Network Testing & Emulation Solutions

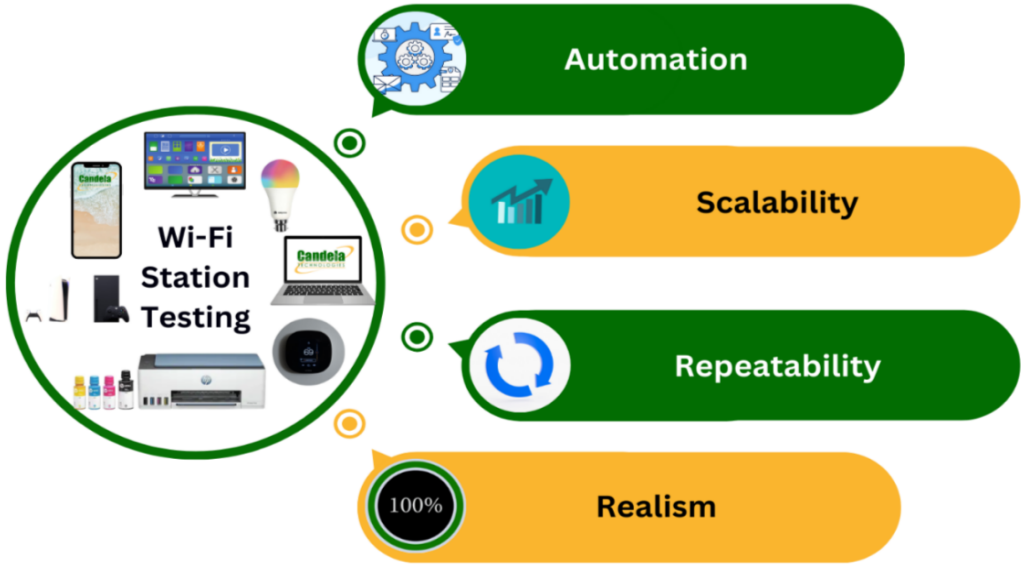
Candela Wi-Fi Station Test Solution

Station Device Testing Scenario

Candela's Station Testing Solution:

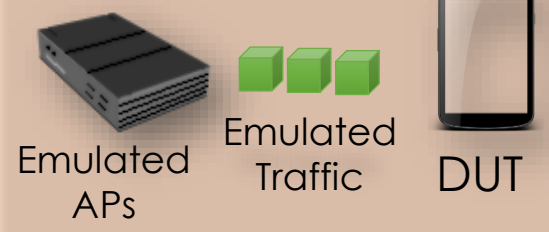
Candela's Station Testing Solution, uses **LANforge**, streamlines the testing process for a wide variety of Wi-Fi-enabled devices. These include wireless printers, scanners, cameras, patient monitors, IoT devices, and consumer electronics such as TVs, laptops, smartphones, and home automation devices like security cameras, thermostats, sensors, and more.

Our solution provides a robust testing environment, by combining automation, scalability, repeatability, and realism, and evaluating a wide range of Wi-Fi-enabled devices.



- ✓ **Automation:** Streamlines testing processes, reducing manual effort and time.
- ✓ **Scalability:** Enables testing across multiple devices and networks simultaneously.
- ✓ **Repeatability:** Ensures consistent and accurate test results across multiple runs.
- ✓ **Realism:** Simulates real-world conditions for reliable performance insights.

Wi-Fi Client Testing Supported Options



Emulated APs / Emulated Traffic

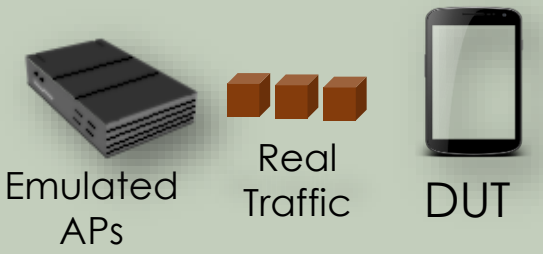
- Provides the most automated, repeatable, configurable and comprehensive test coverage.
- Ideal for early stage dev/QA, benchmarking and comparative testing

BENCHMARKING

Real APs / Emulated Traffic

- For interoperability testing with a known good golden AP from a partner.
- Still provides a high degree of test coverage and automation.
- Ideal for pre-deployment testing

INTEROPERABILITY



Emulated APs / Real Traffic

- Testing scenarios where emulated traffic cannot represent real-traffic.
- Can provide medium level of control but a higher level of realism
- Ideal for testing application specific devices

APP PERFORMANCE

Real APs / Real Traffic

- The most realistic way of testing
- Provides the least amount of control, automation and repeatability.
- Ideal for pre-deployment testing of application specific devices operating on vendor specific networks

END USER EXPERIENCE

Wi-Fi Client TEST REQUIREMENTS

Surveillance Systems

- ✓ Client Connectivity
- ✓ Stability Performance
- ✓ Range Performance
- ✓ Video Performance
- ✓ HD Video Quality
- ✓ Power-save
- ✓ WAN Impairments
- ✓ DFS testing
- ✓ Application Performance
- ✓ Battery Life
- ✓ Security
- ✓ Automation/Test Coverage

Healthcare

- ✓ Connection Reliability
- ✓ Mobility Performance
- ✓ QoS and consistent throughput
- ✓ Security
- ✓ Latency
- ✓ Coexistence on hospital Wi-Fi networks
- ✓ Location Services
- ✓ Proper Device/Network Management
- ✓ Test Services/Consulting
- ✓ Range

Peripheral & Office Equipment

- ✓ Client Connectivity
- ✓ Range Performance
- ✓ Application throughput
- ✓ Low Latency
- ✓ Security
- ✓ HD Video Quality for video conference
- ✓ Tolerance to Interference
- ✓ Proof of Concept /Vendor Selection
- ✓ Power-save
- ✓ Test Services/Consulting

Wearables

- ✓ Client Connectivity
- ✓ Different security, bands, bandwidth
- ✓ DFS/non-DFS channels
- ✓ Range – RvR, RvO
- ✓ Roaming
- ✓ Band steering
- ✓ Powersave
- ✓ Broadband speed (WANlinks)
- ✓ Video streaming
- ✓ Gaming
- ✓ Downloading apps

Consumer Electronics & IOT

- ✓ Client Connectivity
- ✓ HD Video Quality
- ✓ Zero Downtime
- ✓ Cellular and Wi-Fi Handover /Co-existence
- ✓ Range Performance
- ✓ Interference
- ✓ Interoperability
- ✓ Latency for Gaming
- ✓ Range & Roaming
- ✓ Mesh performance
- ✓ Automation
- ✓ DFS Testing

Retail /Industrial

- ✓ Zero Downtime
- ✓ Range Performance
- ✓ Application throughput
- ✓ Low Latency
- ✓ Security
- ✓ Location Services
- ✓ Cellular and Wi-Fi Handover /Co-existence
- ✓ Proof of Concept /Vendor Selection
- ✓ Test Services/Consulting

Wi-Fi Station Testing Scope

- ✓ The following testcases will be executed in Real Test-House and RF Enclosed Chambers based on the test scenario.
- ✓ Depending on the testcase scenario, either it will be executed in Real Test House or RF Enclosed Chambers or in both the environments.
- ✓ The test suite will be executed on Virtual and Real Access points. The commercially available APs will be used for the testing such as ASUS, TP Link, and NETGEAR…etc.
- ✓ Most of the analysis will be done using the Wireshark captures, and appropriate Candela testbed will be used for the testing.

Sr. No.	Test Suite/Test Case	Testcase Description	Pass/Fail Criteria
1	Connectivity Test	1. Connect the DUT to WiFi 6 and WiFi 6E APs. 2. Measure the 4-way handshake, DHCP time using the Wireshark. 3. Check the DUT connected to which SSID, BSSID, Channel, Band, and Bandwidth. 4. Check the Round-Trip Statistics, Link quality, Power level of the connection at the DUT dashboard. 5. Check the push button response time for various DUT operations.	**Pass**: DUT connects to WiFi 6 and WiFi 6E APs, handshake/DHCP completes, correct SSID/BSSID/Channel/Band/Bandwidth shown, round-trip/link stats are within acceptable range, push button responds within specified latency. **Fail**: Failure to connect, incorrect AP details, handshake/DHCP delay beyond threshold, missing or inaccurate metrics, slow/unresponsive button behavior.
2	Multi Band Test	1. Configure the AP to only 2.4GHz band and check the connectivity. 2. Configure the AP to only 5GHz band and check the connectivity. 3. Configure the AP with 2.4GHz and 5GHz with same SSID and authentication and check the connectivity. 4. Verify the statistics mentioned in the testcase 1.	**Pass**: DUT connects successfully to 2.4GHz and 5GHz individually (same SSID), correct band confirmed, metrics match expectations. **Fail**: Connection issues on any band, inability to handle same SSID on multiple bands, incorrect band report.
3	Multi SSID Test	1. Create Multiple SSID on same or multiple APs and check the connectivity. 2. Verify the statistics mentioned in the testcase 1.	**Pass**: DUT connects to all configured SSIDs, reports correct stats. **Fail**: DUT cannot distinguish between SSIDs or fails to connect.
4	Channel Test	1. Configure the AP with channel 1, 6, 11 in 2.4GHz and check the connectivity. 2. Configure the AP with UNII-1, UNII-2, UNII-2e, UNII-3 channels and check the connectivity. 3. Verify the statistics mentioned in the testcase 1.	**Pass**: DUT connects successfully to specified 2.4GHz and UNII channels, reports accurate metrics. **Fail**: DUT fails to connect on valid channels or shows incorrect stats.

Wi-Fi Station Testing Scope

Sr. No.	Test Suite/Test Case	Testcase Description	Pass/Fail Criteria
5	Bandwidth Test	1. Configure the 2.4GHz SSID to 20/40MHz BW and check the connectivity on each BW. 2. Configure the 5GHz SSID to 20/40MHZ BW and check the connectivity on each BW. 3. Verify the statistics mentioned in the testcase 1.	**Pass**: DUT connects on 20/40MHz for 2.4GHz and 20/40MHz for 5GHz, stats verified. **Fail**: Bandwidth setting mismatch or connectivity failure.
6	802.11 Security Test	1. Configure the 2.4GHz and 5GHz SSIDs to Open/WPA/WPA2 security with TKIP and AES encryption and check the connectivity on each security. 2. Verify the statistics mentioned in the testcase 1.	**Pass**: DUT connects securely using Open, WPA/WPA2 with TKIP/AES; metrics verified. **Fail**: Connection issues or failure under specific encryption types.
7	Country Code Test	1. Set the SSID country code to USA, India, and EU countries. Check the connectivity on different channels as per regulatory restrictions. 2. Verify the statistics mentioned in the testcase 1.	**Pass**: DUT connects under USA, EU, India settings, respects restrictions, channel/band compliance. **Fail**: Connection fails or out-of-bound channel usage.
8	Band Steering Test	1. Set the same SSID on 2.4GHz and 5GHz band, increase the distance between DUT and AP, and check the band steering happening when the RSSI changes. 2. Verify the DUT remains connected to AP when the Band steering happens. 3. Check the push button response time for various DUT operations.	**Pass**: DUT successfully steers between bands based on RSSI, maintains connectivity, button response within limits. **Fail**: Failed or delayed steering, disconnection, high button latency.
9	Roaming Test	1. Create roaming setup with 2-3 APs and roam the DUT between the APs. 2. Observe the DUT having the seamless operation while roaming between the APs. 3. Check reassociation request and responses, if de-authenticates, check the reason codes. 4. Check the push button response time for various DUT operations.	**Pass**: Seamless roaming with 2-3 APs, reassociation handled with proper reason codes. **Fail**: Delays, dropped connections, incorrect reassociation handling.

Wi-Fi Station Testing Scope

Sr. No.	Test Suite/Test Case	Testcase Description	Pass/Fail Criteria
10	Adjacent Channel and Co-channel Interference Test	1. Create adjacent channel and co-channel interference while the DUT is connected, check the response time of DUT operations when the interference is present. 2. Check the push button response time for various DUT operations.	**Pass**: DUT remains functional, button responds promptly under interference. **Fail**: Significant latency in the operations, dropped operations.
11	Range Test	1. Increase the distance between the DUT and AP by the step of 10, 20, 30, 40, 50 feet and check the stability of the connection between DUT and AP. 2. Verify the response time of DUT operations when the distance between AP and DUT is changes.	**Pass**: DUT remains connected up to 50 feet with proper DUT operations within the expected duration. **Fail**: Frequent disconnects or unresponsiveness for the DUT operations.
12	Home in a Box Test	1. Simulate various Near Medium Far traffic scenario on LANforge client in a Home in a Box testbed. 2. Check the check the stability of the connection between DUT and AP when the various traffic streams are simulating. 3. Check the push button response time for various DUT operations	**Pass**: DUT maintains connection under traffic load, button responds reliably. **Fail**: Connection drops or unstable under load.
13	Firmware Test	1. Test all the above tests with different firmware version which the customer would like to test.	**Pass**: All test cases pass consistently across firmware versions. **Fail**: Regression issues or test failures post firmware update.
14	Power save/suspend and wake reconnection validation	1. Verify that when a client device enters power-save or suspend mode and subsequently wakes, it can reliably re-establish the Wi-Fi connection without manual intervention. 2. Measure time to reconnect, ensure IP connectivity, and confirm no data loss or authentication failures.	**Pass**: DUT reconnects automatically, no manual intervention, no auth loss. **Fail**: Failure to reconnect or requires user action.
15	Hidden SSID behavior	1. Confirm that clients can successfully connect to a network with a hidden SSID (non-broadcast) by manually configuring the SSID. 2. Test both initial connection and reconnection scenarios. Ensure there is no intermittent disconnect once connected.	**Pass**: DUT connects and reconnects to hidden SSID without drop. **Fail**: Fails to connect or maintain connection.

Wi-Fi Station Testing Scope

Sr. No.	Test Suite/Test Case	Testcase Description	Pass/Fail Criteria
16	Long-term connection stability (soak test)	1. Connect the DUT to an access point. Make sure that the DUT is connected to power. 2. The suspend operation is disabled in the DUT. 3. The sleep and wake up operation is active. 4. Verify the connectivity for 24 hours	**Pass**: DUT remains connected with access point for 24 hours. **Fail**: Connection drops or operation not executable.
17	AP reboot and failover behavior	1. Simulate an access point reboot or outage. 2. Verify that a connected client seamlessly reconnects to another available AP or re-associates with the same AP post-reboot. 3. Measure failover time, authentication success, and packet loss.	**Pass**: DUT reconnects post-reboot seamlessly. **Fail**: Reconnect fails.
18	DHCP lease expiry and IP renewal	1. After the DHCP lease time expires, ensure the client properly renews or reacquires its IP address without disruption. 2. Check that there is no drop in connectivity during the lease renewal process.	**Pass**: DUT renews IP smoothly, no connectivity loss. **Fail**: IP renewal failure or service disruption.
19	Network congestion and its impact on button responsiveness	1. Under high network load, assess how congestion affects DUT responsiveness, such as when manually triggering SSID scan, reconnect, or other DUT operations. 2. The button operations should have minimum latency(≤200 ms latency).	**Pass**: DUT operations response remains within 200 ms . **Fail**: Latency exceeds 200 ms or becomes unresponsive.
20	Aggressive Roaming and Handoff Latency Under Load	1. Place the client in an environment with overlapping APs and heavy traffic. 2. Measure handoff performance (signal threshold triggers, time to reassociate) under load. 3. Validate roaming decision logic and ensure handoff latency is within spec (e.g., <50 ms).	**Pass**: Handoff latency < 50 ms; no drops. **Fail**: Delayed handoff, disconnects, or high latency.
21	DFS Channel Move Handling	1. On detection of radar signals requiring Dynamic Frequency Selection, verify that the AP migrates to a new DFS-compliant channel and the client automatically follows. 2. Measure reconnection delay and test no-traffic windows comply with regulatory limits.	**Pass**: DUT reconnects to DFS-safe channel with minimal delay. **Fail**: Loss of connection or failure to comply with DFS.

Wi-Fi Station Testing Scope

Sr. No.	Test Suite/Test Case	Testcase Description	Pass/Fail Criteria
22	International Channel Move Handling	1. Set the SSID country code to USA, India, and EU countries. Check the connectivity on different channels as per regulatory restrictions. 2. Verify the statistics on the DUT dashboard.	**Pass**: DUT connects under USA, EU, India settings, respects restrictions, channel/band compliance. **Fail**: Connection fails or out-of-bound channel usage.
23	High-Interference with Varying Client Density	1. Introduce RF interference and vary the number of clients connected to the access point. 2. Observe the DUT performance with various supported operations.	**Pass**: DUT performs all the operations in presence of interfence. **Fail**: DUT does not get proper airtime from the access point and operations delays.
24	Rapid SSID Switching	1. Switch the DUT rapidly between multiple SSIDs (e.g., every 30 seconds). 2. Ensure each reconnection is timely, secure authentication is successful, and the system remains stable over repeated transitions.	**Pass**: DUT reconnects quickly with secure auth in < 5s interval. **Fail**: Inconsistent behavior or auth failure
25	WiFi Beacon Loss / Micro Outages	1. Simulate short-term AP signal disruptions (e.g., 100 ms intervals). 2. Ensure the DUT remains associated or quickly recovers without user impact. Validate packet retransmission behavior and reconnection latency.	**Pass**: DUT remains connected or recovers within 1s. **Fail**: Drops connection or takes too long to recover.
26	Negative Test – Corrupted Beacon Frames	1. Simulate delivery of malformed or corrupted beacon frames to verify how the client handles invalid Wi-Fi management data using Virtual Access Point. 2. Confirm that the device does not crash, hang, or misbehave due to malformed headers or timing information.	**Pass**: DUT ignores corrupted frames, remains stable. **Fail**: Crashes, hangs, or malfunctions.
27	RF Storm Test (Noise Injection)	TBD	TBD

Wi-Fi Station Testing Scope

Sr. No.	Test Suite/Test Case	Testcase Description	Pass/Fail Criteria
28	Beacon Starvation + High Latency Combo	1. Simulate a scenario where beacon frames are severely delayed or lost due to congestion or interference, combined with high network latency. 2. Confirm the client continues to function or gracefully degrades and recovers post-impairment.	**Pass**: DUT sustains connectivity despite beacon delays. **Fail**: Disconnects or significant degradation.
29	Low-Level Frame Flooding / Management Frame Injection	1. Flood the Wi-Fi medium with excessive management/control frames (e.g., disassociation, Deauthentication, probe requests). 2. Confirm that the DUT properly authenticates legitimate messages, ignores spoofed ones, and maintains connectivity under attack. 3. The network flooding is feasible with the LANforge.	**Pass**: DUT filters spoofed frames, continues legitimate communication. **Fail**: Auth issues or DUT crashes.
30	(Optional) OTA update via WiFi	1. Need more inputs on the requirements	Need more inputs on the requirements

Surveillance Systems

RvR

Wanlink

Interference

Roaming

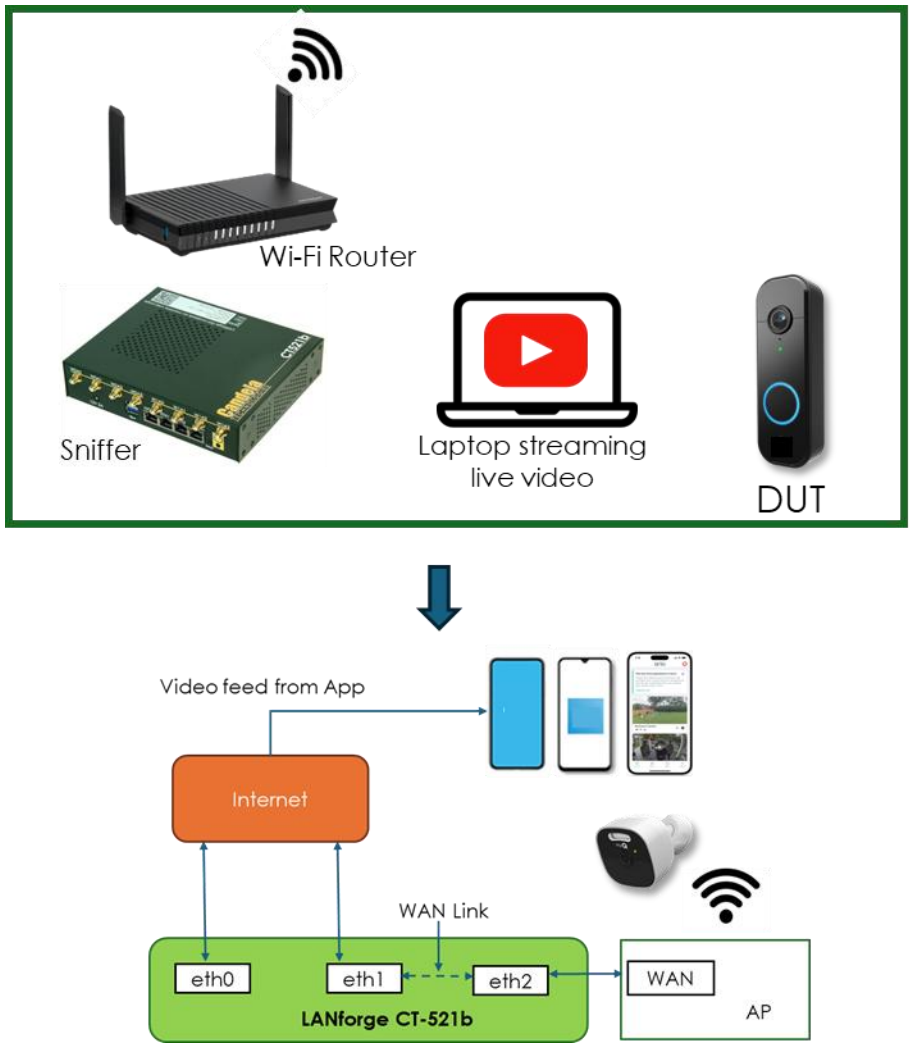
Surveillance Systems

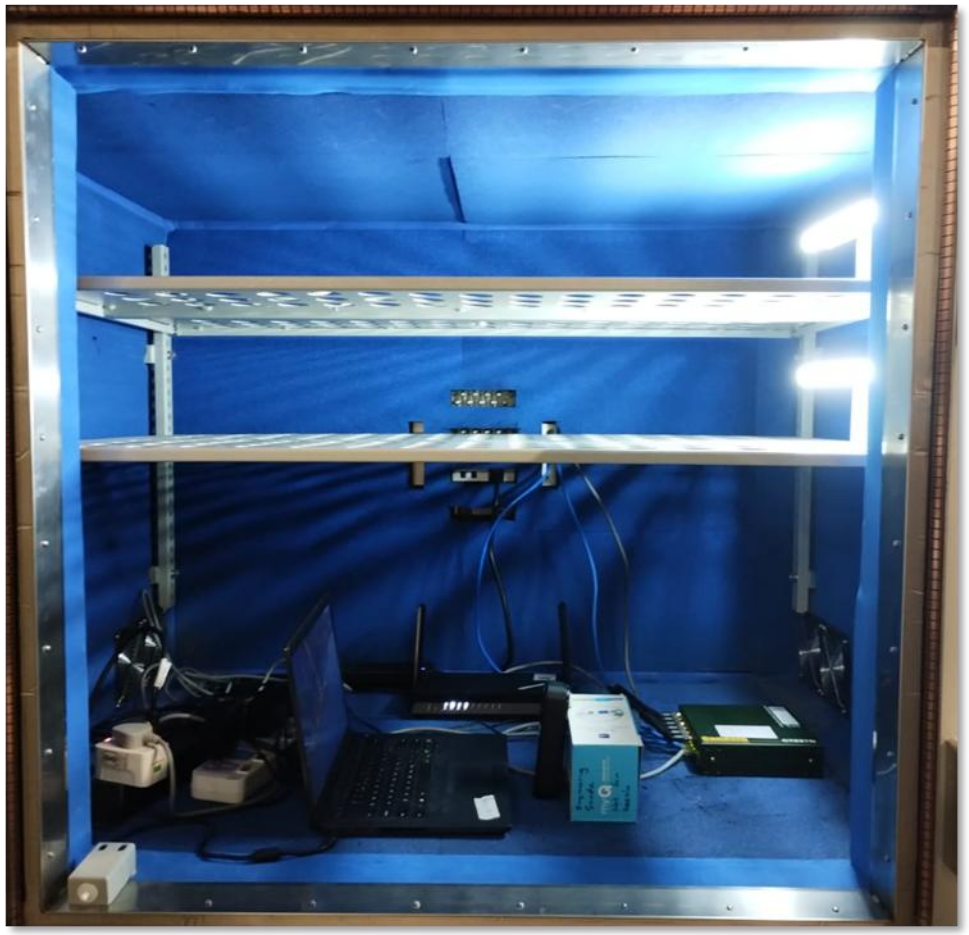
Indoor/Outdoor Surveillance Cameras, Smart Doorbell Keypads, Motion Sensors, Home Security Controllers

Tests:

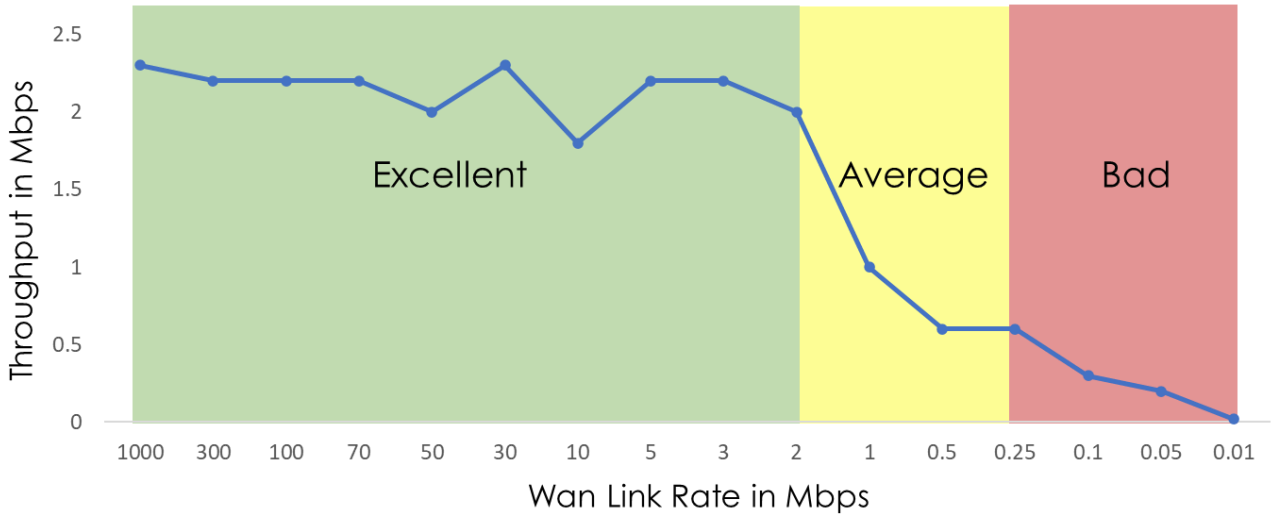
- ✓Long duration operation test
- ✓Stress testing with simultaneous motion and streaming
- ✓Connection times/failures.
- ✓Motion Detection testing and testing other triggers.
- ✓Power consumption profile (sleep, active, peak streaming)
- ✓Performance under limited or fluctuating bandwidth
- ✓Medium Streaming Performance and overall system performance in:
  - ✓Baseline ideal conditions
  - ✓Over distance
  - ✓With Wi-Fi interference
  - ✓With non- Wi-Fi Interference

