Network Testing & Emulation Solutions

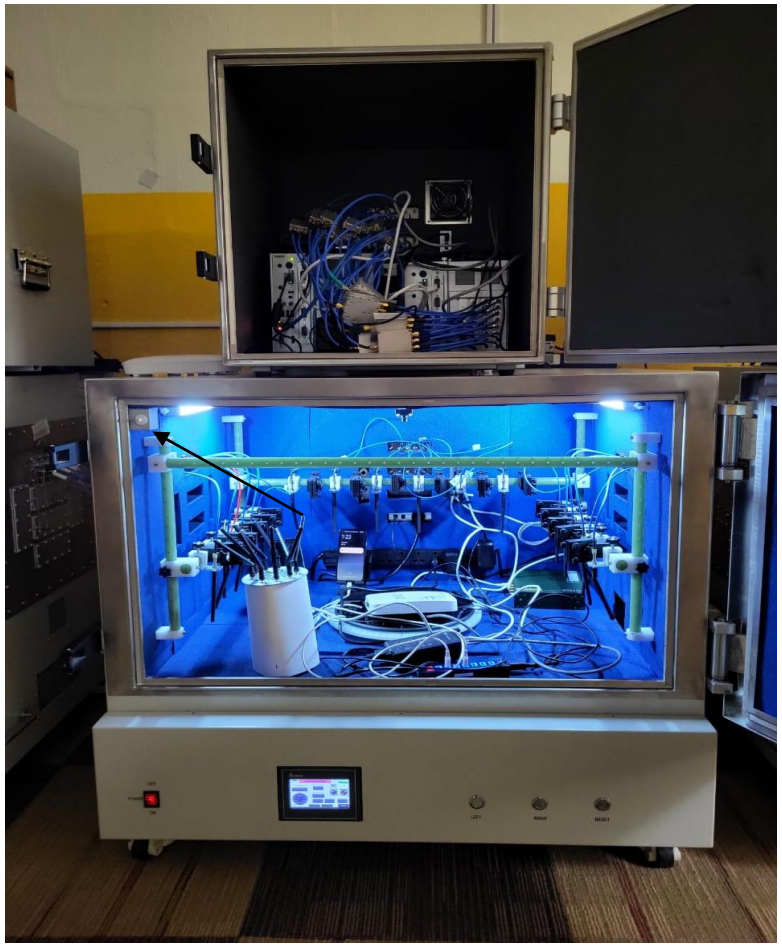
GENERIC VENDOR NEUTRAL TESTING RESULTS

Test Setup1

Our Real Clients Testing Lab includes 70+ real devices spanning various operating systems and Wi-Fi configurations. We conduct a wide range of tests such as video streaming, Zoom conferencing, and other real-time scenarios to generate comprehensive performance reports from the client's perspective. The entire lab is fully automated, remotely accessible, and features a Web UI for test execution and monitoring.

Test Setup2

In addition to this, we have another setup equipped with attenuators to perform tests such as Rate vs. Range, Rate vs. Orientation, Auto Channel Selection, AP Coexistence, Roaming, TR-398 Issue 4 with both Real and Virtual clients.



Test Coverage

Category	Tests Included
Basic Functionality	Basic Client Connectivity
Scale & Load	Scale Clients Test
	Stress Test (12 Hours)
	Mixed Traffic Test
	Port Reset Test
Roaming & Mobility	Roaming Test
	Load Balancing Test
	Band Steering Test
Performance & Traffic	Throughput Test (Incremental Clients)
	QoS Test
	HTTP Test
	Multicast Traffic Test
	YouTube Streaming Test
	Zoom Call Test
	Video Streaming Test
	Ping Plotter Test
	Rate vs Range (RvR) Test
	Dataplane Test
	Real Browser Test
RF & Channel Management	Auto Channel Selection Test
	AP Coexistence Test
Advanced Features	Airtime Fairness Test
	Rate Limiting Test
	Preamble Puncturing Test
	eMLSR Test
	Captive Portal Test

Summary

1. **Basic Client Connectivity:** All 39 devices successfully completed the 4-way handshake and associated with the SSID. Channel utilization remained low across all bands.

2. **Scale Test:** A total of 226 clients connected to the SSID. Some clients failed the 4-way handshake due to the maximum client count being reached on the 5GHz band.

3. **Port Reset Test:** Over 12 hours, 7,200 reset events were triggered, with 5,401 successfully restoring connections. Despite multiple scan and association attempts, some resets did not re-establish connectivity.

4. **QoS Test:** ToS bit prioritization was tested across UDP and TCP. QoS performed well up to 10 clients but became inconsistent with 20 or more. High channel utilization led to client disconnections.

5. **Throughput Test:** Throughput degradation of 80–100Mbps was observed at 25, 35, and 39 clients. High utilization levels caused client deauthentications, with some reconnecting post-test.

6. **Stress Test:** A 12-hour test with 39 devices showed periodic throughput drops of ~100Mbps every four minutes, reducing final throughput to ~612Mbps. Missing beacon packets were identified as a possible cause.

7. **eMLSR Test:** A client was connected on the 6GHz band with QoS traffic, while interference was introduced on the same channel. Upon interference, the link transitioned to 5GHz, but the QoS data flow remained on 6GHz instead of shifting.

Summary

8. **Mixed Traffic Test:** Multiple traffic types ran successfully on 36 devices, but high utilization led to client disconnections. Logs indicated frequent reassociation attempts.

9. **Multicast Traffic Test:** A 25Mbps multicast stream was tested across various OS devices, with all 39 clients receiving traffic as expected, without disconnections.

10. **HTTP Download Test:** All 34 devices successfully downloaded a 25MB file in five minutes. However, eight devices downloaded fewer times than expected, though all remained connected.

11. **Automatic Channel Selection (ACS) Test:** The Automatic Channel Selection (ACS) test was performed on 2.4 GHz, 5 GHz, and 6 GHz bands in AC, AX, and BE modes. Despite the AP being set to "Auto" for channel selection, no channel change occurred during the test. Initial channel assignments were 2.4 GHz → Channel 1, 5 GHz → Channel 36, and 6 GHz → Channel 85. Even with interference introduced on active channels, no channel switch was observed.

12. **AP Coexistence Test:** The AP Coexistence test was conducted across AC, AX, and BE modes on all the 3bands. This test is partially passed, with successful results for co-channel and overlapping interference but a failure in adjacent interference due to a ~300 Mbps throughput shortfall.

13. **Ping Plotter Test:** A Ping Plotter test was conducted with 36 devices for 10 minutes, measuring network connectivity to www.mi.com. Four clients experienced packet loss (12–21 packets), but all remained connected throughout the test.

Summary

14. **Video Streaming Test:** The video streaming test was conducted on all Android devices using the Dash Media source for 15 minutes to assess access point performance and stability. Key parameters measured included buffering events, wait time, per-client video bitrate, and video quality. While most clients streamed successfully, 4 out of 23 devices failed to complete the video within the allotted time, resulting in a reported URL value of 0 for those devices.

15. **Real Browser Test:** A Real Browser test was conducted on all Android devices to browse www.mi.com for 10 minutes. All 22 Android devices successfully accessed the website without any client disconnections throughout the test duration.

16. **YouTube Streaming Test:** A YouTube streaming test was conducted across multiple laptops by providing a YouTube URL and setting the resolution to 720p for 10 minutes. During playback, key statistics such as video resolution, buffer health, total frames, and dropped frames were collected. No significant drops were observed, and buffer health remained consistent across all devices.

17. **Zoom Call Test:** A Zoom call test was conducted across multiple laptops, with one device as the host and others as clients, for a duration of 10 minutes. Key performance metrics, including average latency, jitter, and packet loss, were collected. No significant packet drops were observed in audio or video, and all client devices remained connected throughout the test.

Summary

18. **Roaming Test:** During roaming between the Root AP and Node1, virtual clients experienced deauthentication (**Reason Codes 0x0002, 0x000d, 0x0009**) but reconnected after the 4-way handshake. Real clients showed mixed behavior, one roamed successfully, while others disconnected and rejoined instead of a seamless handoff. When roaming back to the Root AP, all real clients were deauthenticated (**Reason Code 0x0003**) before reconnecting.

19. **Preamble Puncturing Test:** During Preamble Puncturing testing, the VENDOR AP failed to exclude the punctured 20 MHz subchannel (channel 44) when interference was introduced.

20. **Load Balancing Test:** During load balancing testing, the 5 GHz band denied new client associations despite being well below the configured limit. AP logs reported an inability to handle more clients, while the Insight Cloud dashboard incorrectly indicated that the maximum client limit had been reached.

21. **Airtime Fairness Test:** Tested AP's ability to fairly share airtime between two clients under different conditions. Traffic was set to overload the AP, and the test passed if both clients maintained at least 45% of their measured TCP throughput. The test was successful across 5GHz and 6GHz bands in AX and BE modes.

22. **Rate Limiting Test:** Rate limiting was enabled on the AP via Insight Cloud with limits set to 250 Mbps (download) and 140 Mbps (upload). A client on a Tri-band SSID was tested using TCP and UDP and observed that the throughput attained stayed below the set limits, confirming the feature working as expected.

Summary

23. **RVR Test:** RvR testing with and without MLO showed similar throughput across all attenuation levels, indicating no significant performance gain from enabling MLO.

24. **Dataplane Test:** Data plane testing with MLO enabled and disabled showed no measurable throughput improvement. Tests used MTU-sized BE traffic over bgn, an, and a modes.

25. **Band steering Test:** Tested with enabling and disabling different options like MLO, band steering, and 802.11r settings at various distances. In all cases, clients disconnected and reconnected to switch bands, performing a full 4-way handshake.

26. **Captive Portal Test:** Tested with 50 clients, including 2 real devices and 48 virtual clients. In the first scenario, a basic captive portal without URL redirection worked as expected, and all clients were able to view the splash page and authenticate successfully. In the second scenario, redirection to a vendor-hosted website with a custom logo applied via the cloud management platform also functioned correctly, with both real and virtual clients able to view the page and proceed with authentication. In the third scenario, using an external portal with Web/HTTP authentication, the login page displayed properly when the splash page URL was included in the Walled Garden, allowing clients to enter credentials and authenticate. However, when the splash page URL was removed from the Walled Garden, both real and virtual clients failed to load the login interface, resulting in an inability to authenticate.

List of Issues Observed During Testing

Issue Observed	Explanation	Observed In Test
Maximum Client Limit Reached	Some clients failed the 4-way handshake as the 5GHz band hit the client limit.	Scale Test
Link Steered to 5GHz, but QoS Data Flow Remains on 6GHz	When interference triggered band steering from 6GHz to 5GHz, the link moved, but QoS traffic remained on 6GHz instead of shifting to the new band.	eMLSR Test
Port Reset Failures	Out of 7,200 reset events, 1,799 failed to restore connections despite multiple attempts.	Port Reset Test
QoS Inconsistency	QoS worked well up to 10 clients but became unstable with 20+ clients, leading to disconnections.	QoS Test
Throughput Degradation	High channel utilization caused a drop of 80-100Mbps at various client counts and led to deauthentications.	Throughput Test
Periodic Throughput Drops	Every four minutes, throughput dropped by ~100Mbps, reducing the final throughput to ~612Mbps. Missing beacon packets were suspected.	Stress Test
High Utilization Disconnections	Multiple devices experienced disconnections due to excessive channel utilization, leading to frequent reassociation attempts.	Mixed Traffic Test

List of Issues Observed During Testing

Issue Observed	Explanation	Observed In Test
AP Dashboard Displays Incorrect Client Count and Channel Utilization	The AP dashboard continued displaying two MAC clients on 5GHz after all clients disconnected. Additionally, incorrect channel utilization was reported for 6GHz even when no clients were connected.	Dashboard Validation
Auto Channel Selection (ACS) Not Operating as Expected	ACS failed to change channels across all three bands (2.4 GHz, 5 GHz, 6 GHz) despite interference, even when set to "Auto" in the AP dashboard.	ACS Test
Clients Experiencing Deauthentication During Handoff between Aps	Virtual clients experienced deauthentication but successfully reconnected after the 4-way handshake. Real clients exhibited inconsistent behavior, with some failing to roam seamlessly and others being deauthenticated when returning to the Root AP.	Roaming Test
Preamble Puncturing Feature Not Functioning as Expected Across 5GHz and 6GHz Bands	During Preamble Puncturing testing, the DUT AP failed to exclude the punctured 20 MHz subchannel (channel 44) when interference was introduced.	Preamble Puncturing Test
Clients Denied Association on 5 GHz Band Despite Available Capacity	The 5 GHz band rejected new client associations despite being below the configured client limit. AP logs indicated capacity issues, while the dashboard incorrectly reported that the limit had been reached.	Load Balancing Test
No Significant Throughput Improvement with MLO Enabled	Throughput performance with MLO enabled was nearly identical to that with MLO disabled, showing no measurable gain.	DataPlane, RvR Test
Clients Fail to Reach Captive Portal Login Page When Splash URL Is Not in Walled Garden List	When the splash page URL isn't listed in the Walled Garden, real clients fail to load the login page post sign-in prompt, and virtual clients don't trigger the prompt at all.	Captive Portal Test

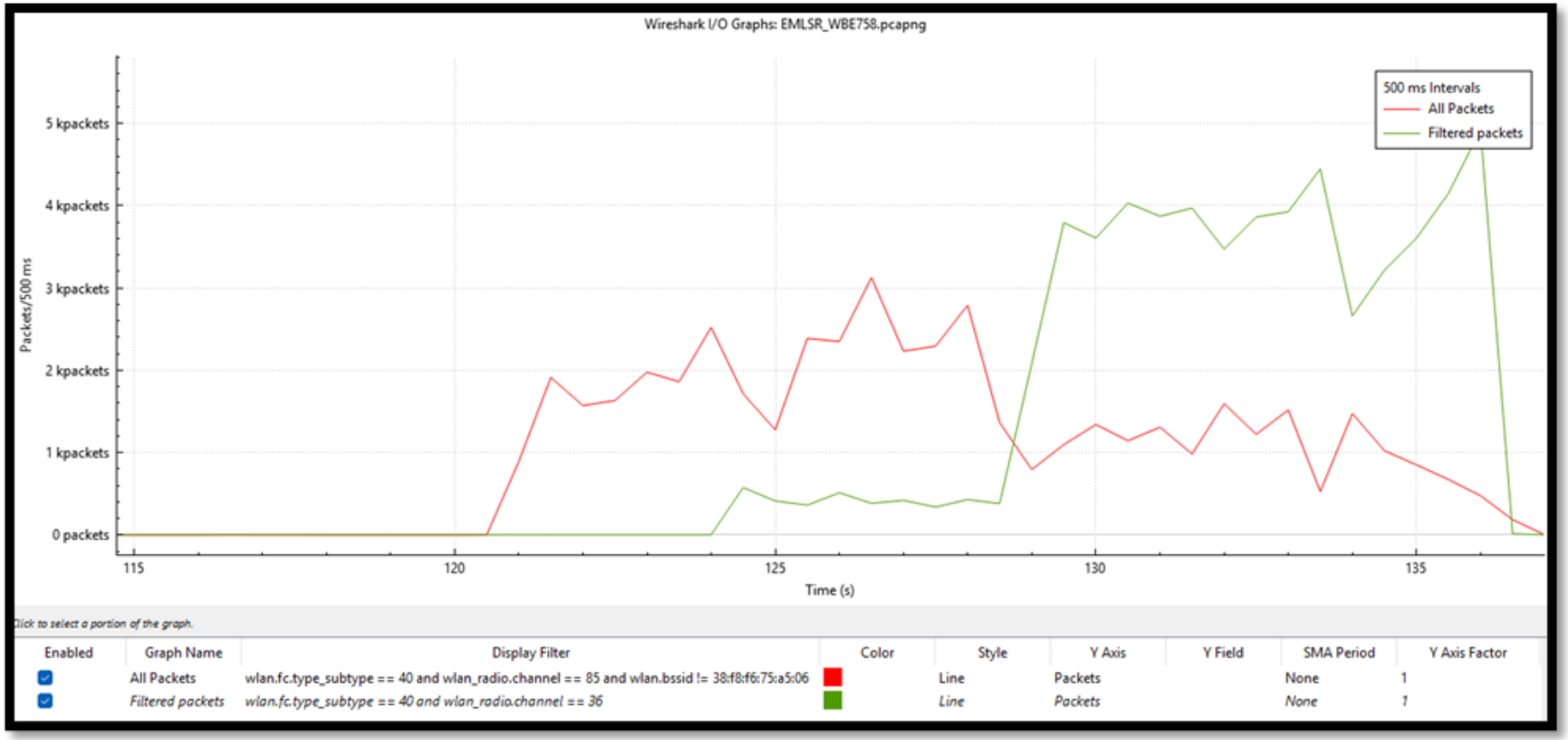
Basic Client Connectivity

- We attempted to connect 39 devices incrementally to the VENDOR AP SSID and observed that all 39 devices successfully completed the 4-way handshake and associated with the AP's SSID.
- Channel utilization was measured across all bands—2.4GHz, 5GHz, and 6GHz—along with the number of clients connected to each band at every step. The average channel utilization recorded was **15% for 2.4GHz, 4% for 5GHz, and 1% for 6GHz**.

