



Field Testing Guide

App Note 44



Table of Contents

1. Scope	5
2. Regulatory Compliance	5
3. Safety Considerations	5
4. Testing Planning and Setup	6
4.1. Environment Selection	6
4.2. Device Under Test (DUT) Selection	6
4.3. Order of Execution	6
4.4. Test Setup	6
4.4.1. Device Configuration	7
Firmware Updates	7
Country Code Compliance	7
Network Configuration	7
HaLow Network Configuration	7
4.4.2. Labelling and Documentation Practices	7
4.4.3. Device Placement	8
Elevation	8
Surrounding devices	8
4.4.4. Device Network Access	8
Local Device Access	8
Best Practices for Local Device Access Testing	9
Remote Device Access	9
Best Practices for Remote Device Access Testing	9
4.4.5. Sanity Checks	10
5. Test Execution	11
5.1. RF Spectrum Capture	11
5.1.1. RF Spectrum Capture Best Practices	11
5.1.2 Recommended Spectrum Analysis Tools	12
5.2. Software Tools For Field Testing	12
5.2.1. iPerf Test Software	12
Local Command Execution	13
Traffic Direction	13
Session Management	13
5.2.2. iPerf Test Parameters	13
5.2.3. Parameters Common to iPerf2 and iPerf3	13
5.2.4. Parameters Specific to iPerf3	13
5.2.5. Other Testing Tools	14
Wireshark/tcpdump	14
Ping	14

OpenWrt Diagnostic Utilities	14
Alternative Performance Tools	14
Custom Automation Scripts	14
6. Data Capture and Debugging	14
6.1. Rate Control Metrics	15
6.2. Signal Strength and Link Quality (RSSI, SNR)	15
6.3. Traffic and Throughput	15
6.4. Association & Link Stability	16
6.4.1. Summary Table of Commands	16
6.5. Test Data Interpretation Guidance	17
6.5.1. Throughput Trends	17
6.5.2. RSSI and Signal Quality	17
6.5.3. Association Stability	17
6.5.4. Environmental Influence	17
6.5.5. Edge Case Behavior	17
7. Optimizing Wi-Fi HaLow Network Performance	19
7.1. Device Height and Placement	19
7.2. Avoiding Metal Near Antennas	19
7.3. Bandwidth and Channel Optimization	19
7.4. Environment Considerations	20
7.5. Cable Management	20
7.6. Diagnostics and Monitoring	20
8. Field Test Case Studies	21
8.1. Testing Scenarios Overview	22
8.1.1. Why This Matters	22
8.2. OTA Case Study	22
8.2.1. Theory of Operation	22
8.2.2. Methodology	22
Equipment	23
Preparing the DUTs	24
Test Execution Procedure	25
Key Metrics to Capture	26
Script Automation	26
8.2.3 OTA Field Test Images	27
8.3. Multi-Station Over-the-Air Case Study	28
8.3.1. Theory of Operation	28
8.3.2 Methodology	28
Preparing the DUTs	30
Conducting the Test	31
8.3.3. Edge-Case Load Scenario Testing	31
Simultaneous Start/Stop	31

Staggered Start/Stop	31
8.3.4. Repeat Testing and Variability Assessment	31
8.4. Range Test Case Study	32
8.4.1 Theory of Operation	32
8.4.2 Methodology	33
Device Configuration and Preparation	34
Remote Access and Connectivity	35
Key Components of the Setup:	36
Equipment	36
Conducting the Continuous Range Test	37
Conducting the Discrete Range Test	38
Key Metrics to Capture	39
Best Practices and Considerations	39
Script Automation	40
Appendix A: RF Spectrum Capture Using the BB60D and Spike Software	41
Capture Ranges and Settings	41
Best Practices for Capture	42
Revision History	43

1. Scope

This application note provides step-by-step instructions for conducting and debugging rigorous field tests using Morse Micro Wi-Fi HaLow evaluation kits. It details proper test planning and setup, efficient test execution and best testing practices to ensure optimal and reproducible results. Additionally, a dedicated section on debugging has been added, offering practical guidance to improve troubleshooting efficiency in the field.

2. Regulatory Compliance

Use of Wi-Fi HaLow devices must comply with local sub-GHz frequency regulations to avoid legal and operational issues. Unauthorized changes to transmission power, antennas, duty cycle or channel/frequency may void certification and lead to fines and/or equipment seizure. Always use certified Morse Micro hardware and refer to your respective national authority for the latest regulatory information.

3. Safety Considerations

To ensure safe and successful field testing, Morse Micro recommends the following:

- **Plan Around Weather** - Schedule testing activities during favorable weather conditions. Field tests should be avoided during rain, snow, or thunderstorms due to heightened safety risks and potential for equipment damage.
- **Wear Appropriate Personal Protective Equipment (PPE)** - Field personnel should wear a wide-brim hat, UV-protective clothing, and sturdy, enclosed footwear to ensure sun protection and safe navigation of test environments.
- **Protect Against Heat and UV Exposure** - On hot days, apply sunscreen liberally, stay hydrated, and take regular breaks to prevent heat-related illnesses such as heat exhaustion and dehydration.
- **Use Protective Storage** - Store all Devices Under Test (DUTs), tools, and accessories in durable, shock-resistant, and weatherproof containers during transportation or when not in use.

Adhering to these safety measures helps to ensure the well-being of field personnel and preserves the accuracy and integrity of field test data.

4. Testing Planning and Setup

A properly documented test plan is essential for conducting any rigorous field test. It serves as a single source of truth, streamlining test execution and ensures consistency across test runs. Additionally, a test plan helps to identify test methodology weaknesses, ensure efficient resource usage and facilitate better test risk management.

4.1. Environment Selection

The selection of the test environment should align with the specific objectives of the field test. Due to ever-changing environmental variables that influence radio performance, the primary challenge of field testing is obtaining “quality” repeatable results. To achieve this, the best practice is to isolate a single test parameter of interest where possible. This means standardizing all other setup parameters i.e. device locations, device height, antennas, antenna orientation, software version etc. Devices should be subjected to field testing at various test locations and distances for a more holistic evaluation of performance.

4.2. Device Under Test (DUT) Selection

Due to the unpredictable nature of field testing, Morse Micro recommends including a pair of benchmark devices in the test plan as well as an identical backup pair. This is helpful for troubleshooting underperforming devices by quickly eliminating the prospect of ‘bad’ or inconsistent hardware. Backup devices are useful in cases where the primary devices under test are damaged in the field due to severe weather or accidents while handling.

4.3. Order of Execution

When testing different hardware or software versions, it is important to interleave the individual test runs to avoid outliers in results. These deviations are caused by fluctuations in environmental conditions over time—such as temperature, humidity, noise floor/interference and moving obstructions. Moreover, each of these interleaved test blocks should be repeated multiple times to amortize the varying effects of the environment on test results.

4.4. Test Setup

Before setup, it is critical to first document all device configurations, including hardware serial numbers, firmware versions, and assigned roles i.e. whether the DUTs are being set up as an access point or station. Comprehensive records of new test environments (supplemented with photographs) should also be gathered to facilitate future analysis and address any potential gaps in documentation.

To mitigate the risk of unintended cross-device pair associations, each device pair should be assigned a unique WiFi HaLow network SSID. This is helpful for long duration field tests where lapses in attention occur. Furthermore, effective coordination between test engineers is essential to guarantee that the correct DUT pairs are operating at any one time.

4.4.1. Device Configuration

A fundamental aspect of field test preparation is ensuring that all DUTs are correctly configured and that these configurations are documented. Configuration documentation supports efficient troubleshooting, enables consistent data interpretation, and facilitates reproducible test results. The following best practices apply to the setup of Morse Micro Wi-Fi HaLow evaluation kits:

Firmware Updates

Verify that each DUT is running the latest Morse Micro OpenWrt image, corresponding to its hardware. Running the latest OpenWrt image is recommended since it incorporates the newest chip firmware which fixes critical bugs as well as improves radio performance.

Country Code Compliance

Ensure that the country code for Wi-Fi HaLow operation is correctly set according to the geographic location of the test. Failure to set the appropriate country code may result in improper channel usage and regulatory violations.

Network Configuration

Assign static IP addresses to each DUT to maintain consistent device identification and minimize ambiguity during testing. Use simple IP addresses to reduce testing friction.

HaLow Network Configuration

Define intuitive and identifiable SSIDs for each Wi-Fi HaLow network. Explicitly configure the Wi-Fi HaLow operating channel to prevent interference with other RF sources, and document this setting within the test report.

For detailed device setup and configuration procedures, refer to the appropriate Morse Micro Evaluation Kit User Guide.

4.4.2. Labelling and Documentation Practices

- Physically label each DUT with its assigned IP addresses and device role.
- Maintain a spreadsheet / document containing device serial numbers, software versions, and any special configurations applied during testing.

- Capture setup images and the initial RF environment.

4.4.3. Device Placement

Elevation

Elevating the DUTs helps mitigate the impact of Fresnel zone interference. Morse Micro engineers typically elevate DUT pairs 2.8 meters off the ground using stainless steel tripods (or studio light stands) during field tests. While the optimal device elevation may vary depending on the specific test case, it is advised to place devices as high as practicable to minimize Fresnel zone interference. Consistent environmental elevation should be maintained along the test route to ensure RF path uniformity and improve the reliability of test results.