Testbed Images



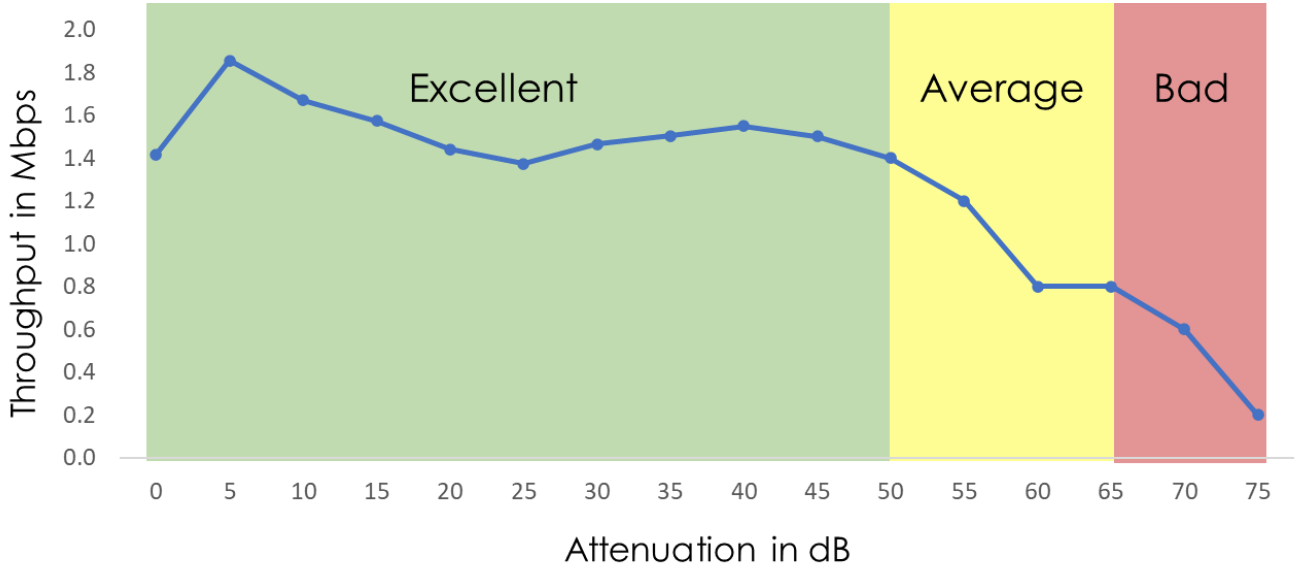


Sample Test Reports



User can have good experience till 2Mbps of link rate, post that there is a decline in throughput

User can have good experience till 50dB attenuation, post that there is a decline in throughput



Broadband speed - Video Observations

Camera 1

Link speed – 1Gbps (Avg)

Link speed – 100Mbps (Avg)

Link speed – 20Mbps (Avg)

Camera 2

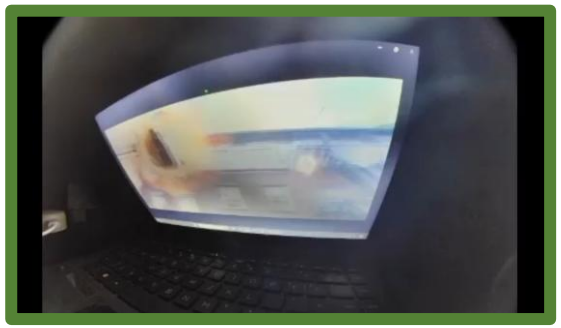
Link speed – 1Gbps (Excellent)

Link speed – 100Mbps (Excellent)

Link speed – 20Mbps (Excellent)

Camera 3

Link speed – 1Gbps (Excellent)



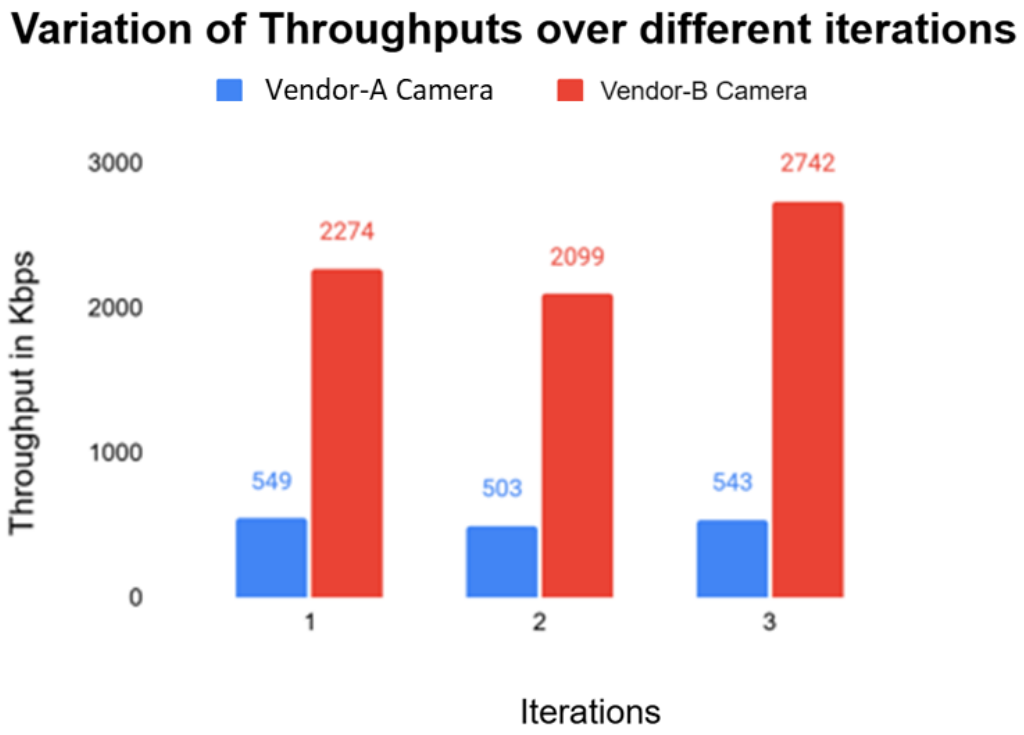
Link speed – 100Mbps (Excellent)

Link speed – 20Mbps (Excellent)

Throughput Test

In this test we have performed the below scenarios:

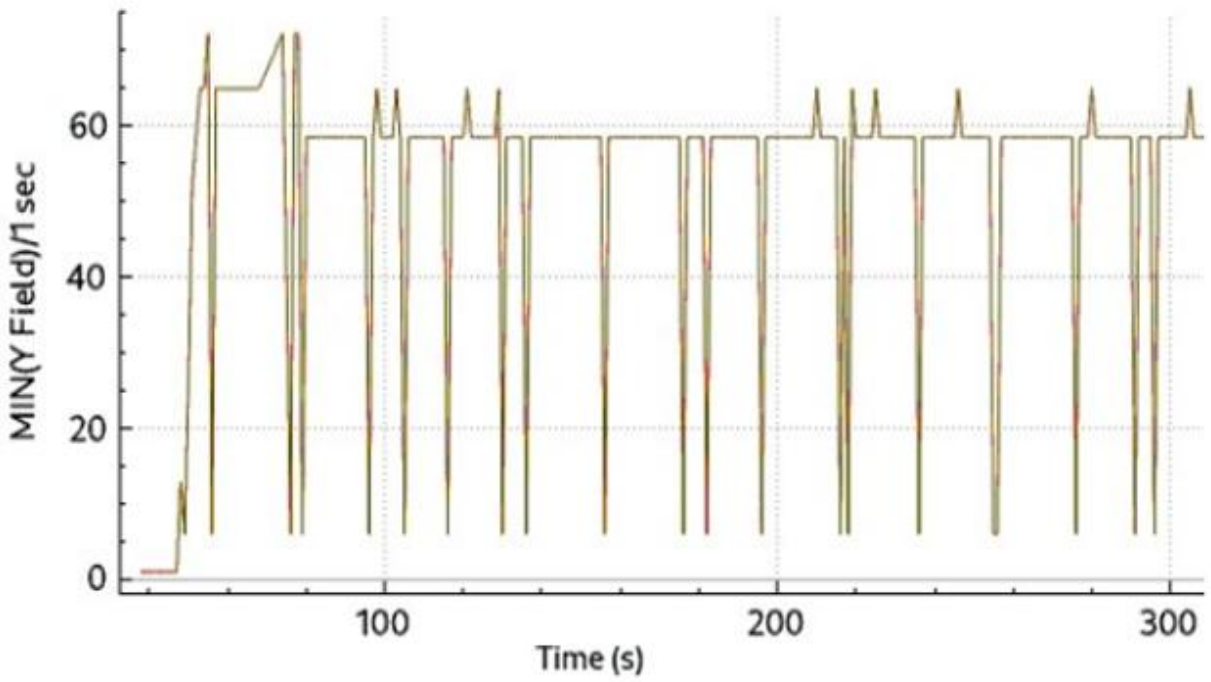
1. Run the live stream, evaluate the throughput for vendor-A and vendor-B cameras
2. Check the video quality and audio-video synchronisation.



- The achieved throughputs are higher with Vendor-B Camera when compared to Vendor-A camera.
- Audio and video synchronisation fails at times and the video playback is not smooth

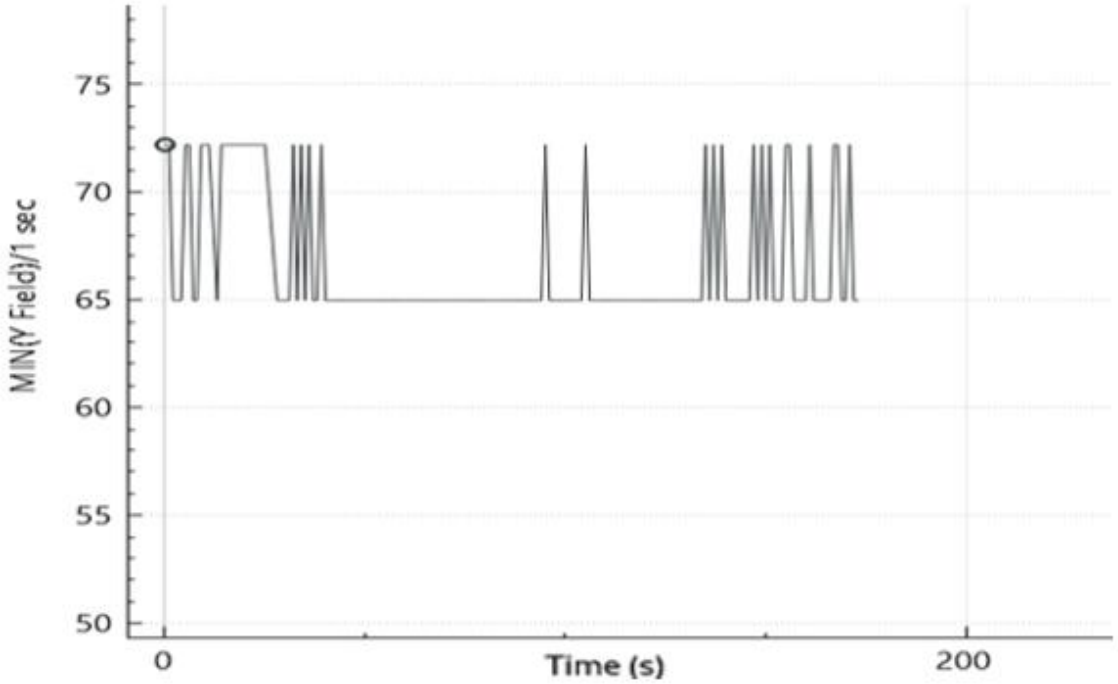
Throughput Test – Lower Throughput Observations

Vendor-A Camera



With the Vendor-A camera the variation of data rate is very high

Vendor B camera



With Vendor B Camera the variation of data rate is very less. The least data rate is around 65 Mbps

Live Video Streaming Test

Realtime scenario:

- In the application we have the live video streaming option, in which we can check the current activity happening near the video keypad. This can be helpful to check if anyone is performing any activity in front of the camera.

Procedure:

- Here we have placed a Tablet in front of the video keypad, such that there will be a motion activity and actions happening near the camera line of sight.
- We also tried to add packet loss while doing the live video streaming to determine the performance of the video keypad.

Observations:

Sno	Packet loss	MCS		Data rate (Mbps)		Throughput (Kbps)		No of QoS frames		Amount of data transferred		Number of retries	
		Vendor-A	Vendor-B	Vendor-A	Vendor-B	Vendor-A	Vendor-B	Vendor-A	Vendor-B	Vendor-A	Vendor-B	Vendor-A	Vendor-B
1	0%	5	7	52	72.2	1529	1936	21072	24277	23MB	29MB	961	3898
2	5%	5	7	52	72.2	1125	2062	17044	25787	17MB	31MB	905	3758
3	10%	7	7	72.2	72.2	262	313	7446	5687	4MB	5MB	1734	837
4	15%	5	7	52	72.2	313	272	4374	6074	5MB	4MB	213	1024
5	20%	No stream	7	No stream	72.2	No stream	273	No stream	6208	No stream	4MB	No stream	986
6	30%		7		72.2		282		6407		4MB		951

Home in a Box Test

Observations with Wi-Fi Interference:

Sno	Channel Utilization	MCS		Data rate (Mbps)		Throughput (Kbps)		No of QoS frames		Amount of data transferred		Number of retries	
		Vendor-A	Vendor-B	Vendor-A	Vendor-B	Vendor-A	Vendor-B	Vendor-A	Vendor-B	Vendor-A	Vendor-B	Vendor-A	Vendor-B
1	20%	5	7	52	72	1322	1771	19427	17136	20MB	19MB	1713	727
2	50%	7	7	72	72	1311	1710	24053	17881	24MB	22MB	927	1049
3	95%	5	7	52	72	830	920	19347	10109	18MB	11MB	3292	1108

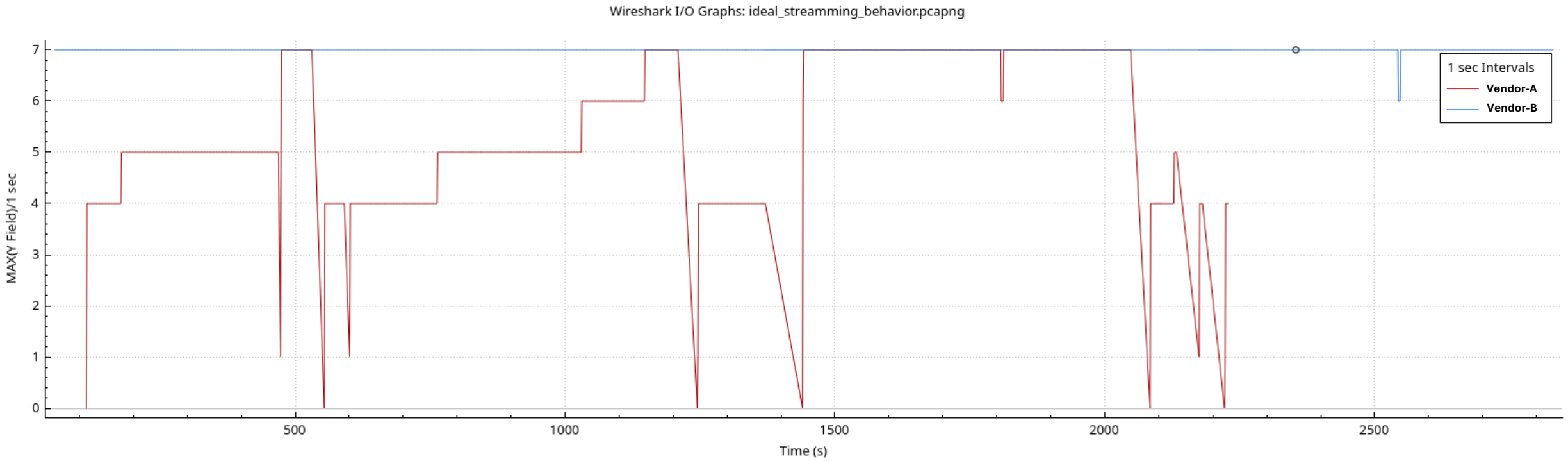
Observations with Zigbee and BLE Interference:

Sno	MCS		Data rate (Mbps)		Throughput (Kbps)		No of QoS frames		Amount of data transferred		Number of retries	
	Vendor-A	Vendor-B	Vendor-A	Vendor-B	Vendor-A	Vendor-B	Vendor-A	Vendor-B	Vendor-A	Vendor-B	Vendor-A	Vendor-B
1	5	7	52	72	1259	1747	15201	23401	17MB	27MB	256	906

- Here we can notice that the vendor-A device is having fluctuations in MCS rates even at 0% channel utilization and it is happening at random intervals.
- Also, the quality of the live streaming is getting dynamically adapted in the vendor-B device due to which there is a better user experience.

Home in a Box Test

MCS Fluctuation with Vendor-A camera



Throughput Test – Lower Throughput Observations

The retransmissions are recorded high in the Vendor-A camera when compared to Vendor-B camera

Retransmissions recorded on the chamberlain device:

- **WLAN retries:** (25.5%)

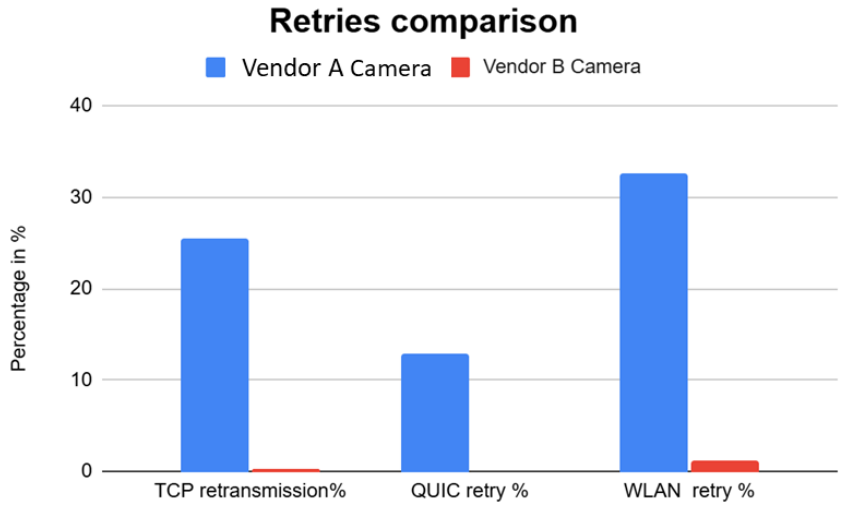
  Layer 2 retries account for 25% of the total data frames sent by the Vendor-A Camera
- **QUIC retries:** (12.9%)

  The video transmission occurs over the QUIC protocol, with retries recorded at approximately 12%.
- **TCP retries:** (32.06%)

  TCP retransmissions are the highest observed, constituting 32% of all TCP packets transmitted during the video session

Retransmissions recorded on the Vendor B Camera:

- **WLAN retries (0.31%) are an TCP retries are 1.18%.**
- Here QUIC protocol is not used for video audio transmission



Achieved Throughput vs Channel Utilization

S No.	Channel Utilisation	Throughput (Mbps)				
		Vendor A Camera	Vendor B Camera	Vendor A Doorbell	Vendor B Doorbell	Vendor C Camera
1	35	0.731	4.819	1.391	2.307	1.063
2	25%	0.674	4.896	1.179	1.694	1.088
3	50%	0.651	4.619	1.052	1.687	1.081
4	75%	0.586	4.497	1.031	1.689	1.085
5	>90%	0.415	2.765	1.055	1.252	0.983

- When increasing the channel utilization using virtual clients, we have observed that the throughput drop across all the devices is quite consistent.
- None of the DUTs disconnected from the network during the test duration but there were frame drops and delays in some scenarios.

Rate vs Range test observations

Attenuation	Vendor-A Camera(Mbps)	Vendor-B Camera(Mbps)	Vendor-A doorbell (Mbps)	Vendor-B Doorbell (Mbps)	Vendor-C Camera (Mbps)
0dB	2.26	4.62	0.33	1.29	1.13
10dB	0.82	4.66	0.83	1.23	1.13
20dB	1.99	4.61	0.94	1.33	1.22
30dB	2.74	4.62	0.23	1.3	1.11
40dB	1.25	4.5	0.36	1.17	1.13
50dB	1.36	4.40	0	1.20	0.10
60dB	0	0.21	0	0	0
70dB	0	0	0	0	0

- When increasing the attenuation using programmable attenuators, we have observed that the throughput drop across all the devices is different.
- Throughput irregularities at different attenuations were seen mostly in the Vendor-A devices. At some attenuations, we could see a throughput spike instead of a dip.
- Vendor-C Camera and Vendor-A doorbell were the devices to disconnect first, both at 60dB attenuation whereas the remaining disconnected at 70 dB.

Motion Detection and Notification Delay Across Devices

Delay between motion detection and app notification							
S No.	**DUT**	**No of trails**	**Minimum time(sec)**	**Maximum time(sec)**	**Average time(sec)**	**Speed**	**Comments**
1	Vendor-A doorbell	5	13	27	16	Good	Detecting motions but delay in reporting.
2	Vendor-B Doorbell	5	3	5	3	Excellent	Quick reporting but low quality initially
3	Vendor-A Security Camera	5	11	24	15	Good	Detecting motions but delay in reporting.
4	Vendor-B Camera pro	5	3	5	3	Excellent	Quick reporting but low quality initially
5	Vendor-C Camera	5	17	40	21	Poor	Performed poorly without setting zones, less sensitive.

- The above observations are recorded without setting up the motion detection zones on the devices app. After creating some movement in the DUT's field of view, we measured the time it took to get a notification in the app.
- We noticed that Vendor-C Camera performed the worst with around 21s avg time whereas the Vendor-B devices performed the best with Vendor-A being in the middle.
- The quality of the video recorded by the Vendor-B devices seems to be low at the beginning of the video but is getting better within the first 5 seconds.

Motion Detection and Notification Delay Across Devices with zones

Delay between motion detection and app notification							
S No.	DUT	No of trails	Minimum time(s)	Maximum time(s)	Average time(s)	Speed	Comments
1	Vendor-A doorbell	5	17	25	20	Poor	Detecting motion instantly but delay in notification. Triggering motion detection out of zone but notification sent only if there is a visual in zone. More sensitive
2	Vendor-B Doorbell	5	5	10	6	Excellent	Delay between triggers is more and less sensitive
3	Vendor-A Security Camera	5	12	19	15	Good	Similar to Vendor-A doorbell but faster notifications
4	Vendor-B Camera pro	5	3	8	5	Excellent	Delay between triggers is more and less sensitive. Bright light is detected as fire and notification sent
5	Vendor-C Camera	5	10	14	12	Good	Performed better with adding zone filters

- We have observed an improvement in Vendor-C Camera device performance after adding zones in the app. None of the APs detected the light in the in-zone as motion. But Vendor-B Camera has sent a notification considering the bright light as 'Fire'.
- Despite adding the zones, Vendor-B devices performed better than the rest with Vendor-C Camera now in the next place after improving it's performance followed by the Vendor-A devices.