Number Of Clients Connected in 2.4GHz Band	2.4GHz (%)	Number Of Clients Connected in 5GHz Band	5GHz (%)	Number Of Clients Connected in 6GHz Band	6GHz (%)
0	12	0	4	0	1
0	0	0	0	0	1
1	18	4	6	0	1
1	17	9	4	0	1
2	17	13	4	0	1
4	16	16	4	0	1
5	16	20	4	0	1
7	18	23	5	0	1
9	18	27	5	0	1
9	18	30	5	0	1

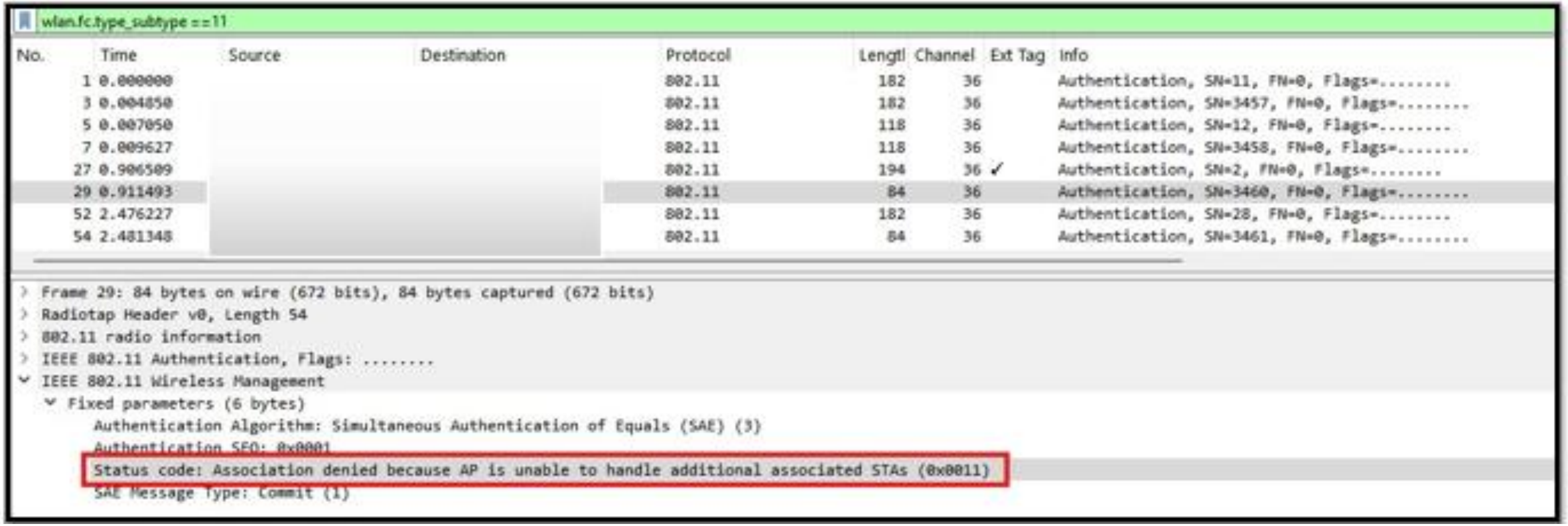
eMLSR Test

- We connected a client on the 6GHz band and triggered QoS traffic on it. Simultaneously, we introduced interference on the same 6GHz channel.
- Upon introducing interference, the link transitioned to 5GHz; however, the QoS data flow remained on 6GHz instead of moving to 5GHz.
- We also tested with the TP-Link Archer 800 and observed that link steering occurred as expected, with the QoS data flow on the steered band.



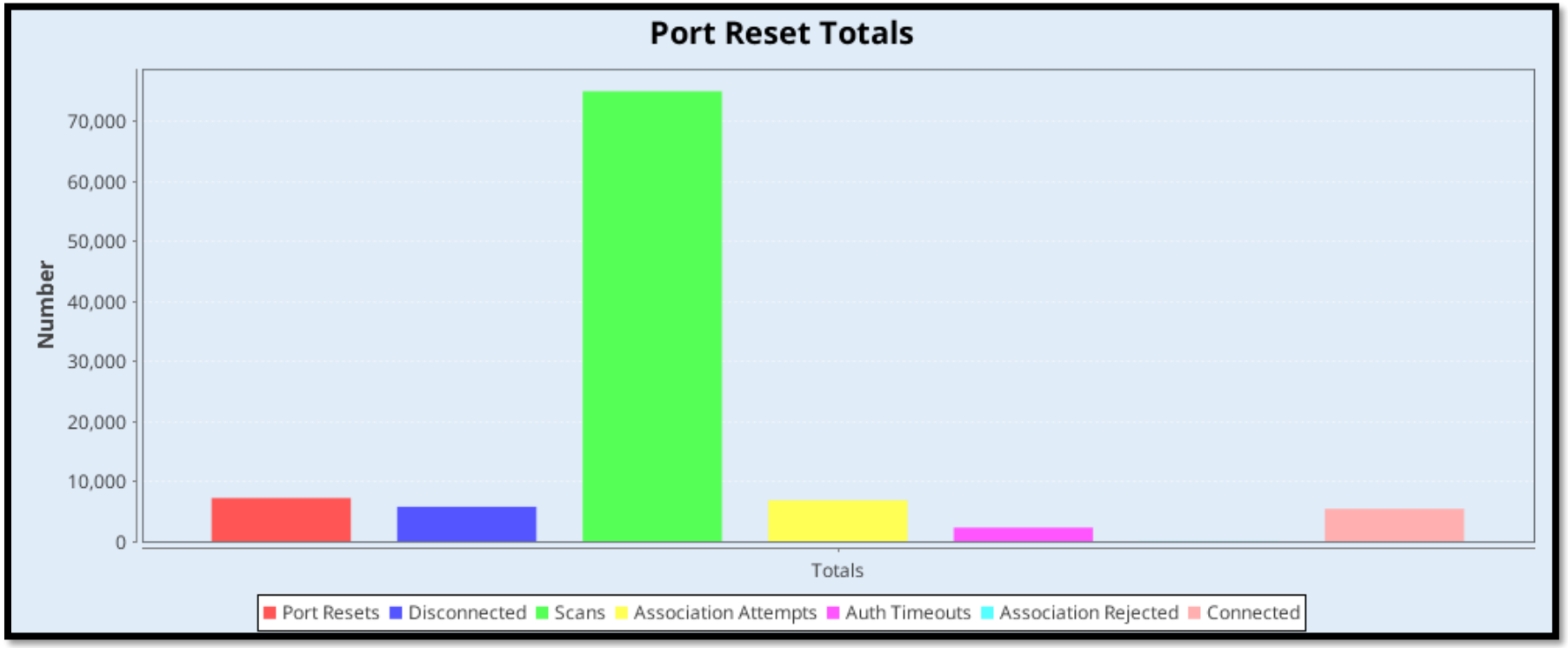
Scale Test

- We have connected a total of 226 clients to a Triband SSID, distributed as follows: 33 clients on 6GHz, 73 clients on 2.4GHz, and 40 clients on 5GHz.
- However, we have observed that some clients experienced a 4-way handshake failure and were unable to connect to the SSID.
- Upon checking the packet capture, we found that the affected clients displayed the following Status code: **"Association denied because AP is unable to handle additional associated STAs."**



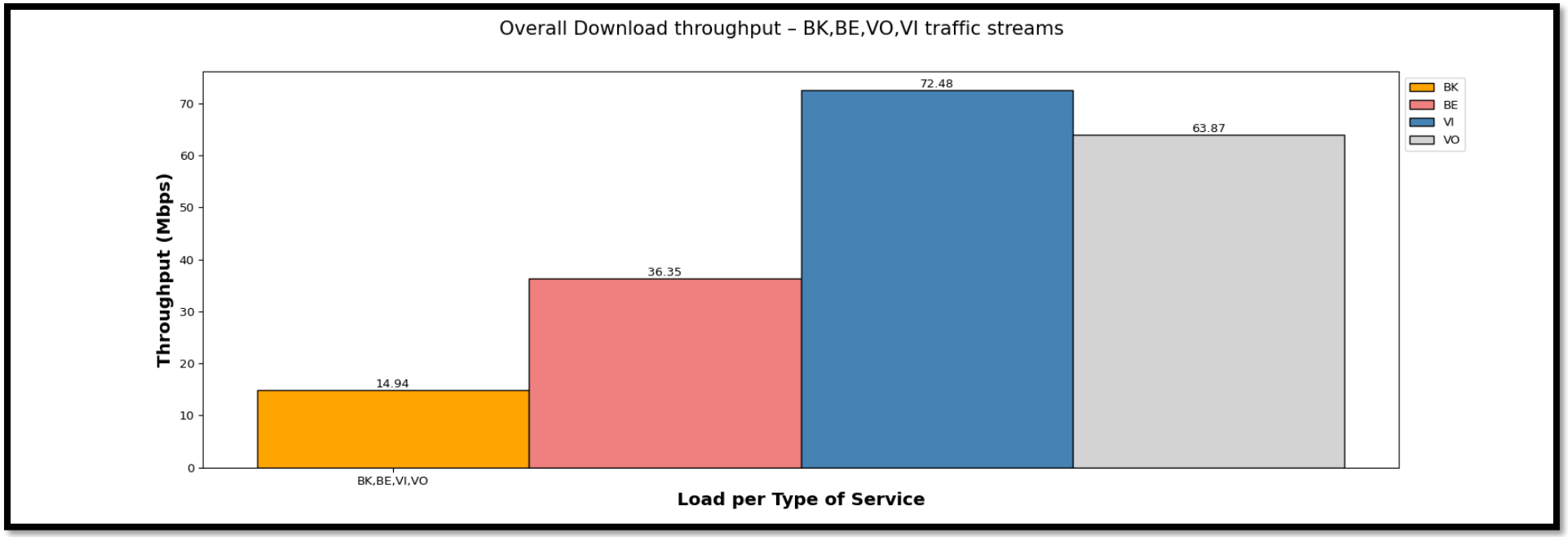
Port Reset Test

- A Port Reset Test was executed over a 12-hour duration with a concurrent port reset count of 50.
- A total of 7,200 port reset events were triggered during the test.
- Out of these, 5,401 resets successfully re-established connections.
- A total of 75,046 scan attempts and 6,822 association attempts. Despite these attempts, only 5,401 associations were successfully completed.



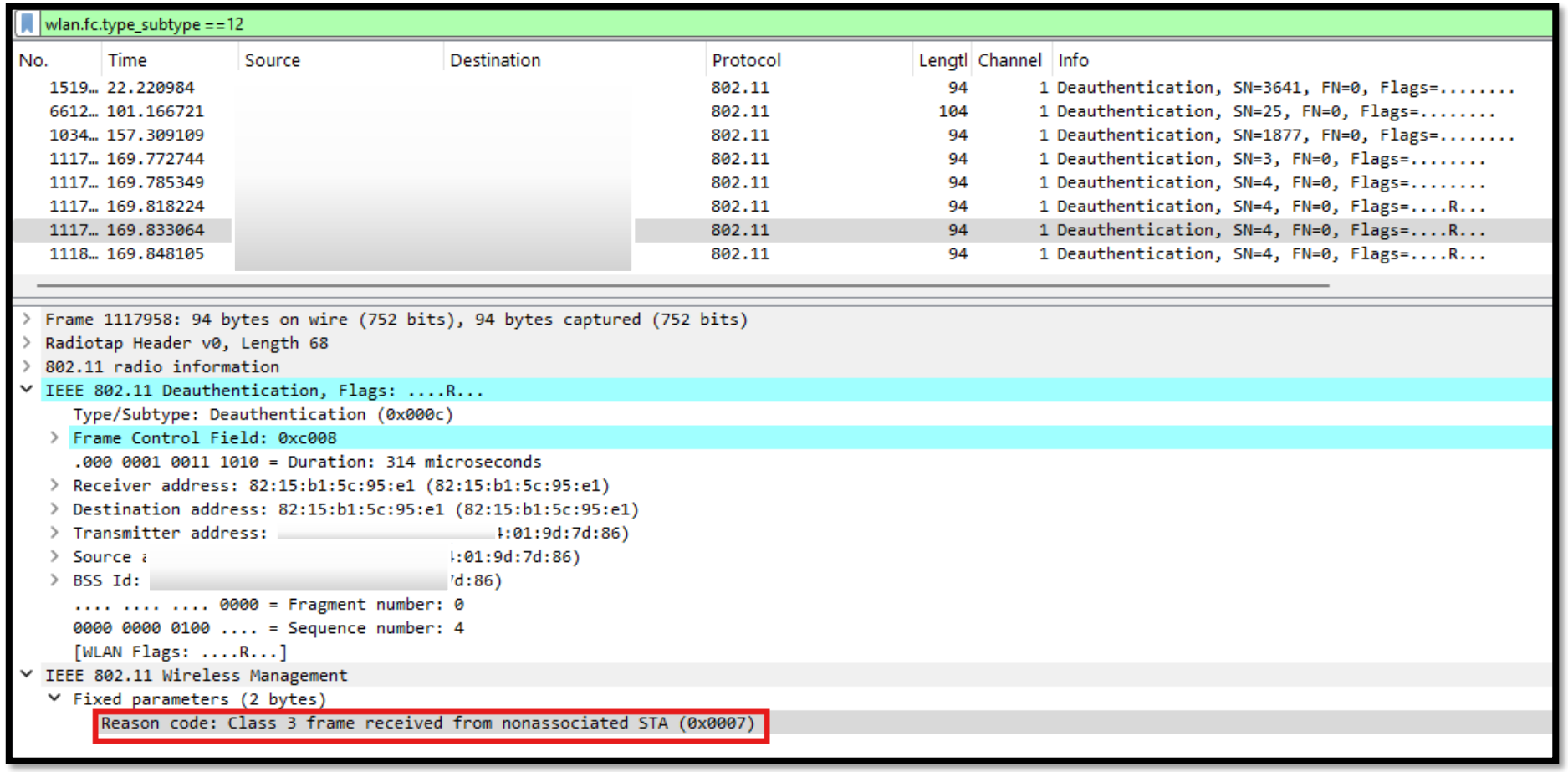
QOS Test

- A QoS traffic throughput test was conducted on 39 real devices to verify ToS bit prioritization across UDP and TCP protocols. Testing was performed in incremental order with 1, 5, 10, 20, 30, and 39 clients.
- With 1, 5, and 10 clients, QoS prioritization worked as expected, and no client disconnections occurred.
- However, with 20 or more clients, the prioritization was inconsistent, with Video (VI) receiving the highest priority, followed by Voice (VO), Best Effort (BE), and Background (BK).
- The Channel Utilization of 5G Band is 92% and 2G band is 94%.



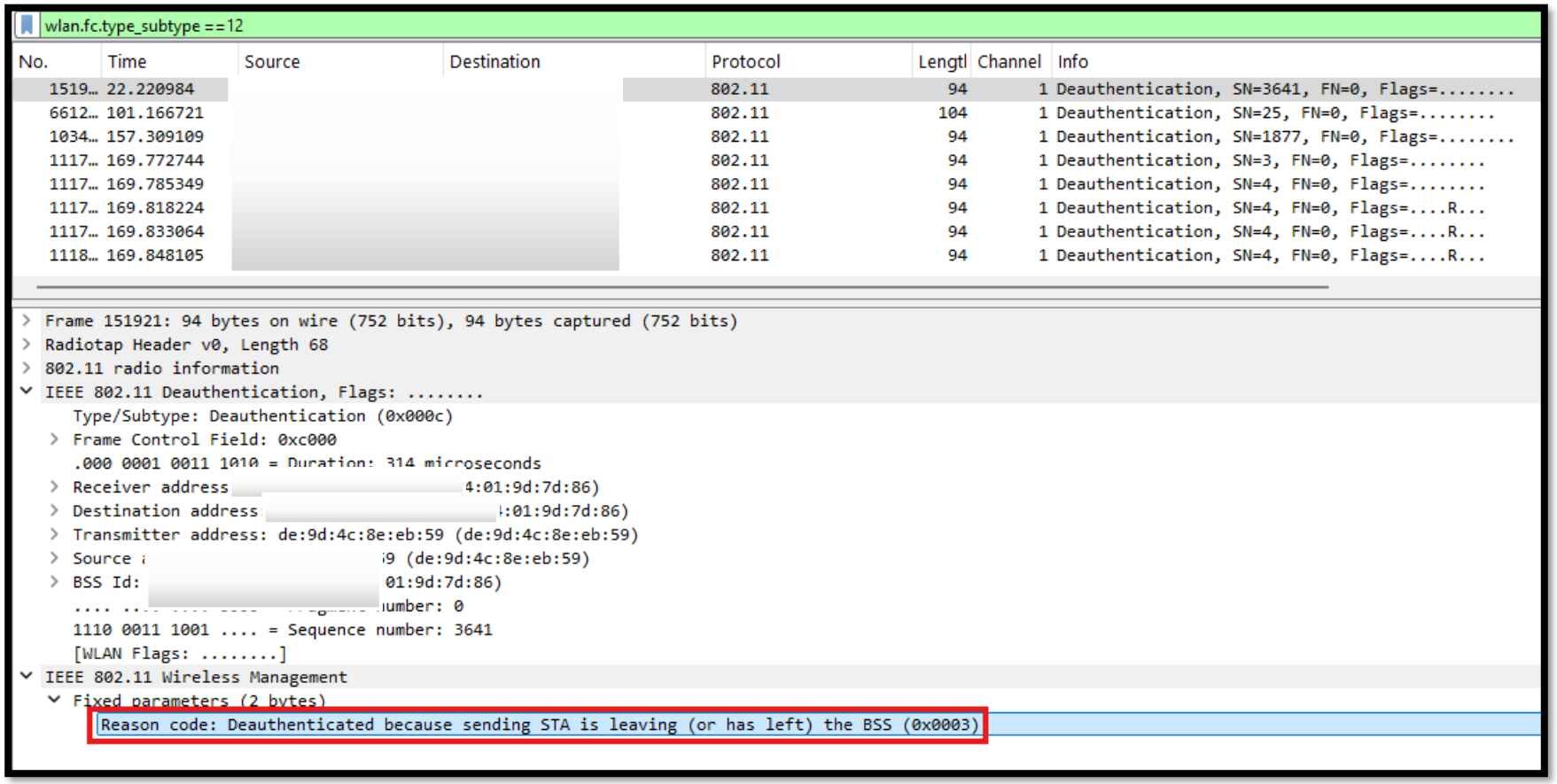
QOS Test

- Even in the VENDOR AP logs, we observe that two clients are being rejected as they are considered non-associated clients. When checking the deauthentication reason code for these clients, we see the reason code as **"Class 3 frame received from non-associated STA (0x0007)"**, with the source being the AP.