Surrounding devices

The area surrounding each DUT should be kept clear of electronic devices that could introduce radio frequency (RF) noise or otherwise interfere with test accuracy. For example, certain portable power banks may emit substantial electromagnetic noise, potentially elevating the local noise floor by several decibels close to the DUT. Morse Micro suggests positioning portable batteries and other peripheral hardware at a distance from the DUT, using extended USB power cables where possible. Furthermore, the routing and positioning of all cables—including power and Ethernet—should be kept consistent throughout testing to avoid introducing additional uncontrolled variables.

4.4.4. Device Network Access

Consideration must be given to the method of remote accessing the DUTs during testing. For instance, executing network traffic generation or diagnostic commands on a Wi-Fi HaLow device often requires direct access, which can be established remotely or through a local physical connection. To ensure accurate performance measurements, it is recommended to avoid backhauling shell commands, network metrics and chip performance statistics over the Wi-Fi HaLow network, as this introduces additional traffic and will degrade performance.

Local Device Access

Testing with local device access involves establishing a direct physical connection to the DUT via interfaces such as serial, USB, or Ethernet. This approach provides two key advantages:

- **Reliable Access** - Physical connections (e.g., serial or local Ethernet) are less susceptible to latency, interference, or dropouts compared to remote links, making them ideal for debugging and setup verification.

- **Reduced Interference** - Separating the control interface from the HaLow radio prevents any unintended interference with the network under test, preserving the integrity of performance measurements.

Best Practices for Local Device Access Testing

- Ensure that the physical interface does not introduce unintended RF noise or interference, particularly in sensitive testing environments.
- Where needed, secure the physical connection using tape or similar means to keep the connection physically secure.
- Document the connection method used, and capture photographs of the setup.

Remote Device Access

Testing with remote device access utilizes an external network—such as an isolated Wi-Fi connection (e.g. 2.4/5 GHz) or cellular connection—to interface with the DUT. This method is advantageous in scenarios where direct physical access is limited.

- **Limited Physical Access** - In large-scale deployments or extensive outdoor field tests, it may not be feasible to manually access each device. This is where remote device access is ideal.
- **Inconvenient Device Location** - Remote access enables ongoing monitoring and control without requiring test personnel to relocate, thereby improving operational efficiency and test continuity.

Note: The use of external networks for remote access, such as 3G cellular, may introduce interference in Wi-Fi HaLow operating channels. Consult your national regulatory body and conduct a pilot comparison before using this form of remote device access in the field to ensure it does not compromise the accuracy of test results.

Best Practices for Remote Device Access Testing

- Utilize a reliable and isolated backhaul connection for remote device access to ensure stable and interference-free communication.
- Refrain from using the Wi-Fi HaLow network under test for device management or data collection, as this can introduce additional load and interference that may compromise the accuracy of test results.
- Employ secure communication protocols—such as SSH or VPN tunnels—to safeguard data integrity and maintain secure access to the DUTs.
- Continuously monitor the latency and reliability of the remote access link, as fluctuations can impact command responsiveness, and data retrieval.

While Morse Micro engineers prioritize local device access for testing due to its reliability and low setup overhead, remote device access is necessary in specific scenarios—such as long distance

range testing—where the station device is mobile, and the test scale is extensive. An example remote device access setup is outlined in the [Range Test Case Study](#).

4.4.5. Sanity Checks

Recommended sanity checks before test execution include:

- Powering on all the devices using the intended test power source.
- Confirming that the software and hardware versions are correct and up to date.
- Verifying that all device interfaces are correctly initialized.
- Validating that all HaLow devices pairs successfully associate at close range.
- Confirming that iPerf can be executed manually on the Wi-Fi HaLow interfaces.

5. Test Execution

5.1. RF Spectrum Capture

Before conducting any field test, Morse Micro advises to capture the RF spectrum at the test site. This establishes the environmental noise floor and identifies any sources of interference. The main interference of concern is interference inside the DUT's operating bandwidth. Any in-band interference will directly mix with the Wi-Fi HaLow signal, reducing the Signal-to-Noise Ratio (SNR) and degrade performance. It is also important to consider the near-band interference, which can have indirect effects on the device performance. Some possible interference effects are:

- **Adjacent Channel Interference** - Leakage from nearby frequencies into the operating channel, especially when nearby transmitters are very strong.
- **Intermodulation** - Nonlinear mixing of two or more signals, often from nearby transmitters, producing spurious signals that may fall into the operating band and degrade receiver performance.
- **Receiver Desensitization** - Strong nearby signals overwhelm the receiver's front end, reducing sensitivity to desired weak signals.

5.1.1. RF Spectrum Capture Best Practices

To facilitate comprehensive test result analysis, it is crucial to measure the RF spectrum at both ends of the communication link.

- **Capture Location** - Conduct and log RF spectrum captures at all relevant DUT positions to identify local environmental noise and potential interference sources.
- **Spectrum Ranges** - Acquire measurements across in-band, near-band, and out-of-band frequency ranges to obtain a comprehensive interference profile. For example, when conducting a test in the 8MHz operating bandwidth in the AU country region, the following ranges would give a comprehensive read of the RF environment:
 - In-band: 8MHz span centered at 924MHz.
 - Near-band: 20MHz span centered at 924MHz.
 - Out-of-band: 200MHz span centered at 924MHz.
- **Baseline and Monitoring** - Establish a baseline noise profile with all DUTs powered off, and perform periodic re-captures throughout the testing session to monitor for temporal RF variations.
- **Antenna Orientation** - Use one or more of the antennas deployed in the test setup during spectrum capture. The spectrum analyzer should be held in a manner that replicates the antenna orientation used during testing, to maintain measurement fidelity.

For reliable results, position and align antennas precisely and thoroughly document all analyzer settings (e.g., resolution bandwidth, reference level). Set the analyzer's reference level

approximately 5–10 dB above the expected signal peaks to prevent distortion while preserving measurement resolution. For example, if signals are expected around –40 dBm, a –30 dBm reference level provides enough headroom for strong peaks and ensures accurate, clean captures.

5.1.2 Recommended Spectrum Analysis Tools

The Signal Hound BB60D is a real-time portable spectrum analyzer that is very helpful for RF spectrum captures in the field. This device is portable and compact and offers good dynamic range, capture speed, and accuracy.



Figure 1: Signal Hound BB60D Spectrum Analyzer

For detailed, device-specific spectrum capture procedures, recommended tools, and analysis techniques, refer to Appendix A.

5.2. Software Tools For Field Testing

A variety of established throughput and diagnostic tools are available to support Wi-Fi HaLow field-testing. At Morse Micro, the primary tool used to evaluate throughput performance of Wi-Fi HaLow devices is **iPerf**.

5.2.1. iPerf Test Software

Accurate throughput measurement is a critical component of Wi-Fi HaLow field-testing. To facilitate this, iPerf is widely used for generating and measuring both TCP and UDP traffic between devices. This tool is pre-installed on all Morse Micro OpenWrt-based evaluation kits, including the MM6108-EKH01-05, MM8108-EKH01-01, MM8108-EKH19-01, and MM-HL1-EXT platforms.

For development kits based on the proprietary MM IoT SDK—such as MM6108/MM8108 EKH05 and MM6108 EKH08—iPerf2 is utilized as a lightweight and efficient alternative. To ensure optimal radio performance, all DUTs should operate on the latest firmware version with the appropriate Board Configuration File (BCF).

Local Command Execution

Execute commands directly on the DUT via local (e.g. USB/Ethernet) or remote (e.g. 2.4GHz Wi-Fi) access.

- Server Mode: The traffic receiving device runs the iPerf Server.
- Client Mode: The transmitting device initiates traffic to the server.

Traffic Direction

It is recommended to evaluate both uplink (STA → AP) and downlink (AP → STA) performance to validate the performance of each DUT's HaLow radio in both transmission and reception modes. This is particularly critical in long-range or high-interference environments, where device placement and surrounding conditions may cause asymmetry in the communication link.

Session Management

Prior to initiating a new iPerf test, it is advisable to terminate any previously active iPerf sessions. This prevents conflicts and overlapping data streams that may compromise the accuracy of performance measurements.

5.2.2. iPerf Test Parameters

The iPerf tool invokes command line arguments that act as test parameters for each iPerf test. Some important parameters used in testing are given below. Refer to the iPerf documentation for a full list of parameters.

5.2.3. Parameters Common to iPerf2 and iPerf3

- **Bitrate: -b <bitrate>** - For UDP tests, set a target bitrate that reflects expected deployment scenarios. Excessively high bitrates can overload device host processors (as the packets need to be randomly generated) and cause artificially low throughput readings. Typically, Morse Micro engineers set this value as "31M" i.e. 31Mb/s.
- **Test Duration: -t <time>** - Short tests (10–20 seconds) are usually sufficient, but a longer test can be used to validate stability as the rate control algorithm settles.
- **UDP Mode: -u** - Uses UDP instead of the default TCP.
- **Interval: -i <interval>** - Reports results every <interval> seconds.

5.2.4. Parameters Specific to iPerf3

- **Initial Delay (Omit Time): -O <omit time>** - Include an initial delay, generally around 5 seconds, to account for TCP protocol slow start.
- **Reverse Mode: -R** - Reverses the direction of the traffic. Used to switch between uplink and downlink testing.