Roaming:

Realtime Scenario:

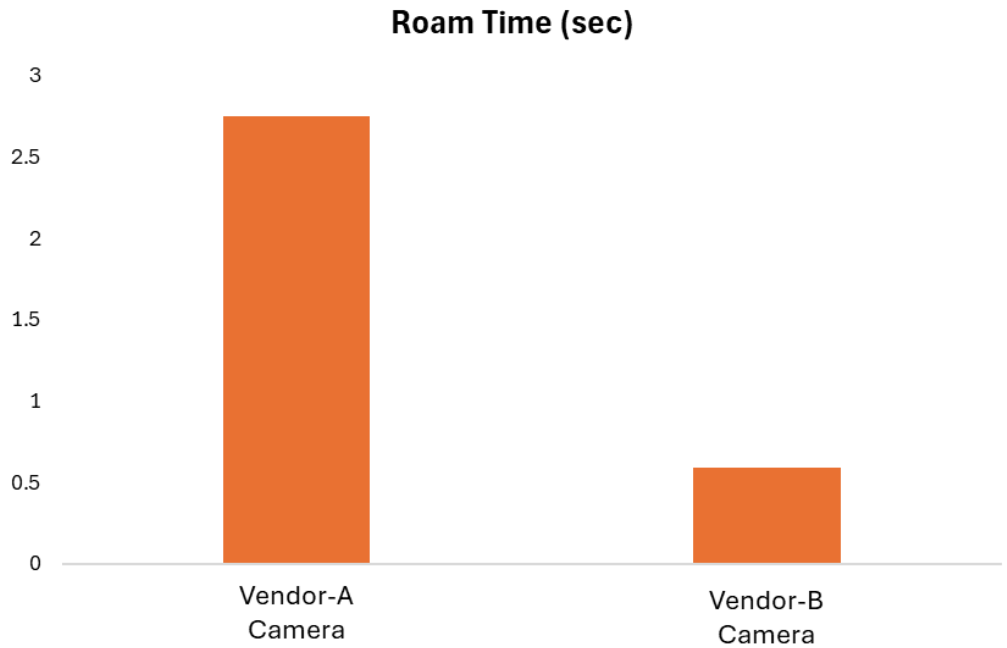
- Roaming is intended to check how seamlessly the client connects to a nearby AP when it is getting distant from the currently connected AP

Procedure:

- As Vendor-A camera is mostly intended not to be a mobile device, we checked what would happen when one AP goes into power outage and there is another nearby AP available with same configuration as the current AP

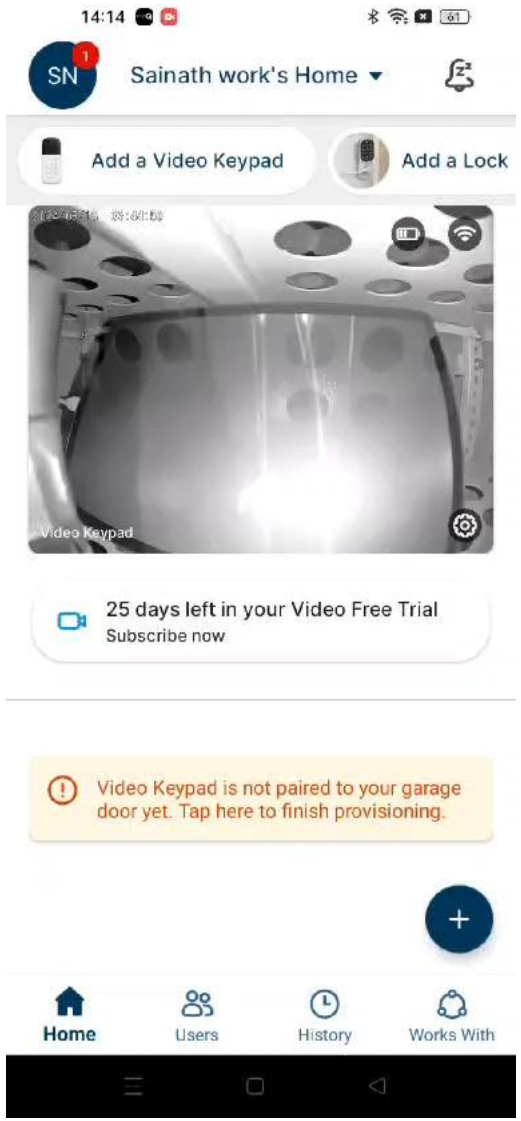
Observations:

- Roam time for vendor-A camera is comparatively higher than ring
- Vendor-A camera took 5 seconds to perform active scanning after the current AP went down, whereas the Vendor-B camera did active scanning 0.6 seconds after current AP going down
- This caused a delay in roam time for Vendor-A camera when compared to Vendor-B camera

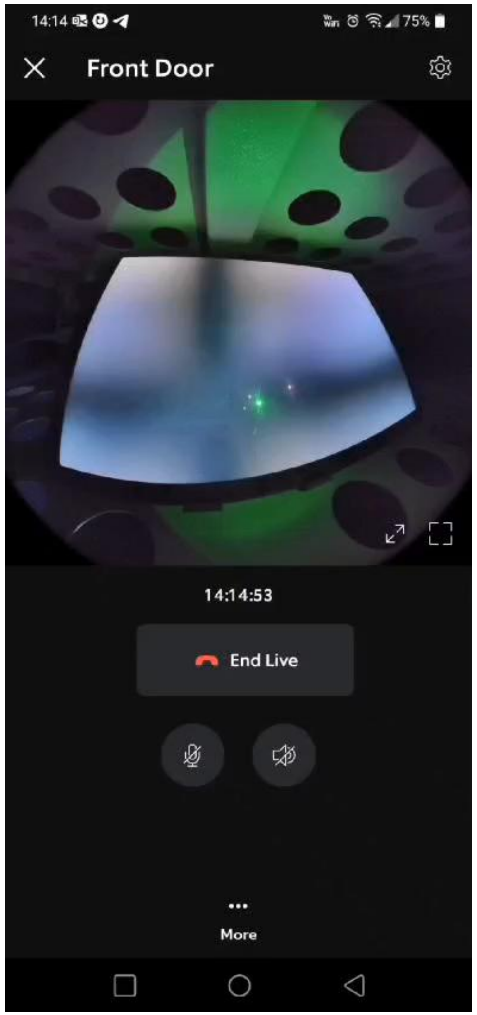


Roaming:

User experience:



Vendor-A Camera



Vendor-B Camera

Consumer Electronics

Consumer Electronics

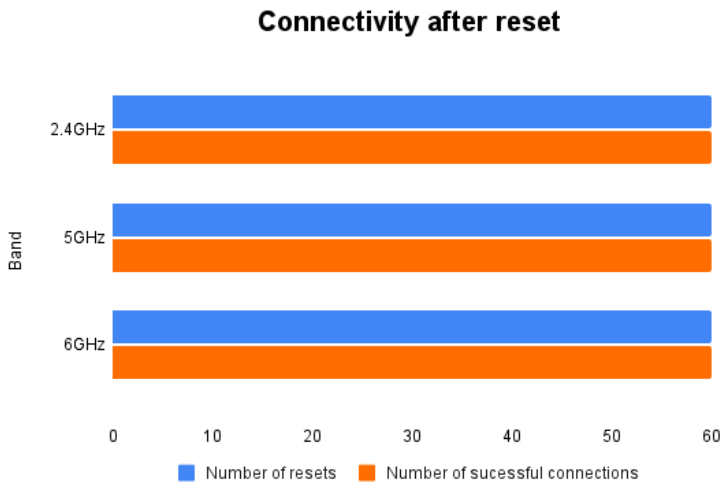
Smart TVs, Game consoles, Laptops, Smart Speakers, Smart Washing machines, Smart Refrigerators, Smart vacuum cleaners

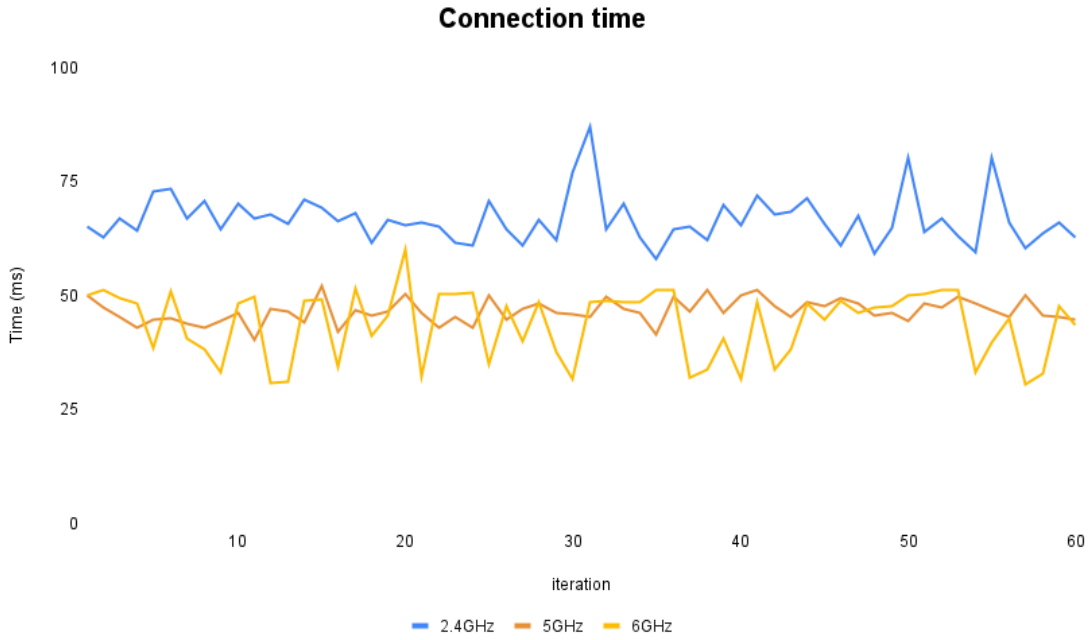
Tests:

- ✓Basic Client connectivity
- ✓Client connectivity with different security
- ✓Range Performance
- ✓Video Quality Performance
- ✓Long duration operation test
- ✓Interference test
- ✓Power consumption test
- ✓DFS Testing
- ✓Performance with WAN Impairments
- ✓Latency Test

Connectivity test

Objective: To verify the connectivity state and connection times of the device after resetting the Wi-Fi interface multiple times





Observation

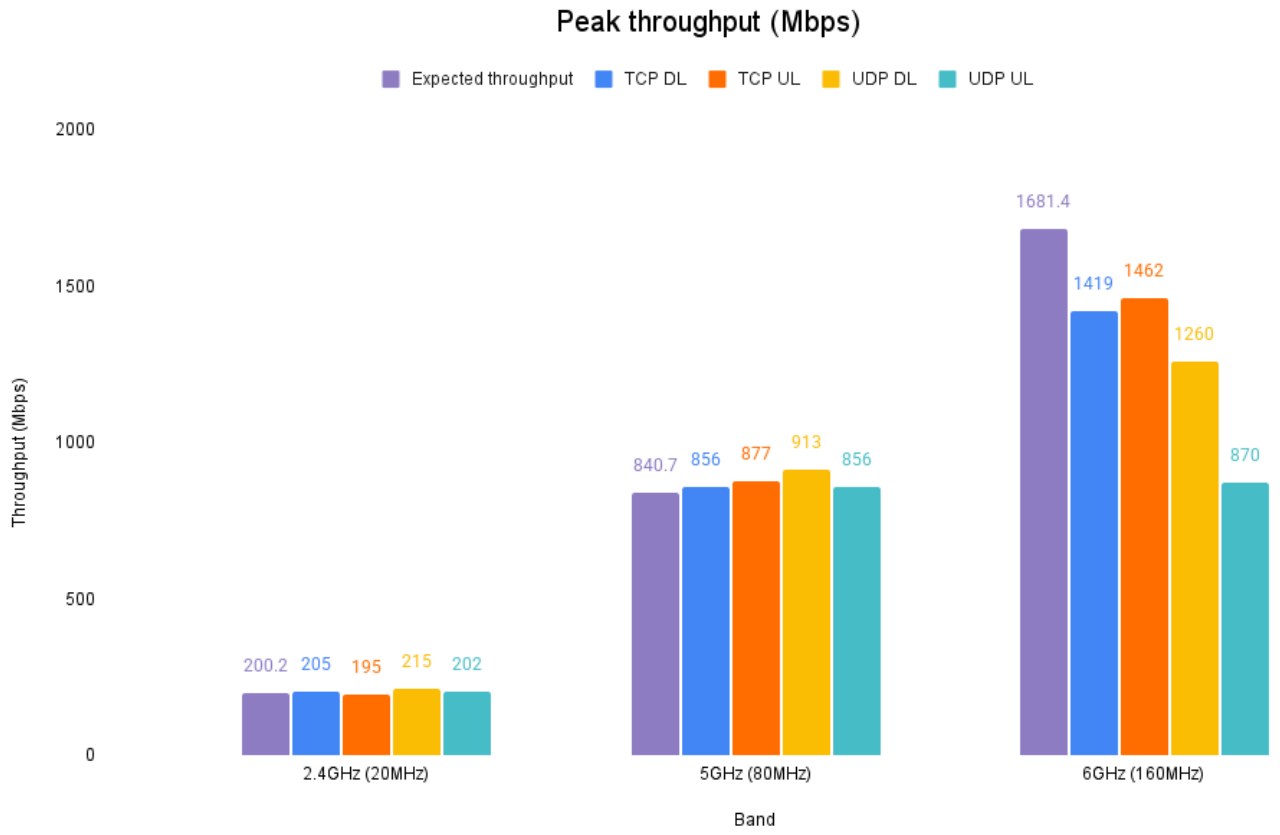
- Connected **successfully for all 60 iterations** across all bands
- Connection time on 2.4GHz is **slightly higher (around 10ms)** when compared to 5GHz and 6GHz

Note

- Connection time is measured from Probe request to EAPOL message 4

Peak performance test

Objective: To verify the maximum performance of the STA device in ideal RF conditions across multiple bands in different bandwidths

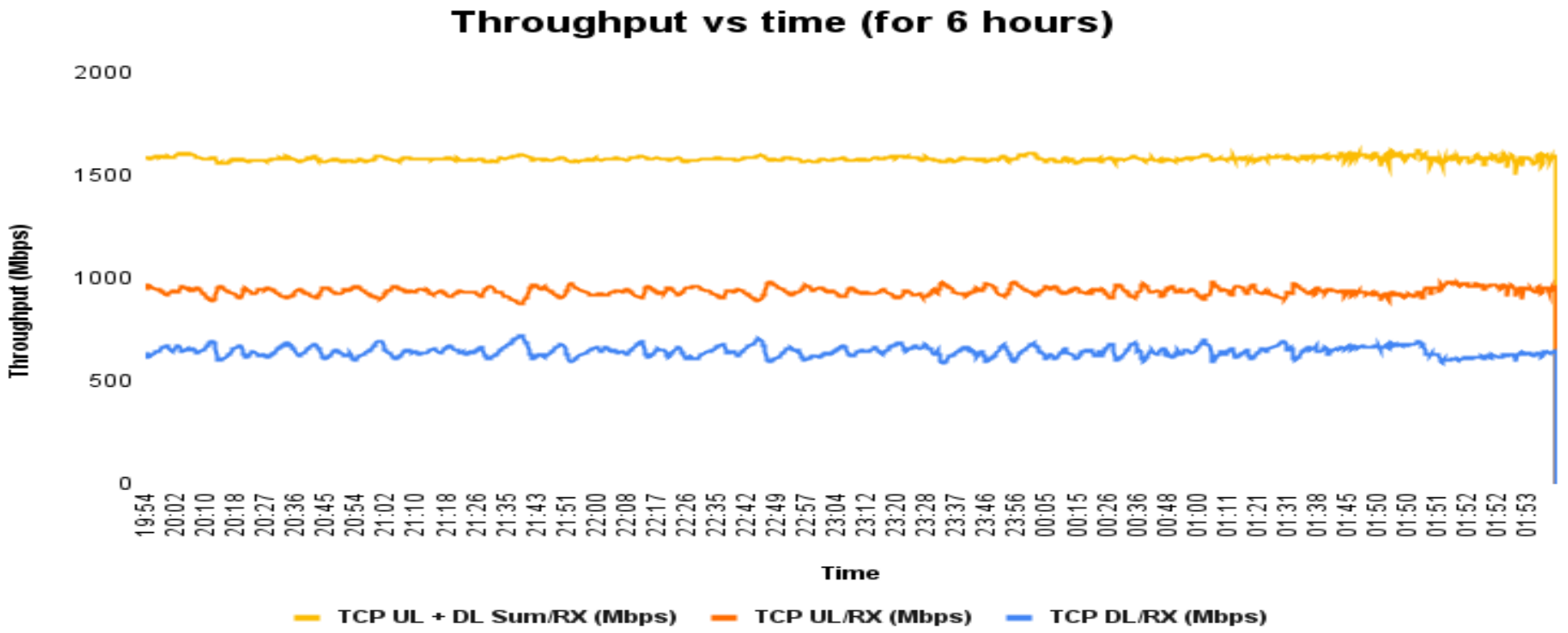


Observation

- Performance on **2.4GHz (20MHz) and 5GHz (80MHz) is good** as the device reached expected throughput value
- Achieved throughput is **less** when compared to expected throughput on **6GHz** band with 160MHz bandwidth

Stability test

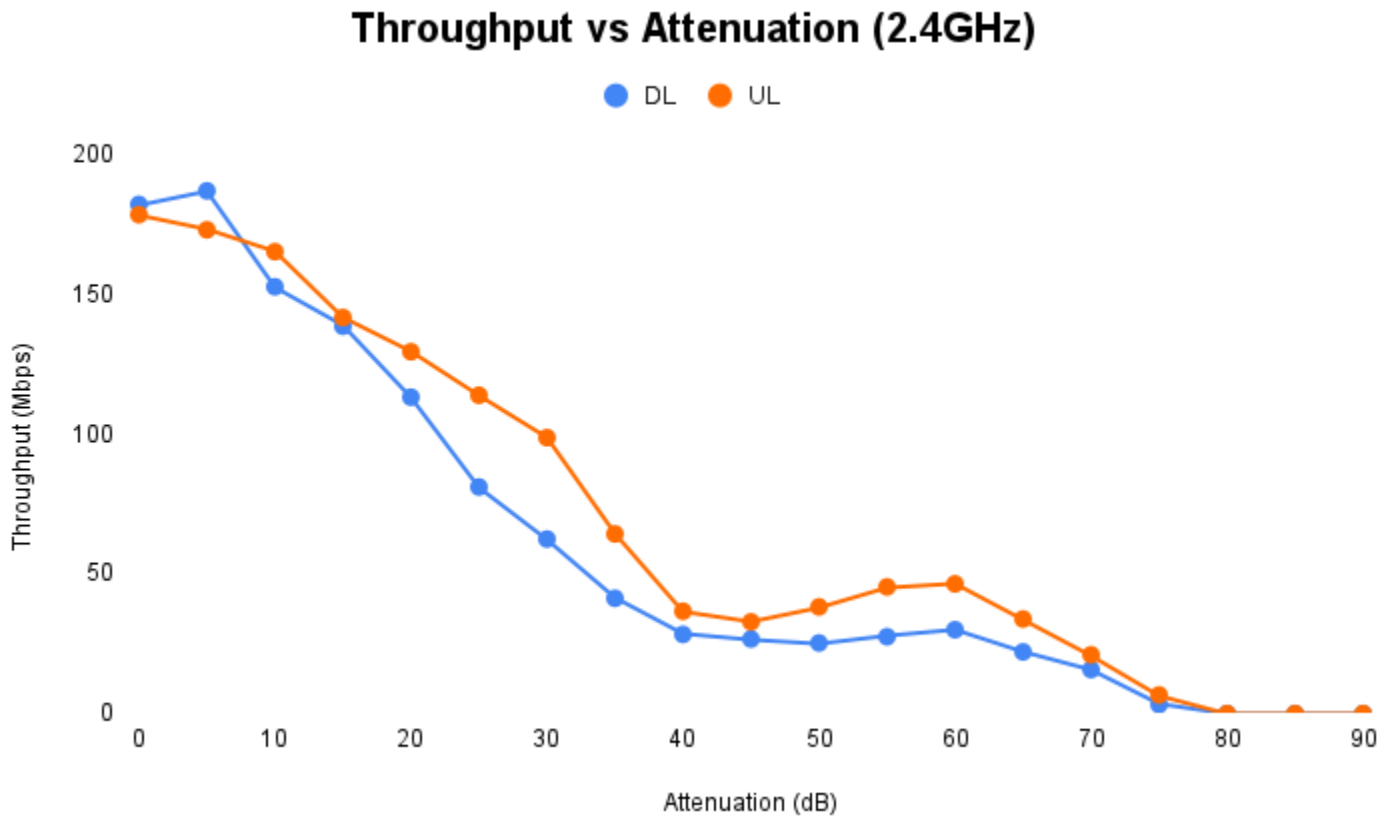
Objective: To verify the stability of the STA by running a throughput test for 6 hours and monitor for performance dips or crashes



Observation

- Device **exhibited good stability** with no performance dips or crashes

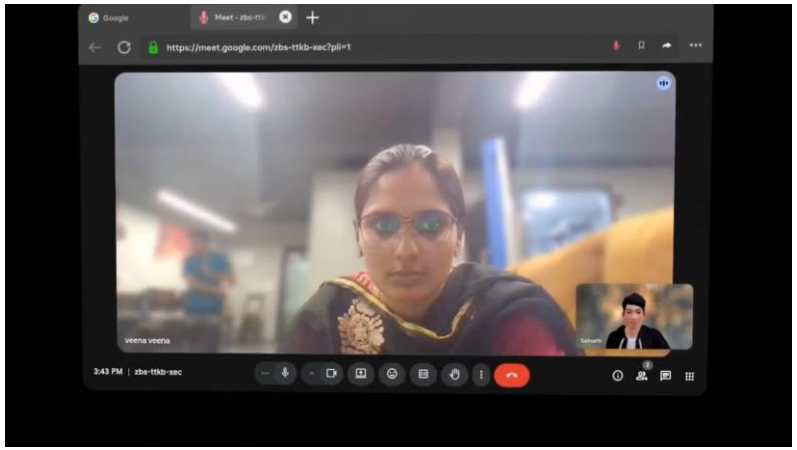
Rate vs Range test



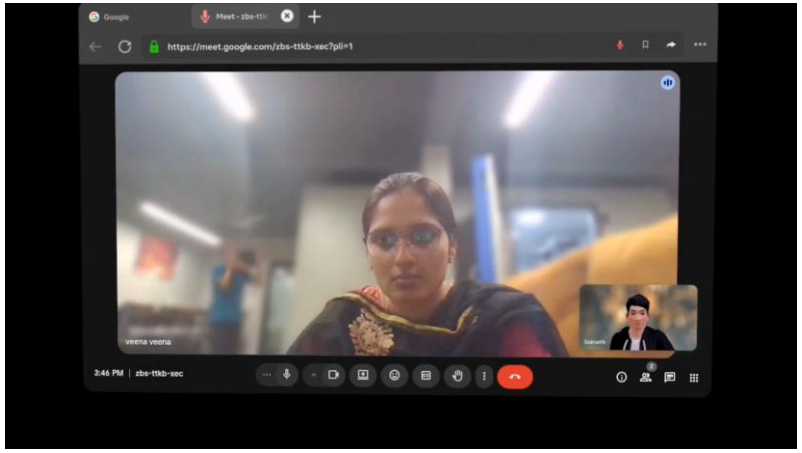
Observation

- Exhibited good range by staying connected till many attenuation levels
- At far distance **(-82dBm RSSI)**, the user experience went **bad** while having a google meet

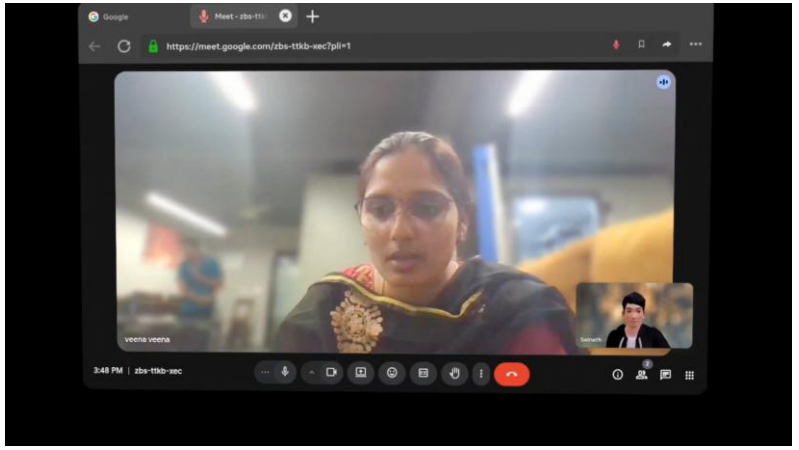
User experience – Rate vs Range



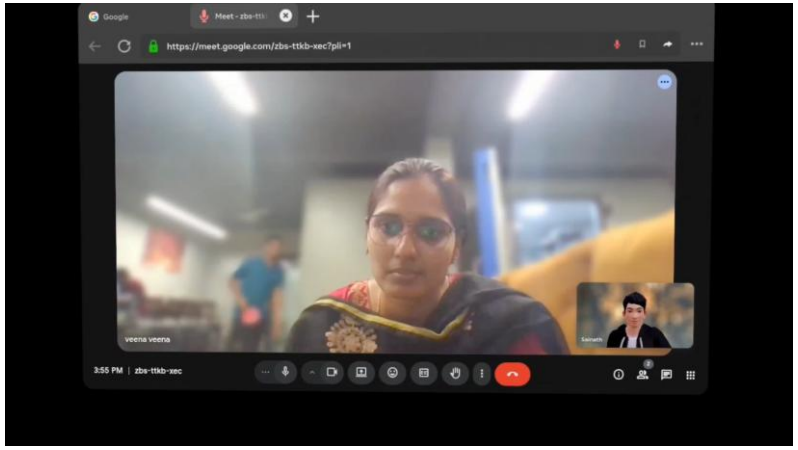
RSSI: -45dBm (excellent)



RSSI: -55dBm (excellent)



RSSI: -65dBm (good)

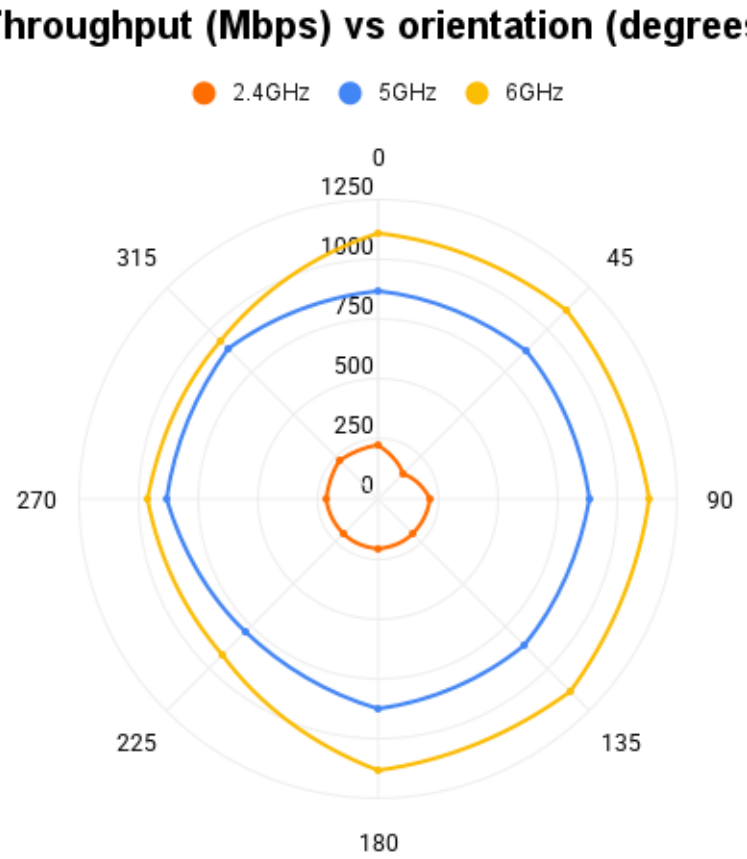


RSSI: -75dBm (average)

RSSI: -82dBm (bad)

Rate vs Orientation test

Objective: To verify the throughput behavior of the STA device at various orientations



Observation

- Slight throughput dips are seen at **45° for 2.4GHz** band and **225° for 5GHz, 6GHz** bands

User experience – Rate vs Orientation

0 degrees (excellent)

60 degrees (excellent)

120 degrees (excellent)

180 degrees (excellent)