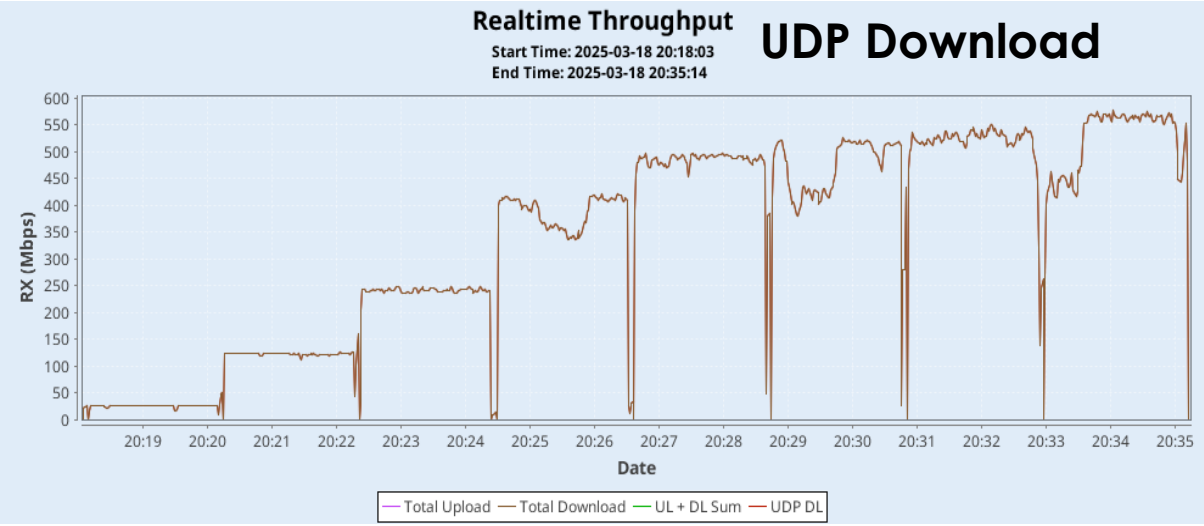
QOS Test

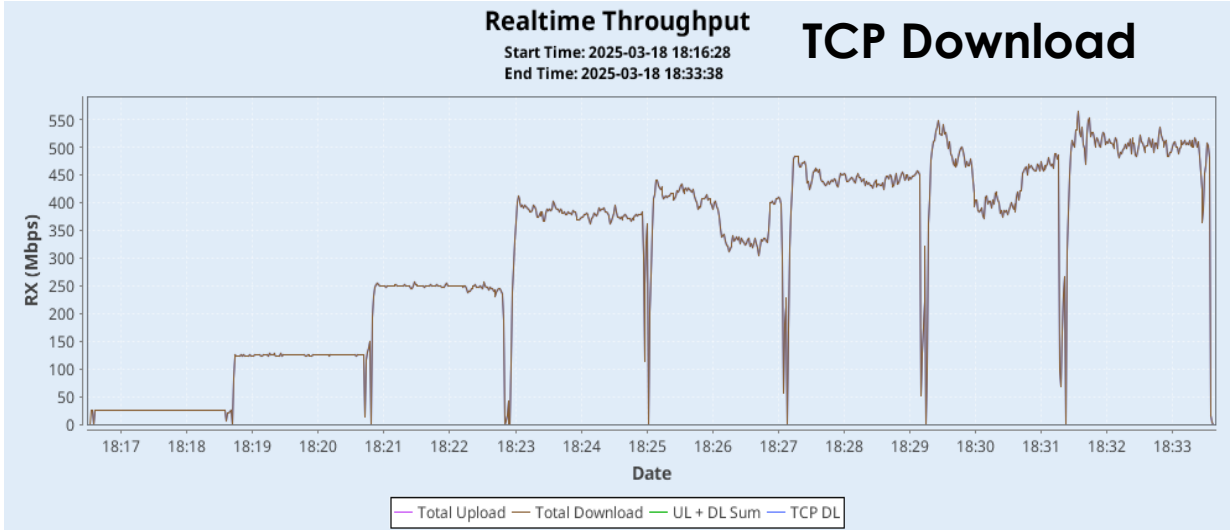
- Additionally, when the QOS test was performed with 35 or more clients, we observed client disconnections in the middle of the test . 5-7 clients were deauthenticated with the following reason codes: "Reason code: Previous authentication no longer valid (0x0002)" and "Deauthenticated because sending STA is leaving (or has left) the BSS (0x0003)".



Throughput test with incremental client count

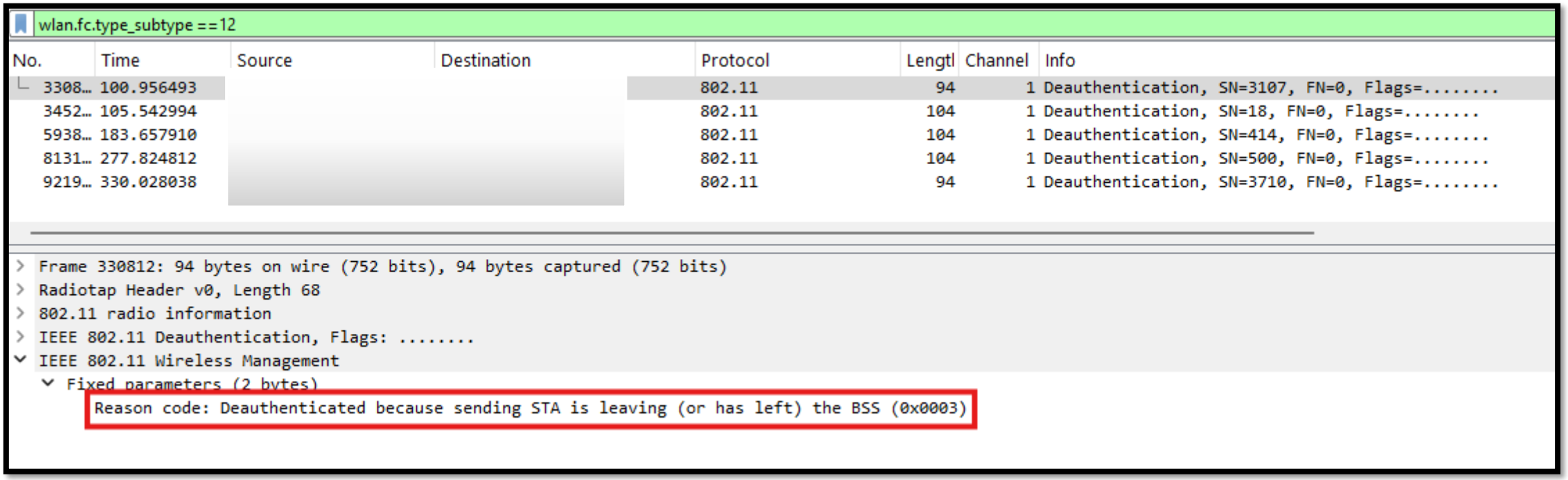
- The Throughput test was conducted on both download and upload directions using TCP and UDP protocols across various loads (10Mbps, 20Mbps, 25Mbps per client) with a total intended load of 1Gbps for 39 clients.
- A throughput drop of 80–100Mbps was observed at client increments of 25, 35, and 39 when running the Download traffic with both the UDP and TCP Protocols.





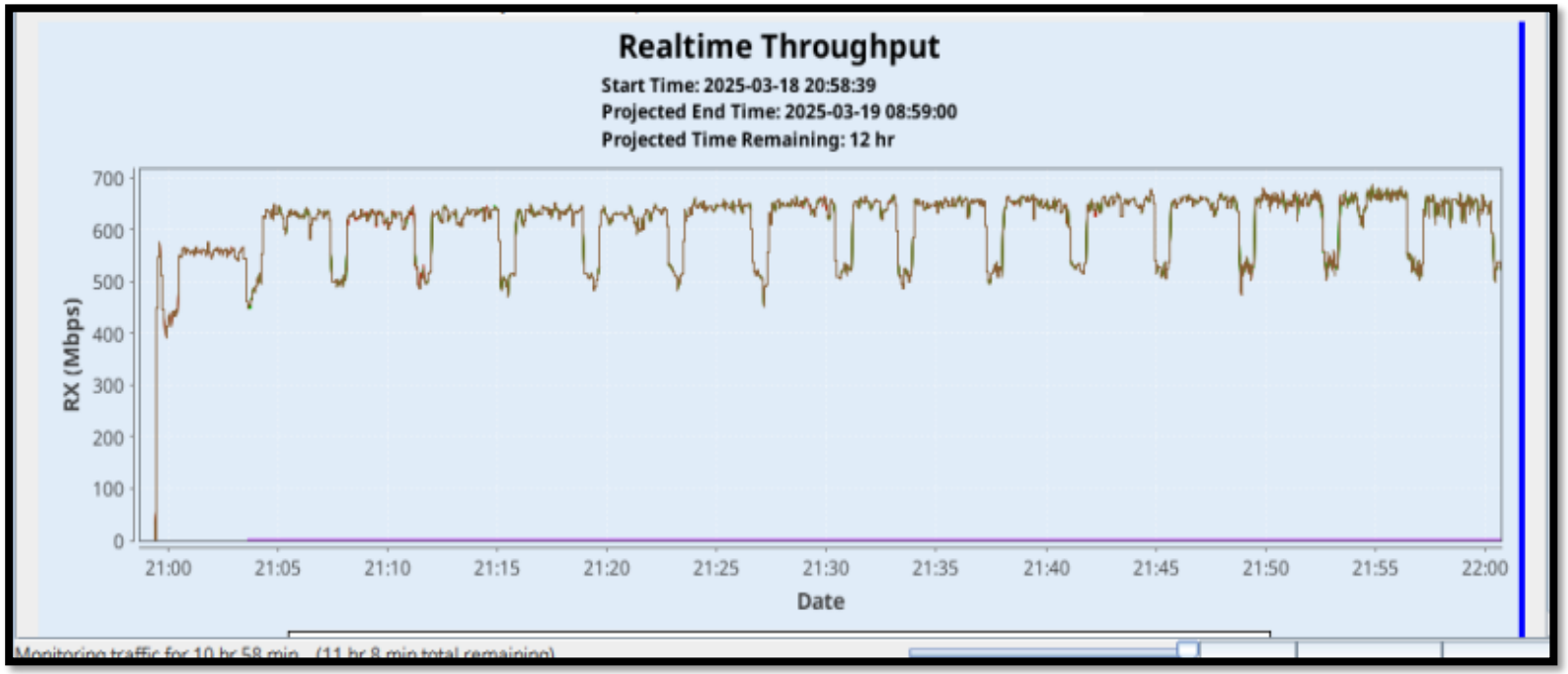
Throughput test with incremental client count

- While running UDP upload traffic with an Intended load of 1Gbps with 39 clients, five devices were deauthenticated with reason code 0x0003 ("Deauthenticated because sending STA is leaving or has left the BSS").
- Wi-Fi logs show that deauthenticated clients re-initiated the 4-way handshake mid-test, with some reconnecting after the test completion.
- At the time of disconnections, channel utilization was at 95% (2.4GHz) and 92% (5GHz).



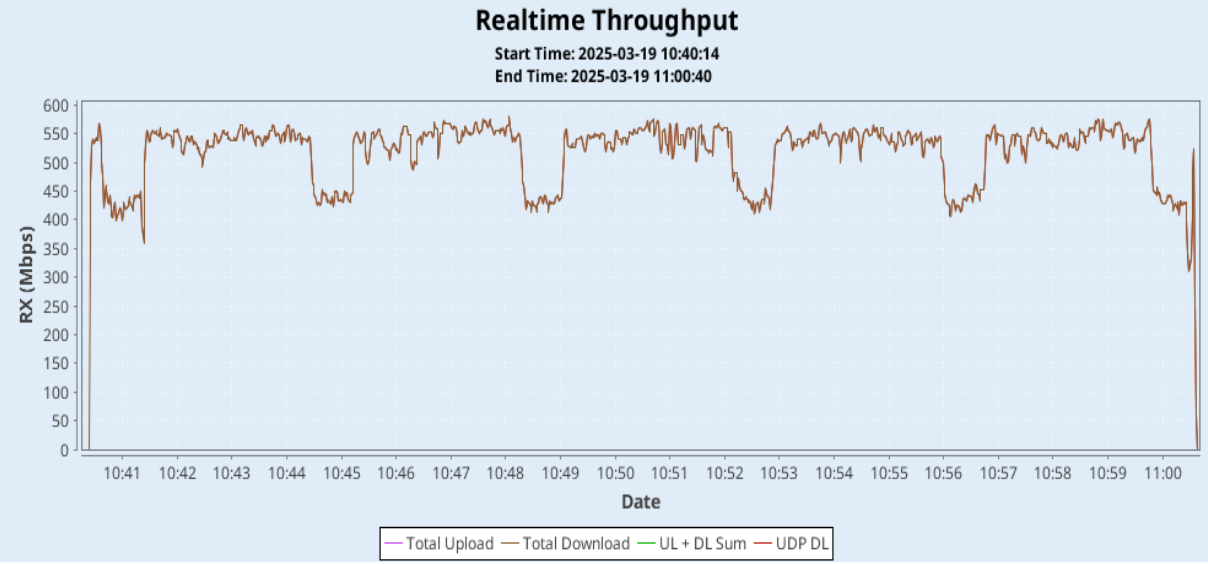
Stress Test

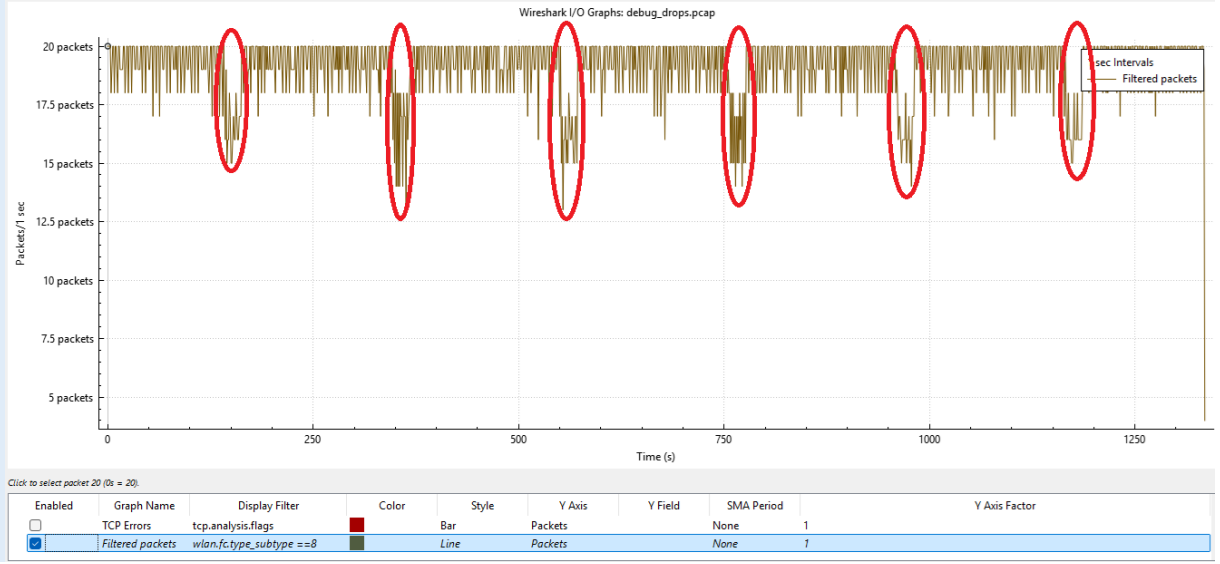
- Triggered a 12 hours Long run (Stress) test with 39 Real Devices (Mix of OS Devices) with Intended load of 1Gbps Where, 28 devices got connected to 5Ghz band and 11 devices got connected to 2.4Ghz band.
- During the 12-hour stress test, periodic throughput drops (around 100Mbps) were observed every 4 minutes.
- The Throughput attained after the completion was around 612Mbps. Due to these periodic throughput drop there was a significant impact on the throughput attained.



Stress Test

- To investigate further, a 20-minute test was conducted with the same load, and packet captures were analyzed. The I/O graphs indicate that at the points where throughput drops occurred, beacon packets were missing from the AP
- This issue is not client-specific, as it was observed across both AP models and was seen with both real and virtual clients, including tests with a single client.