5.2.5. Other Testing Tools

In addition to iPerf2 and iPerf3, several supplementary tools can be used which provide additional diagnostic and troubleshooting capabilities:

Wireshark/tcpdump

Wireshark and **tcpdump** are widely used tools for capturing and analyzing packet-level traffic between DUTs. These tools enable detailed inspection of protocol interactions, detection of retransmissions or packet loss, and identification of potential low-level performance bottlenecks.

Ping

Ping is a simple tool for performing latency and connectivity checks. It provides a quick way to monitor round-trip times and packet loss rates, serving as a preliminary stability assessment before running further in-depth throughput testing.

OpenWrt Diagnostic Utilities

OpenWrt includes some utilities that can be used to provide valuable diagnostic insights, for example:

- **iw** and **iwinfo** allow monitoring of signal strength, noise levels, and link quality.
- **ip** commands report the interface status and IP address configurations.
- **route** gives information useful for debugging IP routing issues.

Alternative Performance Tools

While iPerf2 and iPerf3 remain the preferred tools for throughput testing, alternatives such as **netperf** and **nttcp** can be used if specific test scenarios or legacy compatibility requirements arise.

Custom Automation Scripts

For large-scale field deployments or repetitive testing, custom scripts (using Python or shell) can help to automate test execution, log collection and data analysis. This will ensure consistency across test scenarios and facilitates generation of comprehensive performance reports.

6. Data Capture and Debugging

Effective testing of Morse Micro Wi-Fi HaLow devices hinges on structured data collection across four key areas:

- Modulation and Coding Scheme (MCS) behavior.
- Received Signal Strength and link quality.
- Traffic and throughput.
- Association stability.

Instead of repeating commands throughout, we focus below on what to **observe, analyze, and optimize**, with the full command reference in the summary table at the end.

6.1. Rate Control Metrics

Understanding dynamic adaptations of the MCS rate and bandwidth sheds light on link efficiency and device responsiveness to environmental changes.

What to Watch:

- Sudden drops or frequent toggling in MCS index.
- High retry counts despite high SNR.
- Misalignment between theoretical and actual throughput.

Diagnostic Actions:

- Logging MCS trends over time.
- Filtering for high-retry MCS levels.
- Correlating MCS changes with link quality dips.

6.2. Signal Strength and Link Quality (RSSI, SNR)

Signal and noise metrics are fundamental for diagnosing physical layer issues, like poor antenna alignment or interference.

What to Watch:

- RSSI fluctuations tied to movement.
- SNR degradation in high-traffic zones.

Optimize By:

- Smoothing RSSI data using moving averages.
- Logging alongside GPS or location data.
- Comparing SNR with retry and error rates.

6.3. Traffic and Throughput

Packet counts, retry ratios, and error rates are crucial to identify bottlenecks or firmware misbehavior under load.

What to Watch:

- Disparities in Tx/Rx counts in chip statistics.
- High Tx errors or low throughput despite good link metrics.
- Correlation between increased load and retransmissions.

Optimize By:

- Visualizing traffic over time using Grafana or Python scripts.
- Logging Tx/Rx counters periodically for long-term trend analysis.

6.4. Association & Link Stability

Validating persistent link association is critical for long-duration or roaming tests.

What to Watch:

- Peer MAC address dropouts.
- Repeated association/disassociation events.
- Sudden resets of uptime or connection counters.

Optimize By:

- Monitoring **dmesg** or kernel logs alongside **iw** output.
- Flagging unexpected MAC changes in automated test logs.

6.4.1. Summary Table of Commands

Metric	Command	Notes
Rate control & throughput	morse_cli -i wlan0 stats -j	JSON output for easy parsing.
Signal metrics (RSSI)	iw wlan0 station dump	Real-time link-level data.
Continuous rate stats	watch -n 1 "morse_cli -i wlan0 stats"	Snapshots every second. Some filtering with grep might be required for visibility.
Continuous signal stats	watch -n 1 "iw wlan0 station dump"	Real-time updates for signal strength.

Association status	<code>iw wlan0 station dump</code>	Check peer MAC and link status.
MMRC (Morse Micro Rate Control) Table	<code>cat /sys/kernel/debug/ieee80211/phy0/morse/mmrc_table_csv</code>	MMRC Table.

Table 1: Helpful debug commands

6.5. Test Data Interpretation Guidance

Interpreting the data collected during field-testing is critical for evaluating the performance and reliability of a Wi-Fi HaLow deployment. The following framework provides guidance for analyzing key performance indicators:

6.5.1. Throughput Trends

Examine throughput measurements—both uplink and down link, across TCP and UDP protocols—under various scenarios and distances. Consistently high and stable throughput indicates strong link quality, while notable declines may reveal performance bottlenecks or environmental interferences.

6.5.2. RSSI and Signal Quality

Evaluate Received Signal Strength Indicator (RSSI) and Signal-to-Noise Ratio (SNR) to determine whether device orientation and placement are optimal. Persistently low RSSI values may suggest misalignment, excessive path loss, or suboptimal antenna configuration.

6.5.3. Association Stability

Track disassociations or connection losses throughout the test period, particularly in range-based or multi-station test scenarios. Frequent link instability may point to configuration issues or hardware limitations that warrant further investigation.

6.5.4. Environmental Influence

Leverage RF spectrum captures and GPS-based location data to correlate observed performance with environmental conditions. Identify patterns of degradation that coincide with known interference sources, physical obstructions, or changes in terrain.

6.5.5. Edge Case Behavior

In multi-station testing, Morse Micro measures how the access point performs under both **simultaneous** and **staggered** traffic load scenarios:

- **Simultaneous traffic** - All devices send data at the same time, creating a burst of activity that stresses the network and exposes its limits.
- **Staggered traffic** - Devices send data at slightly offset times, simulating more realistic behavior where activity is distributed and the network operates under a rolling load.

Analyzing these scenarios provides a deeper understanding of the access point's scalability and its ability to manage dynamic, unpredictable client behavior. This structured approach transforms raw test results into actionable insights, supporting performance optimization and guiding informed deployment of your Wi-Fi HaLow network.

7. Optimizing Wi-Fi HaLow Network Performance

To achieve the best possible performance from your Wi-Fi HaLow network, consider these key factors:

7.1. Device Height and Placement

- **Elevation Matters** - Raising antennas helps to overcome obstructions and extend signal range. Aim for an elevation that minimizes Fresnel zone interference. In many field tests, a height of approximately 2.8 meters is a good starting point. Adjust based on the specific environment.
- **Clear Line of Sight (LOS)** - Where possible, establish a clear, unobstructed path between devices. Even small obstacles can significantly reduce signal strength.
- **Minimize Clutter** - Keep the area around antennas clear of objects that might absorb or reflect radio waves.

7.2. Avoiding Metal Near Antennas

- **Metal Reflects RF** - Metal surfaces can reflect radio frequency (RF) signals, leading to multipath interference and reduced signal strength.
- **Keep Distance** - Ensure that antennas are located a reasonable distance from large metal objects, such as metal walls, roofs, or large appliances.
- **Antenna Orientation** - If unavoidable metal objects are present, experiment with antenna orientation to minimize negative impacts.

7.3. Bandwidth and Channel Optimization

- **Channel Selection** - Choose a channel with minimal interference. Conduct a spectrum scan using tools like the Signal Hound BB60D (as mentioned in [Appendix A](#)) to identify occupied frequencies and select a clear channel.
- **Channel Width** - Wi-Fi HaLow may offer different channel bandwidth options. Selecting the appropriate bandwidth will depend on the deployment and testing scenario and consider the trade-off between throughput and range. Wider bandwidths generally allow for higher throughput, but may also be more susceptible to interference and have shorter ranges.
- **Minimize Co-Channel Interference** - If multiple networks are in close proximity, ensure each is operating on a different channel to avoid co-channel interference.

7.4. Environment Considerations

- **Trees and Foliage** - Vegetation can absorb RF signals, especially at higher frequencies. In areas with dense foliage, consider elevating devices higher or finding more open paths.
- **Weather Conditions** - Weather conditions, such as rain or humidity, can sometimes affect signal propagation. While Wi-Fi HaLow is designed for robustness, documenting weather conditions during testing is important for context.
- **Terrain** - Hills or valleys can create shadowing effects or alter signal paths. Evaluate terrain when planning device placement.

7.5. Cable Management

- **Cable Quality** - Use high-quality cables that are properly shielded to reduce interference and signal loss.
- **Cable Routing** - To reduce interference, avoid running sensitive signal cables (e.g., RF, USB) alongside power cables or near electrical noise sources. While Ethernet and power cables are less susceptible, maintaining cable separation is still recommended.
- **Cable Length**: Minimize cable length where possible. Longer cables can lead to signal attenuation.

7.6. Diagnostics and Monitoring

- **Real-Time Metrics** - Utilize tools like **morse_cli** and **iw** to monitor real-time metrics such as RSSI, SNR, and retry rates. These metrics provide valuable insights into link quality and potential issues.
- **Log Analysis** - Regularly review logs for errors or performance anomalies. Use this information to fine-tune network settings and troubleshoot problems.