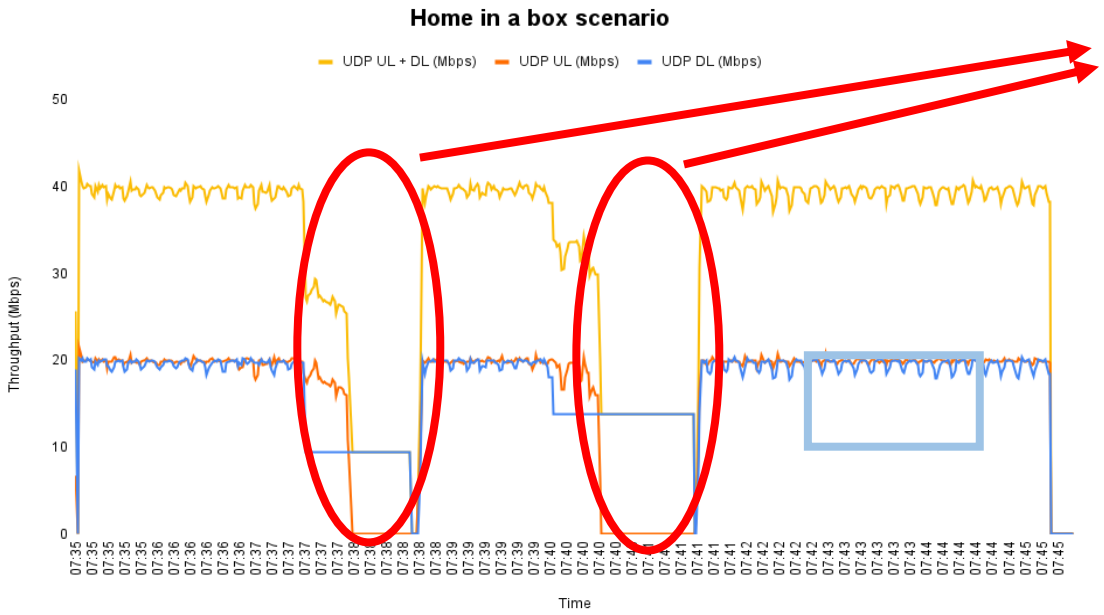
240 degrees (excellent)

300 degrees (excellent)

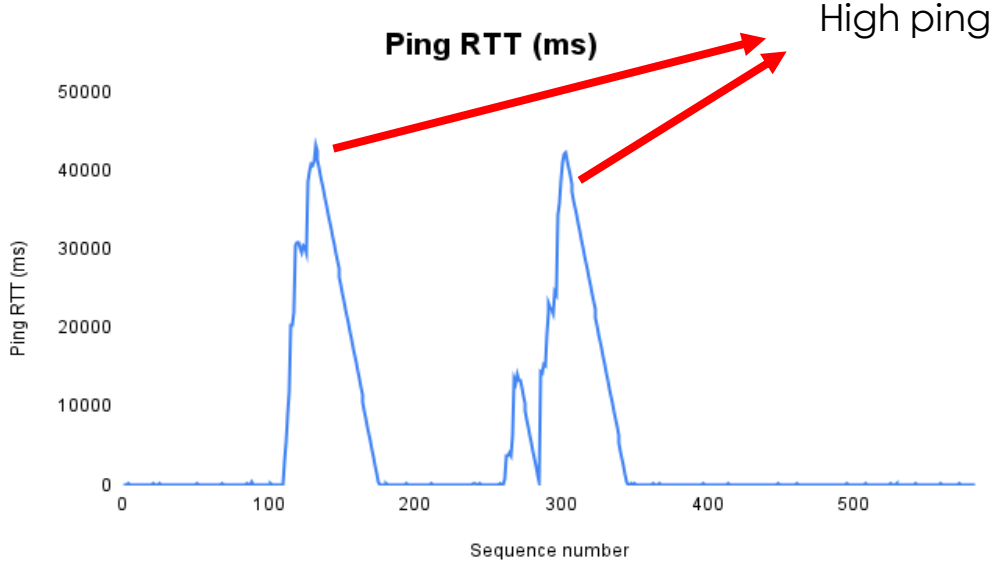
Observation

- Good user experience in all the above orientation points while watching 360° video on YouTube

Home in a Box test



Performance dropped when Home in a Box traffic profiles are active



High ping RTT

- Performance is **badly impacted** when Home in a Box traffic scenarios are active leading to dips in achieved throughput. The ping round trip time went to abnormally high values (beyond 40 seconds) when realistic home traffic profiles were running

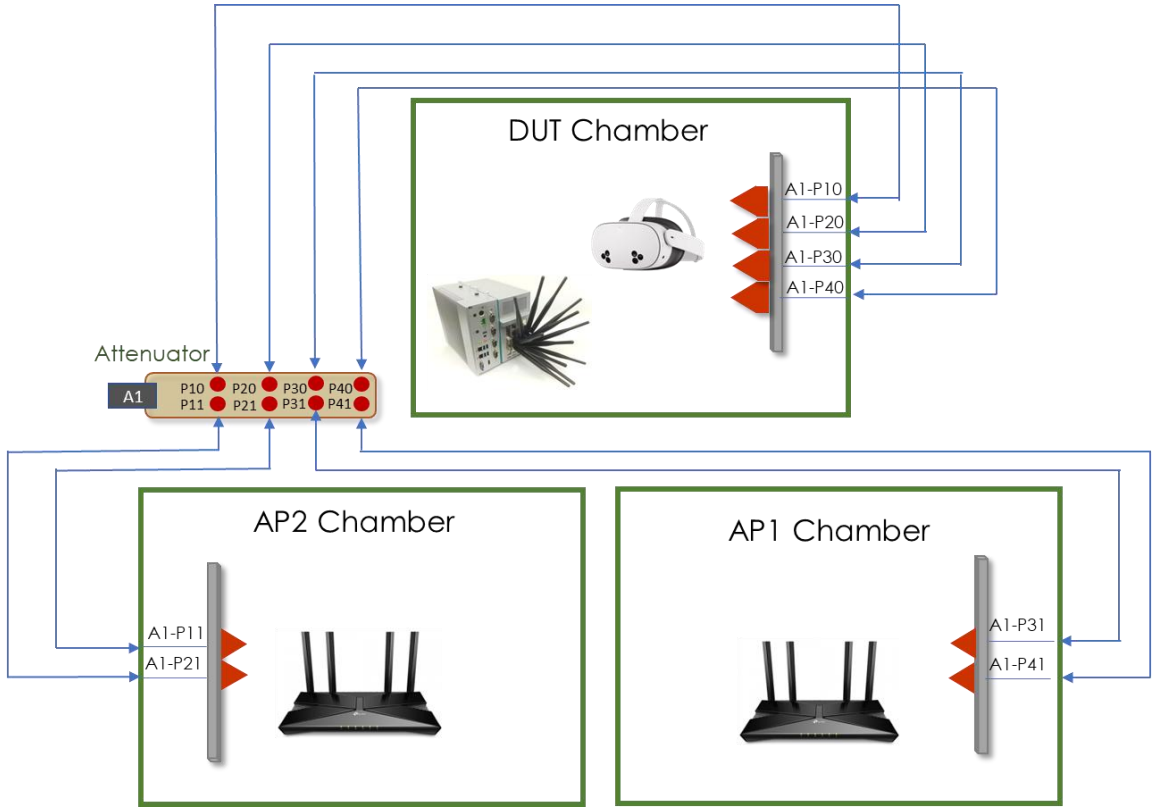
User experience – Home in a box

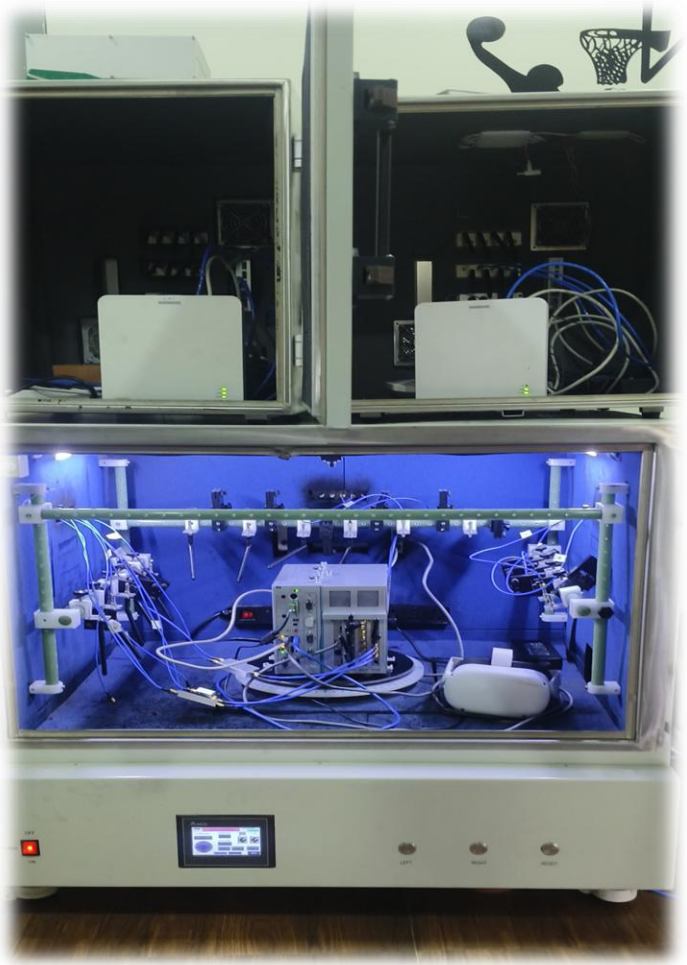
Observation

- The YouTube live video was interrupted and stopped playing when Home in a Box scenario is running leading to bad user experience

Roaming

Testbed topology:

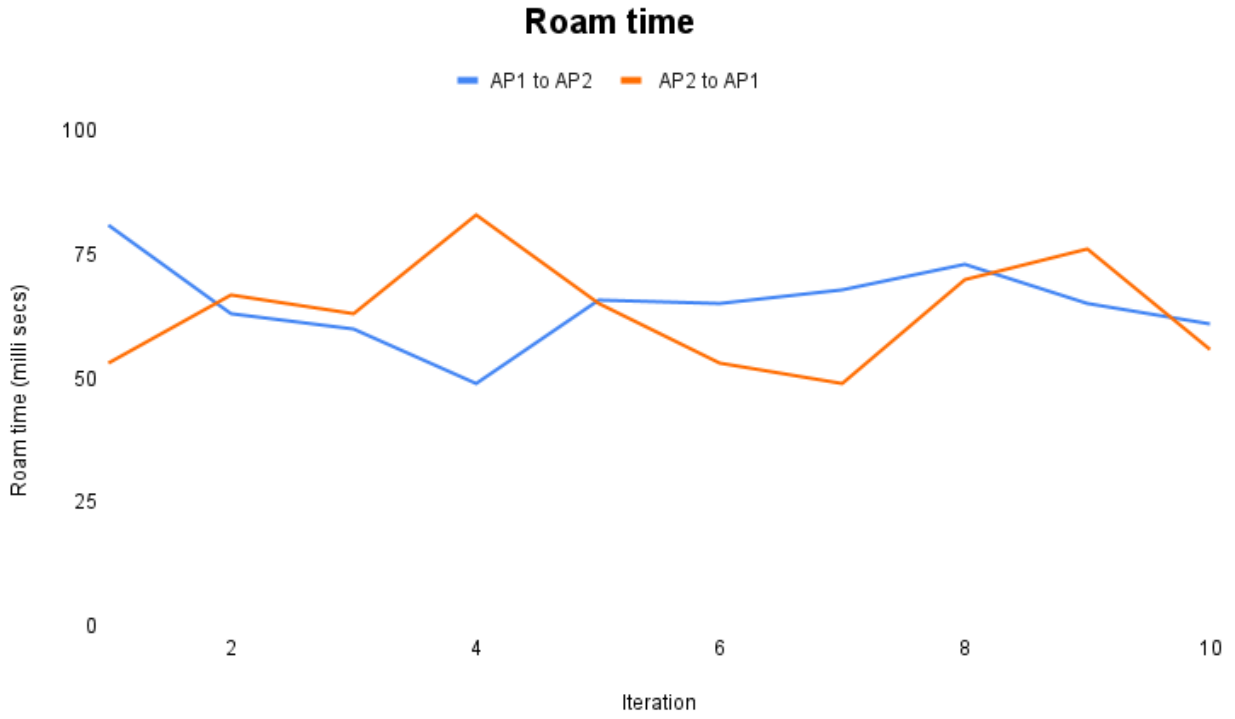




Roaming

Objective: To verify the roaming behavior of STA and analyze the roam times while roaming from AP1 to AP2 and vice-versa

Iteration	Roam Status (AP1 to AP2)	Roam Status (AP2 to AP1)
1	Success	Success
2	Success	Success
3	Success	Success
4	Success	Success
5	Success	Success
6	Success	Success
7	Success	Success
8	Success	Success
9	Success	Success
10	Success	Success



Observation

- Roaming is **successful** for every iteration and roam times are within 100ms

Peripheral & Office Equipment

Healthcare Devices

Smart Printers, Smart Scanners, Smart Projectors, Tablets, Conference accessories (speaker, projector)

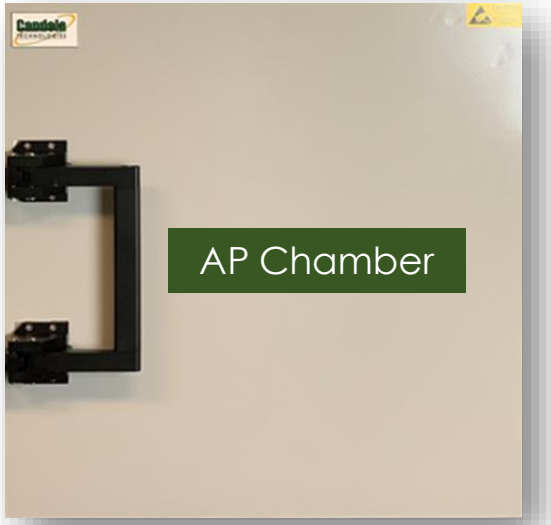
Tests:

- ✓ Basic Client connectivity
- ✓ Range Performance
- ✓ Long duration operation test
- ✓ Latency test
- ✓ Video Quality Tests
- ✓ ACI/CCI Test
- ✓ Interference test
- ✓ DFS Testing
- ✓ Performance with WAN Impairments

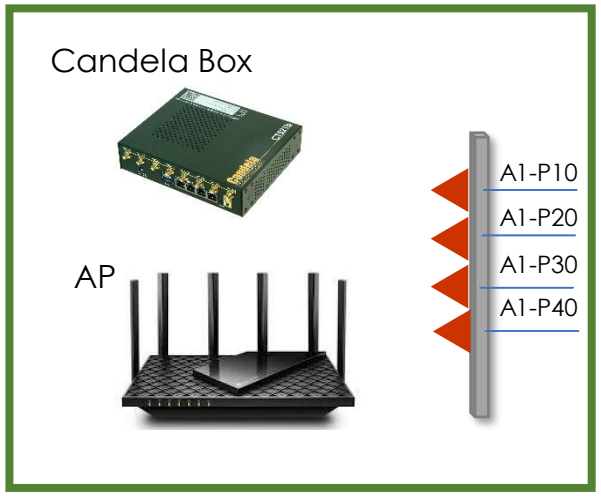
DUT: Smart Printer

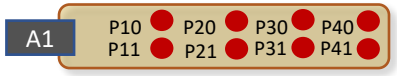
Parameter	Smart Printer	AP1	AP2	AP3
Model Name	-	ASUS ROG AX6000	NETGEAR INSIGHT	ADTRAN SDG8733
Wi-Fi Support	802.11 b/g/n	802.11ax	802.11ax	802.11be
Frequency Band	Only 2.4GHz	2.4GHz & 5GHz	2.4GHz, 5GHz & 6GHz	2.4GHz, 5GHz & 6GHz
NSS	1x1	4X4	4x4	4x4
Bandwidth Support	20MHz	160MHz	160MHz	320MHz
Vendor	Broadcom	Broadcom	Qualcomm	Mediatek

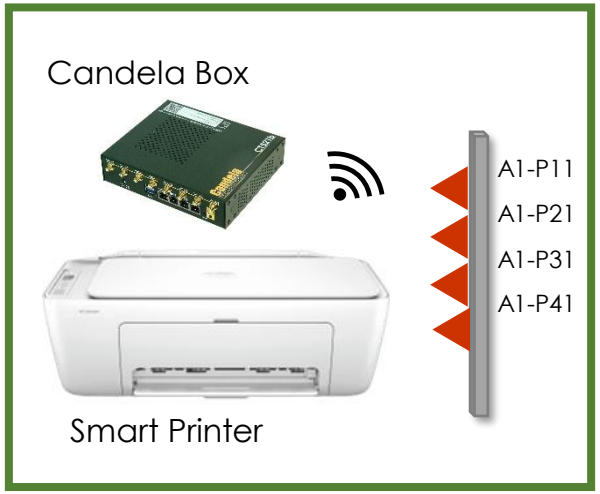
Testbed Topology



Programmable Attenuator







Printer Performance across different chipsets

Comparison of Printer Performance with various chipsets				
Testcase		**AP1 [Broadcom]**	**AP2 [Qualcomm]**	**AP3 [Mediatek]**
Client Connectivity	Open	648ms	806ms	626ms
	WPA/WPA2 Personal	663ms	899ms	729ms
	WPA2 Personal	824ms	884ms	790ms
	WPA3 Personal	1477ms	1467ms	1470ms
Performance w.r.t Range [Print command execution time]	Near	6.5s	8s	8s
	Far	15s	25s	12s
Performance w.r.t Congestion [Print command execution time]	Low	7s	8s	11s
	High	39s	43s	39s

- For the client connection test, the overall connection times were observed to be higher, as mentioned in the previous slide. Among the three APs, connection times were consistently higher with the Qualcomm (AP2) and Mediatek (AP3) APs compared to Broadcom (AP1).
- With Qualcomm (AP2), both the connection times and command execution durations were noticeably higher than with the other two chipsets.
- The printer exhibited better performance with Mediatek (AP3) under far-distance conditions, whereas Broadcom (AP1) showed optimal behavior at near distances.

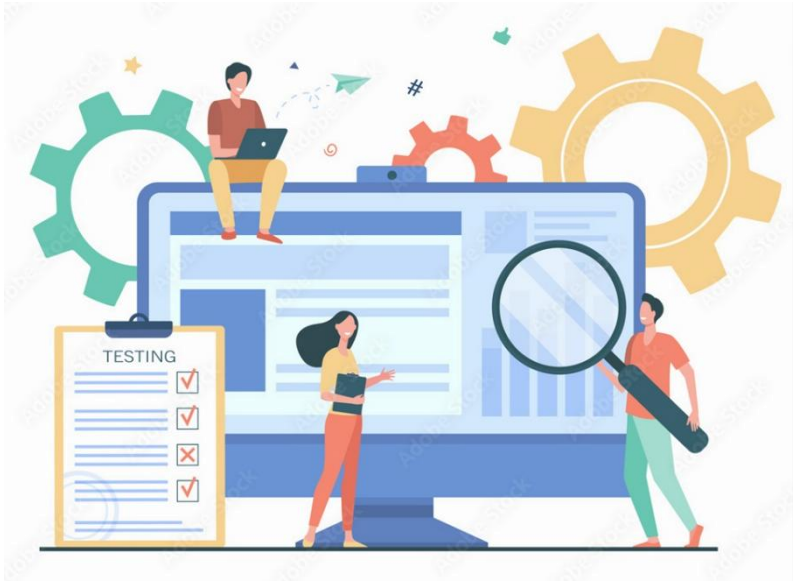
Client Connectivity

- The objective of this testcase is to verify if the smart printer can connect to any Wi-Fi network with different securities and measure the connection times.
- We verified client connectivity across different security modes - **Open, WPA/WPA2, WPA2 & WPA3** and recorded the connection times.
- Under ideal conditions, a connection time of less than 300 ms is generally considered a good result.
- We observed **quite higher connection times** across various security modes in ideal environment (no traffic/load). Below are the results with **AP1 [Broadcom]:**

S No.	Security Type	Connection Status	Connection time(ms) with AP1 [Broadcom]
1	Open	Associated with the AP and obtained IP address	648
2	WPA/WPA2 Personal	Associated with the AP and obtained IP address	663
3	WPA2 Personal	Associated with the AP and obtained IP address	824
4	WPA3 Personal	Associated with the AP and obtained IP address	1477

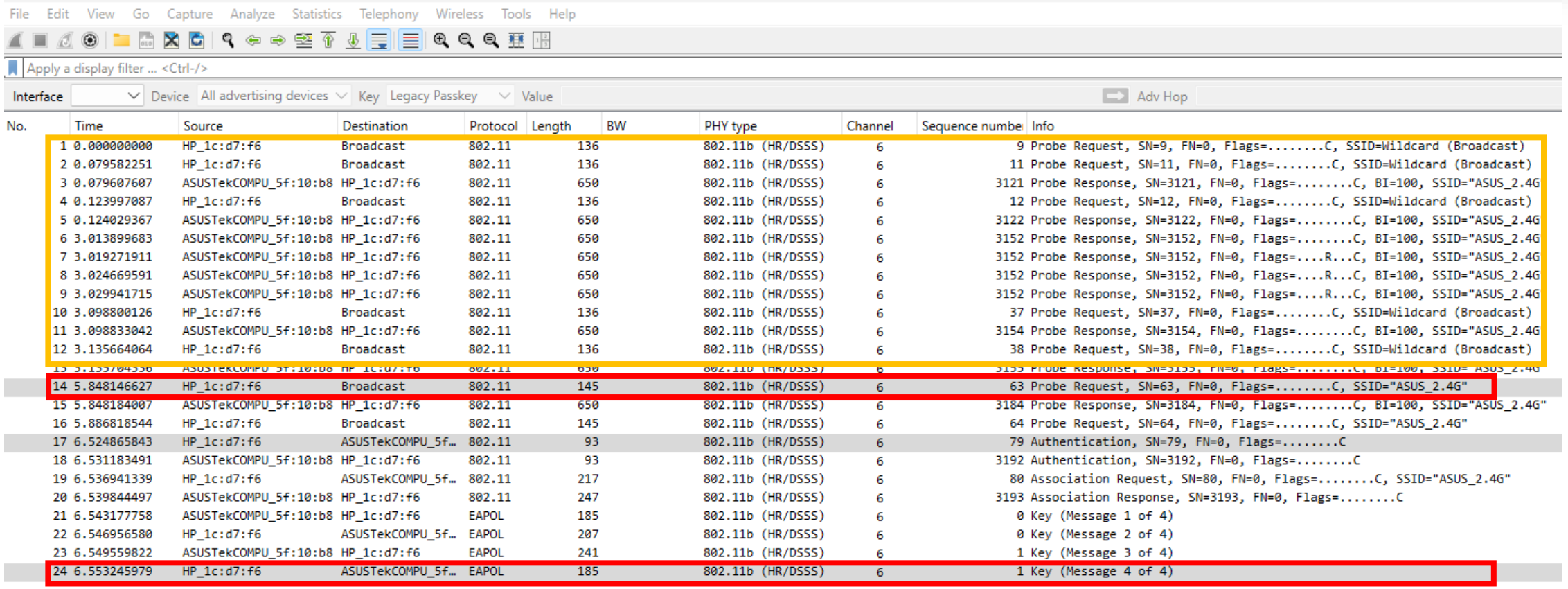
Client Connectivity – Higher connection times debug

S No.	Connection Process with AP1[Broadcom]	Time taken by Printer (ms)	Time taken by Candela client(ms)
1	Overall client connectivity	**705ms**	**119ms**
2	Probe request → Auth request	**676ms**	**44ms**
3	Auth request → EAPOL Message 4	29ms	76ms



- For the total 705ms client connectivity time, the time taken from probe request to authentication frame was observed to be around **676ms**.
- While the authentication request → EAPOL message 4 is completed within **29ms**.
- The Printer is taking some time to process the Probe Response frame and then send the Authentication request frame.
- This behavior is observed multiple times and with different APs.

Client Connectivity – Higher connection times debug



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Interface Device All advertising devices Key Legacy Passkey Value Adv Hop

No.	Time	Source	Destination	Protocol	Length	BW	PHY type	Channel	Sequence numbe	Info
1	0.000000000	HP_1c:d7:f6	Broadcast	802.11	136		802.11b (HR/DSSS)	6	9	Probe Request, SN=9, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
2	0.079582251	HP_1c:d7:f6	Broadcast	802.11	136		802.11b (HR/DSSS)	6	11	Probe Request, SN=11, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
3	0.079607607	ASUSTekCOMPU_5f:10:b8	HP_1c:d7:f6	802.11	650		802.11b (HR/DSSS)	6	3121	Probe Response, SN=3121, FN=0, Flags=........C, BI=100, SSID="ASUS_2.4G
4	0.123997087	HP_1c:d7:f6	Broadcast	802.11	136		802.11b (HR/DSSS)	6	12	Probe Request, SN=12, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
5	0.124029367	ASUSTekCOMPU_5f:10:b8	HP_1c:d7:f6	802.11	650		802.11b (HR/DSSS)	6	3122	Probe Response, SN=3122, FN=0, Flags=........C, BI=100, SSID="ASUS_2.4G
6	3.013899683	ASUSTekCOMPU_5f:10:b8	HP_1c:d7:f6	802.11	650		802.11b (HR/DSSS)	6	3152	Probe Response, SN=3152, FN=0, Flags=........C, BI=100, SSID="ASUS_2.4G
7	3.019271911	ASUSTekCOMPU_5f:10:b8	HP_1c:d7:f6	802.11	650		802.11b (HR/DSSS)	6	3152	Probe Response, SN=3152, FN=0, Flags=....R...C, BI=100, SSID="ASUS_2.4G
8	3.024669591	ASUSTekCOMPU_5f:10:b8	HP_1c:d7:f6	802.11	650		802.11b (HR/DSSS)	6	3152	Probe Response, SN=3152, FN=0, Flags=....R...C, BI=100, SSID="ASUS_2.4G
9	3.029941715	ASUSTekCOMPU_5f:10:b8	HP_1c:d7:f6	802.11	650		802.11b (HR/DSSS)	6	3152	Probe Response, SN=3152, FN=0, Flags=....R...C, BI=100, SSID="ASUS_2.4G
10	3.098800126	HP_1c:d7:f6	Broadcast	802.11	136		802.11b (HR/DSSS)	6	37	Probe Request, SN=37, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
11	3.098833042	ASUSTekCOMPU_5f:10:b8	HP_1c:d7:f6	802.11	650		802.11b (HR/DSSS)	6	3154	Probe Response, SN=3154, FN=0, Flags=........C, BI=100, SSID="ASUS_2.4G
12	3.135664064	HP_1c:d7:f6	Broadcast	802.11	136		802.11b (HR/DSSS)	6	38	Probe Request, SN=38, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
13	3.135704536	ASUSTekCOMPU_5f:10:b8	HP_1c:d7:f6	802.11	650		802.11b (HR/DSSS)	6	3153	Probe Response, SN=3153, FN=0, Flags=........C, BI=100, SSID="ASUS_2.4G
14	5.848146627	HP_1c:d7:f6	Broadcast	802.11	145		802.11b (HR/DSSS)	6	63	Probe Request, SN=63, FN=0, Flags=........C, SSID="ASUS_2.4G"
15	5.848184007	ASUSTekCOMPU_5f:10:b8	HP_1c:d7:f6	802.11	650		802.11b (HR/DSSS)	6	3184	Probe Response, SN=3184, FN=0, Flags=........C, BI=100, SSID="ASUS_2.4G"
16	5.886818544	HP_1c:d7:f6	Broadcast	802.11	145		802.11b (HR/DSSS)	6	64	Probe Request, SN=64, FN=0, Flags=........C, SSID="ASUS_2.4G"
17	6.524865843	HP_1c:d7:f6	ASUSTekCOMPU_5f…	802.11	93		802.11b (HR/DSSS)	6	79	Authentication, SN=79, FN=0, Flags=........C
18	6.531183491	ASUSTekCOMPU_5f:10:b8	HP_1c:d7:f6	802.11	93		802.11b (HR/DSSS)	6	3192	Authentication, SN=3192, FN=0, Flags=........C
19	6.536941339	HP_1c:d7:f6	ASUSTekCOMPU_5f…	802.11	217		802.11b (HR/DSSS)	6	80	Association Request, SN=80, FN=0, Flags=........C, SSID="ASUS_2.4G"
20	6.539844497	ASUSTekCOMPU_5f:10:b8	HP_1c:d7:f6	802.11	247		802.11b (HR/DSSS)	6	3193	Association Response, SN=3193, FN=0, Flags=........C
21	6.543177758	ASUSTekCOMPU_5f:10:b8	HP_1c:d7:f6	EAPOL	185		802.11b (HR/DSSS)	6	0	Key (Message 1 of 4)
22	6.546956580	HP_1c:d7:f6	ASUSTekCOMPU_5f…	EAPOL	207		802.11b (HR/DSSS)	6	0	Key (Message 2 of 4)
23	6.549559822	ASUSTekCOMPU_5f:10:b8	HP_1c:d7:f6	EAPOL	241		802.11b (HR/DSSS)	6	1	Key (Message 3 of 4)
24	6.553245979	HP_1c:d7:f6	ASUSTekCOMPU_5f…	EAPOL	185		802.11b (HR/DSSS)	6	1	Key (Message 4 of 4)

- To further debug the high connection times, we analyzed the packet capture and observed that the client continued to send probe request frames even after receiving a probe response from the AP.
- As shown in the above snapshot, client connectivity time recorded with **AP1 [Broadcom]** in one iteration is **705ms**.