Realtime graph showing periodic throughput drops

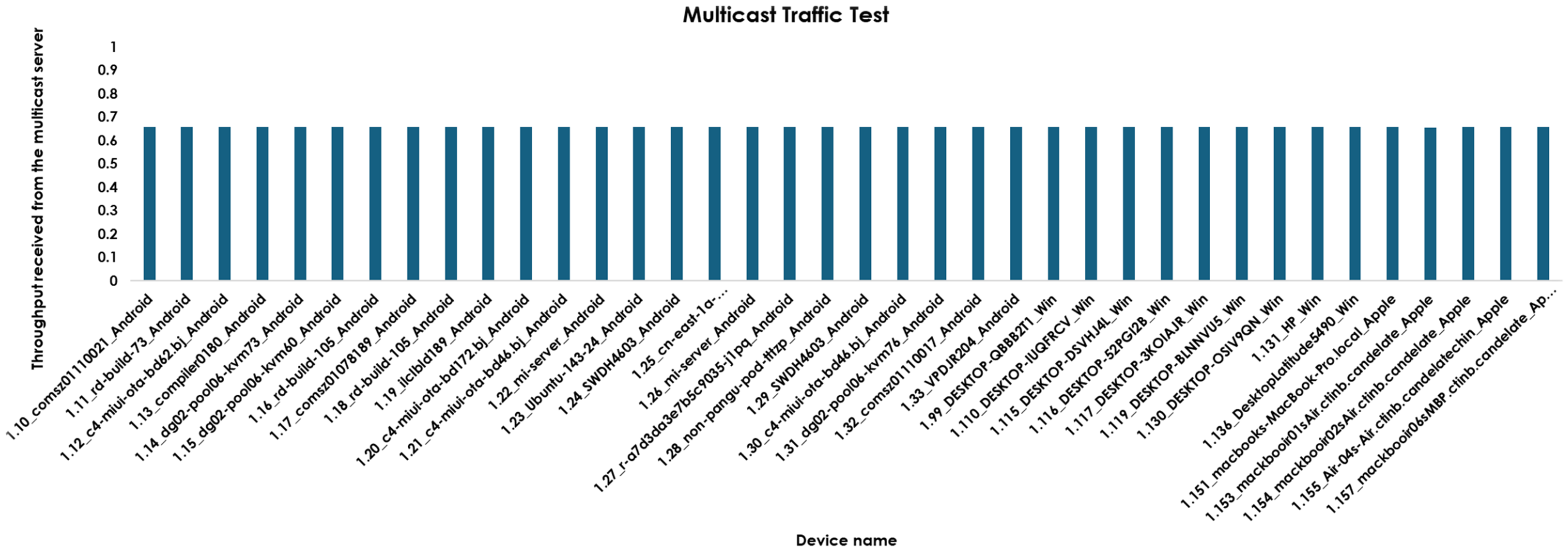
I/O graph indicating beacon packets lost from the AP side

Mixed Traffic Test

- To measure the performance and stability of the VENDOR AP, we triggered multiple traffic types (Ping, QoS, FTP, HTTP, and Multicast) on 36 real devices (Android, Windows, and MacBook) for a duration of 420 minutes.
- In this test, we configured various traffic profiles, including connection streams with different ToS configurations such as Voice, Video, Backend, and Best Effort as part of QoS. Additionally, we initiated FTP and HTTP file downloads for all available clients.
- We also initiated ping sessions, including pings to a global IP. All traffic types were simultaneously initiated across all 36 clients.
- We observed that all traffic types started as expected, and all 36 clients were able to run their respective traffic sessions successfully. However, during the test, some clients disconnected from Wi-Fi and displayed deauthentication messages. At the time of disconnection, the channel utilization was 94% on the 5GHz band and 95% on the 2.4GHz band.
- Out of the 36 clients, 15 were deauthenticated in the middle of the test, showing the following reason codes: **0x0002**: "Previous authentication no longer valid“ and **0x0003**: "Deauthenticated because the sending STA is leaving (or has left) the BSS“.
- Also from the VENDOR AP dashboard page, in the Notifications tab we are observing log messages related to clients getting disconnected from the AP SSID and try to reassociate with the AP SSID back.

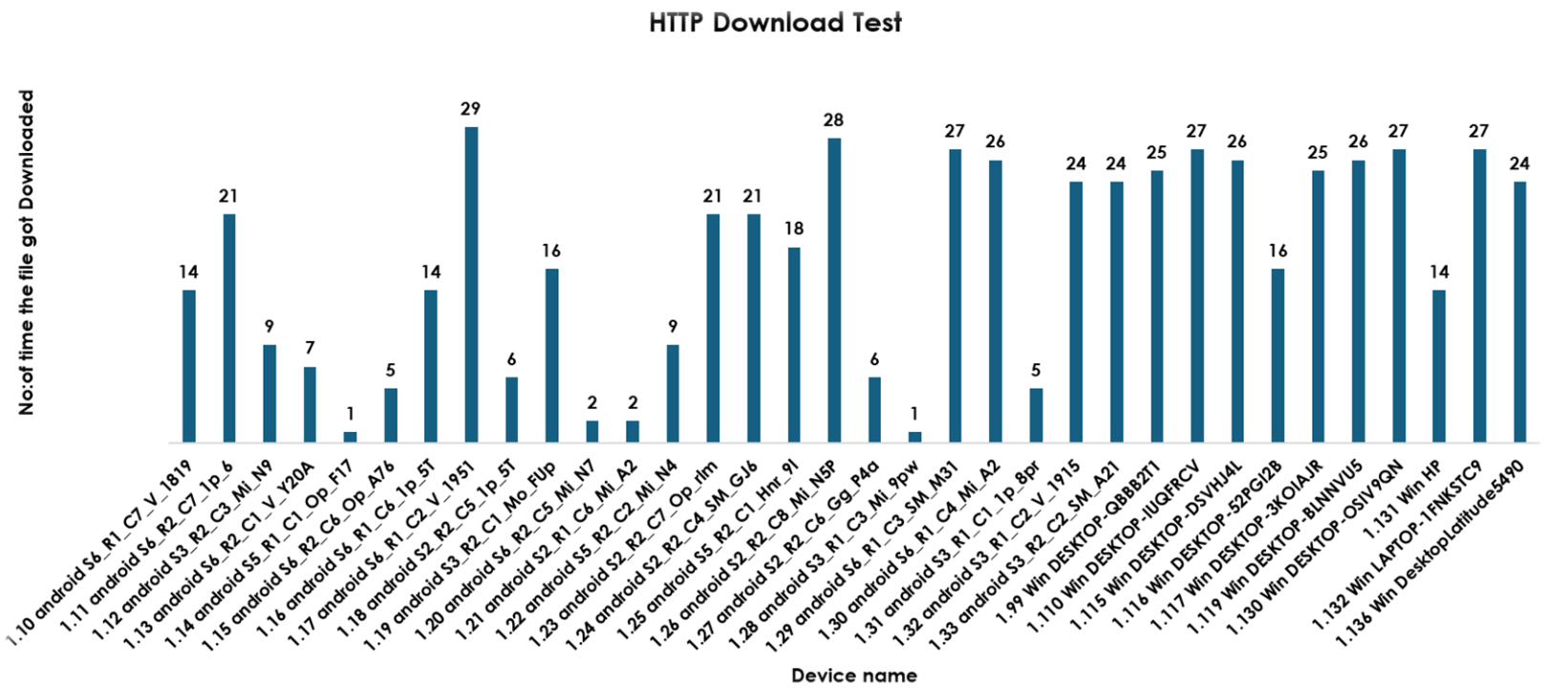
Multicast Traffic Test

- By Creating a Multicast server of Intended load 25Mbps on Upstream port performed the Multicast traffic on all the OS devices (Android, Windows and MacBook).
- All 39 clients were able to receive the traffic as expected from the Multicast server and there were no client disconnection observed during the test.



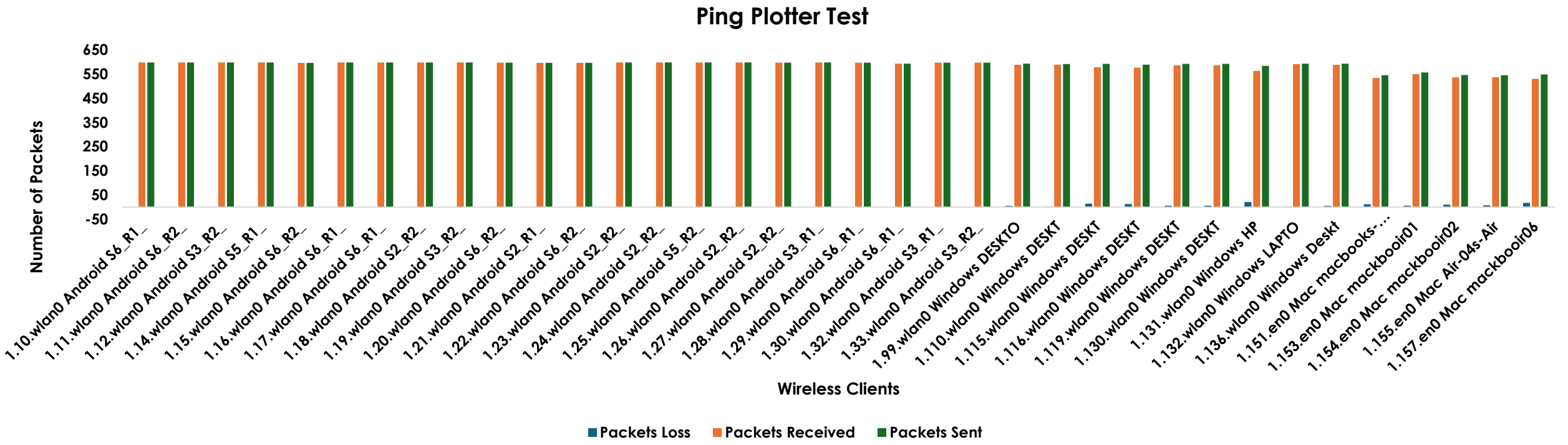
HTTP Download Test

- We have executed HTTP Download test with file size 25Mbps on all the Real devices (Androids, Windows, and MacBooks) individually for a duration of 5 mins.
- All the 34 devices connected to 5Ghz and 2.4Ghz band were able to download the 25Mbps file in the 5mins duration. However, 8 clients downloaded the 25MB file less than 10 times, unlike the other devices.
- All the devices remained to be in Connected state throughout duration of test.



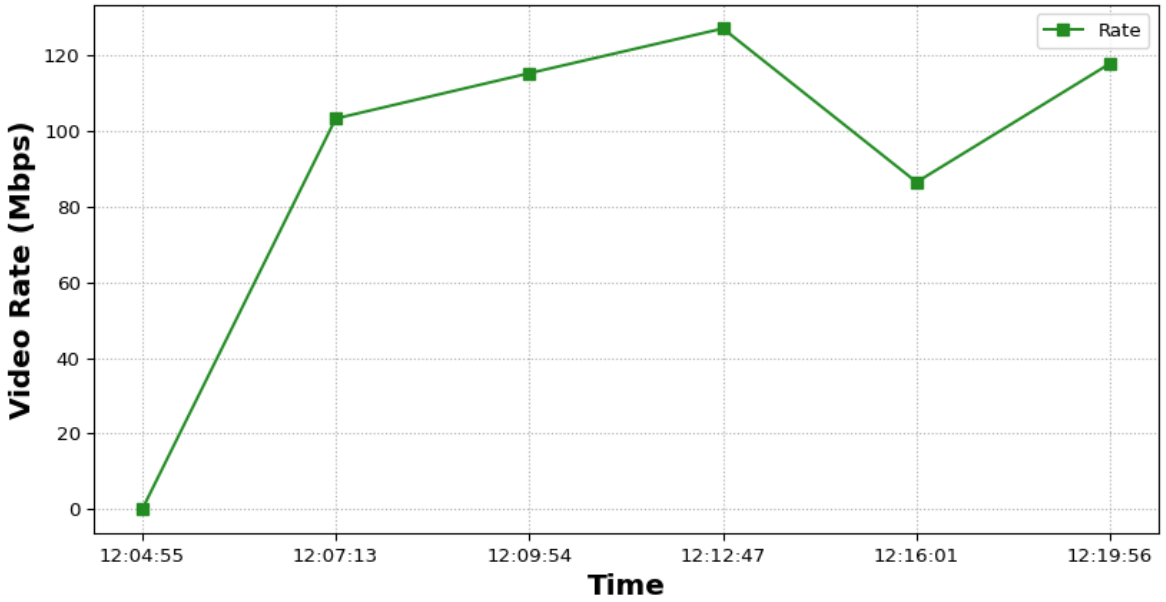
Ping Plotter Test

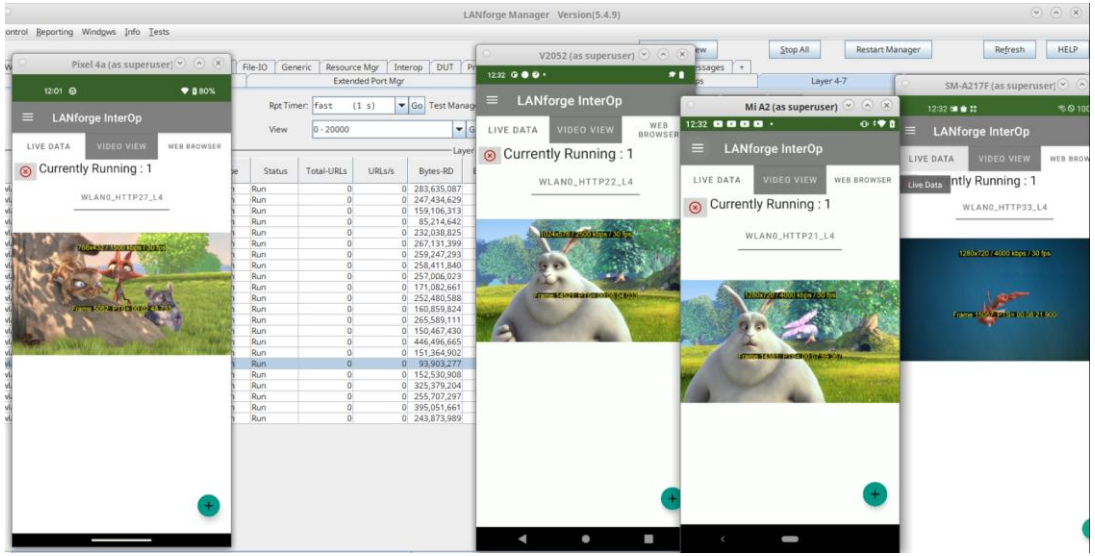
- We executed a Ping Plotter test to assess network connectivity for specified clients by measuring the round-trip data packet travel time while pinging www.mi.com for a duration of 10 minutes with 36 devices.
- Throughout the test, we collected data on client status, packets sent, packets received, and packets dropped.
- Out of 36 clients, 4 experienced packet loss ranging from 12 to 21 packets. However, all clients remained connected throughout the test duration.



Video Streaming Test

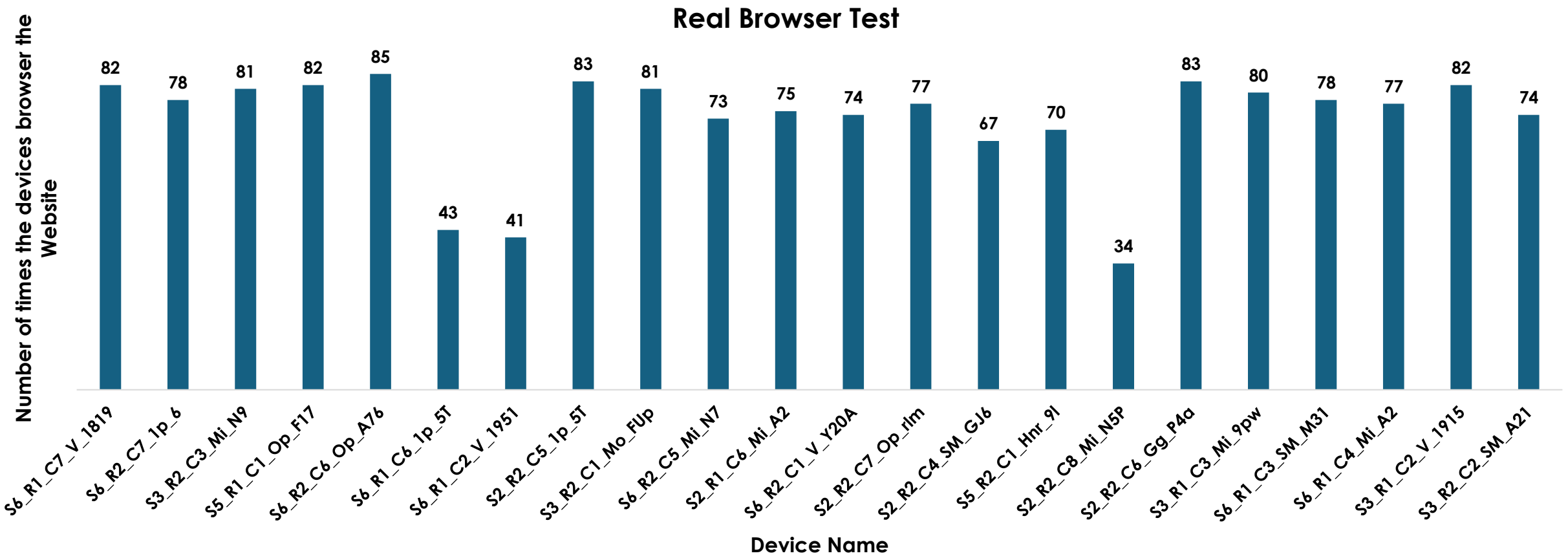
- We have Conducted a video streaming test on all Android devices using the Dash Media source for 15 minutes to evaluate access point performance and stability.
- Measured parameters include the number of buffers, wait time, per-client video bitrate, and video quality.
- All clients streamed the video as expected; however, 4 out of 23 clients could not complete the video within the given duration, resulting in a reported URL value of 0 for those devices.