By considering these factors, the user can significantly improve the performance and reliability of their Wi-Fi HaLow network.

8. Field Test Case Studies

A comprehensive field-testing program for Wi-Fi HaLow devices comprises multiple test types, each designed to evaluate specific dimensions of device performance and environmental resilience. These tests are critical in verifying that the devices meet operational standards and perform reliably under real-world conditions.

To illustrate the application of these methodologies, the following chapter presents detailed case studies focused on three foundational test scenarios that form the core evaluation framework at Morse Micro:

- **Over-the-Air (OTA) Static Test** - Evaluates device performance in both Line-of-Sight (LOS) and Non-Line-of-Sight (NLOS) environments, with emphasis on throughput and link stability across varying propagation conditions.
- **Multi-Station OTA Test** - Assesses network behavior under concurrent loads from multiple devices, providing insight into access point scalability, collision handling, and overall throughput distribution.
- **Range Test** - Measures performance across increasing distances to define the effective operational range and evaluate link quality at the fringe of coverage.

These case studies provide practical guidance on structuring and executing field tests, while also offering a framework for interpreting the resulting data to inform deployment strategies and product enhancements.

Prior to executing each test, the RF noise environment is characterized using a Signal Hound BB60D Spectrum Analyzer. The table below summarizes the average and maximum in-band Power Spectral Density (PSD) values recorded at the selected test locations.

The following table provides example data to illustrate typical environmental noise observed during site characterization. These values are representative only and may vary based on time, location, and environmental conditions.

Location	Google Maps Link	In-Band PSD (dBm/Hz)
Narabeen Beach	📍 Narrabeen Beach	-154.62 (Average) -147.34 (Maximum)
Parade Grounds Centennial Park	📍 Parade Grounds	-154.27 (Average) -150.99 (Maximum)
Seven Mile Beach	📍 Seven Mile Beach	-155.31 (Average) -151.61 (Maximum)

Table 2: Typical environmental noise at select locations.

8.1. Testing Scenarios Overview

To ensure Morse Micro Wi-Fi HaLow devices perform reliably in real-world conditions, the devices are tested in a variety of outdoor environments. These test setups fall into two categories:

- **Line-of-Sight (LOS)** - Devices are placed with a clear, unobstructed path between them. This allows us to measure maximum performance, such as range and speed, under ideal conditions.
- **Non-Line-of-Sight (NLOS)** - Devices are tested in more realistic, obstructed environments (e.g. behind buildings or trees), where interference and obstacles affect performance—similar to what you'd find in urban or industrial settings.

8.1.1. Why This Matters

These scenarios help to:

- Benchmark best-case performance (LOS).
- Understand how the devices handle real-world challenges (NLOS).
- Optimize the technology to meet different deployment needs (e.g., smart cities, agriculture, logistics).

8.2. OTA Case Study

8.2.1. Theory of Operation

The Over-the-Air (OTA) test evaluates Wi-Fi HaLow performance by positioning a pre-configured Access Point (AP) and Station (STA) at a fixed distance to establish a wireless link. Devices are associated over the HaLow interface, and network traffic is generated using **iPerf3** to measure throughput in both directions (uplink and downlink) across **UDP** and **TCP** protocols. This test is conducted under controlled conditions and serves to validate baseline throughput and link stability, providing a reference for comparison with other test scenarios.

8.2.2. Methodology

This test setup comprises a single Access Point (AP) and Station (STA) pair. While fully controlled environmental conditions are not feasible in over-the-air (OTA) testing, efforts are made to ensure reasonable consistency across test runs. Both Line-of-Sight (LOS) and intentionally configured Non-Line-of-Sight (NLOS) scenarios are assessed to establish baseline performance across representative propagation conditions.

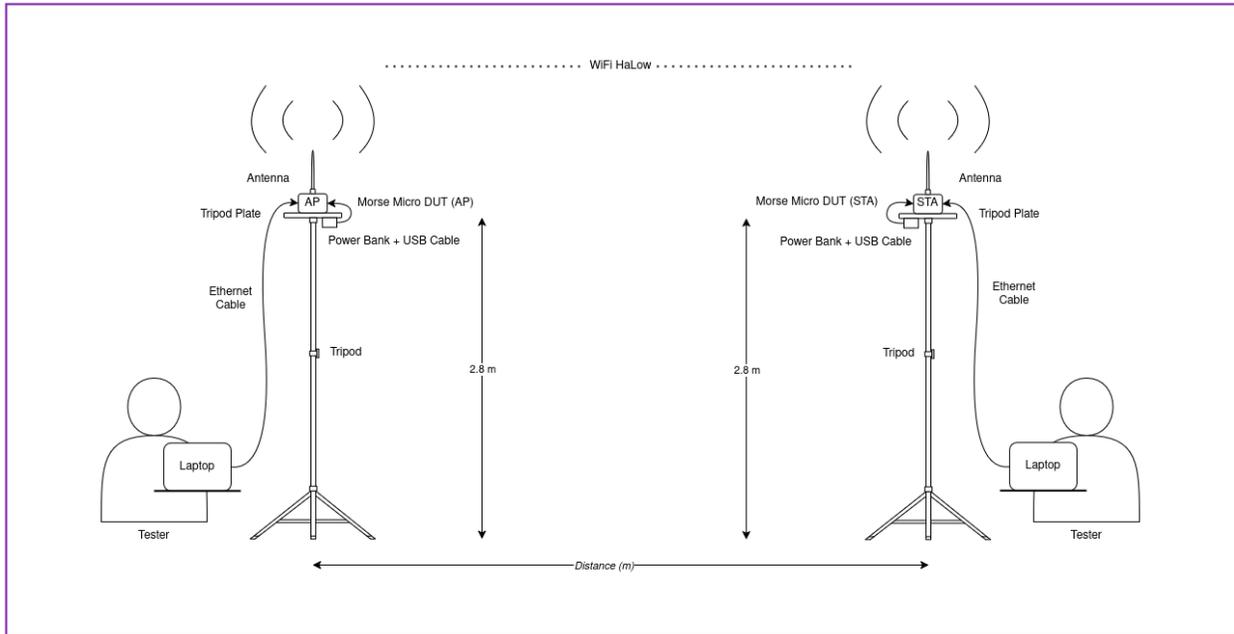


Figure 2: OTA diagram.

Equipment

Ensure the following items are available and prepared before initiating the test:

- **Devices Under Test (DUTs)** – Pre-configured with appropriate firmware and network settings.
- **Tripods (×2)** – For stable elevation of each DUT during testing.
- **Plastic Tripod Plates (×2)** – To mount and support multiple DUTs on each tripod.
- **Pulse Larsen W1063M Antennas (×2)** – 1 dBi gain dipole antennas, compatible with Morse Micro evaluation kits.
- **Ethernet Cables (×2, 5 meters)** – For wired communication and device configuration. If the laptop lacks a built-in Ethernet port, an appropriate USB-to-Ethernet adapter (USB-A or USB-C) will be required.
- **Portable Power Banks (×4)** – With USB power cables to supply reliable power to all DUTs.
- **Spectrum Analyzer** – Including necessary RF cables for capturing environmental noise and interference levels.
- **RF Tape (≥1 roll)** – For securing cables and components.
- **Scissors (×1 pair)** – For trimming tape and other materials as needed.
- **Laptops (×2)** – Equipped with Ethernet adapters for test control and data collection.
- **Protective Storage Case (e.g. Pelican case)** – For safe transport and storage of devices and accessories.

Note: Verify that all equipment is fully functional and charged (where applicable) prior to deployment.

Preparing the DUTs

To ensure reliable and repeatable Over-the-Air (OTA) test results, prepare the Morse Micro evaluation kits as follows:

1. Firmware Installation

- Ensure that all evaluation kits are running the latest applicable **OpenWrt** firmware.
- For **MM6108-EKH01-05US** and **MM8108-EKH01-01** models, remove and flash the micro-SD cards to streamline the update process.

2. Country Code Configuration

- Refer to the **Evaluation Kit User Guide** and configure the country code according to the geographic location of the test to ensure regulatory compliance.

3. Network and Device Settings

- Retain the default device **hostname** and leave the **password field empty** unless otherwise required.
- Configure one device as the **Access Point (AP)** and the other as the Station (STA).
- Maintain default **Ethernet IP addresses** (typically **10.42.0.1**).
- Set the **HaLow network password**.
- Assign static **HaLow IP addresses**, e.g:
 - AP: **192.168.1.1**
 - STA: **192.168.1.2**

4. SSID Assignment

- Use the same SSID for each individual device pair.
- Assign **unique SSIDs** for different device pairs to avoid unintended associations (e.g. **mm6108-ekh01-ota**, **mm8108-ekh01-ota**).

5. Device Association Verification

- Confirm device association using the web UI or SSH with commands such as:
 - **iwinfo**
 - **iw wlan0 station dump**
 - **iw wlan0 link**
- Perform a basic connectivity check using ping or an initial iPerf test to validate link functionality.

6. Pre-Test Separation Requirements

- Before running iPerf3, ensure that:
 - Devices are connected with **≥30 dB attenuation**, or
 - Devices are fitted with antennas and spaced **at least 1m apart**.

7. Identification and Labelling

- Physically label each device with identifying information (e.g., IP address, role, SSID) to reduce confusion and ensure correct test execution during field deployment.