Client Connectivity under congestion

- The objective of this testcase is to verify if the smart printer can connect to an AP under congestion with different securities and measure the connection times. Below are the test results with AP1 [Broadcom].

S No.	Security	Channel Utilization	Connection Status	Connection time(ms) with AP1 [Broadcom]
1	Open	10%	Associated and obtained IP address	649
2		50%	Associated and obtained IP address	656
3		>90%	Associated and obtained IP address	675

S No.	Security	Channel Utilization	Connection Status	Connection time(ms) with AP1 [Broadcom]
1	WPA/ WPA2	10%	Associated and obtained IP address	671
2		50%	Associated and obtained IP address	679
3		>90%	Associated and obtained IP address	742

S No.	Security	Channel Utilization	Connection Status	Connection time(ms) with AP1 [Broadcom]
1	WPA2	10%	Associated and obtained IP address	705
2		50%	Associated and obtained IP address	711
3		>90%	Associated and obtained IP address	1076

S No.	Security	Channel Utilization	Connection Status	Connection time(ms) with AP1 [Broadcom]
1	WPA3	10%	Associated and obtained IP address	1548
2		50%	Associated and obtained IP address	1564
3		>90%	Associated and obtained IP address	1710

- In all the scenarios, the connection time is above 600ms and it was more than 1second for WPA3 security mode which is quite high.

Sample Test Results

- We verified print actions and print quality in two different conditions:
  1. Under various congestion levels: Low, High congestions
  2. At various distances: Near, Far

S No.	Parameter	Test Results with AP1 [Broadcom]		Test Results with AP2 [Qualcomm]		Test Results with AP3 [Mediatek]	
		Without congestion	With congestion	Without congestion	With congestion	Without congestion	With congestion
1	Channel Utilisation	7-10%	96%	15%	95%	10%	94%
2	Photo size	1.7MB	1.7MB	1.7MB	1.7MB	1.7MB	1.7MB
3	Print Type	Black & White	Black & White	Black & White	Black & White	Black & White	Black & White
4	Print command execution time	7s	39s	8s	43s	11s	39s

- Print command execution time is the time from tap 'print' to printer starting to pull paper.
- In the first subtest, initially the printer was connected to the wi-fi network and then congestion was then introduced by running TCP traffic from an additional client(candela station) traffic in the same environment.
- The printer performed well with both APs under ideal conditions (no congestion). However, when there is high congestion, command execution latency was significantly higher with AP1 compared to AP2.

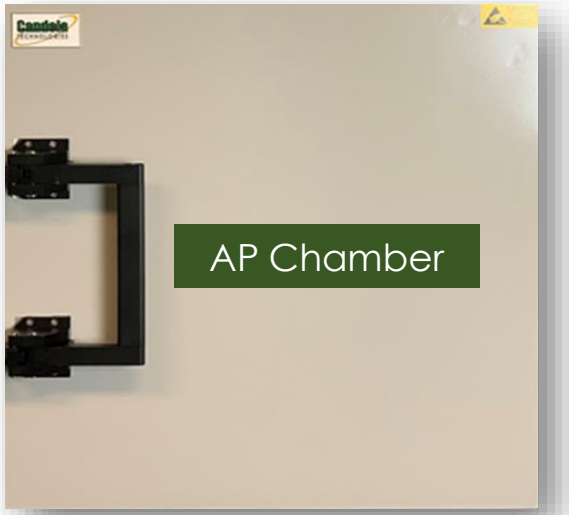
Sample Test Results

Performance at Near and Far distances:

S No.	Parameter	Test Results with AP1 [Broadcom]		Test Results with AP2 [Qualcomm]		Test Results with AP3 [Mediatek]	
		At Near distance	At Far distance	At Near distance	At Far distance	At Near distance	At Far distance
1	Channel Utilisation	7-10%	96%	15%	95%	10%	94%
2	Photo size	1.7MB	1.7MB	1.7MB	1.7MB	1.7MB	1.7MB
3	Print Type	Black & White	Black & White	Black & White	Black & White	Black & White	Black & White
4	Print command execution time	6.5s	15s	8s	25s	8s	12s

- For this test, the distance is emulated using programmable attenuator and the performance is evaluated at near and far distances with all three APs.
- At Near distance, the command execution took almost same time with all APs with just 1.5s variation between AP1 and AP2, AP3.
- However, at far distance, the execution time increased to 15 seconds with AP1, 25 seconds with AP2 and 12s with AP3. AP2 [Qualcomm] exhibited quite higher responsive times at far distance.

Test Setup



Programmable Attenuator

AP Chamber

STB Chamber

Test Results Summary

S. No.	Testcase	VENDOR-A Model 1 STB	VENDOR-A Model 2 STB	VENDOR-B STB	Observations
1	Basic Client Connectivity	GOOD	GOOD	GOOD	• We verified basic connectivity of Vendor-A TV boxes with different securities, and both connected to Wi-Fi successfully. • We observed that the 2.4 GHz SSIDs were not displayed in the Wi-Fi network list. However, when the 2.4 GHz SSID and password were entered manually, both STBs connected to the 2.4 GHz network successfully.
2	Peak Throughput	POOR	POOR	GOOD	• We observed that Vendor-A Model 1 STB achieved more throughput compared to Model 2 while running TCP Downlink scenario. • We observed that both STBs rebooted when the intended UDP downlink load was increased to more than 600 Mbps.
3	Rate vs Range Test	GOOD	EXCELLENT	GOOD	• The Model 1 STB got disconnected to the AP around –84 dBm while the Model 2 STB got disconnected to the AP around –94 dBm.
4	YouTube Video Streaming Performance over Distance	GOOD	EXCELLENT	GOOD	• The Vendor-A Model 2 maintained highest quality over a long range with stable buffer, while the Vendor-A Model 1 showed quality drop from 2160p to 1080p at 15 dB attenuation. No video buffering was observed with both DUTs.
5	YouTube Live Streaming Performance over Distance	GOOD	EXCELLENT	GOOD	• The Vendor-A Model 2 maintained highest quality live streaming over a long range, while the Vendor-A Model 1 showed quality drop from 2160p to 1080p at 15 dB attenuation.

Note: The Score included in this presentation is based on the testing experience and is not industry standard rating.

Test Results Summary

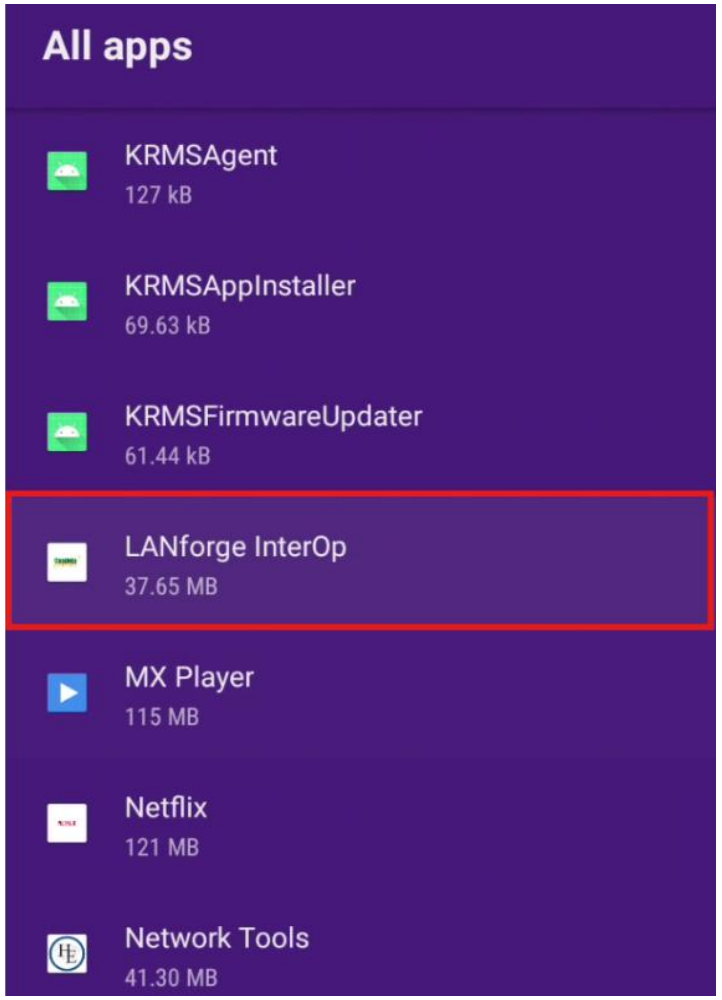
S No.	Testcase	Vendor-A Model 1 STB	Vendor-A Model 2 STB	VENDOR-B STB	Observations
6	YouTube Live Streaming Under congestion with Multiple Clients (Near, Medium, Far Distance)	GOOD	GOOD	GOOD	• Both the TV boxes maintained stable buffer health across Near, Medium & Far distances. • No frame drops or buffering were observed in both TV boxes at any distance during streaming.
7	YouTube Video Streaming Under congestion with Multiple Clients (Near, Medium, Far Distances)	GOOD	EXCELLENT	GOOD	• Both the TV boxes maintained stable buffer health across Near, Medium and Far Distances. However, a quality drop was observed in Vendor-A Model 1 STB from 4K to 2K at medium distance, while the Vendor-A Model 2 STB maintained highest quality across all distances. • No frame drops or buffering were observed in both TV boxes at any distance during streaming.
8	Multicast Traffic Performance (1hr run)	GOOD	GOOD	GOOD	• PLAY Vendor-A Model 1 STB achieved a Multicast Throughput of 23.7 Mbps and 4B achieved 24.1Mbps with given multicast traffic of 25Mbps.
9	Multicast Traffic Performance (8hrs run)	GOOD	GOOD	FAIR	• Both the TV boxes achieved a Multicast Throughput of around 24 Mbps with given multicast traffic of 25Mbps.

Note: The Score included in this presentation is based on the testing experience and is not industry standard rating.

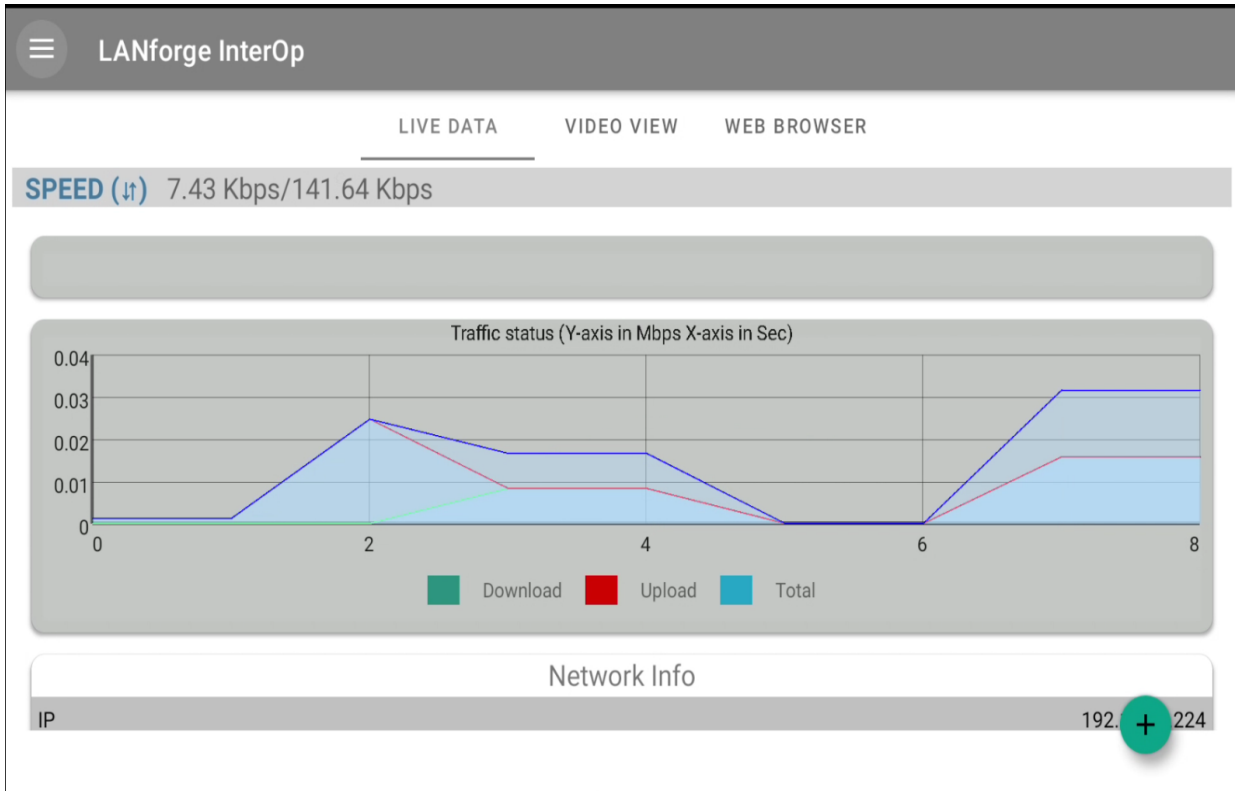
LANforge InterOp

- As the Vendor-A STB uses Android OS, we enabled Developer options and USB debugging, and installed our endpoint software, "**LANforge InterOp**" APK, on the STB for testing.

App List in Vendor-A STB



LANforge InterOp UI in Vendor-A STB



Basic Client Connectivity

Test Objective

- The objective of this test is to verify if the Vendor-A STB can connect to any Wi-Fi network with different securities and measure the connection times.

Observations:

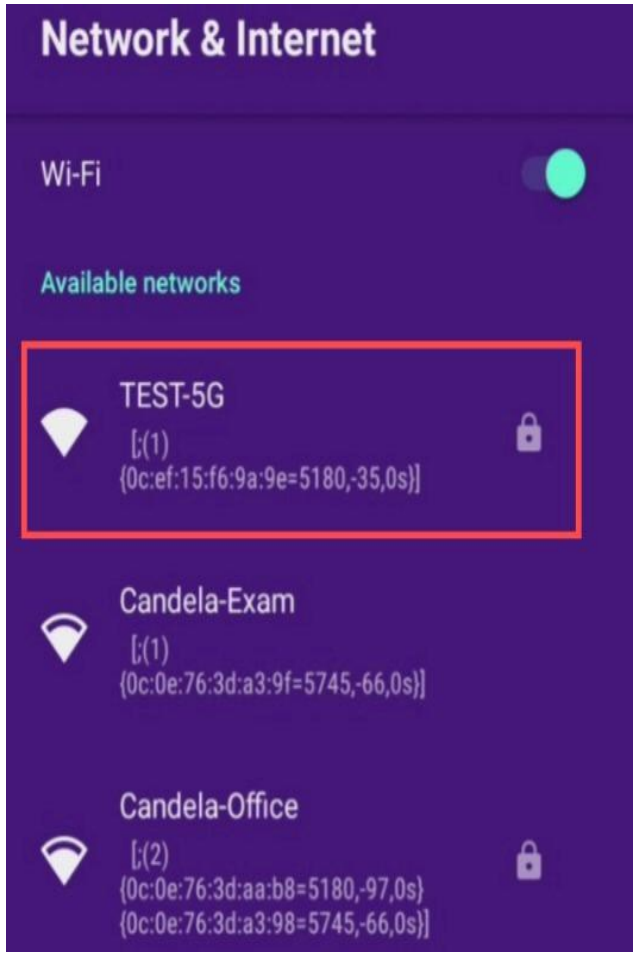
- We observed that both TV boxes (Box 4A & Box 4B) were able to connect to the AP **successfully** with Open, WPA, WPA2, and WPA3 security configurations.
- During the Wi-Fi scan **only 5GHz SSID's were listed** in the Available Networks.
- 2.4GHz SSID's were not listed in the Available Wi-Fi networks.
- But, when the 2.4GHz network details (SSID and Password) were entered manually, the TV Box got connected to the 2.4GHz SSID.
- We verified this behavior with another vendor Set-Top Box, and we could see both 2.4GHz and 5GHz Network SSID's listed in the Wi-Fi scan without any manual entry.

Basic Client Connectivity

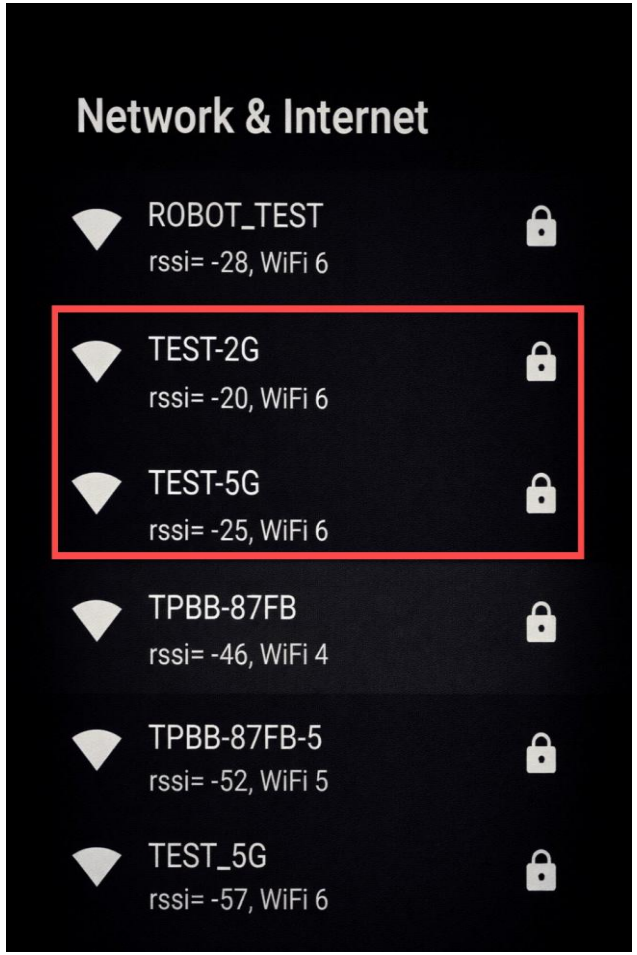
Set-Top Box Wi-Fi Network List Snapshots:

- As shown in the images below, both 2.4 GHz and 5 GHz SSIDs are displayed in the Wi-Fi scan on the vendor-B STB, whereas only 5 GHz SSIDs are displayed on the Vendor-A STB.

Vendor-A STB



Vendor-B STB



Peak Throughput Test

Test Objective:

- The objective of this test is to verify the Peak Throughput of the TV BOX.
- This test measures the throughput performance that include TCP & UDP traffic in download directions for both 2.4GHz and 5GHz.
- Below are the TCP Download test results:

Peak Throughput Performance in 5GHz: 80 MHz Bandwidth						
TV Box Model	AP Configuration	Traffic Type	PHY Rate (Mbps)	Intended Load (Mbps)	Achieved Throughput (Mbps)	Percentage Achieved (%)
Vendor-A Model 1 STB	802.11ax 80MHz 2x2	TCP-DL	1201	1000	767	76.76
Vendor-A Model 2 STB	802.11ax 80MHz 2x2	TCP-DL	1201	1000	621	62.10

- Both Model 1 and Model 2 STBs were **Rebooted** when the intended load was given more than 600Mbps.

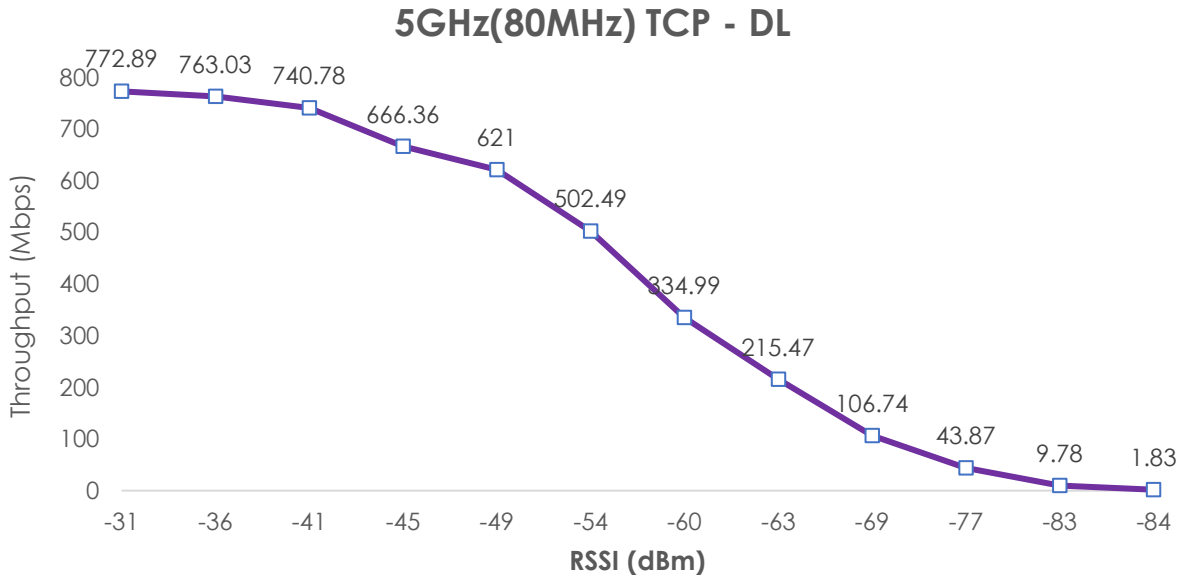
Rate vs Range

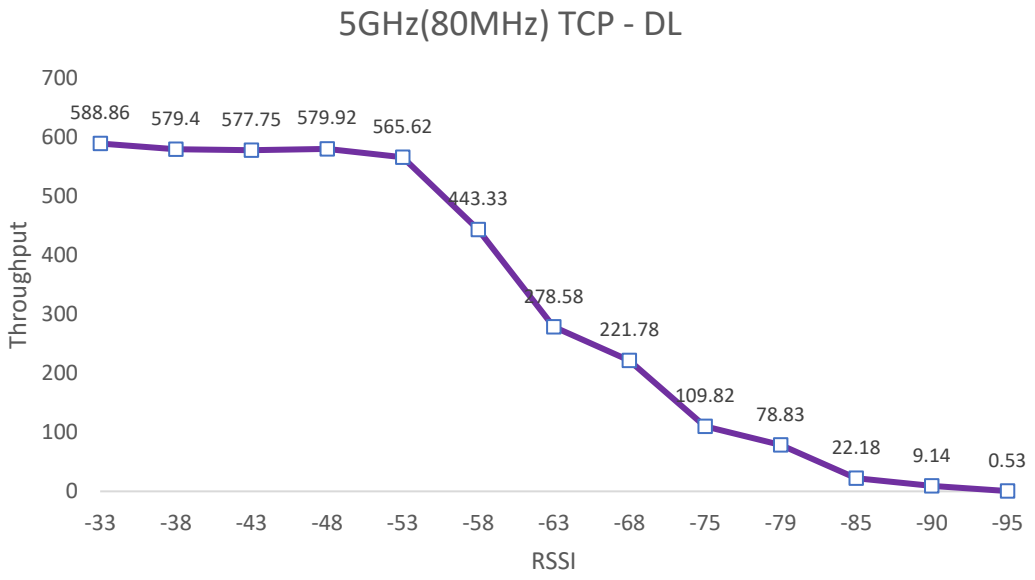
Test Objective:

- This test measures the Performance over distance of the Device under test. Distance is emulated using programmable attenuator and a throughput test is run at each distance/RSSI step and plotted on a chart.

Observations:

- In the TCP download scenario, Vendor-A Model 1 STB achieved a maximum throughput of 772.89 Mbps, while Vendor-A Model 2 STB achieved 589 Mbps.
- Vendor-A Model 1 STB disconnected from the network at an RSSI of −84 dBm, and Vendor-A Model 2 STB disconnected at −95 dBm.



