless	646.00 Kbps	377.00 Kbps	131.77 Kbps	167.84 Kbps	81.00 Kbps
□		OnePlus85G	--	72[redacted]	1	8 min 30 s		d/Wireless	296.00 Kbps	351.00 Kbps	86.31 Kbps	214.99 Kbps	103.00 Kbps
□		Galaxy-S10e	--	D4[redacted]	2	6 min 30 sec		Wired/Wireless	284.00 Kbps	299.00 Kbps	130.02 Kbps	194.79 Kbps	130.00 Kbps
□		OnePlus7Pro	--	8A[redacted]	1	4 min 0 sec		Wired/Wireless	81.00 Kbps	238.00 Kbps	32.10 Kbps	146.25 Kbps	159.00 Kbps
□		Galaxy-S10e	--	FA[redacted]	2	5 min 30 sec		Wired/Wireless	355.00 Kbps	333.00 Kbps	151.68 Kbps	248.72 Kbps	152.00 Kbps

33% poor application experience

By hovering over the Application Experience bar, we observed 33 percent poor application experience for one of the OnePlus8 clients.



Search for MAC/ IP Address/ User Name/

Apps Dashboard > Application Health (Affected Clients) > Zoom

Clients

OnePlus8SG (...

Name OnePlus8SG

User Name --

MAC Address [redacted]

IPv4 Address [redacted]

The client is facing **Low data rate** and **Low RSSI** because of the following reasons:

- **Poor Coverage** - All access points at this location saw the client with less than the -70 dBm RSSI threshold.

Client Connection Logs

Jan 18, 2021 9:06:41 AM

Successfully Connected

AAA Latency: --

Average Latencies (IPv4): DHCP: 15ms, DNS: 10ms

Average Latencies (IPv6): DHCP: --, DNS: --

DHCP Server IPv4: [redacted]

DNS Server IPv4: [redacted]

Jan 17, 2021 8:45:55 PM

Successfully Connected

AAA Latency: --

Average Latencies (IPv4): DHCP: 25ms, DNS: 10ms

Average Latencies (IPv6): DHCP: --, DNS: --

DHCP Server IPv4: [redacted]

Recommendations

Poor Coverage

All access points at this location saw the client with less than the -70 dBm RSSI threshold.

In Radio Settings, set Transmit Power Selection to 'Auto' at location **//Locations/LAB Performa...** If you are using dual-radio access points, make sure Background Scanning is enabled in Device Settings.

Consider adding more access points at the location ***/LAB Performance Testin...** to mitigate the coverage holes.

Root causes analysis of one of the affected clients showed the Low Data Rate and Low RSSI was because of poor coverage. The lightbulb icon shows the remediation suggestions offered by the Inference Engine on the right panel. Such recommendations include Background Scanning enablement and adding more APs to the location for better coverage.

Mist: FAIL

This feature is not supported.

About Miercom

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

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

Use of This Report

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

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, 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.