Following these steps will ensure that devices are correctly prepared, reducing variability and supporting consistent, high-quality test results.

Test Execution Procedure

To ensure consistent and reliable test results, follow the steps below during Over-the-Air (OTA) test execution:

1. Site Setup

- Transport all required equipment to the test location.
- Assess and document the **environmental conditions** (e.g., temperature, weather, RF surroundings).

2. RF Baseline Capture

- With all devices powered off, perform a baseline **RF spectrum scan** to establish the ambient noise floor at the test site.

3. Device Initialization and Association

- Power on the Access Point (AP) and Station (STA).
- Verify device association using terminal commands such as:
 - **iwinfo**
 - **iw wlan0 station dump**
 - **iw wlan0 link**

4. Throughput Testing (iPerf3)

- Execute iPerf3 tests in the following traffic directions to assess bidirectional and protocol-specific performance:
 - **UDP uplink** (STA → AP)
 - **UDP downlink** (AP → STA)
 - **TCP uplink** (STA → AP)
 - **TCP downlink** (AP → STA)

5. Test Repetition and Variation

- Repeat each test multiple times to ensure consistency.
- Vary **device orientation** and **distance** to capture performance across different propagation scenarios.
- Use **interleaved test runs** to reduce the influence of environmental variability over time.

6. Multi-Location Testing

- Relocate the device pair to each designated test position and repeat the above steps at each site.

7. Data Collection

- Collect and organize all relevant **iPerf3 logs**, **association status outputs**, and **spectrum analyzer snapshots** for post-test analysis.

Adhering to this structured procedure ensures high-quality data collection and meaningful comparison across test scenarios and locations

Key Metrics to Capture

During each test scenario, ensure the following data is recorded for comprehensive performance analysis:

- **Throughput Results** - Measured using iPerf3 for both uplink and downlink across TCP and UDP protocols, with throughput reported in units such as Kbps, Mbps, or Gbps. Use the `-f` option (e.g., `-f m` for Mbps) to select the preferred unit format.
- **Link-Level Metrics** - Collected via `morse_cli` and `iw`, including:
 - Received Signal Strength Indicator (RSSI).
 - Signal-to-Noise Ratio (SNR).
 - Link margin.
 - Additional radio-level statistics as applicable.
- **Association Status** - Verify that the AP and STA maintain continuous association throughout the test duration to ensure data validity.
- **Environmental Noise Floor** - RF spectrum data captured using a spectrum analyzer to characterize in-band and near-band interference conditions at each test location.

Capturing these metrics enables accurate interpretation of test results and supports effective debugging and performance optimization.

Script Automation

To enhance efficiency and ensure consistency, iPerf3 testing and metric logging should be **automated using scripts**. These scripts should be designed to:

- Verify device association prior to each test run.
- Initiate traffic generation for all test directions and protocols.
- Capture and store throughput results, link-level statistics, and environmental data.

By automating these tasks, the test process becomes more repeatable, less prone to human error, and significantly more scalable across multiple scenarios and locations.

8.2.3 OTA Field Test Images



Figure 3: 2x DUT pair test.

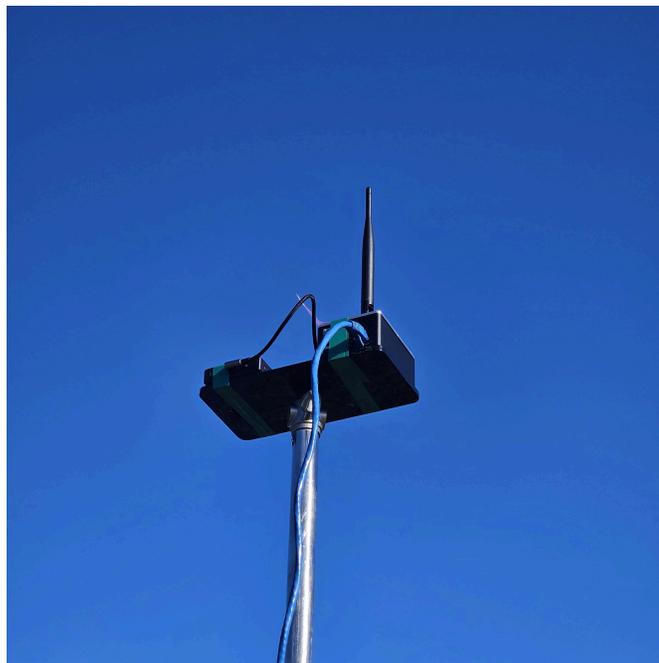


Figure 4: Elevated DUT setup.

8.3. Multi-Station Over-the-Air Case Study

8.3.1. Theory of Operation

The **multi-station Over-the-Air (OTA)** test builds upon the standard OTA methodology to assess the performance of a single Wi-Fi HaLow Access Point (AP) under concurrent load from multiple Stations (STAs). Two configurations are tested: point to multi-point (AP → STAs, downlink), and multi-point to point (STAs → AP, uplink). Each of these configurations is also tested with both UDP and TCP protocols.

When operating in downlink mode, a single **iPerf2** server is started on each STA and multiple iPerf2 clients, each connecting to one STA, are started on the AP. In uplink mode, each STA executes one client all connecting to the same iPerf2 server running on the AP.

As a result, throughput is measured for **UDP uplink, UDP downlink, TCP uplink, and TCP downlink** for each STA. This test simulates real-world scenarios in which multiple devices connect, transmit, and receive data simultaneously, providing insight into the AP's capacity, scalability, and ability to manage concurrent traffic streams.

8.3.2 Methodology

This test may be conducted using various physical configurations and device placements, depending on the specific real-world scenario being simulated. Common layout strategies include:

- **Equidistant Radial Layout** - Stations (STAs) are symmetrically positioned around the Access Point (AP) to establish uniform Line-of-Sight (LOS) conditions, ideal for baseline multi-client performance evaluation.
- **Asymmetric Layouts** - STAs are placed at varying distances from the AP—such as near/far or in a linear corridor—to emulate diverse network topologies and examine range-based performance variability.
- **Dense Cluster Testing** - Multiple STAs are positioned in proximity to evaluate the AP's ability to manage collisions, congestion, and simultaneous transmission events in high-density deployments.

These configurations help to characterize the AP's behavior under differing spatial and interference conditions, offering insights into deployment-specific performance.

Each test includes two **edge-case load scenarios** designed to fully characterize the Access Point's (AP's) performance under high-demand conditions:

- **Simultaneous Start/Stop** - All Stations (STAs) initiate data transmission concurrently and cease transmission at the same time. This scenario simulates peak concurrent load, providing

insight into the AP's ability to handle maximum simultaneous traffic and smoothly transition between low and high load.

- **Staggered Start/Stop** - STAs join the network at predefined intervals, initiating data transmission as they connect. Once all STAs are active and transmitting, they disconnect in the same staggered sequence. This scenario mimics incremental and dynamic network loading and unloading, closely resembling behavior in real-world deployments where devices connect and disconnect over time.

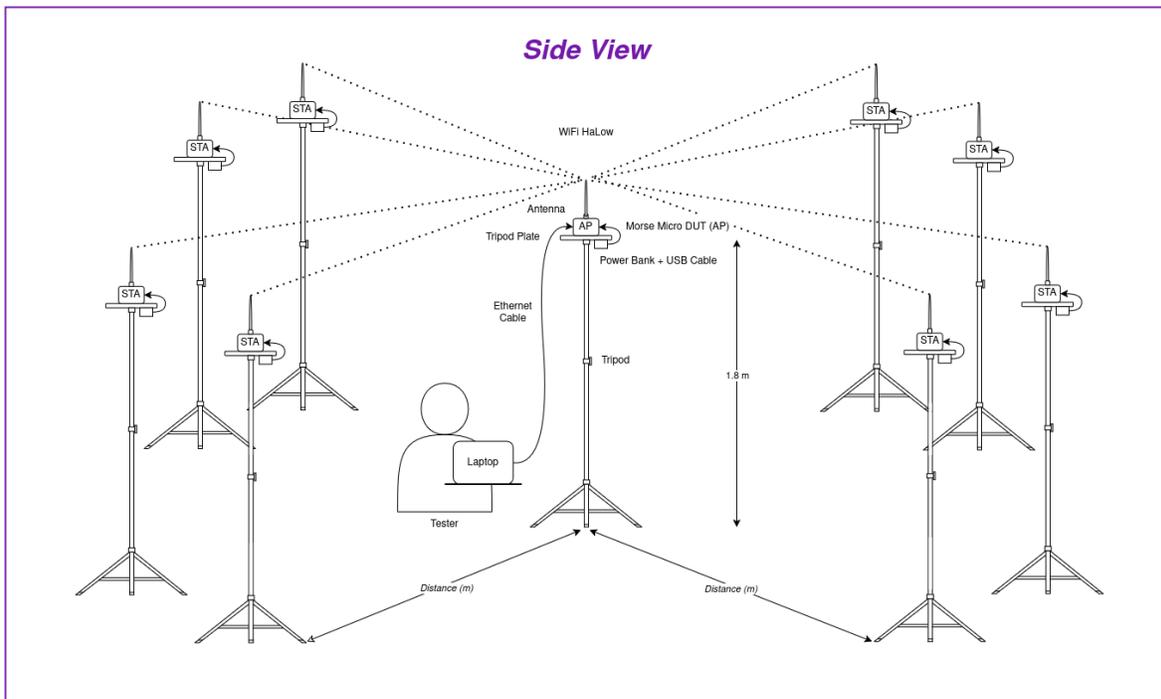


Figure 5: Multi-station OTA side view.