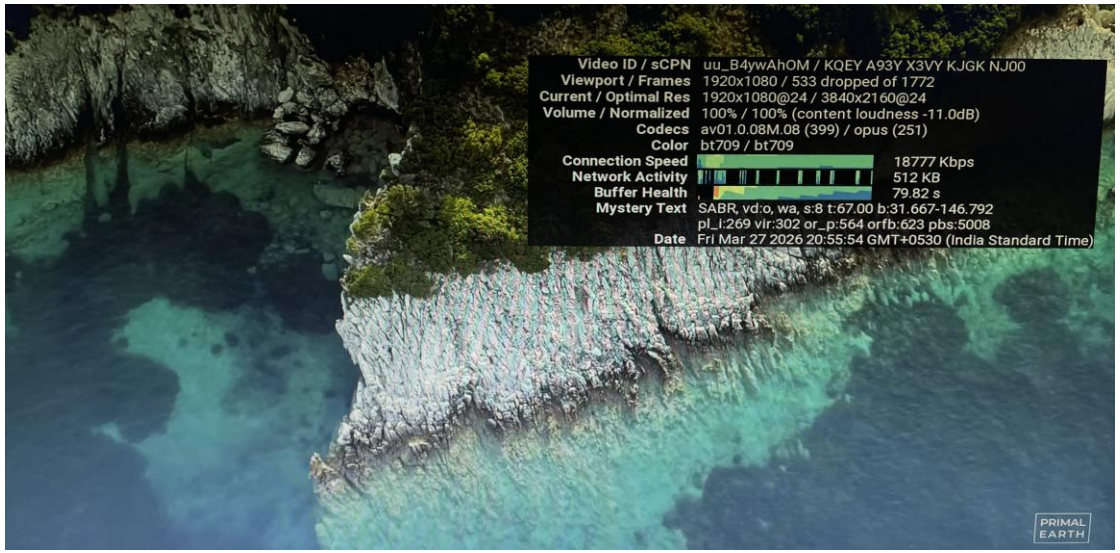


‘YouTube Video’ Streaming Performance over Distance

Test Objective:

- This test evaluates the YouTube video streaming performance of the TV Box over varying distances.
- The distance is emulated using a programmable attenuator in a controlled environment. At each attenuation step, we collected streaming performance metrics such as resolution, dropped frames, and buffer health using the Stats for Nerds feature in the YouTube application.

YouTube Stats while Video Streaming



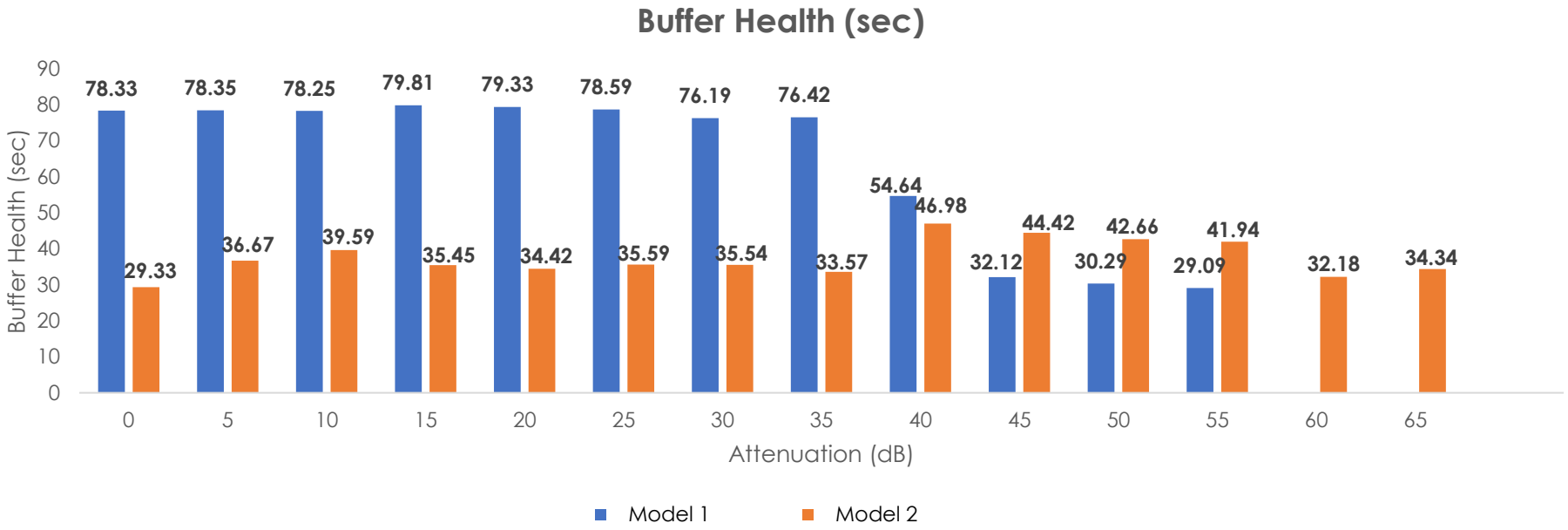
Stats	Observations
Dropped Frames	• Zero dropped frames were observed in both Tv Boxes across all attenuation levels.
Video Quality	• With Vendor-A Model 1 STB, the video quality dropped from 2160p to 1080p at around 15 dB attenuation. • With Vendor-A Model 2 STB, the video maintained 2160p quality across all attenuation levels.

YouTube Video Streaming Performance over Distance

Observations:

Buffer Health:

- Buffer Health represents how much how much duration of video youtube is able to buffer in advance to avoid playback hitches and dropouts.
- During the test, no video buffering was observed.
- With Vendor-A Model 1 STB, Buffer health remained high (~75 sec) at lower attenuation but starts decreasing after ~35 dB and eventually drops to 0 at 60 dB, After 60 dB the TV Box is disconnected resulting in streaming to stop completely.
- With Vendor-A Model 2 STB, Buffer health remained stable (~30 sec) across most attenuation levels and drops to 0 at 70 dB, After 70 dB the TV Box disconnected to the Network resulting in streaming to stop completely.

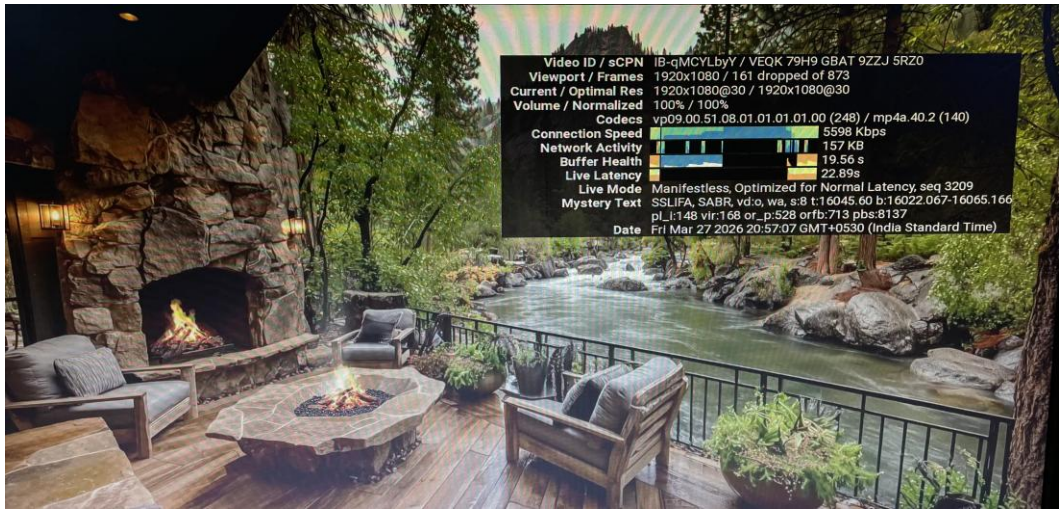


‘YouTube Live’ Streaming Performance over Distance

Test Objective:

- This test evaluates the YouTube Live streaming performance of the Set-Top Box (STB) over varying distances.
- The distance is created using a programmable attenuator in a controlled environment. Streaming performance metrics such as resolution, dropped frames, and buffer health are collected using the Stats for Nerds feature in the YouTube application.

YouTube Stats while Live Streaming



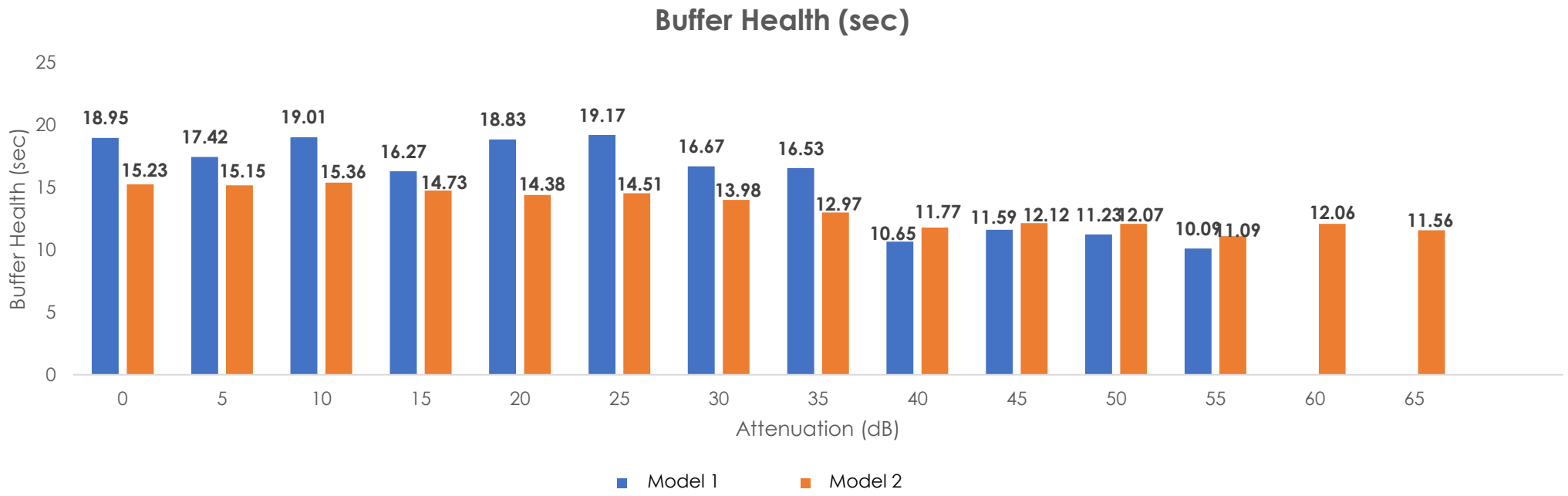
Stats	Observations
Dropped Frames	• With Vendor-A Model 1 STB, there were zero frame drops until 35dB after that there were 388 dropped frames. • With Vendor-A Model 2 STB, there were zero frame drops across all the attenuation steps.
Quality	• With Vendor-A Model 1 STB, the Live Stream quality dropped from 2160p to 1080p at around 15 dB and got dropped from1080p to 720p at around 40dB. • With Vendor-A Model 2 STB, the Live Stream maintained 2160p quality across all attenuation steps.

YouTube Live Streaming Performance over Distance

Observations:

Buffer Health

- During the test, no video buffering was observed in most of the attenuation steps.
- With Vendor-A Model 1 STB, buffer health remained higher (~16 – 19 sec) across most attenuation levels and drops to 0 at 60dB, After 60dB attenuation, the TV Box disconnected from the network.
- With Vendor-A Model 2 STB, buffer health remained stable (~ 11- 15 sec) at almost all attenuation levels and drops to 0 at 70 dB, After 70dB attenuation, the TV Box disconnected from the network.



'YouTube Live' streaming performance under Congestion

Test Objective

- To evaluate the **YouTube Live** streaming performance of the PLAY TV Box under congestion with multiple clients operating in the same band, and to assess the TV box performance at near, medium, and far distances from the AP similar to real world scenarios.

Test Procedure

- YouTube performance was assessed at different channel utilization levels such as baseline 3%, 25%, 50%, and 90% or higher.
- At each utilization level, different distances between the setup box and the AP were emulated, with RSSI of approximately −30 dBm for near, −50 dBm for medium, and −70 dBm for far.
- A total of 10 stations are emulated in the Candela box to create Channel Congestion.

Key Performance Metrics

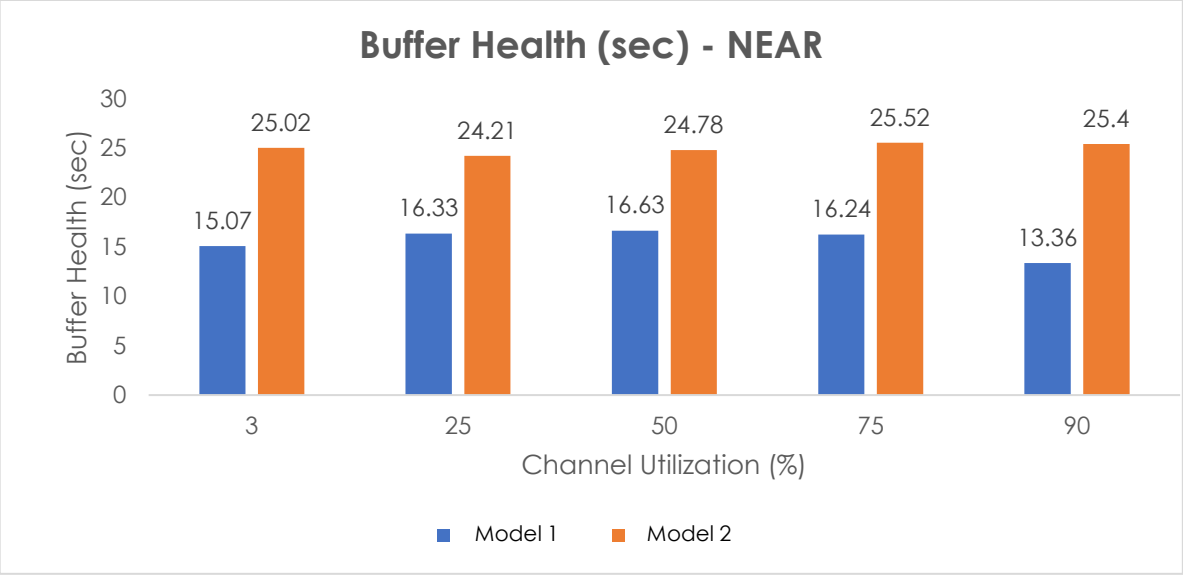
- ✓ **Dropped number of frames:** Shows how many video frames were dropped during playback.
- ✓ **Buffer health:** Represents how much video in seconds is already loaded and ready to play.
- ✓ **Live latency:** Indicates the delay between the live stream server and what is shown on the device.

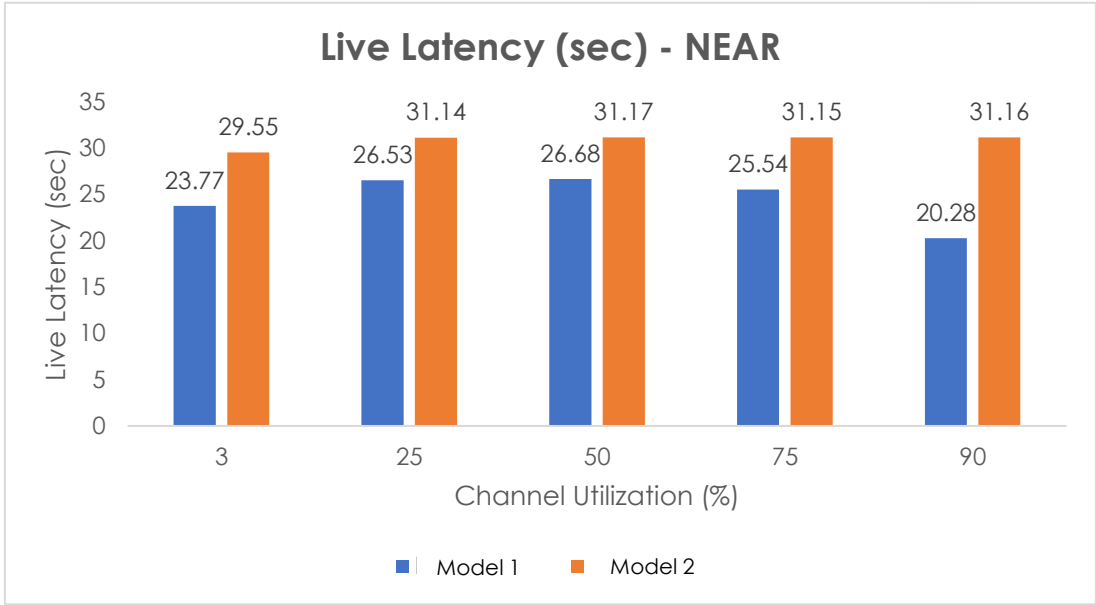
Observations

- Both TV boxes **performed well** across near, medium, and far distance scenarios, consistently streaming in 4K resolution without any frame drops or buffering.

‘YouTube Live’ Streaming Under Congestion At NEAR Distance

- Vendor-A Model 1 STB maintained a buffer health of ~13–16 seconds, whereas Vendor-A Model 2 STB maintained a higher buffer health of ~24–25 seconds.



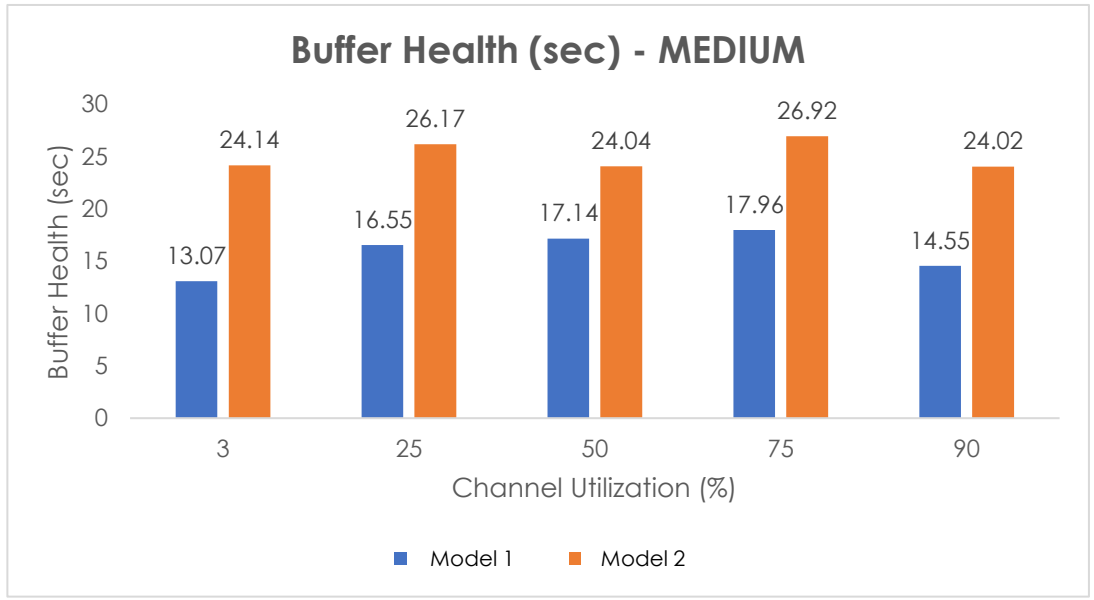


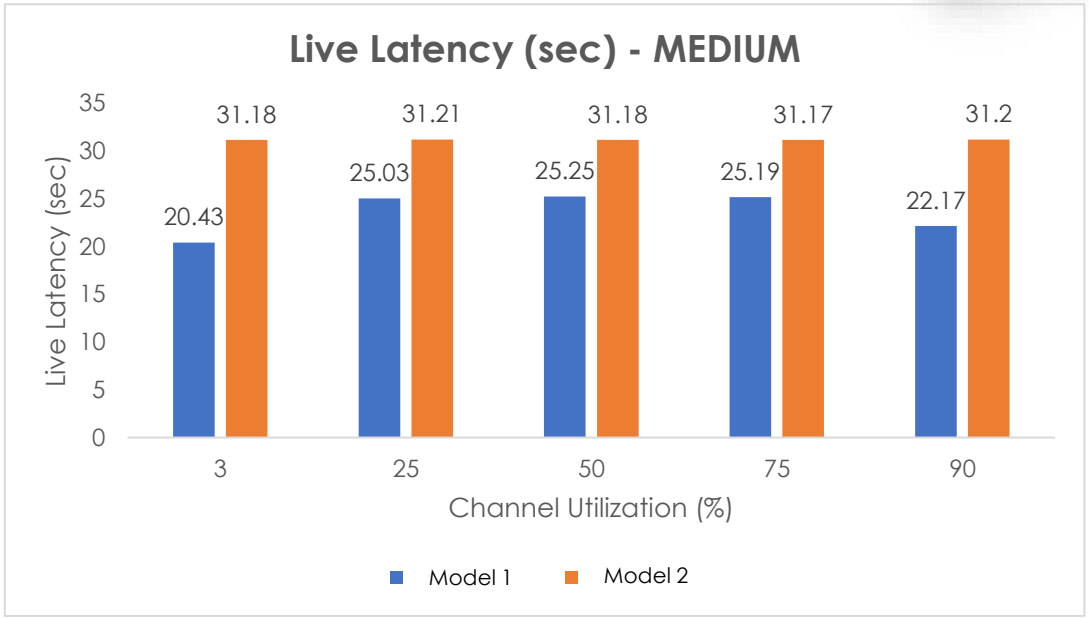
Model 2

- Vendor-A Model 1 STB maintained a live latency of ~20–26 seconds, whereas Vendor-A Model 2 STB maintained a live latency of ~29–31 seconds.

‘YouTube Live’ Streaming Under Congestion at MEDIUM distance

- Vendor-A Model 1 STB maintained a buffer health of ~13 – 17 seconds, whereas Vendor-A Model 2 STB maintained a higher buffer health of ~24–26 seconds.

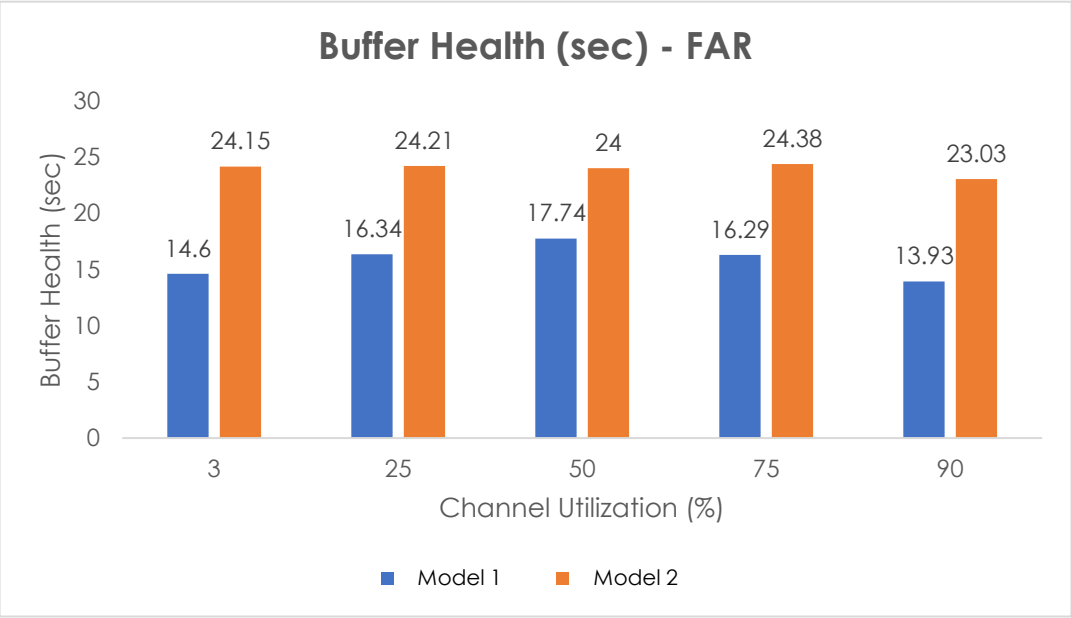


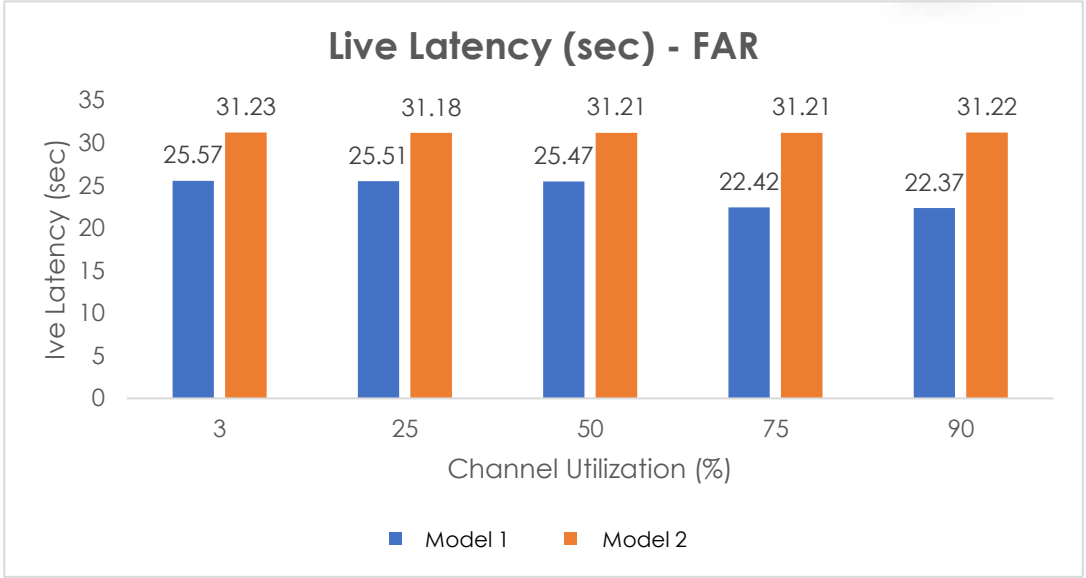


- Vendor-A Model 1 STB maintained a live latency of ~20–25 seconds, whereas Vendor-A Model 2 STB maintained a latency of ~31 seconds.

‘YouTube Live’ Streaming Under Congestion at FAR distance

- Vendor-A Model 1 STB maintained a buffer health of ~13–17 seconds, whereas Vendor-A Model 2 STB maintained a higher buffer health of ~24 seconds.





- Vendor-A Model 1 STB maintained live latency of ~22-25 seconds , whereas Vendor-A Model 2 STB maintained live latency of ~ 31 seconds.

'YouTube Video' streaming performance under congestion

Test Objective

- To evaluate the **YouTube video** streaming performance of the PLAY TV Box under congestion with multiple clients operating in the same band, and to assess the TV box performance at near, medium, and far distances from the AP.