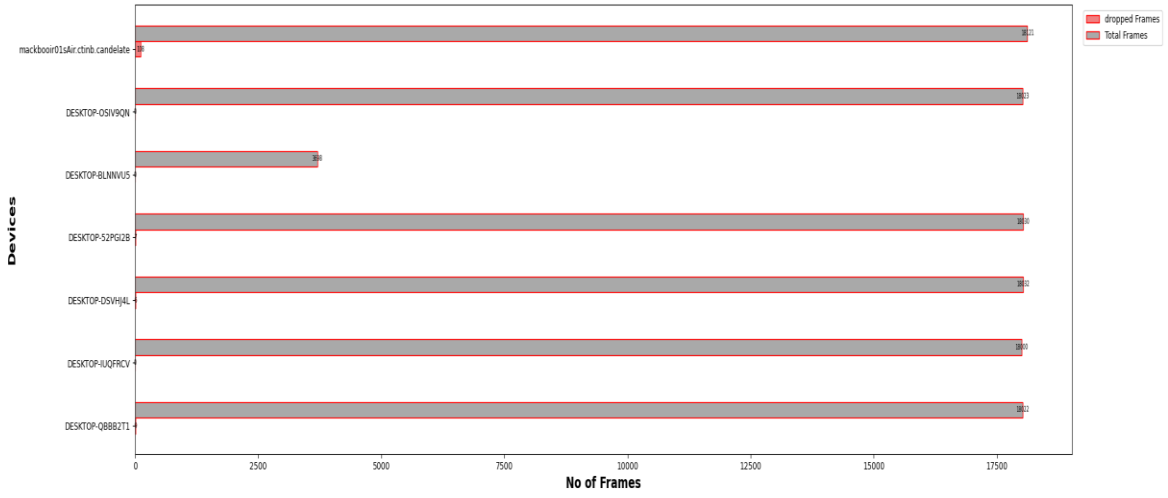
Real Browser Test

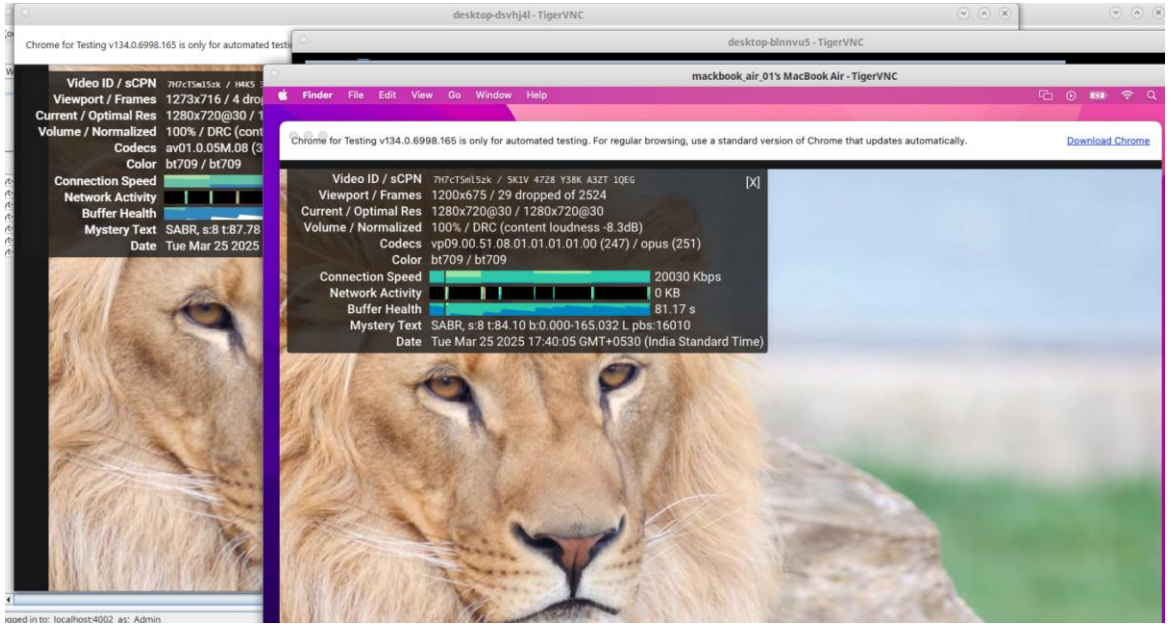
- We have Conducted a Real Browser test on all Android devices and browser a website www.mi.com for a duration of 10mins.
- All the 22 Android devices were able to browse the website provided as expected and there were no client disconnections seen throughout the test duration.



YouTube Streaming Test

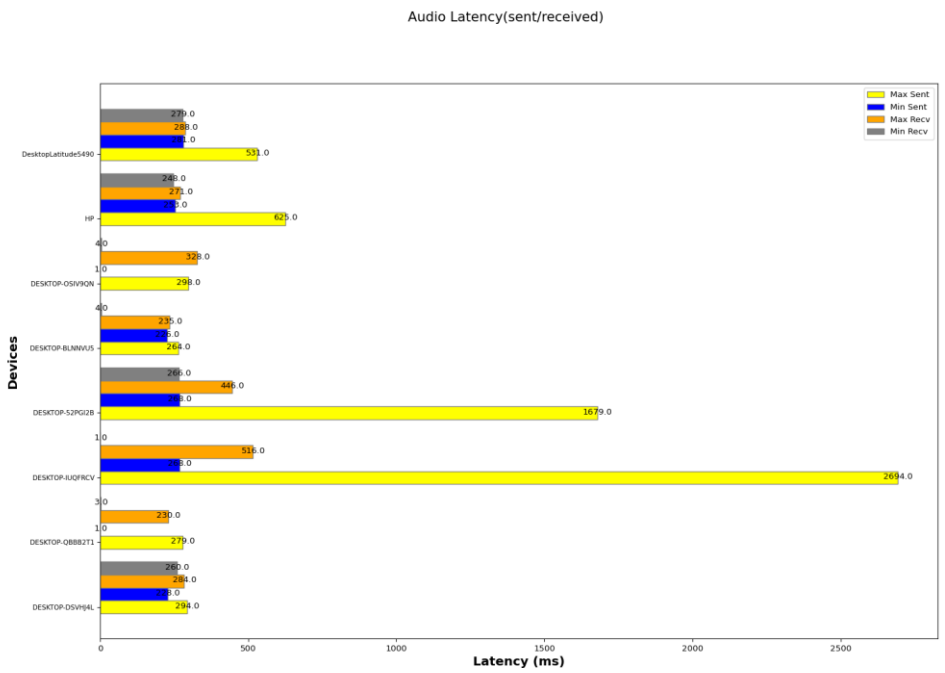
- We have Conducted a YouTube streaming test across multiple laptops by providing a YouTube URL and set the resolution to 720p for a duration of 10minutes.
- When the YouTube video is playing on the laptop devices, we have collected key statistics such as video resolution, buffer health, total frames, and dropped frames throughout the test duration.
- There were no significant drops seen throughout the test and the buffer health of each device is consistent.

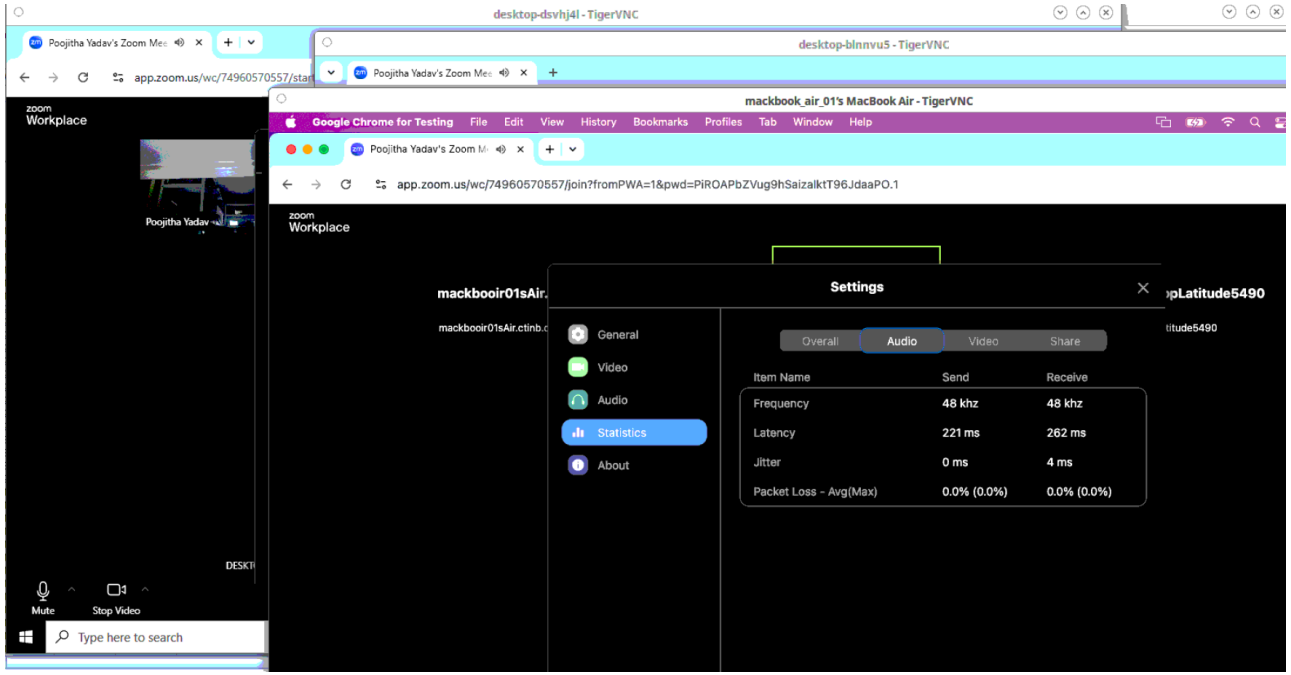




Zoom Call Test

- We conducted a Zoom call test across multiple laptops, selecting one device as the host and the others as clients. The test was performed for a duration of 10 minutes.
- Once the Zoom call test started on the laptops, we collected key statistics on the performance of audio and video, including average latency, jitter, and packet loss.
- No significant packet drops were observed in either audio or video throughout the test, and all client devices remained connected for the entire duration.





Automatic Channel Selection (ACS) test

- The Automatic Channel Selection (ACS) test was conducted across all three bands (2.4 GHz, 5 GHz, and 6 GHz) in AC, AX, and BE modes.
- Despite the AP being configured with "Auto" channel selection in the Radio and Channel settings, no channel change occurred during the test.
- The AP initially assigned the following channels: 2.4 GHz → Channel 1, 5 GHz → Channel 36, 6 GHz → Channel 85
- Interference was introduced on the same channels where clients were connected. However, No channel switch was observed on any of the bands despite interference.

6.5.3 Automatic Channel Selection Results

Type	Result	Value	P/F Value	Notes
Configuration NOTE	INFO			Using LANforge AP for Alien Interferer.
Configuration NOTE	INFO			Configured to skip 2.4GHz band test.
Configuration NOTE	INFO			Configured to skip N/AC test.
Configuration NOTE	INFO			Configured to skip 2.4GHz band test.
AX 5Ghz ch: 42 BW: 80	FAIL	36	Not 42	Interferer Channel: 42 BW: 80 DUT Channel: 36 Prohibited channels: 36 - 48 STA: STA-RSSI Data/Beacon: -48/-48 Rx-Rate: 6M Tx-Rate: 245M 802.11an-AX-80-2x2 36 Color: 57 Interferer STA: STA-RSSI Data/Beacon: -64/-57 Rx-Rate: 360.3M Tx-Rate: 122.5M 802.11an-AX-80-1x1 36 Color: 0 Upstream Port: STA-RSSI Data: -74 Rx-Rate: 122.5M Tx-Rate: 720.6M Activity: 45% 802.11an-AX-80- 36 Color: 0
AX 5Ghz ch: 58 BW: 80	PASS	36	Not 58	Interferer Channel: 58 BW: 80 DUT Channel: 36 Prohibited channels: 52 - 64 STA: STA-RSSI Data/Beacon: -48/-48 Rx-Rate: 6M Tx-Rate: 245M 802.11an-AX-80-2x2 36 Color: 57 Interferer STA: STA-RSSI Data/Beacon: -69/-66 Rx-Rate: 360.3M Tx-Rate: 216.1M 802.11an-AX-80-1x1 52 Color: 0 Upstream Port: STA-RSSI Data: -78 Rx-Rate: 216.1M Tx-Rate: 360.3M Activity: 93% 802.11an-AX-80- 52 Color: 0
				Interferer Channel: 106 BW: 80 DUT Channel: 36

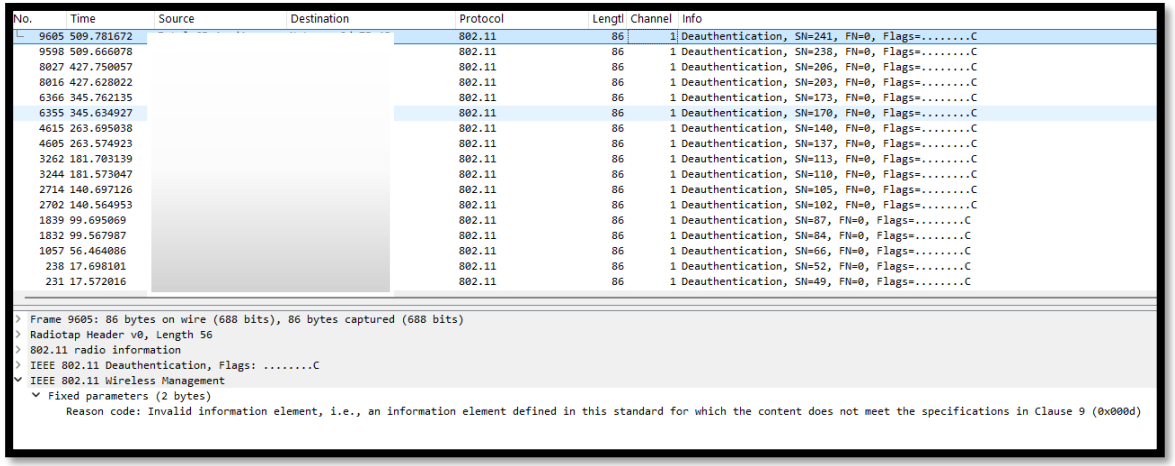
AP Coexistence test

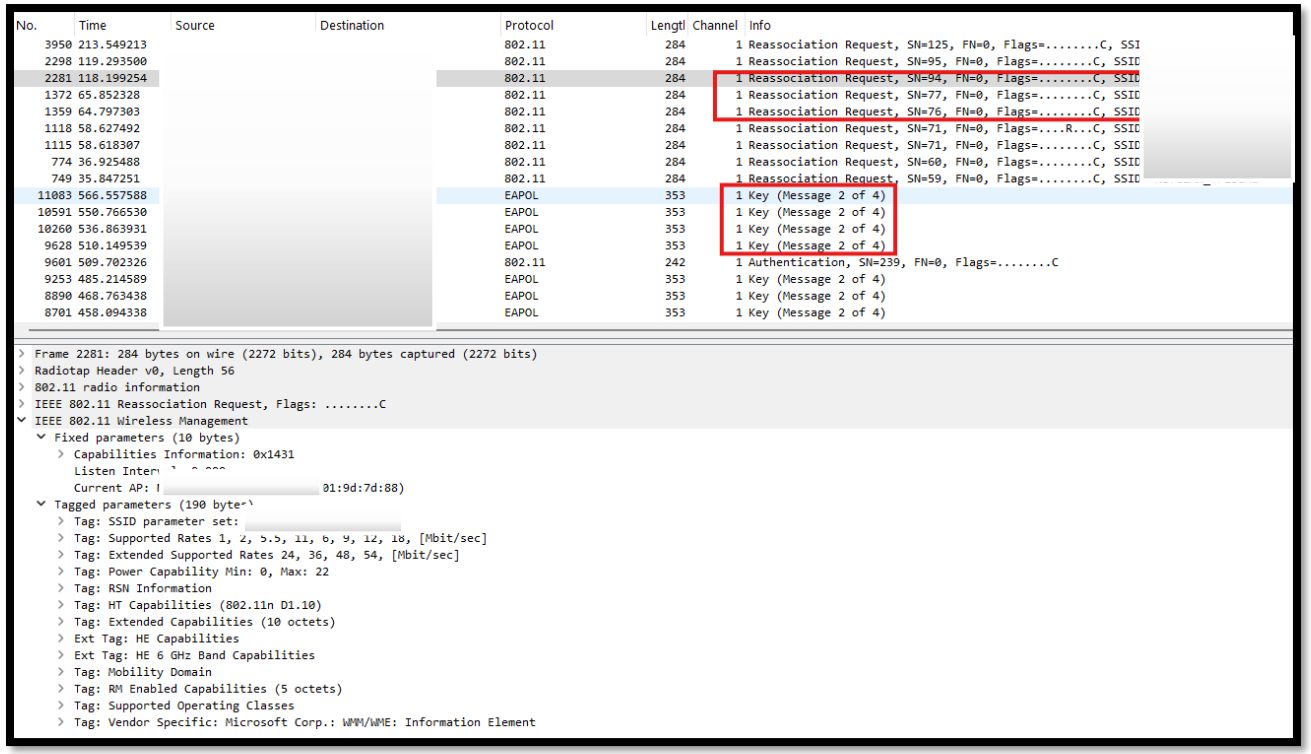
- The AP Coexistence test was conducted across all three bands in AC, AX, and BE modes.
- With Co-Channel Interferer and Overlapping Interferer: The throughput met the Pass/Fail criteria, resulting in a Pass.
- With Adjacent Interferer: The throughput fell below the Pass/Fail criteria, with a difference of approximately 300 Mbps between the attained throughput and the Pass/Fail value, leading to a Fail in this scenario.
- Overall Result: The test is partially passed, indicating potential coexistence challenges in adjacent interference scenarios.