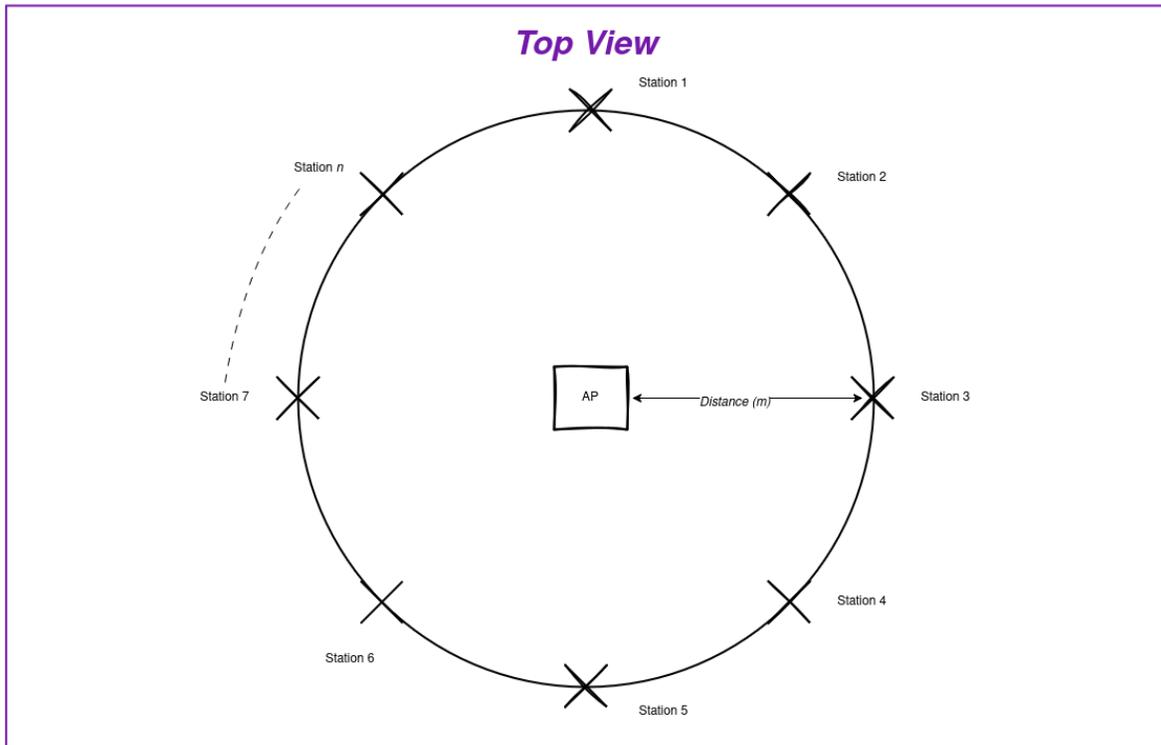


Figure 6: Multi-station OTA top view.

Preparing the DUTs

Prior to deployment, complete the following steps to ensure all DUTs are properly configured for multi-station testing:

- **Firmware Installation** - Install the latest OpenWrt firmware images on all DUTs to ensure consistent performance and compatibility.
- **HaLow IP Addressing** - Assign each STA a unique and intuitive static IP address within the HaLow subnet (e.g. 192.168.1.2, 192.168.1.3, etc.), and configure the AP with the standard address 192.168.1.1.
- **Ethernet Interface Configuration** - Set Ethernet interface IPs uniformly across all devices (e.g. 10.42.0.1) in case debugging or configuration changes are required.
- **Device Labelling** - Physically label each DUT with its assigned IP address and station number to prevent setup errors and simplify data correlation during testing.
- **Connectivity Validation** - Confirm successful associations between the AP and all STAs by conducting ping tests or short iPerf2 sessions prior to field deployment.

Proper preparation of DUTs is critical to minimize errors in the field and ensure consistent, high-quality test results across all stations.

Conducting the Test

Site Preparation:

- Perform RF spectrum scans to document the environmental noise profile and identify potential sources of interference.

Device Placement:

- Position the Access Point (AP) and all Stations (STAs) according to the predetermined **physical layout** (e.g., radial, asymmetric, or clustered).
- Maintain **consistent antenna height and orientation** across all devices. Clearly document whether the scenario is Line-of-Sight (LOS) or Non-Line-of-Sight (NLOS) for test reproducibility.

Baseline Validation:

- Access the AP via SSH to verify that all STAs have successfully associated.
- Perform brief ping tests or short iPerf2 runs to validate basic connectivity and link performance prior to executing the full test.

8.3.3. Edge-Case Load Scenario Testing

Simultaneous Start/Stop

- Initiate UDP and TCP traffic in both uplink and downlink directions from all STAs simultaneously.
- Measure and record aggregate throughput, per-station performance, and AP handling capacity under peak concurrent load conditions.

Staggered Start/Stop

- Start traffic to/from stations at defined time intervals.
- After all STAs are active, terminate traffic in the same staggered order.
- Monitor how network performance scales and stabilizes throughout the load buildup and release phases.

8.3.4. Repeat Testing and Variability Assessment

- For deployments involving multiple device sets, repeat the entire testing process to compare performance across hardware batches.
- Explore additional configurations—such as varying antenna placement, heights, or topologies—to simulate different real-world deployment scenarios and validate robustness under varied conditions.

Thorough execution of this procedure enables a complete assessment of network scalability, performance distribution, and access point resilience under real-world multi-client conditions.



Figure 7: Multi-station setup pre-elevating DUT devices.

8.4. Range Test Case Study

8.4.1 Theory of Operation

The range test is designed to evaluate the maximum operational distance of Wi-Fi HaLow links under real-world conditions. This test is performed by gradually moving the Station (STA) away from a fixed Access Point (AP), while conducting short, repeated throughput tests. These frequent measurements provide high-resolution insight into how performance degrades with distance.

Short test intervals are used to enable the capture of different throughput metrics (i.e. protocols and directions), and to interleave measurements from different devices, minimizing the impact of environment changes over time (e.g., wind, movement of people, transient interference).

To correlate throughput with actual distance, GPS dongles are employed. Additionally, a dedicated LTE dongle is used to backhaul test results to the cloud in real time, ensuring that no performance data is transmitted over the HaLow link under test. This separation maintains the integrity of the throughput measurements.

8.4.2 Methodology

The range test can be conducted using one of two methods, depending on the requirements of the deployment scenario:

- **Continuous Method** - The Station (STA) is moved gradually away from the Access Point (AP), with throughput measurements taken at regular intervals during continuous motion. This approach provides a high-resolution view of performance over distance.
- **Discrete Method** - The STA is relocated in predefined steps to specific test points, pausing at each location to conduct throughput tests. This might be more efficient and simplify logistics under some scenarios.

In both methods, testing is conducted with only one HaLow interface pair active at any given time, thereby minimizing radio frequency (RF) interference and ensuring clean, isolated data collection.

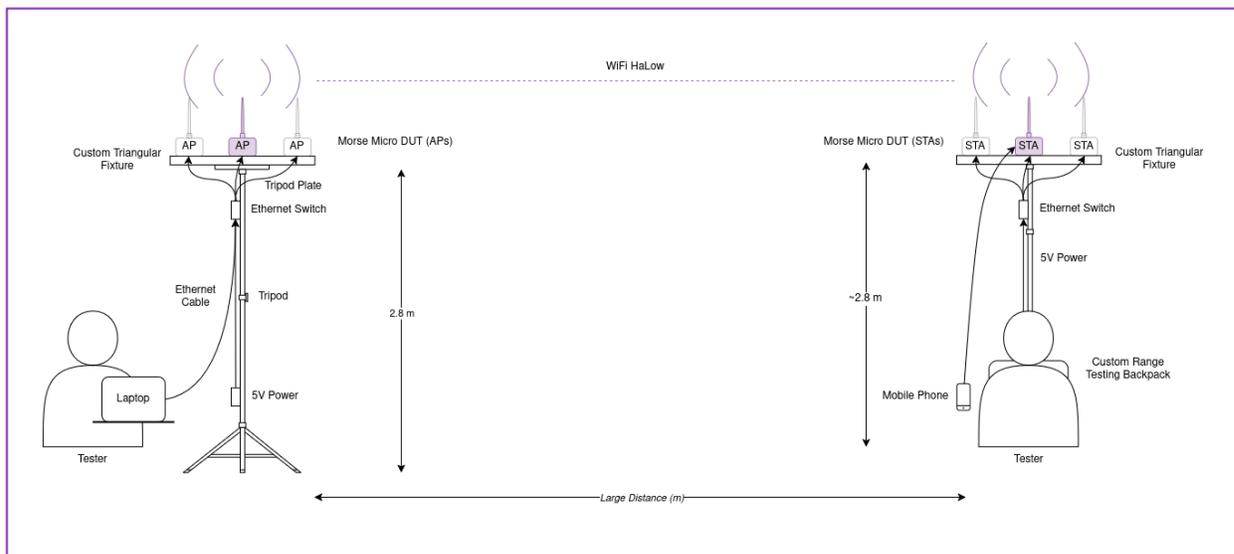


Figure 8: Range Test setup (side view).