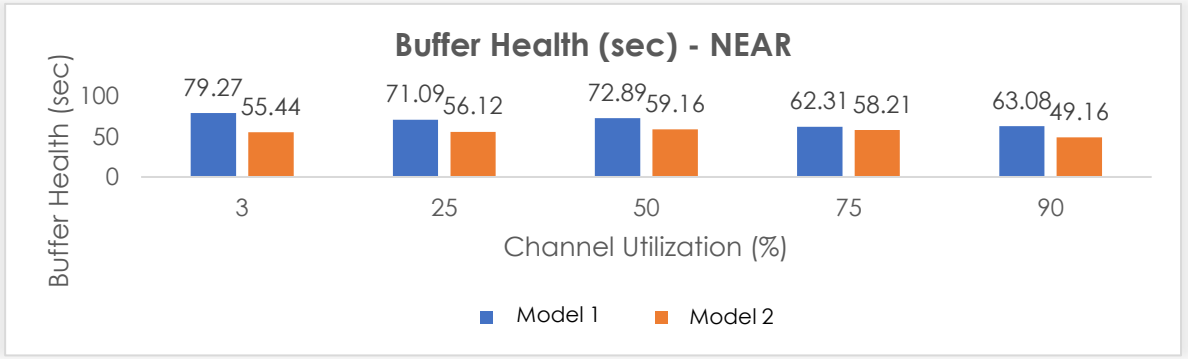
Test Procedure

- YouTube performance was assessed at different channel utilization levels such as baseline 3%, 25%, 50%, and 90% or higher.
- At each utilization level, different distances between the setup box and the AP were emulated, with RSSI levels of approximately −30 dBm for near, −50 dBm for medium, and −70 dBm for far.
- A total of 10 stations are emulated in the Candela box to create Channel Congestion.
- Streaming performance was evaluated by collecting metrics such as resolution, dropped frames, and buffer health using the Stats for Nerds feature in the YouTube application.

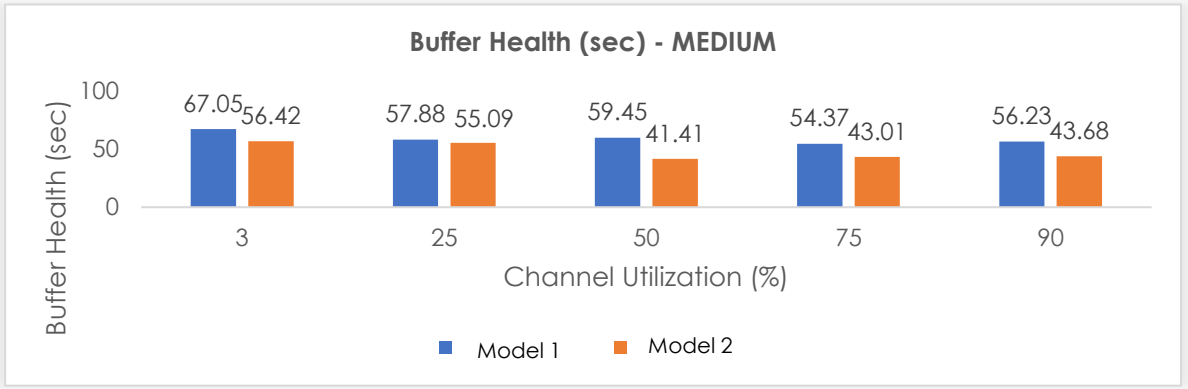
Observations

- No Frame drops or buffering were observed on both the TV Boxes during video streaming.
- The **PLAY Vendor-A Model 1 STB** showed **quality drop** from **2160p (4K) to 1440p (2K)** at medium distance while the PLAY Vendor-A Model 2 STB maintained highest streaming quality over all the near, medium, far distance scenarios.

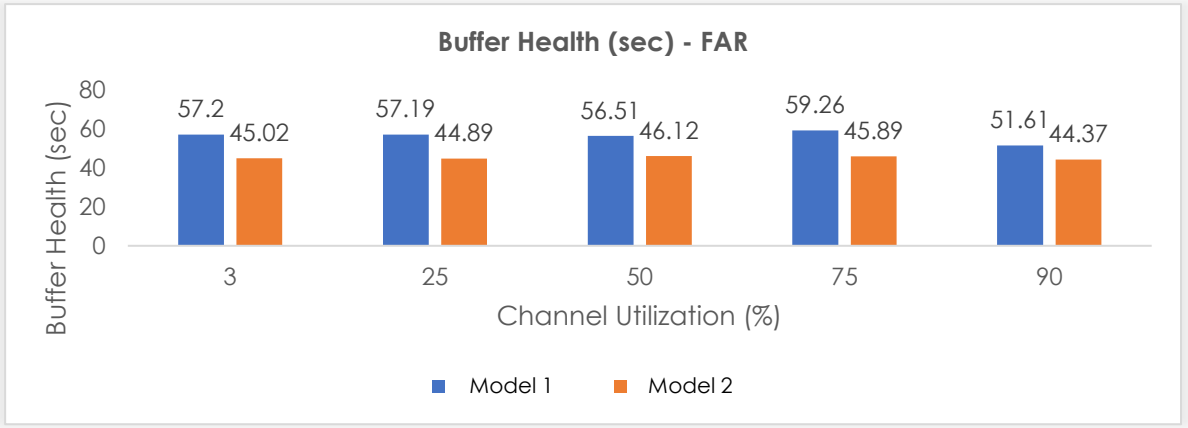
YouTube Video Streaming Under Congestion with Multiple Clients



- Vendor-A Model 1 STB maintained higher buffer health of ~63 –79 seconds, whereas Vendor-A Model 2 STB maintained buffer health of ~49–59 seconds.



- Vendor-A Model 1 STB maintained a higher buffer health of ~41– 56 seconds, whereas Vendor-A Model 2 STB maintained a buffer health of ~41 – 56 seconds.



- Vendor-A Model 1 STB maintained a buffer health of ~51–59 seconds, whereas Vendor-A Model 2 STB maintained a buffer health of ~45 seconds.

Multicast performance

Test Objective

- The Objective of this test is to evaluate the multicast performance of the PLAY TV BOX under multi-client conditions by simulating a realistic network environment using multiple virtual stations.

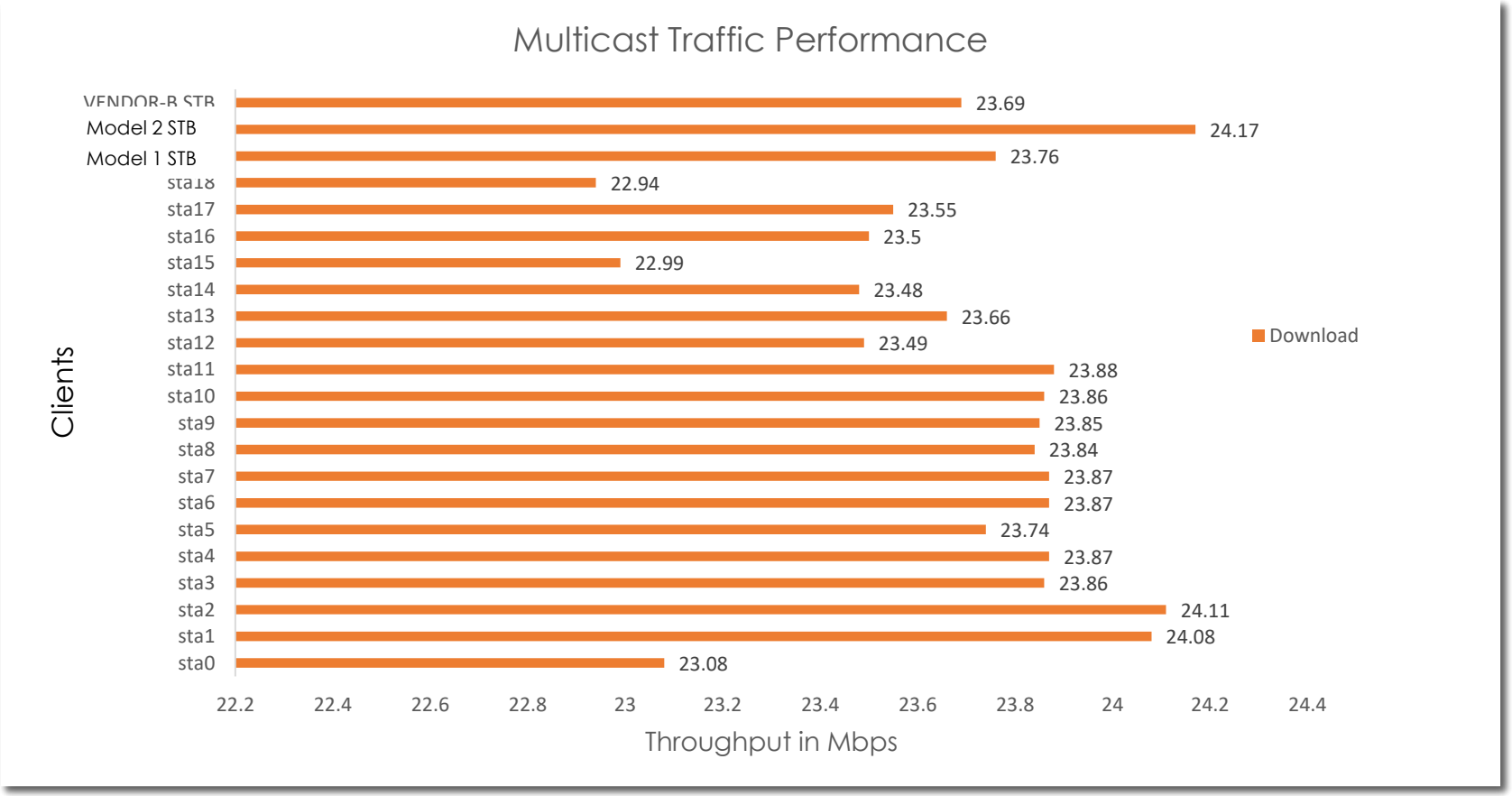
Test Procedure:

- Multicast server is the AP's wired client.
- A total of 22 stations (802.11ax) have joined the multicast group on the multicast server hosted on the Candela box, with 19 stations emulated and three TV boxes (Vendor-A Model 1 STB, Vendor-A Model 2 STB and Vendor-B STB).
- The test was performed with all 22 stations for one hour using multicast traffic of 25 Mbps with ToS set to Video (VI).
- The same test was performed for eight hours to check the stability and Multicast performance of the TV boxes.

Multicast Traffic Performance – 1hr Run

Observations:

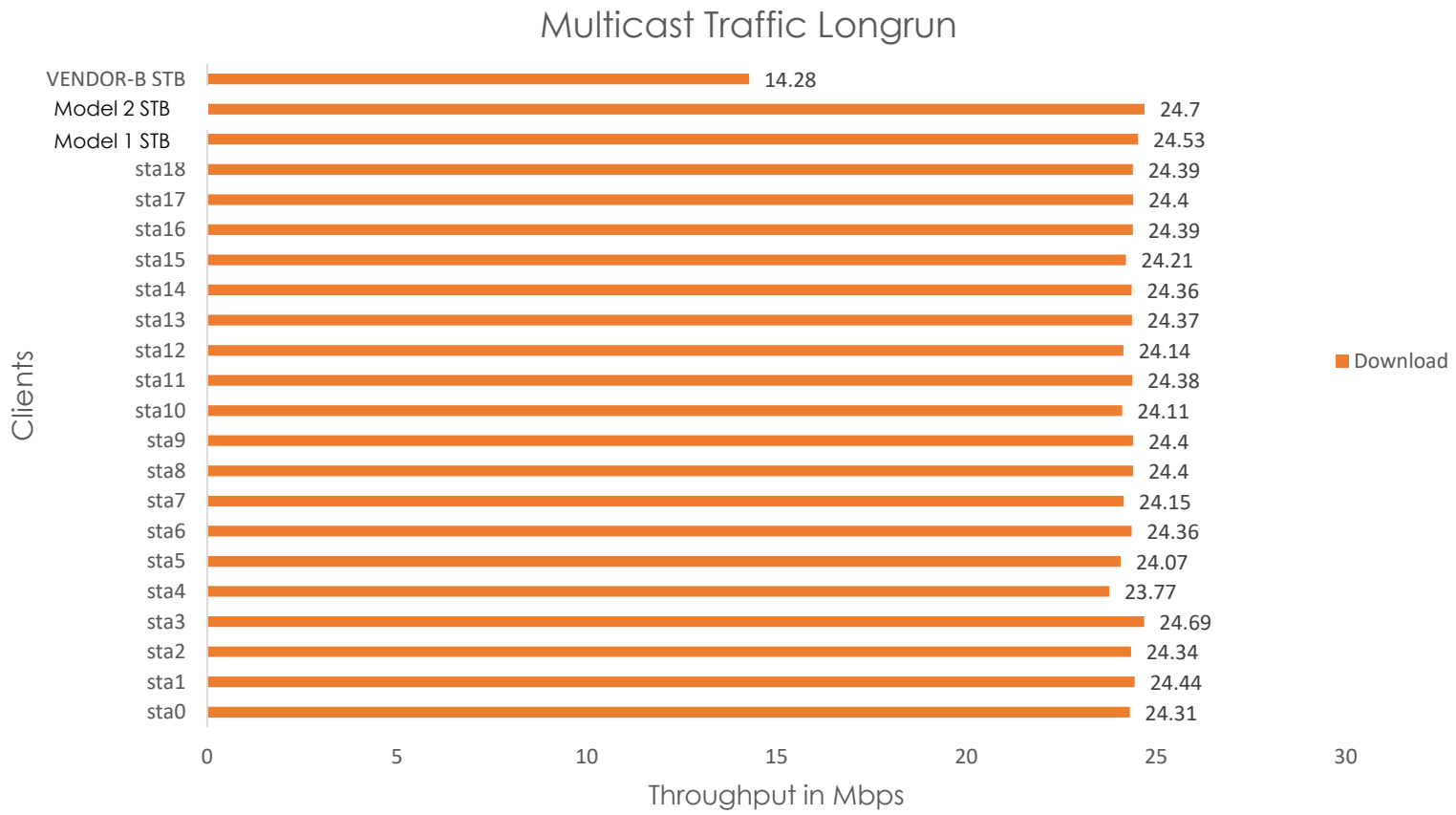
- The PLAY TV Boxes have performed on par with the Vendor-B STB.
- The Multicast throughput received at Vendor-A Model 1 STB is **23.7Mbps** and at Vendor-A Model 2 STB is **24.1Mbps.** While the Multicast throughput received at Vendor-B STB is **23.6Mbps.**



Multicast Traffic Performance – 8hrs Run

Observations:

- Initially, both Model 1 & Model 2 and Vendor-B STB Boxes maintained a similar multicast throughput of around 24 Mbps. However, over time, Vendor-B failed to maintain this throughput consistently, with its average throughput dropping to 14 Mbps. There is no such throughput drop with Vendor-A Model 1 STB/4B. PLAY TV Boxes outperformed the Vendor-B STB in the long run.



Wi-Fi Station & Router Lab Capabilities

- ✓ **Validate compatibility of diverse Wi-Fi stations**
  - Smart TVs, Gaming Consoles, Printers, Health Smart Devices, etc. with globally deployed routers and access points.
- ✓ **Test interoperability across router ecosystems**
  - Various Wi-Fi standards (802.11be/ax/ac/n)
  - Frequency bands (2.4GHz, 5GHz, 6GHz)
  - Channel Bandwidths
  - Chipset vendors
  - Regional regulatory domains, and firmware versions.
- ✓ **Evaluate device behavior under various test conditions**
  - Client connectivity with Open, WPA, WPA2, and WPA3 security types
  - Performance testing with and without load
  - Interference scenarios involving co-channel and adjacent-channel overlap
  - Rate vs. Range analysis to measure throughput degradation over distance
  - Long-term stability across continuous association and roaming sessions

Wi-Fi Station Categories

Smartphones

Tablets

Laptops

Smart TVs

Gaming Consoles

Streaming Devices

Printers & Scanners

Smart Appliances

Smart Speakers

IoT Devices

Security Devices

Health Smart Devices

Wearables

Top Residential Wi-Fi Access Points by Region

North America
- Netgear Orbi RBE973S
- TP-Link Deco BE85 / BE63
- ASUS GT-BE98 Pro
- Amazon Eero Max 7
- ASUS RT-BE96U
- Netgear Nighthawk RS700S
- TP-Link Archer BE800
- Linksys Atlas Max 6E
- Ubiquiti UniFi U6-Pro
- Google Nest WiFi Pro

Europe
- AVM FRITZ!Box 7590 AX (Popular in Germany, Austria)
- TP-Link Deco BE85 / XE75
- Netgear Orbi RBE973S
- ASUS RT-BE96U
- Google Nest WiFi Pro
- TP-Link Archer BE800
- Ubiquiti UniFi U6+
- Huawei WiFi AX3
- D-Link Eagle Pro AI M32
- Tenda Nova MW6

Asia
- TP-Link Archer BE805 / BE800
- Xiaomi BE7000 (Wi-Fi 7)
- Huawei WiFi AX3 / AX6
- ASUS TUF AX6000
- TP-Link Deco XE75
- Netgear Nighthawk RS700S
- D-Link DIR-X5460
- Mercusys MR80X
- Tenda RX9 Pro
- JioAirFiber Router (India-specific)

South America
- TP-Link Deco XE75
- TP-Link Archer AX73
- ASUS RT-AX86U
- Netgear Nighthawk AX8
- TP-Link Deco X60
- D-Link EXO AX5400
- Mercusys Halo H80X
- Huawei WiFi AX3
- Xiaomi Mi Router AX1800
- Intelbras Twibi Giga

Africa
- TP-Link Deco X20 / X60
- TP-Link Archer AX20
- Tenda AC23
- Netgear Nighthawk AX1800
- Huawei WiFi AX3
- D-Link DIR-841
- TP-Link C6 v4
- Xiaomi Mi Router 4A
- Mercusys AC12G
- ZTE MF286C (LTE CPE with Wi-Fi)

Australia
- TP-Link Deco BE85 / XE75
- Netgear Orbi RBE973S
- ASUS GT-BE98 Pro
- Amazon Eero Max 7
- TP-Link Archer BE800
- Telstra Smart Modem Gen 3
- D-Link Eagle Pro AI M32
- ASUS RT-AX86U
- Ubiquiti UniFi U6-LR
- Google Nest WiFi Pro

This list is referred from Internet Source

List of Tests Supported.

Tests	All Station Types	Smart TVs	Streaming Devices	Security Cameras	Gaming Consoles	Printer
Client Connectivity	✓	✓	✓	✓	✓	✓
Open, WPA, WPA2, WPA3	✓	✓	✓	✓	✓	✓
Country Regulations, FCC USA, ETSI (Europe), India (WPC), Others	✓	✓	✓	✓	✓	✓
Frequency Bands - 2.4 GHz, 5 GHz, 6 GHz	✓	✓	✓	✓	✓	✓
Channel Bandwidths - 20 MHz, 40 MHz, 80 MHz, 160 MHz, 320 MHz	✓	✓	✓	✓	✓	✓
Channel Switch Behavior	✓	✓	✓	✓	✓	✓
Ping Performance – No Load on AP	✓					
Ping Performance – 30%, 50%, 70% Load on AP	✓	✓	✓	✓	✓	✓
Rate vs Range	✓	✓	✓	✓	✓	✓
Roaming – Daisy Chain, Star Topology	✓	✓	✓	✓	✓	✓
Short run test - 1 Hour	✓	✓	✓	✓	✓	✓
Long run test - 8 Hours	✓	✓	✓	✓	✓	✓
TCP & UDP Throughput (iPerf-Supported)	-	✓	✓	✓	✓	✓
Throughput vs different packet sizes (iPerf-Supported)	-	✓	✓	✓	✓	✓
Quality of Service (iPerf-Supported)	-	✓	✓	✓	✓	✓
4K Streaming and OTT application performance	-	✓	✓	-	-	-
Motion Detection	-	-	-	✓	-	-
Latency tests while playing games	-	-	-	-	✓	-
Latency tests while printing with different file sizes	-	-	-	-	-	✓

Router Performance Matrix Example

Brand	Model	Connectivity	Performance	Stability
Asus	Model-x	5	4	2
Tenda	Model-x	4	3	4
ipTIME	Model-x	5	5	3
Adtron	Model-x	3	4	5
D-Link	Model-x	4	3	1
TP-Link	Model-x	3	2	3
Vodafone	Model-x	5	1	4
Linksys	Model-x	4	3	4
TP-Link	Model-x	5	2	5
OPTUS	Model-x	3	5	1
Tenda	Model-x	3	5	1
Airtel Xtream Fiber	Model-x	5	2	4
Netgear	Model-x	5	4	5
GX	Model-x	4	1	1
Airtel	Model-x	4	1	1
Jio	Model-x	4	3	2
Eero	Model-x	5	4	3
Juniper	Model-x	4	4	5
Shasta	Model-x	4	3	1
Sky UK	Model-x	3	2	3

Brand	Model	Connectivity	Performance	Stability
Fortinet	Model-x	5	4	2
Ruckus	Model-x	4	3	4
EnGenius	Model-x	5	5	3
Technicolor	Model-x	3	4	5
Sagemcom	Model-x	4	3	1
Arcadyan	Model-x	3	2	3
Sercomm	Model-x	5	1	4
CommScope	Model-x	4	3	4
Actiontec	Model-x	5	2	5
Digisol	Model-x	3	5	1
Meraki	Model-x	3	5	1
Huawei	Model-x	5	2	4
ZTE	Model-x	5	4	5
Ubiquiti	Model-x	4	1	1
Orange	Model-x	5	3	4
Linksys	Model-x	4	3	4
Google	Model-x	5	2	5
Aruba Networks (HPE)	Model-x	3	5	1
Cisco	Model-x	5	4	3
Freebox	Model-x	3	5	1

Client Connectivity with Open, WPA2 and WPA3 Security

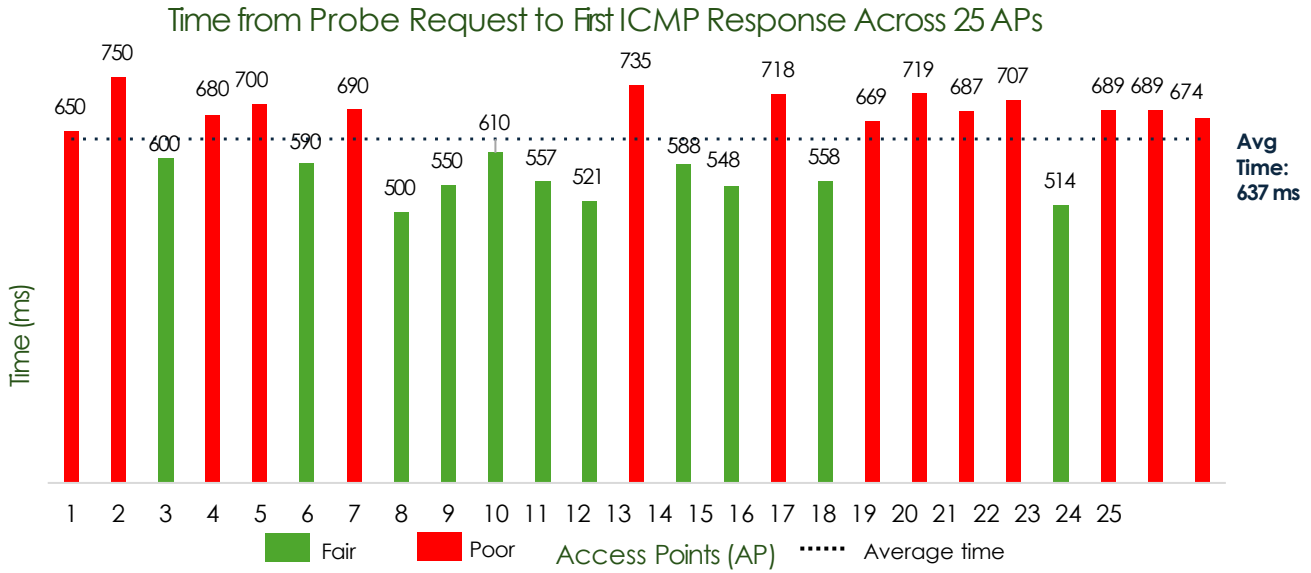
- ✓ To evaluate the connectivity performance of client devices (STAs) across multiple Access Points (APs) configured with **Open (unencrypted)/ WPA2/WPA3** security types.
- ✓ The evaluation is conducted over multiple iterations per AP, capturing key metrics including:
  - ✓ **Time taken from probe request to successful association**
  - ✓ **DHCP lease acquisition time**
  - ✓ **Time taken from probe request to first ICMP (ping) response**
- ✓ The results are then compared across various AP models to identify **variations in connection responsiveness and performance** under different security configurations.

Pass/Fail Criteria:

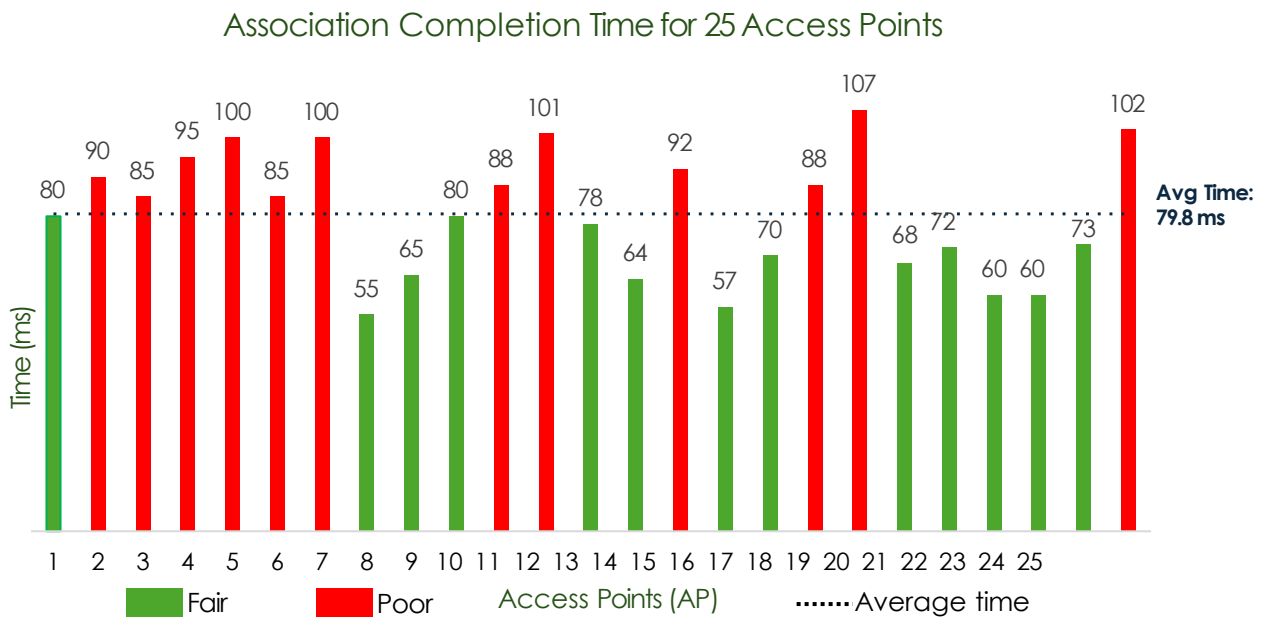
- ✓ If the STA does not connect to the AP, it is considered a **fail** for that particular AP.
- ✓ If the STA takes more time to complete any of the following steps: probe request to association, DHCP lease acquisition, or probe request to first ICMP response compared to the average time across all APs, it is considered poor performance.