AX 5Ghz ch: 36 Idle Interferer	PASS	889	713	Req: 713.48 Mbps Rpt: 888.87 Mbps DUT BW: 80 STA-RSSI Data/Beacon: -52/-48 Rx-Rate: 1.201G Tx-Rate: 1.201G 802.11an-AX-80-2x2 36
AX 5Ghz ch: 36 Co-Channel Interferer	PASS	497	300	Req: 300.41 Mbps Rpt: 497.19 Mbps DUT BW: 80 STA-RSSI Data/Beacon: -52/-48 Rx-Rate: 1.201G Tx-Rate: 1.201G 802.11an-AX-80-2x2 36 Alien Offered Load: 118.05 Mbps Alien Throughput: 117.86 Mbps Intf-STA-RSSI Data/Beacon: -67/-65 Rx-Rate: 360.3M Tx-Rate: 29.2M 802.11an-AX-80-1x1 36 Intf-VAP-RSSI Data: -73 Rx-Rate: 29.2M Tx-Rate: 360.3M Activity: 92% 802.11an-AX-80- 36
AX 5Ghz ch: 36 Overlapping Interferer	PASS	531	300	Req: 300.41 Mbps Rpt: 531.38 Mbps DUT BW: 80 STA-RSSI Data/Beacon: -52/-48 Rx-Rate: 1.201G Tx-Rate: 1.201G 802.11an-AX-80-2x2 36 Alien Offered Load: 74.06 Mbps Alien Throughput: 72.77 Mbps Intf-STA-RSSI Data/Beacon: -65/-63 Rx-Rate: 229.4M Tx-Rate: 29.2M 802.11an-AX-40-1x1 36 Intf-VAP-RSSI Data: -73 Rx-Rate: 29.2M Tx-Rate: 206.5M Activity: 95% 802.11an-AX-40- 36
AX 5Ghz ch: 44 Adjacent Interferer	FAIL	403	794	Req: 794.25 Mbps Rpt: 403.03 Mbps DUT BW: 40 STA-RSSI Data/Beacon: -52/-48 Rx-Rate: 1.201G Tx-Rate: 1.201G 802.11an-AX-80-2x2 36 Alien Offered Load: 74.06 Mbps Alien Throughput: 43.18 Mbps Intf-STA-RSSI Data/Beacon: -67/-64 Rx-Rate: 172M Tx-Rate: 29.2M 802.11an-AX-40-1x1 44 Intf-VAP-RSSI Data: -73 Rx-Rate: 3.6M Tx-Rate: 68.8M Activity: 95% 802.11an-AX-40- 44

Hard Roaming Test (Virtual Clients)

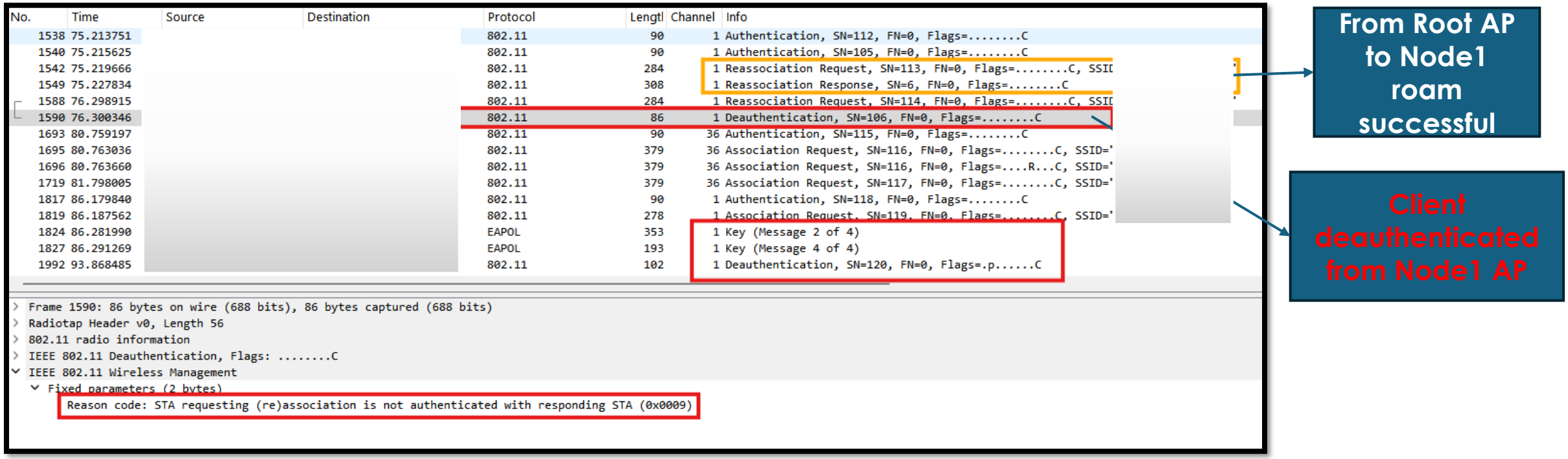
- When a Virtual client is moving from Root AP to Node1, it is first sending a reassociation request.
- However, we observed deauthentication messages with the following reasons:
  - 0x0002: Previous authentication no longer valid (0x0002)
  - 0x000d: There is an invalid information element in the request.
- Despite these deauthentication events, the 4-way handshake completes successfully, and the client is ultimately able to connect to Node1 without issues.





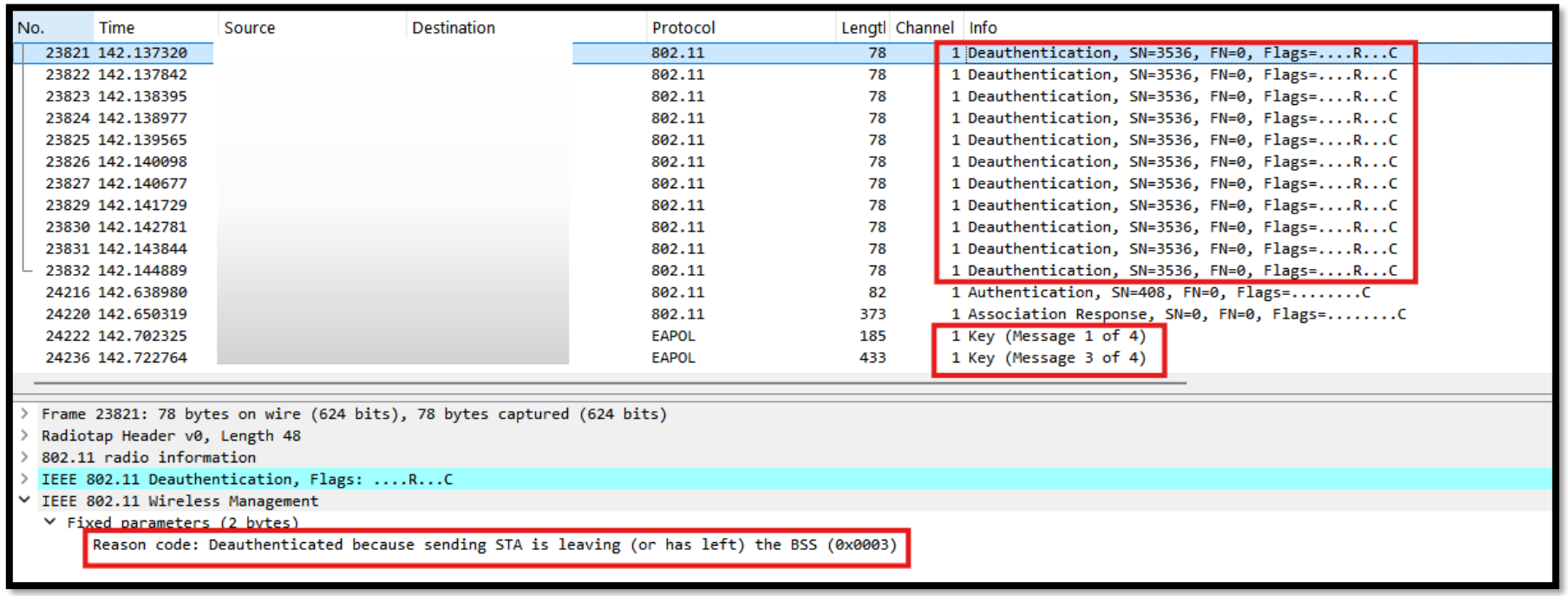
Soft Roaming Test (Virtual Clients)

- A client was connected to the SSID, and attenuation was increased in 5dB steps to observe roaming behavior from the Root AP to Node1 and Vice Versa.
- When roaming from the Root AP to Node1, the handoff was successful. The reassociation response was received from Node1, allowing the client to roam without issues.
- When roaming from Node1 back to the Root AP, the client was deauthenticated with Reason code: STA requesting (re)association is not authenticated with responding STA (0x0009). After completing the 4-way handshake, it is reconnecting back to the Root AP.



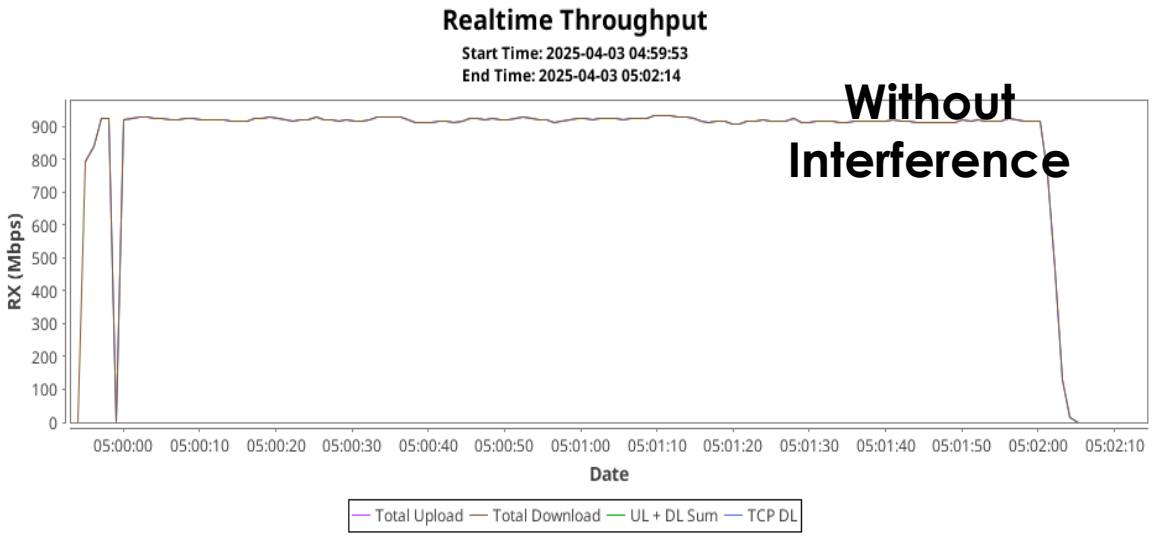
Soft Roaming Test (Real Clients)

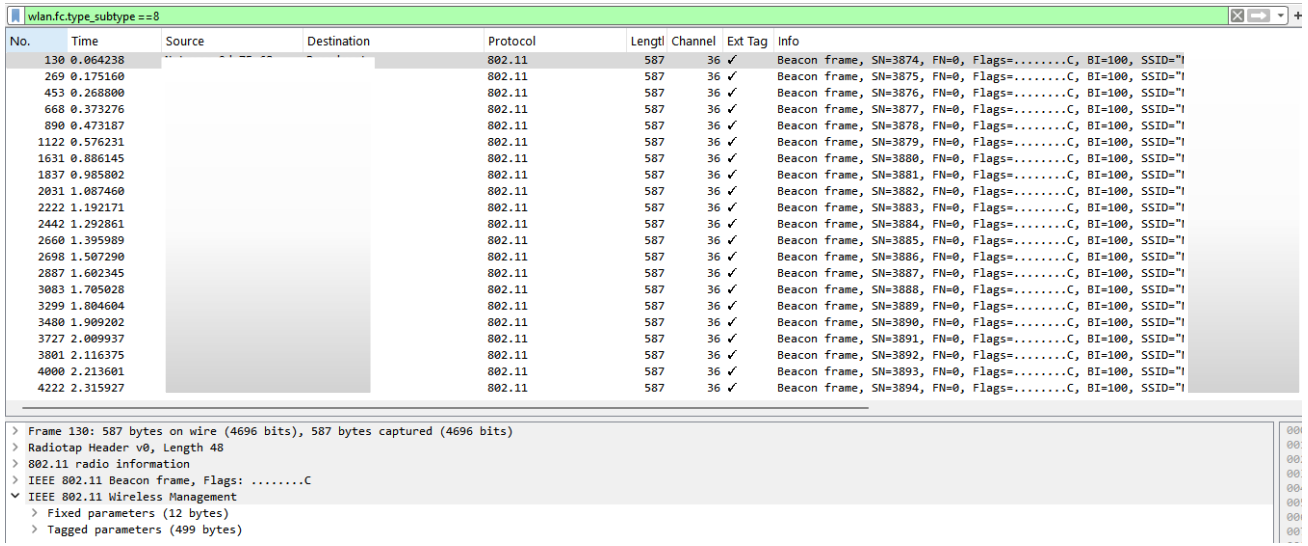
- 3 real clients were connected to the SSID, and attenuation was increased in 5dB steps to observe their roaming behavior.
- When roaming from the Root AP to Node1, one client (Pixel 4a) successfully roamed. The reassociation response was received from Node1, confirming the successful handoff. However, the other two clients disconnected and then reconnected.
- When roaming from Node1 back to the Root AP, all 3 real clients were deauthenticated. The deauthentication reason code was "Deauthenticated because sending STA is leaving (or has left) the BSS (0x0003)." After completing the 4-way handshake, they reconnected to the Root AP.



Preamble Puncturing Test

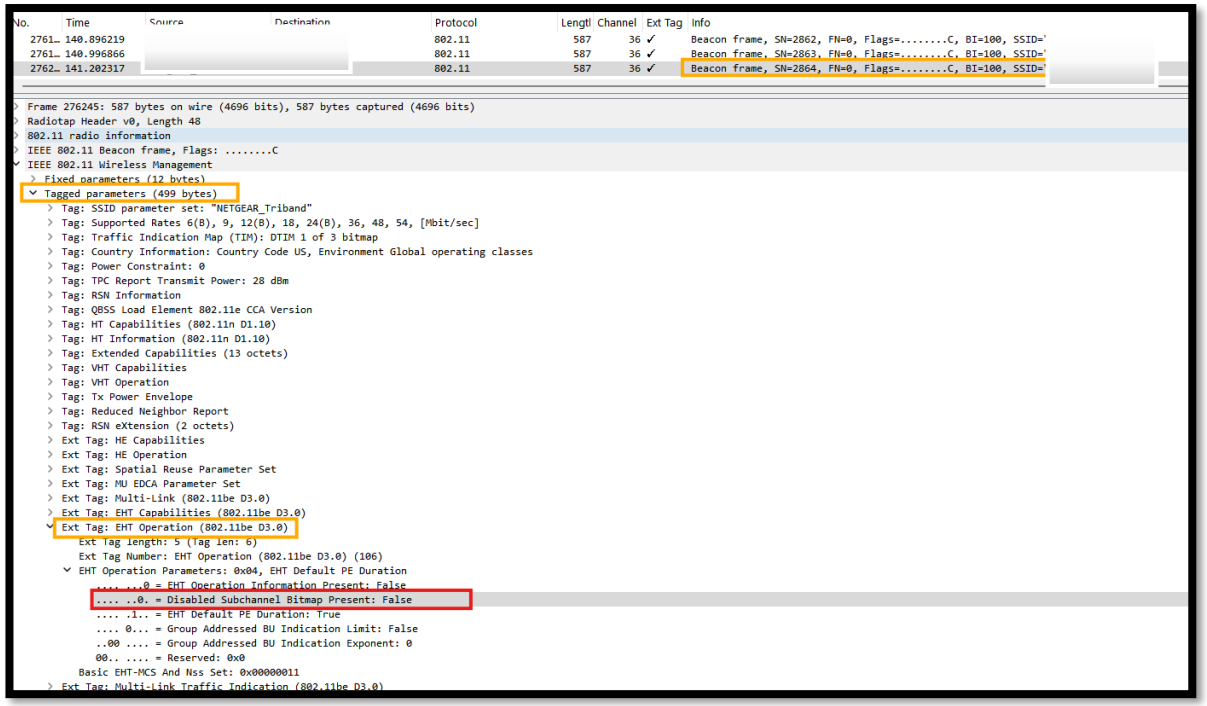
- The Preamble Puncturing test was conducted to evaluate whether the Device Under Test (DUT) AP can effectively utilize the remaining non-punctured bandwidth when interference affects specific portions of the spectrum. Testing was performed on both the 5 GHz and 6 GHz bands.
- Without interference, when the client is connected to the 5 GHz band, the achieved throughput is approximately 915 Mbps. We observed that throughput performance degradation under interference was significantly lower compared to ideal conditions.
- When the Station (STA) initially associates with the Access Point (AP) and a throughput test is conducted in the absence of interference, data transmission is occurring over the full 80 MHz channel bandwidth.