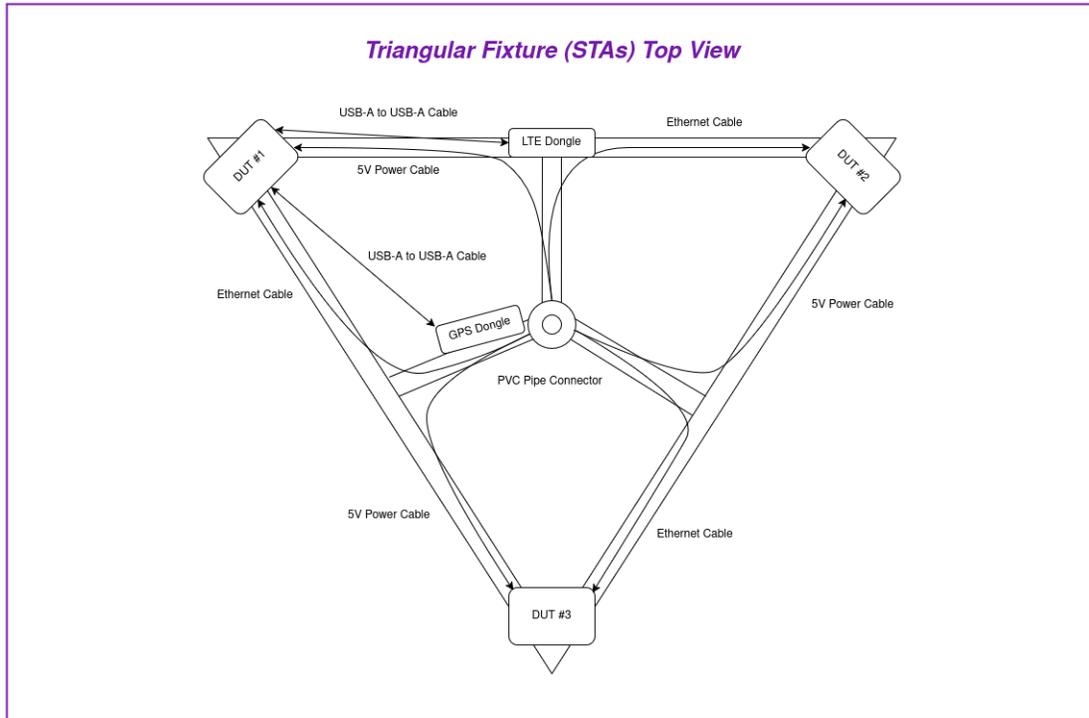


Figure 9: Range Test triangular fixture (top view).

Device Configuration and Preparation

To ensure consistent and reproducible results during range testing, apply the following configuration steps to all DUTs:

- **Firmware Installation** - Install the latest OpenWrt firmware images on all DUTs to guarantee optimal performance and compatibility with testing tools and configurations.
- **Static IP Configuration** - Assign static IP addresses to each DUT to avoid address conflicts.
 - Use intuitive HaLow addressing schemes—for example:
 - AP: 192.168.1.1
 - STA: 192.168.1.2
 - Configure Ethernet interfaces with a consistent out-of-band control address (e.g., 10.42.0.1 (DUT1), 10.42.0.2 (DUT2), 10.42.0.3 (DUT3)).
- **IP Conflict Mitigation**- Ensure that the chosen static IP range does not overlap with common DHCP pools, particularly when using remote connectivity solutions such as phone hotspots, 4G dongles, or portable routers.
- **Labeling and Identification** - Physically label each DUT with its assigned IP address and role (e.g., AP or STA) to prevent confusion during field setup and data collection.
- **Connectivity Verification** - Conduct baseline ping tests between the AP and STA to confirm proper association and functional communication before initiating the range test sequence.

Accurate configuration and validation of DUTs are essential to ensure reliable performance measurements and streamlined field execution.

Remote Access and Connectivity

To enable secure and reliable control of the Devices Under Test (DUTs) and facilitate efficient data capture during field-testing, each DUT is connected to a Virtual Private Network (VPN) using OpenVPN configuration files. These configuration files are uploaded via the device's graphical user interface (GUI).

This VPN setup enables test engineers to:

- **Remotely access and manage each DUT** via SSH over an isolated and secure network connection.
- **Monitor test execution** by collecting and uploading performance data in real time.
- **Troubleshoot and reconfigure DUTs** as necessary—without requiring physical access to devices deployed in the field.

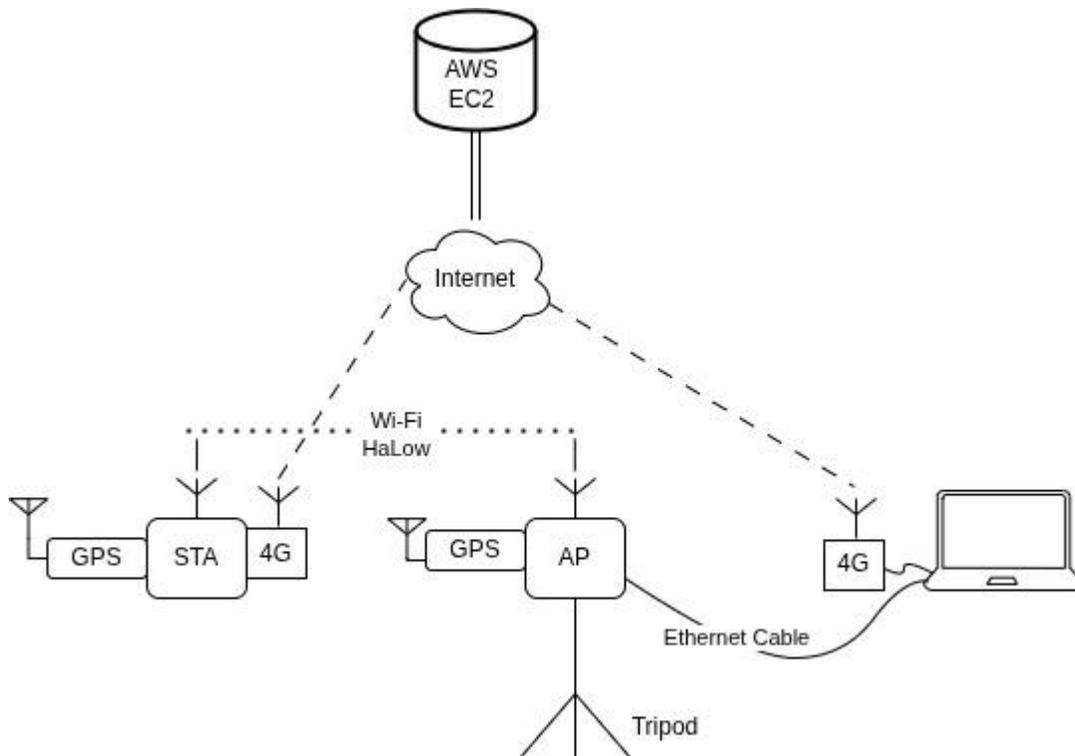


Figure 10: Remote Access setup.

Key Components of the Setup:

To support secure, real-time monitoring and control during range testing, the following system configuration is used:

Tester's Laptop:

- Connects to the internet via a cellular data hotspot, offering portability and flexibility in the field.
- Establishes a VPN tunnel for secure access and management of the Devices Under Test (DUTs).

Access Point (AP) Device:

- Wired directly to the tester's laptop using an Ethernet cable.
- Does not use a 4G connection independently; instead, it leverages the laptop's VPN connection to receive configuration commands and execute test scripts.
- Serves as the central node for Wi-Fi HaLow connectivity throughout the test.

Station (STA) Device:

- Equipped with a 4G USB dongle to provide independent internet backhaul.
- Establishes its own VPN tunnel over the cellular network, fully isolating management and telemetry traffic from the test network.
- Communicates with the AP over the Wi-Fi HaLow link, where all performance measurements are conducted.

Wi-Fi HaLow Link:

- Represents the test network connecting the AP and STA.
- All throughput and performance measurements are carried out over this link, ensuring test data is unaffected by control or backhaul communications.

This architecture allows test engineers to remotely manage devices, collect logs, and adjust test parameters in real time—without interfering with the performance of the network under evaluation.

Equipment

Ensure the following items are prepared and available before conducting the test:

- Wi-Fi HaLow Devices:
 - 2 × MM6108-EKH01
 - 2 × MM8108-EKH01
- Networking Hardware:
 - 2 × 5V Ethernet switches for connecting DUTs and test equipment
- Power Supply:
 - 6 × Portable power banks (with at least one spare for redundancy)
- Connectivity & Telemetry:

- 1 × GPS dongle for location tracking
- 1 × LTE dongle for cellular data backhaul
- Mounting Equipment:
 - Tripods and custom mounting fixtures (e.g. triangular backpack mounts)
 - Antennas compatible with DUTs
- Environmental Monitoring:
 - Spectrum analyzer with necessary cables to assess RF noise conditions
- Computing Equipment:
 - Laptops with chargers for controlling tests and collecting data
 - USB cables and adapters for power, data, and device interfaces
- Transport and Safety:
 - Protective carrying cases (e.g. Pelican cases)
 - Non-conductive tape for securing devices and cable management

Verify that all equipment is fully operational, charged, and labeled before deployment to ensure seamless execution in the field.