Additional Info:

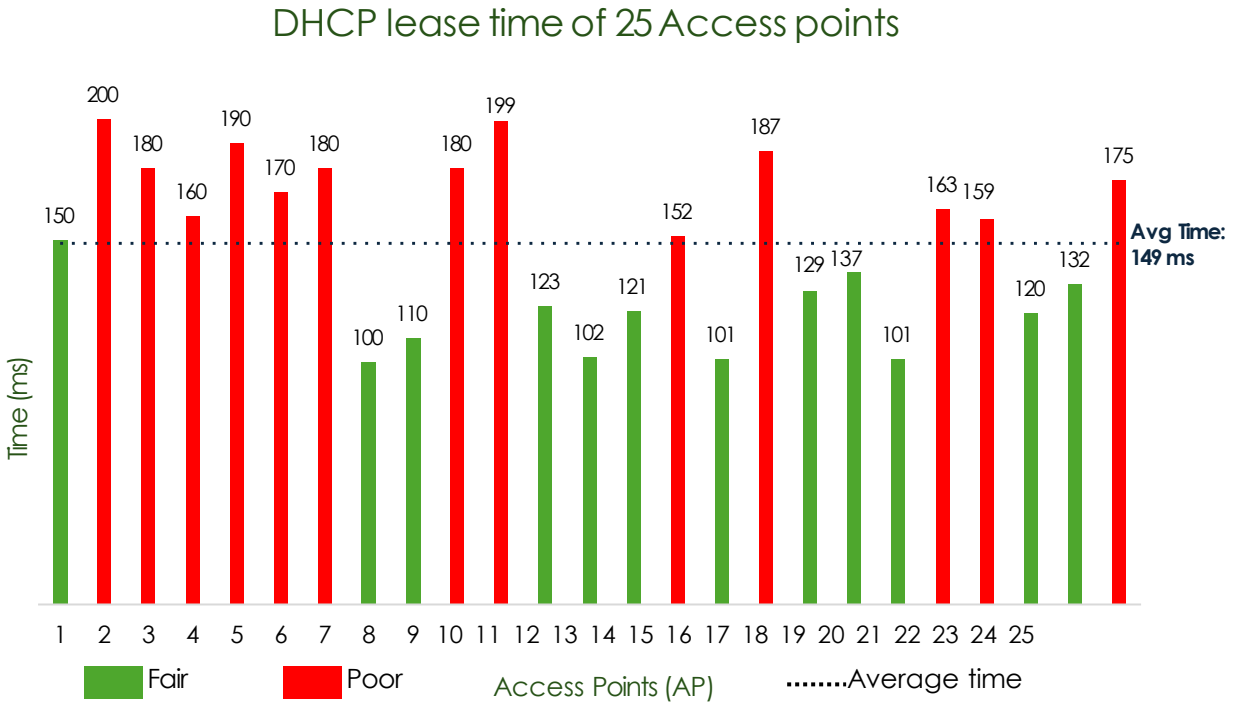
- ✓ A report will be generated in PDF or PPT format, along with corresponding CSV data



Client Connectivity with Open, WPA2 and WPA3 Security

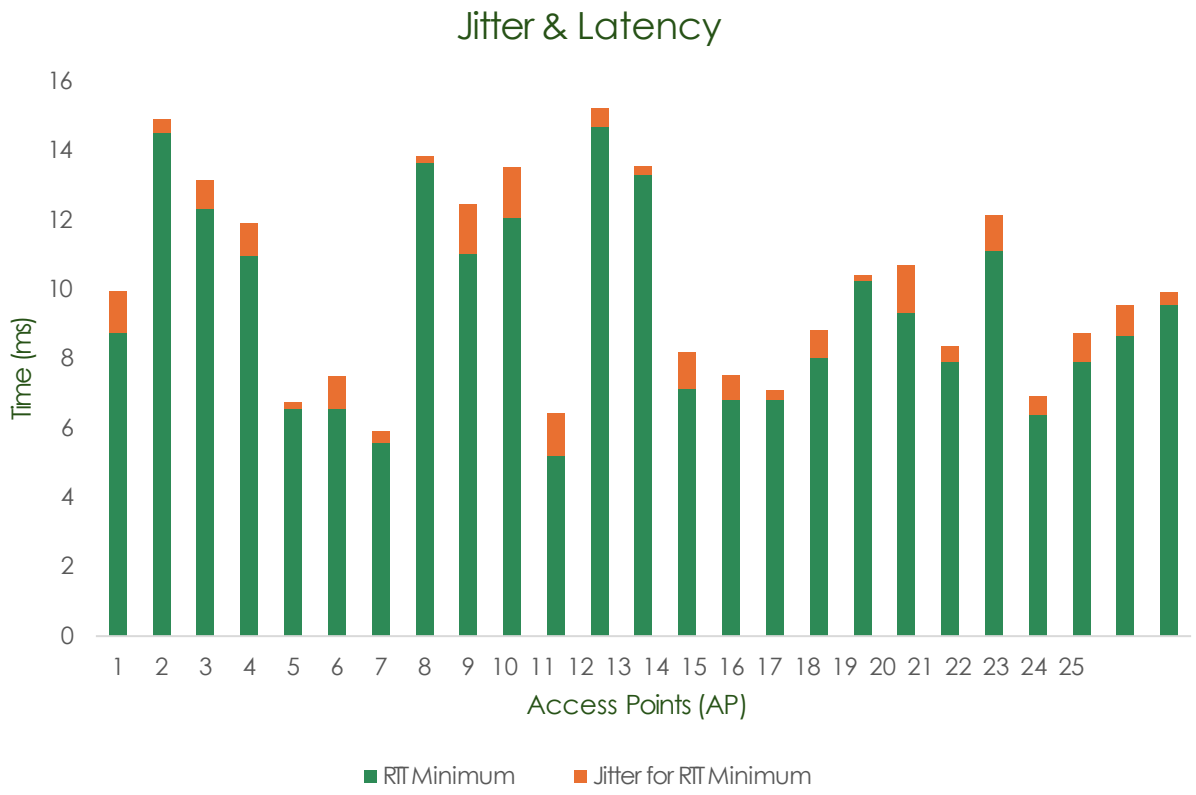


- The STA completed the probe request to first ICMP response in equal to or less than the average time (63.7 ms) on 11 out of 25 APs.
- On 13 APs, the STA completed the probe request to association in ≤79.8 ms.
- The STA completed the DHCP process in ≤ 149 ms on 12 APs.



STA Performance Under AP Load Conditions

- ✓ To evaluate the Wi-Fi performance of client devices (STAs) when other clients are already connected to the Access Point (AP) and generating active traffic, with channel utilization levels of 30%, 50%, and 70%, across multiple APs configured with WPA2 security.
- ✓ The evaluation is performed on each AP, capturing key metrics including:
  - **Round Trip Time (RTT):** Minimum, Maximum, and Average Latency
  - **Jitter (Packet Delay Variation)**
  - **Ping Success Rate (%)**
  - ✓ The results are compared across various AP models to identify variations in **connectivity** and **performance** under the WPA2 security configuration.
- ✓ Pass/Fail Criteria
- ✓ If the STA **disconnects from Wi-Fi** or consistently experiences **loss of 50 to 100 packets**, it is considered a **Fail** for that AP.
- ✓ If the STA shows **higher-than-average values** for any of the following:
  - **Maximum, Minimum, or Average Latency**
  - **Packet Loss**
  - **Jitter**
  - **Ping Success Rate (%)**
    compared to the average across all APs, it is considered **Poor Performance**.
- ✓ Additional Information
- ✓ A detailed report will be generated in **PDF or PPT format**, along with corresponding **CSV data**.



Rate vs Range

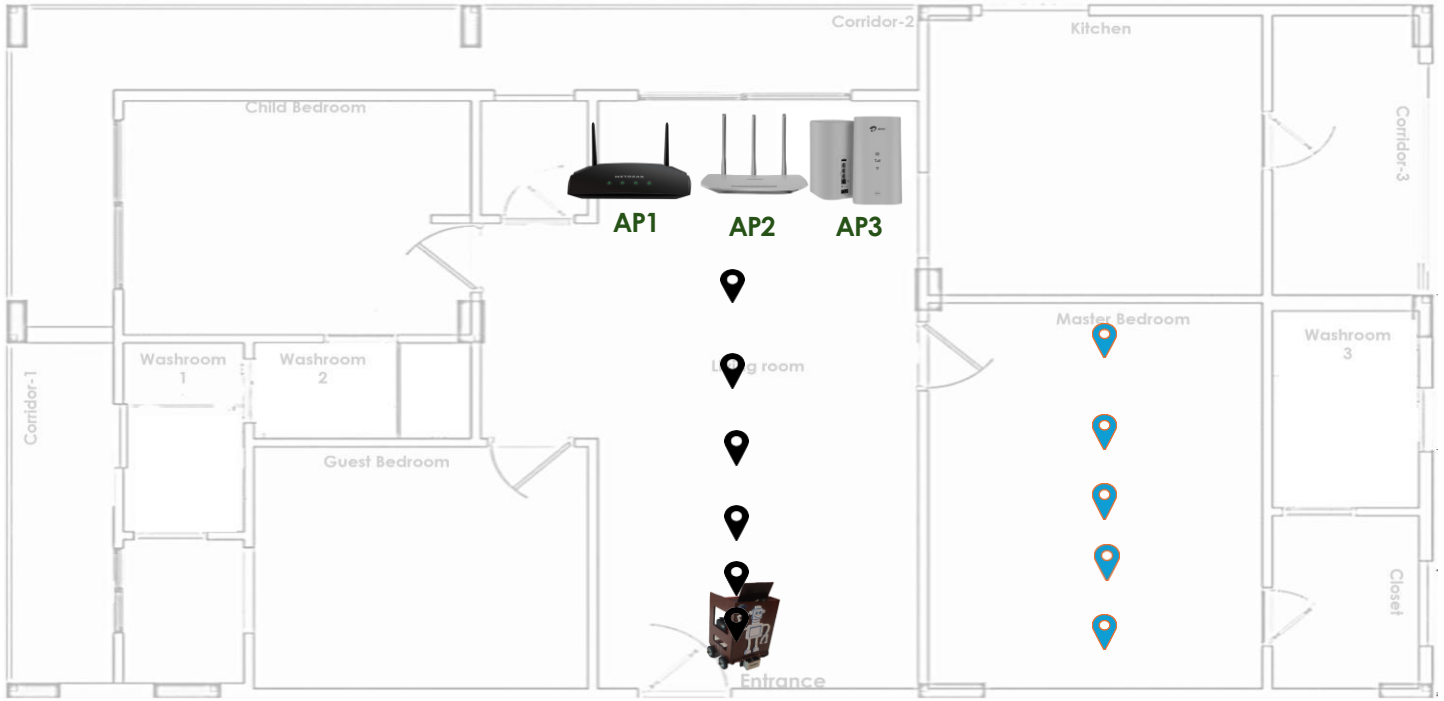
- ✓ Evaluate Wi-Fi performance of client devices (STAs) connected to multiple Access Points (APs) at distances of 3, 6, 9, 12, 15, and 18 feet under WPA2 security.
- ✓ For each AP and distance, the following metrics are measured:
  - **Round Trip Time (RTT):** Minimum, Maximum, and Average Latency
  - **Jitter (Packet Delay Variation)**
  - **Ping Success Rate (%)**
- ✓ Results are compared across APs to identify performance differences.
- ✓ Tests under both line-of-sight and non-line-of-sight conditions can be performed using different bands, bandwidths, and regulatory settings

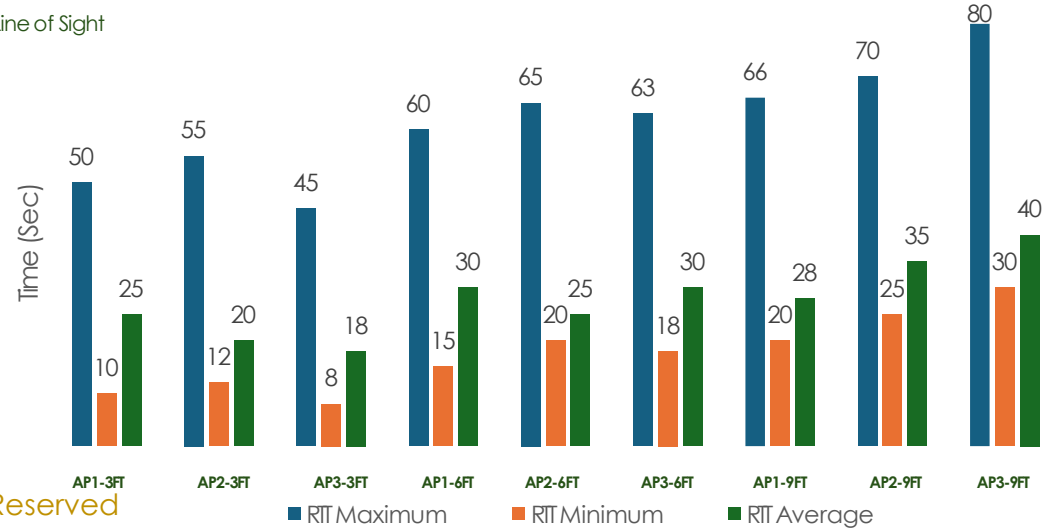
Pass/Fail Criteria

- ✓ **Fail:** STA disconnects or has 50–100 packet loss
- ✓ **Poor Performance:** Higher-than-average values in RTT, Jitter, Packet Loss, or Low Ping Success Rate (%)

Additional Info

- ✓ A detailed report will be provided in PDF/PPT format with CSV data.
- ✓ Device is placed on Robot.





Stability Test

- ✓ Evaluate the long-term Wi-Fi stability of client devices (STAs) connected to multiple Access Points (APs) over an extended duration (e.g., 1 hours) under WPA2 security.
- ✓ Monitor each STA-AP connection continuously and capture the following metrics:
  - **Connection Drops / Re-associations**
  - **Ping Success Rate (%) over time**
  - **Latency Trends (RTT - Min, Max, Avg)**
  - **Jitter Stability**
- **Packet Loss Events**

Pass/Fail Criteria

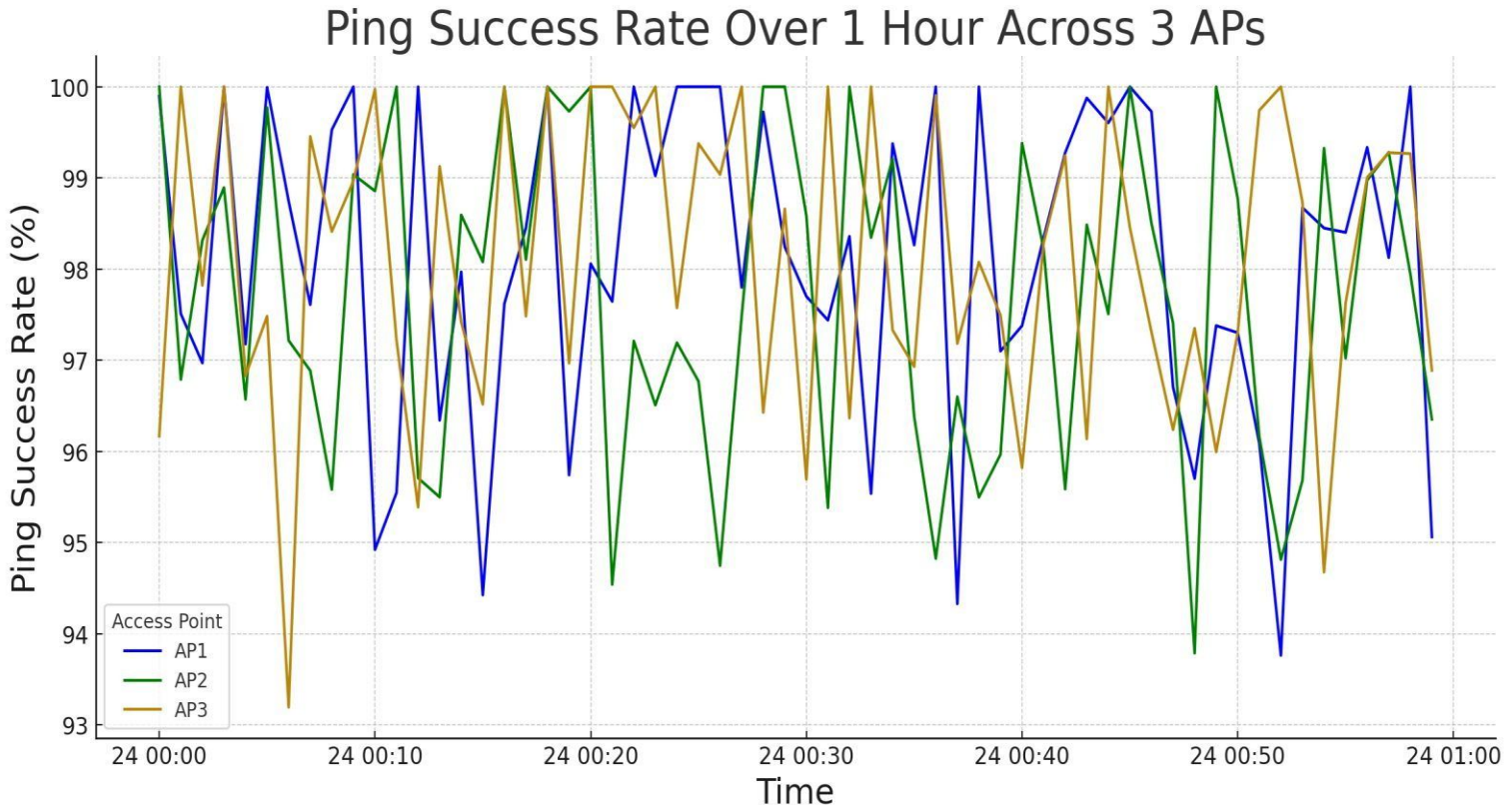
Fail: STA disconnects unexpectedly or frequently re-associates

Poor Performance:

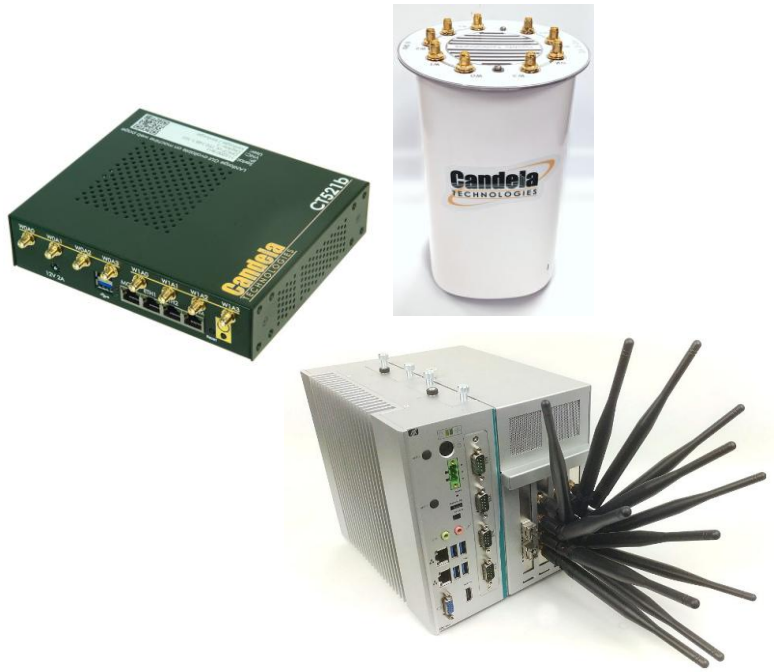
- High jitter or latency drift over time
- Decreased ping success rate
- Sudden spikes in packet loss

Additional Info

Performance will be logged periodically, and the final repor will include time-based plots, summary charts, and comparison tables. Output formats: PDF/PPT with raw data in CSV.



LANforge vAP Capabilities



LANforge (Traffic generator, vAP emulation, test automation)

- ✓ Supports 802.11 a/b/g/n/ac/ax/be
- ✓ Frequency Bands Supported: 2.4GHz, 5GHz, 6GHz
- ✓ Bandwidth: 20/40/80/160/320 MHz
- ✓ MIMO: 1X1/2X2/3X3/4X4
- ✓ Securities: Personal & Enterprise [Open, OWE, WPA, WPA2, WPA3, 802.1x]
- ✓ Supports 802.11 k/v/r
- ✓ QoS [VO, VI, BE, BK]
- ✓ OKC/PKC Roaming
- ✓ Configurable Beacon Interval
- ✓ Other Features:
  - ✓ Supports 802.11d (Regulatory domains)
  - ✓ Supports 802.11h (DFS)
  - ✓ Ignore certain management frames such as Probes, Authentication requests, Associations
  - ✓ Force De-authentication
  - ✓ Channel Switching with CSA
  - ✓ Custom Wi-Fi commands such as *bgscan*

Low Level CLI Commands

add_arm_endp	Add an Armageddon (Kernel accelerated UDP) endpoint
add_cx	Add a cross-connect to a test-manager
add_cd	Add a Collision Domain (grouping of WanLinks)
add_cd_endp	Add an Endpoint to a Collision Domain
add_cd_vr	Add a Virtual Router to a Collision Domain
add_file_endp	Add a File endpoint to the LANforge Manager
add_gen_endp	Add a Generic endpoint to the LANforge Manager
add_l4_endp	Add a Layer-4 endpoint to the LANforge Manager
add_channel_group	Add a grouping of DS0 channels to be used by PPP
add_ppp_link	Add a PPP interface connection
add_t1_span	Add a T1/E1 SPAN to the LANforge Manager
add_voip_endp	Add a VOIP endpoint to the LANforge Manager
add_vr	Add or modify a Virtual Router object
add_vr_bgp	Add BGP configuration to a virtual router
add_bgp_peer	Add/Modify BGP peer configuration to a virtual router
add_vrcx	Add or modify a Virtual Router Connection Endpoint
add_vrcx2	Modify a Virtual Router Connection Endpoint object
set_vrcx_cost	Modify a Virtual Router Connection interface cost
add_endp	Add an endpoint to the LANforge Manager
add_event	Add a new event or modify an existing one
add_bond	Add a Linux Bond Device
add_br	Add a Linux Bridge Device
add_mvlan	Add a MAC based VLAN (Requires kernel support)
add_rdd	Add a Redirect-Device (Requires kernel support)
add_gre	Add a GRE Tunnel device
add_sec_ip	Add or update secondary IP Address(es)
add_vlan	Add an 802.1Q VLAN (Requires kernel support)
add_venue	Add/modify a Venue
add_sta	Add/modify a WIFI Virtual Station (Virtual STA) interface
add_vap	Add/modify a WIFI Virtual Access Point (VAP) interface
add_monitor	Add/modify a WIFI Montior interface
add_tm	Create and add a new test manager to the system
add_group	Create a new test group
add_tgcx	Adds CX to test group
add_wl_endp	Add a WanLink (ICE) endpoint to the LANforge Manager

add_wanpath	Add a WanPath (ICE) personality to a WanLink
admin	Various admin commands
apply_vr_cfg	Apply all of the virtual routing settings
cancel_vr_cfg	Cancel a virtual-router configuration process
clear_cx_counters	Clear counters for one or all cross-connects
clear_endp_counters	Clear counters for one or all endpoints
clear_cd_counters	Clear counters for one or all Collision Domains
clear_group	Clears all cross-connects in a test group
clear_port_counters	Clear one or all port counters or other items
clear_resource_counters	Clear counters on one or all resources
clear_wp_counters	Clear WanPath counters for one endpoint
discover	Force discovery of nodes on the management
diag	Get diagnostic information from the LANforge
notify_dhcp	Handle input from the DHCP client process
do_pesq	Start a PESQ calculation
file	Download files through LANforge API
gossip	Send a message to everyone else logged in
getintxrate	Get tx pps rate over the last 3 seconds
getinrxrate	Get rx pps rate over the last 3 seconds
getinrxbps	Get rx bpsrate over the last 3 seconds
gettxpkts	Get the total tx packets sent
getrxpkts	Get the total rx packets sent
getpktdrops	Get the total packets dropped
getavglatency	Get the average latency for an endpoint
getrxporterrpkts	Get the total error packets detected
getrxendperrpkts	Get the total error packets detected
getipadd	Get the IP for an endpoint
getmask	Get the IP Mask for an endpoint
getmac	Get the MAC address for an endpoint
?	Show help for command(s)
init_wiser	Initialize the Wiser NCW/HNW module
licenses	Print out license information. See also: set_license
load	Load a previously saved test database
login	Login as the client who's name you enter
create_client	Create a new client

log_level	Query or modify the logging level
motd	Get the message of the day (alerts
nc_show_endpoints	Non-Cached Show one or all endpoints
nc_show_pesq	Non-Cached Show PESQ results
nc_show_ports	Show one/all ports for one/all
c_show_ports	Show one/all ports for one/all resources
nc_show_channel_grps	Show one/all ChannelGroups for one/all resources
nc_show_spans	Show one/all Spans for one/all resources
nc_show_vr	Show one/all Virtual Routers for one/all resources
nc_show_vrcx	Show one/all Virtual Router Connections
nc_show_cd	Show one/all Collision Domains
nc_show_ppp_links	Show one/all PPP Links for one/all resources
probe_port	Probe & report low-level details for a port
probe_ports	Check for the existence of new (virtual) interfaces
port_reset_completed	notify LANforge the reset has completed
exit	Log out of the LANforge control server
report	Configure server-side reporting
reset_port	Reset an Ethernet port or ports
reset_serial_span	Reset a serial span
reboot_os	Restart the OS on a remote resource
rm_attenuator	Remove Attenuator
rm_cd	Remove a Collision Domain
rm_cd_endp	Remove an Endpoint from a Collision Domain
rm_cd_vr	Remove a Virtual Router from a Collision Domain
rm_endp	Remove one or all endpoints
rm_channel_group	Remove a channel group
rm_event	Remove one or more events from the event log
rm_group	Deletes a new test group
rm_threshold	Remove existing threshold-alert
rm_tgcx	Removes CX from test group
rm_venue	Remove a venue
rm_vr	Remove one or all Virtual Routers
rm_vrcx	Remove one or all Virtual Router Connections
rm_span	Remove a Serial Span
rm_ppp_link	Remove a PppLink