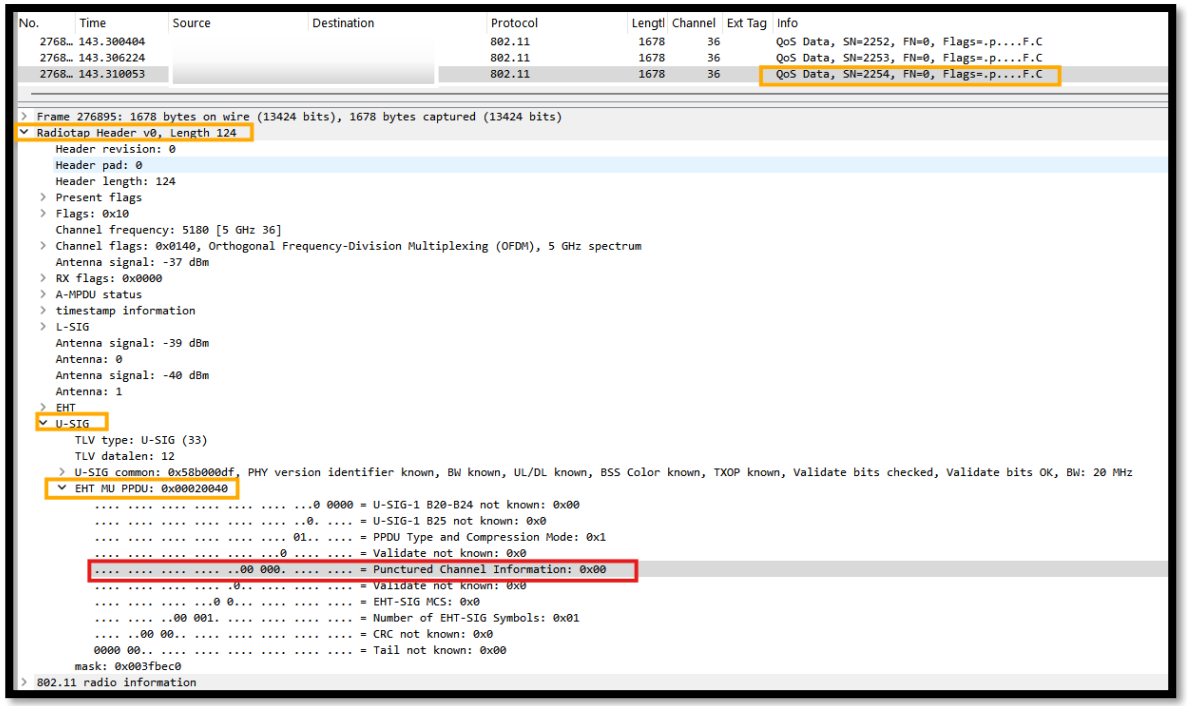




Preamble Puncturing Test

- With interference, the 20 MHz subchannel (channel 44) within the 80 MHz allocation should be excluded from transmission. This should be reflected in the Punctured Channel Information field of the QoS Data frame, which should be set to 0x03, indicating that channel 44 is punctured. However, the observed behavior of this DUT does not align with expectations.
- Even under interference, the **EHT Operations Field**: The "Puncturing Bitmap" in the Beacon Frame was set to **"False,"** indicating that no 20 MHz channel was punctured.
- Additionally, in the **QoS U-SIG Field**, the U-SIG field in the QoS frame displayed **"00 000,"** indicating "**Punctured Channel Information: 0x00".**



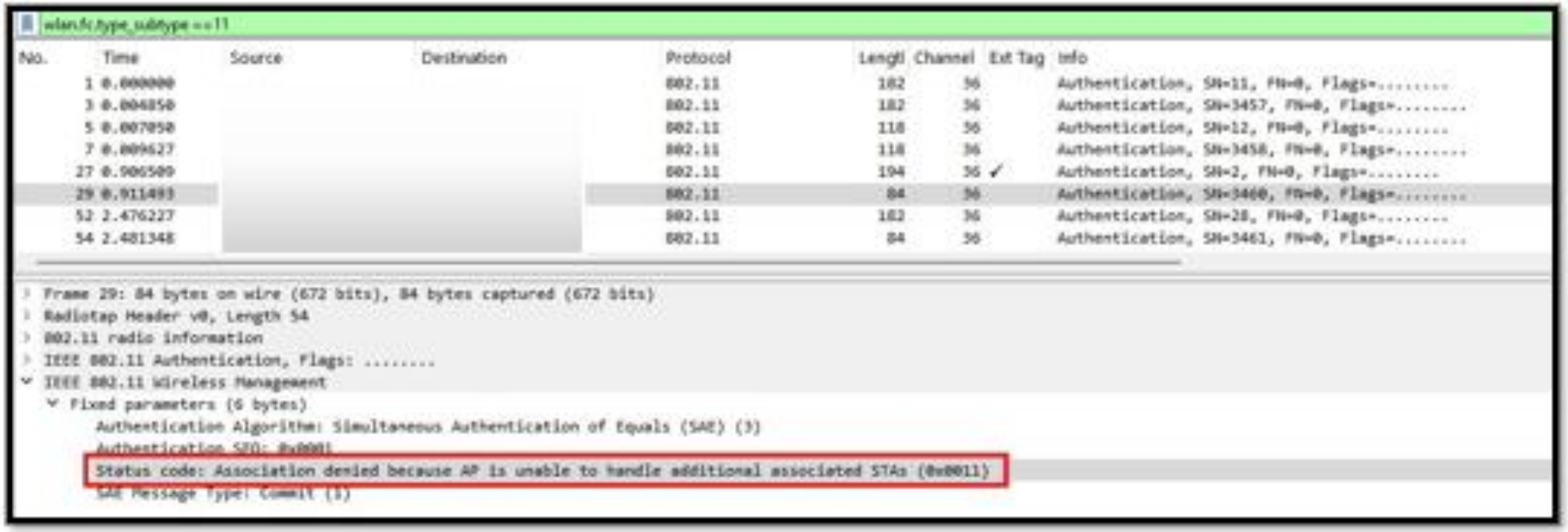


Load Balancing Test

- Conducted a load balancing test verify whether the VENDOR AP can successfully admit or reject clients based on user-defined thresholds, including the RSSI Threshold, Channel Utilization Threshold, and Max Client Threshold.
- **Load Balancing Disabled:** 14 clients connected to the 2.4 GHz band, 29 clients to the 5 GHz band, and 2 clients to the 6 GHz band.
- **Load Balancing with Balance on Client Rx RSSI Enabled:**
  - The minimum signal strength thresholds were set as follows: 2.4 GHz: -25 dBm, 5 GHz Low: -30 dBm, 5 GHz High: -30 dBm and 6 GHz: -30 dBm
  - Despite these thresholds set, clients with RSSI values above the thresholds remained connected.
  - The two clients that were initially connected to the 6 GHz band disconnected and re-associated with the 5 GHz band.
  - After this change, the client distribution was 14 clients on 2.4 GHz and 31 clients on 5 GHz.
- **Load Balancing with Balance on Channel Utilization Enabled:**
  - Maximum channel load thresholds were configured as follows: 2.4 GHz: 70%, 5 GHz Low: 75%, 5 GHz High: 75%, 6 GHz: 65%
  - All clients remained connected, and the distribution remained unchanged (14 clients on 2.4 GHz and 31 clients on 5 GHz).

Load Balancing Test

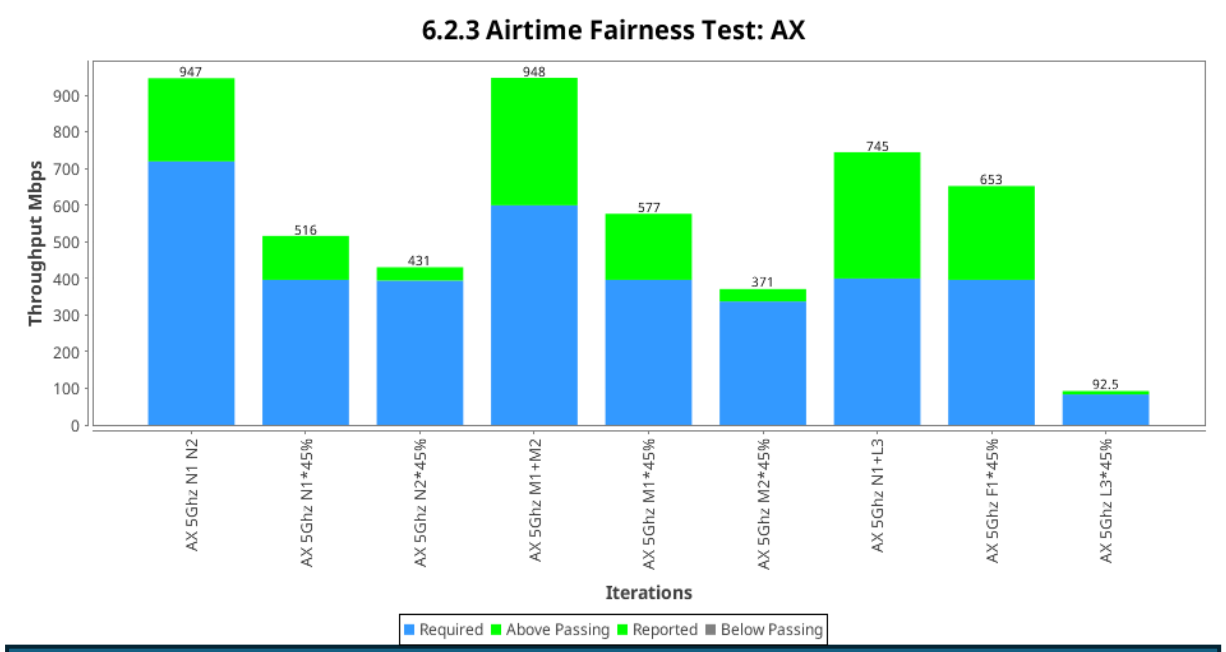
- **Load Balancing with Maximum Number of Clients per Radio Enabled:**
  - Thresholds were set as follows: 2.4 GHz-15 clients, 5 GHz Low: 20 clients, 5 GHz High: 20 clients and 6 GHz: 10 clients.
  - Initially, 13 clients connected to 2.4 GHz, 31 clients to 5 GHz, and 1 client to 6 GHz.
  - Once the 2.4 GHz band reached 15 clients, additional clients were denied with the expected message: "Association denied for 1c:c1:0c:36:1d:f8 as maximum client count reached on 2.4 GHz.“
  - However, on the 5 GHz band, despite only 7 clients being connected, no additional clients were able to associate. AP logs and packet captures displayed the following message: "Status code: Association denied because AP is unable to handle additional associated STAs (0x0011).“



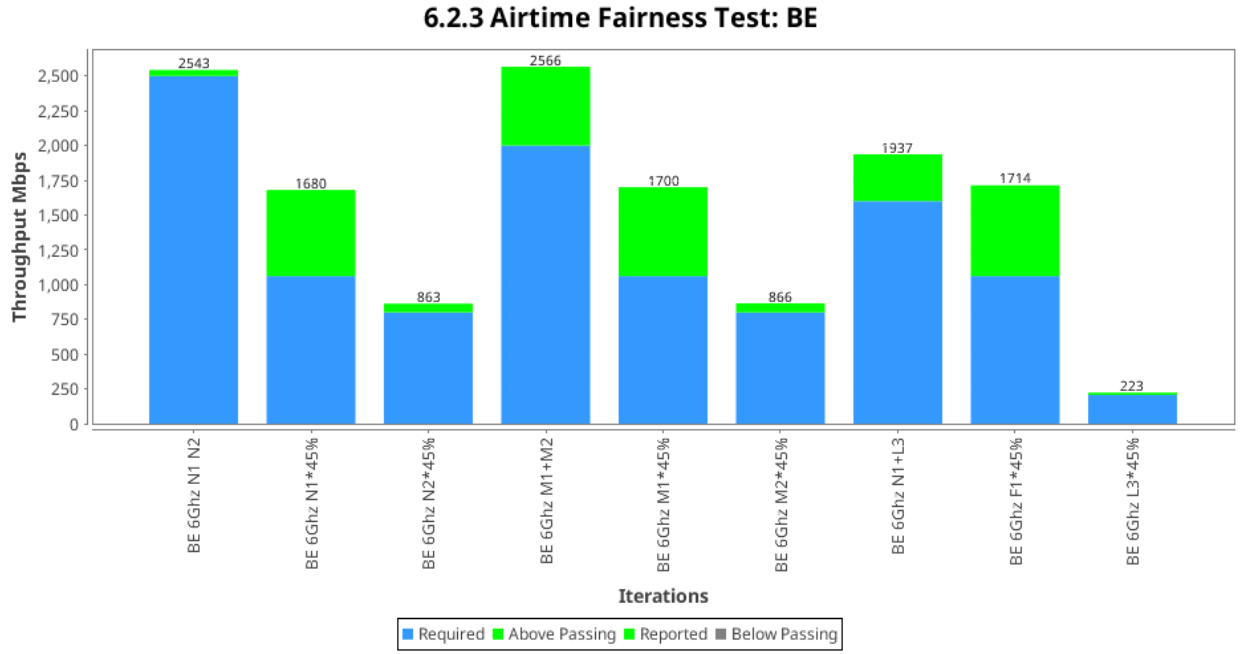
Airtime Fairness Test

- Conducted the Airtime Fairness Test to assess the Wi-Fi device's ability to ensure fair airtime usage between clients. The setup involves two client stations: one consistently configured in an optimal state, while the second alternates between optimal, weak signal, and legacy mode configurations.
- For each scenario, the maximum TCP throughput of each station is first measured independently. Based on these values, UDP traffic is then generated — 75% of the measured TCP throughput on Station 1 and 50% on Station 2. This combination intentionally overdrives the access point, leading to frame drops.
- The test is considered a pass if both stations achieve at least 45% of their respective TCP throughput values while transmitting the defined UDP traffic concurrently. This ensures that the AP maintains a fair distribution of airtime even under load and varying client conditions.
- We have conducted this test on both 5GHz (80MHz Bandwidth) and 6GHz (320MHz Bandwidth) bands with AX and BE modes and overall, the Airtime fairness test is passed in all the combinations attaining throughput more than the Pass/Fail criteria value with both the modes.

Airtime Fairness Test



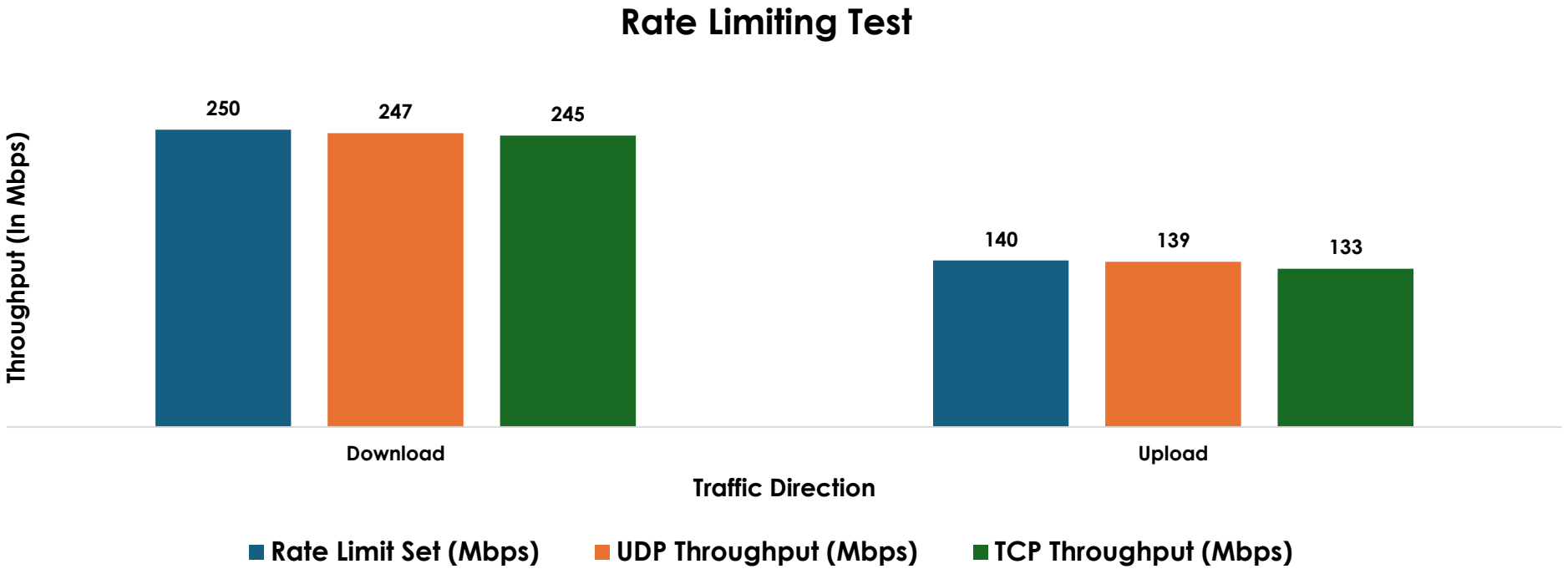
With Client connected to 5GHz Band in AX Mode (80MHz Bandwidth)



With Client connected to 6GHz Band in BE Mode (320MHz Bandwidth)

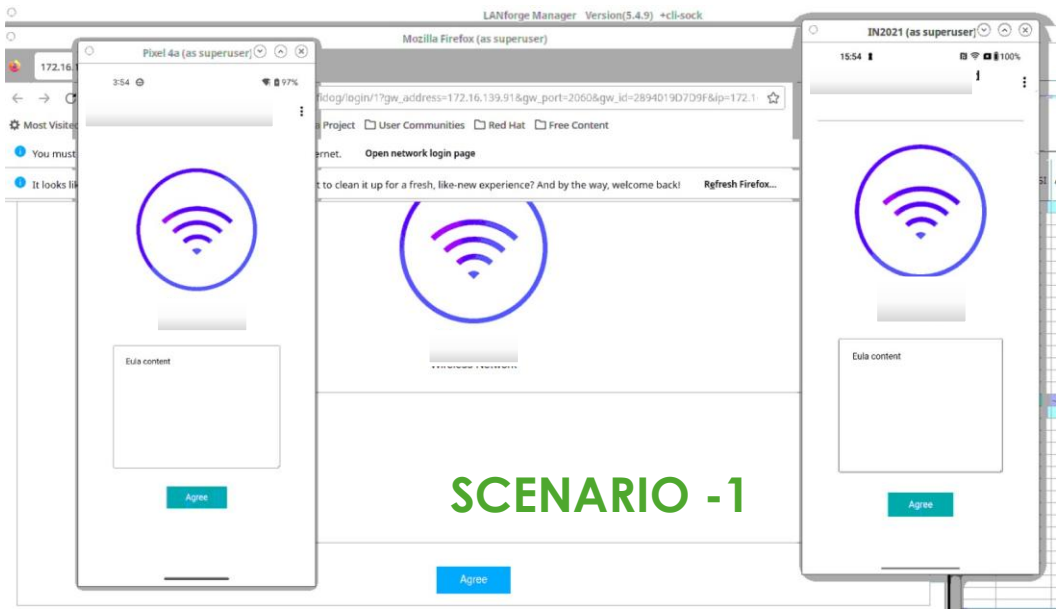
Rate Limiting Test

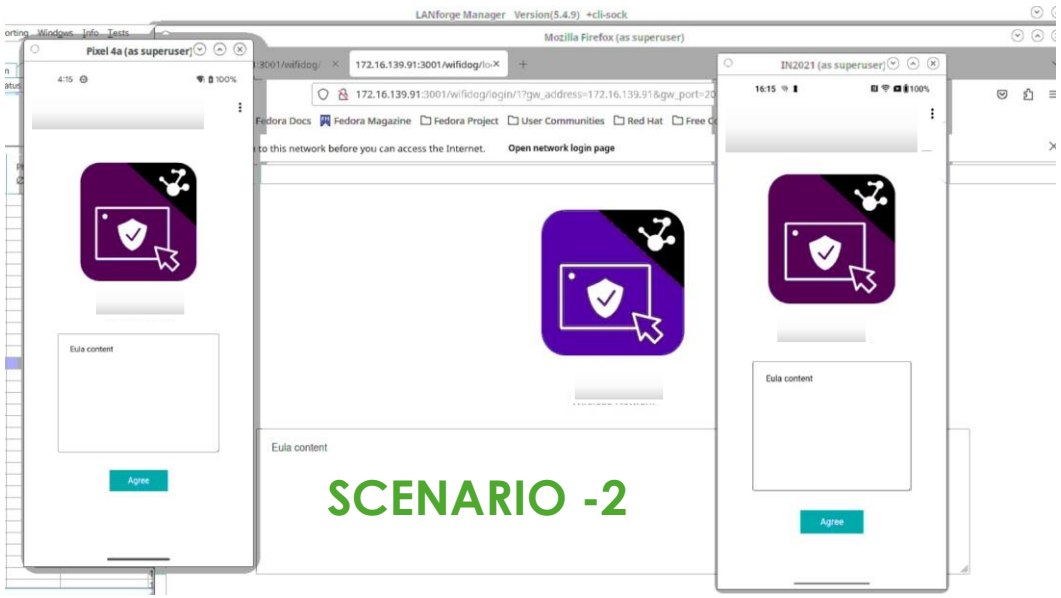
- Conducted the Rate Limiting test by enabling the rate limiting feature on the AP via the Insight Cloud. The download and upload rate limits were configured to 250 Mbps and 140 Mbps, respectively.
- A client device was connected to the Tri-band SSID, and throughput tests were performed to measure both download and upload speeds using TCP and UDP protocols.
- As expected, after enabling the rate limiting feature on the AP, the client was only able to achieve throughput values below the configured rate limits, thereby confirming that the feature is functioning as intended.



Captive Portal Test

- We conducted Captive Portal testing with a total of 50 clients, including 2 real devices and 48 virtual clients.
- **Scenario 1 – Basic Captive Portal (No Redirection):** A standard captive portal without URL redirection was configured on the Access Point. Upon connecting to the SSID, the captive portal page was displayed correctly on both real and virtual clients. After accepting the terms, internet access was successfully granted to all clients.
- **Scenario 2 – Captive Portal with URL Redirection:** A captive portal with redirection to the splash website and a custom logo was configured on the VENDOR AP Cloud. This scenario also worked as expected. The captive portal page was presented correctly, and users were redirected to the specified URL after accepting the terms.

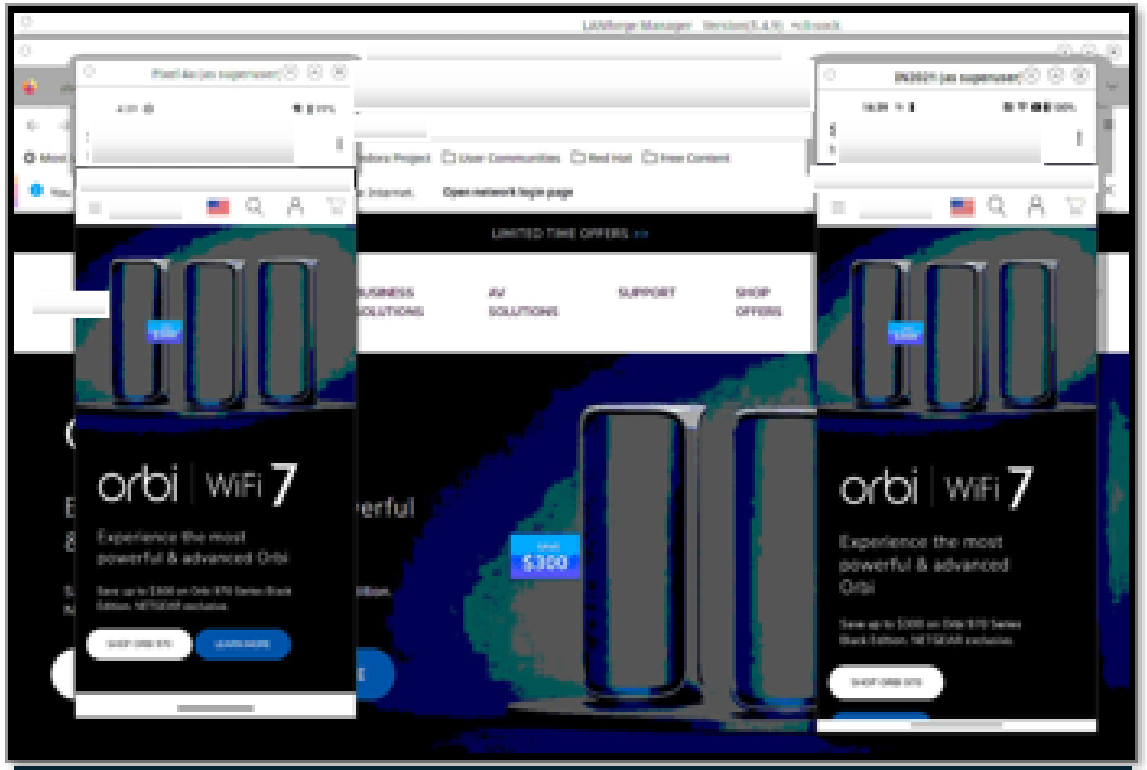




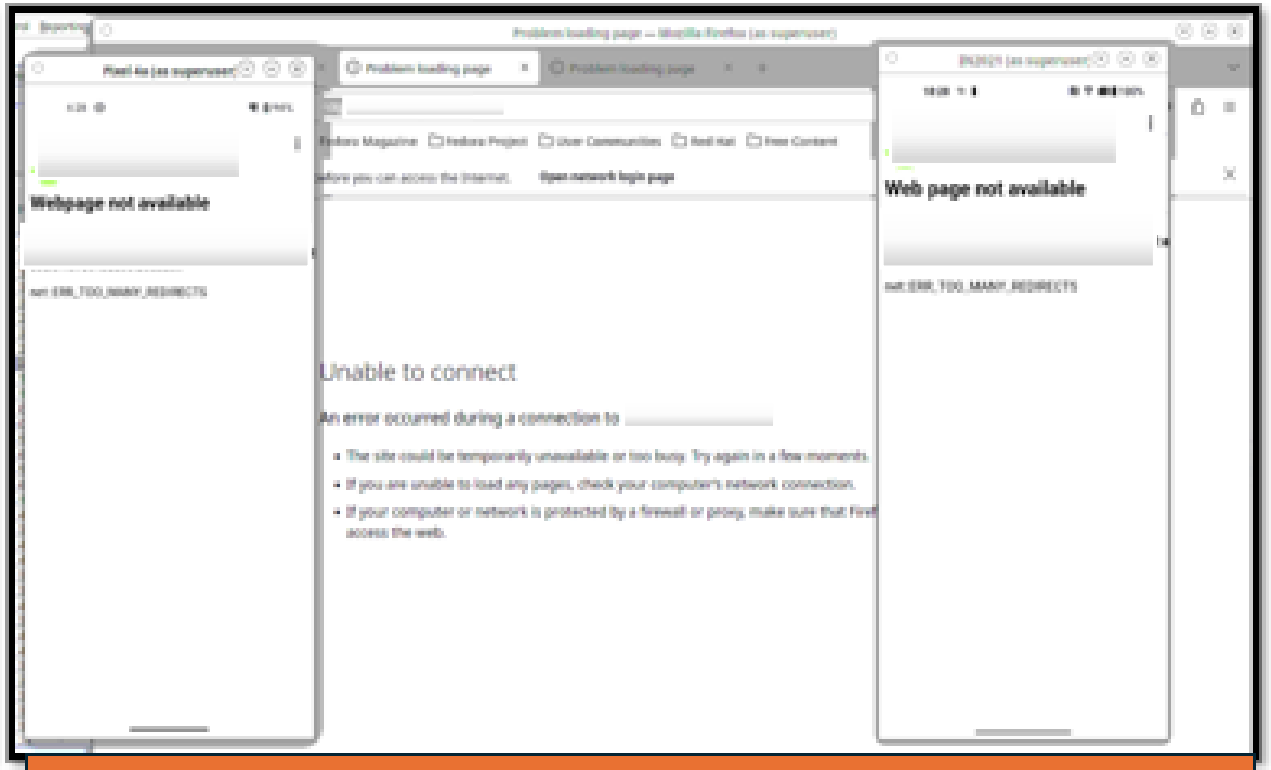
Captive Portal Test

- **Scenario 3 – External Captive Portal with Web/HTTP Authentication:** An external captive portal was configured with Web/HTTP authentication, including a secret and keyphrase.
- When the required splash URL was included in the Walled Garden, virtual clients were able to access the URL directly. Real clients prompted for sign-in/authentication, and upon user interaction, were redirected to the splash page.
- However, when the splash page URL was excluded from the Walled Garden, the expected behavior was for clients to be redirected to the login page to enter the secret and keyphrase. Instead:
  - Real clients displayed a "Sign in to network" prompt, but upon clicking it, a "Webpage not available" error appeared, and the login page was not shown.
  - Virtual clients failed to trigger a login popup and instead showed a "Unable to connect" error.
- As a result, when the splash page URL was not part of the Walled Garden, both real and virtual clients were unable to access the internet, and the expected login page was not presented.

Captive Portal Test



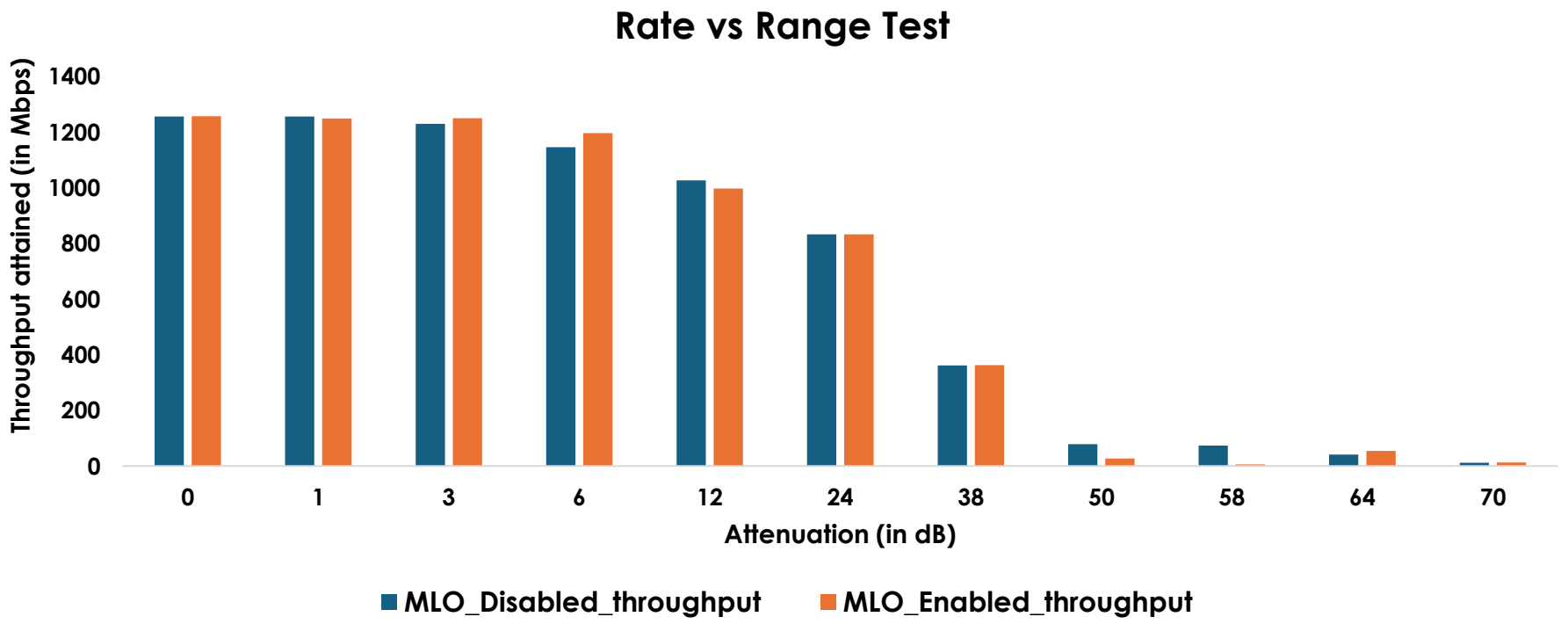
When the required splash URL was included in the Walled Garden, clients were able to access the URL directly



When the splash page URL excluded from the Walled Garden, both real and virtual clients were displayed a "Sign in to network & Unable to connect" prompt, and the expected login page was not presented.

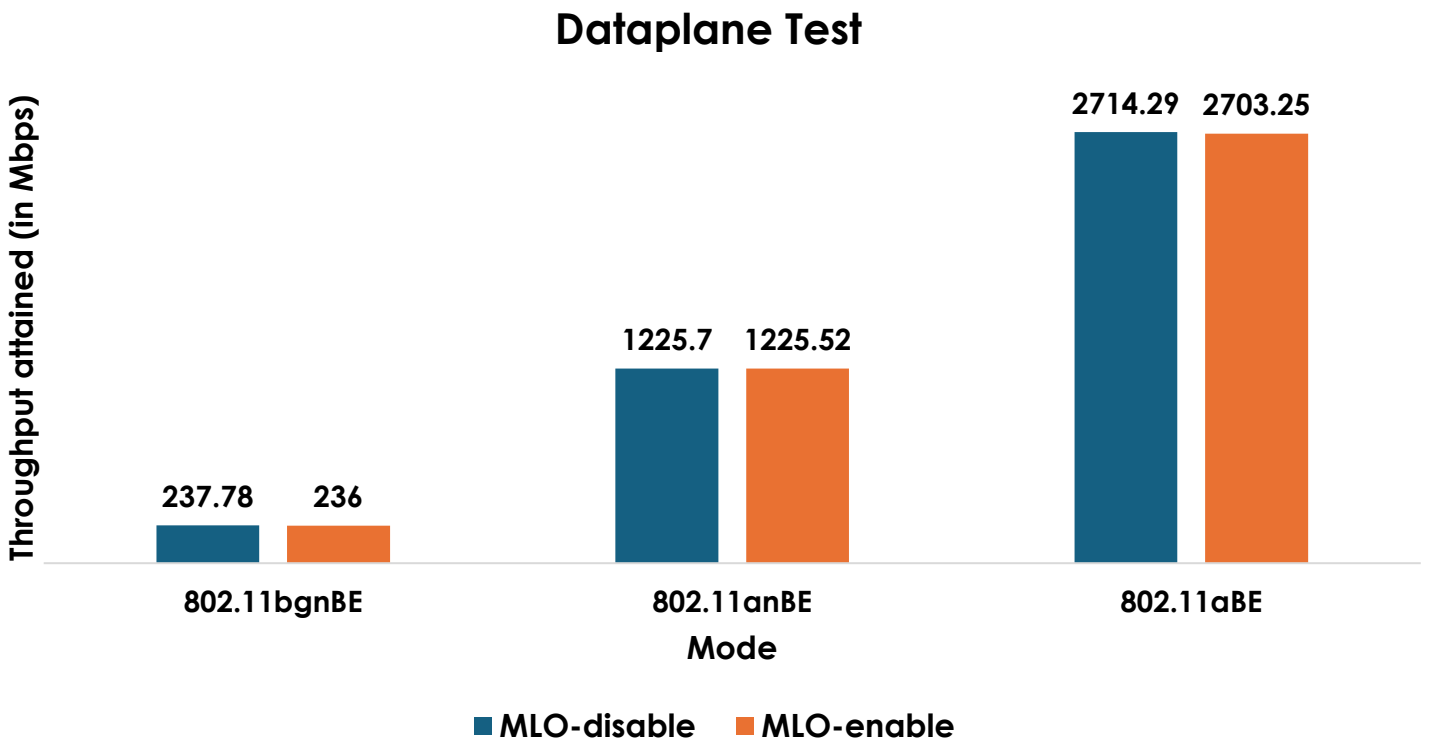
Rate vs Range

- RvR (Rate vs Range) testing was conducted under both MLO-enabled and MLO-disabled configurations. The throughput comparison graph illustrates performance across various attenuation levels: 0, 1, 3, 6, 12, 24, 38, 50, 58, 64, and 70 dB.
- The results indicate that enabling MLO did not result in significant throughput improvements compared to the non-MLO configuration. Throughput remained largely consistent across all attenuation levels in both modes, with no notable performance gains observed when MLO was enabled.



Data-Plane Test

- Data plane test was conducted under both MLO-enabled and non-MLO configurations. The tests utilized MTU-sized packets over best-effort (BE) traffic across **bgn**, **an**, and **a** modes.
- The results show that enabling MLO did not provide any measurable improvement in throughput compared to the non-MLO setup.



Mode	MLO-disable	MLO-enable
802.11bgnBE	237.78	236
802.11anBE	1225.7	1225.52
802.11aBE	2714.29	2703.25

Band steering

- Band steering was tested across multiple configurations, including combinations of MLO enabled/disabled, band steering enabled/disabled, and 802.11r enabled/disabled.
- Testing was conducted by varying the client-to-AP distance using programmable attenuators to simulate near, medium, and far range scenarios.
- Across all scenarios, band steering was observed to occur by disconnecting from the current band and reconnecting to the target band. During this transition, the client consistently performed a full 4-way handshake.
- Even with 802.11r enabled, clients did not utilize fast transition (FT). Instead, the full 4-way handshake was observed in each case, indicating that 802.11r was not being leveraged during the band steering process.