Conducting the Continuous Range Test

Follow the steps below to conduct a controlled, high-resolution range test of Wi-Fi HaLow devices:

1. Initial Setup
 - Mount the Access Point (AP) on a stationary tripod.
 - Mount the Station (STA) in a mobile configuration (e.g. backpack-mounted), with antennas securely attached.
 - Ensure all power banks are fully charged and properly connected.
2. Network & Device Initialization
 - Connect both AP and STA to the VPN network.
 - Attach the 4G USB dongle to the STA and the GPS dongles to both devices to enable real-time telemetry and location tracking.
3. RF Environment Validation
 - Use a spectrum analyzer to scan the test frequency band and confirm that the selected operating channel is free from interference.
4. Device and Script Activation
 - Power on both devices and the test laptop running automation scripts.
5. Test Execution – Continuous Walk
 - Begin the automated test loop:
 - Collect GPS location data from both AP and STA.
 - Run short-duration iPerf3 tests in all traffic directions:
 - TCP uplink and downlink
 - UDP uplink and downlink
 - Capture real-time statistics, including:
 - RSSI

- Chip-level metrics
 - MMRC (rate control) tables
 - Monitor results for anomalies and, if necessary, pause or abort the test for debugging.
6. Progressive Movement
 - Gradually walk away from the AP with the STA device while the test loop runs, continuing until device association is lost.
 7. Repeat Testing (if required)
 - Repeat the procedure using different device sets or configurations to collect comparative range data.

This methodology ensures high-resolution insight into performance degradation with distance and supports detailed analysis of link stability and range limits.

Conducting the Discrete Range Test

Follow the steps below to perform a range test using predefined measurement locations:

1. Initial Setup
 - Position the Access Point (AP) and Station (STA) on tripods at the designated starting location.
 - Connect the 4G and GPS dongles to their respective devices.
 - Power on both devices to begin system initialization.
2. Pre-Test RF Validation
 - Use a spectrum analyzer to record the ambient RF noise floor at the starting location.
 - Select a clear operating channel to avoid interference during testing.
3. Connectivity Check
 - Confirm device association between the AP and STA.
 - Verify that iPerf3 can be executed successfully in both directions.
4. Testing at Each Location at each predefined test point:
 - Collect GPS coordinates to establish exact positioning.
 - Capture relevant device performance metrics, including signal strength and rate control data.
 - Run iPerf3 tests for:
 - TCP uplink and downlink
 - UDP uplink and downlink
 - After testing, power down the devices, relocate the STA to the next location, and repeat the process.
5. Test Automation and Logging
 - Use a custom test script to automate test execution and data capture at each point.
 - Ensure all results are accurately timestamped and logged, enabling correlation with distance and environmental variables during analysis.

The discrete test method offers controlled, repeatable measurements across fixed distances, providing reliable data for range profiling and performance benchmarking.

Key Metrics to Capture

Ensure the following data points are collected at each test location to enable thorough performance analysis:

- **Throughput Measurements** - Collected using iPerf3 for both UDP and TCP, in uplink and downlink directions.
- **Signal Metrics** - Include Received Signal Strength Indicator (RSSI), Signal-to-Noise Ratio (SNR), and link stability indicators to assess connection quality.
- **Rate Control Data** - Extract MMRC (Morse Micro Rate Control) information using the morse_cli tool to monitor dynamic modulation and coding scheme adjustments.
- **GPS Location Data** - Used to correlate measured throughput and link quality with precise distance between the AP and STA.
- **Environmental RF Noise** - Captured with a spectrum analyzer to document in-band and near-band interference levels at each location.

Capturing these metrics enables high-resolution analysis of Wi-Fi HaLow performance over distance and under varying environmental conditions.

Best Practices and Considerations

To ensure accurate, reliable, and repeatable range test results, the following best practices should be observed:

- **Use GPS-Based Distance Measurement** - Employ GPS tracking to measure the distance between the Access Point (AP) and Station (STA) accurately. Avoid relying solely on signal strength, which can be affected by environmental factors.
- **Label Equipment Clearly** - Physically label all DUTs and tripods with identifying information (e.g., IP address, device role) to streamline field operations and avoid configuration errors.
- **Continuously Monitor Association Status** - Regularly check that the STA remains associated with the AP throughout the test to preserve data integrity.
- **Ensure Adequate Power Supply** - For extended testing sessions, confirm that laptops, power banks, and other critical equipment have sufficient charge or backup power to avoid interruptions.
- **Lock Cellular Dongles to Clear Frequencies** - Configure cellular dongles to use only frequencies that do not overlap or approach HaLow.
- **Validate Baseline Connectivity** - At the start of each range test, verify connectivity between the AP and STA using basic tests (e.g., ping, iPerf) to ensure proper configuration.

- **Minimize RF Interference** - Enable only one pair of HaLow interfaces at a time during testing. Use a spectrum analyzer to monitor and log changes in the RF environment for later correlation with performance data.

Script Automation

Custom test scripts can significantly streamline the range testing process, reducing manual intervention and improving repeatability. Key automated functions include:

- **Association Verification** - Automatically checks that the AP and STA are properly associated before initiating any throughput tests, ensuring the validity of collected data.
- **iPerf3 Orchestration** - Manages the execution of uplink and downlink tests for both UDP and TCP traffic. Scripts handle result logging, manage retries in case of failure, and ensure consistent execution parameters.
- **Location Tracking** - Collects GPS data from each device and calculates the actual separation distance using the haversine formula, providing accurate spatial context for throughput results.
- **Device Management** - Temporarily disables or “mutes” non-participating devices during active testing to avoid RF interference and ensure clean, isolated test conditions.
- **Error Handling** - Monitors for errors during execution. If a fault is detected, the script will log the issue and either retry the operation or exit gracefully, preserving the integrity of the dataset.



Figure 11: Range testing fixture (AP).

Appendix A: RF Spectrum Capture Using the BB60D and Spike Software

This appendix provides step-by-step guidance and hardware specific best practices for capturing spectrum data using the Signal Hound BB60D spectrum analyzer and Spike software.

Spectrum Analyzer Device	Signal Hound BB60D
Antenna	Pulse Larsen W1063M (bundled with evaluation kits)
Software	Spike, with Occupied Bandwidth and Total Power measurements enabled

Capture Ranges and Settings

The following table summarizes the recommended capture settings for RF spectrum analysis using the BB60D spectrum analyzer and Spike software. These settings ensure that measurements are consistent, reliable, and directly comparable across different test locations and conditions.

Parameter	Recommended Setting	Notes
Capture Type	Average trace, Maximum hold trace	Captured at each DUT location for comprehensive environmental assessment.
Capture Ranges	8 MHz, 20 MHz, 200 MHz	Covers in-band, near-band, and out-of-band environmental noise.
Occupied Bandwidth	Enable “Total Power” in Spike software and record.	Provides integrated noise power for each range.
Amplitude Reference Level	-60 dBm to -40 dBm	Ensures that the environmental noise floor is measured.
Resolution Bandwidth (RBW)	Record RBW value used (e.g., 10 kHz or 100 kHz)	Set based on desired measurement resolution; note this in the test report.
Antenna	Pulse Larsen W1063M (bundled with evaluation kits)	Use the same antenna as used during DUT testing for consistency.

Antenna Orientation	Vertical, pointed towards the sky	Minimizes reflections and interference from nearby surfaces or electronics.
----------------------------	-----------------------------------	---

Table 4: Morse Micro Spike software settings for spectrum capture.

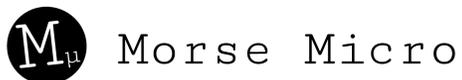
Best Practices for Capture

- Use one of the antennas actively used in testing to ensure representative noise measurements.
- Hold the analyzer vertically, with the antenna pointed to the sky to minimize reflections and nearby electronic noise.
- Record average and maximum hold traces, noting any peaks or outliers in the environmental noise floor.
- Perform captures at each DUT location and document parameters (antenna orientation, RBW, and environmental conditions).
- Refer to the BB60D and Spike software manuals for detailed operational instructions and calibration recommendations.

Revision History

Release Number	Release Date	Release Notes
01	04-Aug-2025	Initial release

Morse Micro provides this information "as is" without warranties of any kind, express or implied. No guarantee is made as to the accuracy, completeness, or suitability of this information or Morse Micro's products for any specific purpose. Use of this information and products is at the user's sole risk. Morse Micro products are not designed or tested for use in mission-critical systems, and should not be used in such applications. Performance specifications are based on internal testing and are believed to be reliable; however, they are not guaranteed. It is the Buyer's responsibility to test and validate all product performance, compatibility, and compliance, both in isolation and within end applications. Morse Micro assumes no liability for the use or application of any product, circuit, or information described herein. No license or other rights—express or implied—are granted under Morse Micro's intellectual property. This document contains proprietary information of Morse Micro and is subject to change without notice.



Morse Micro Pty. Ltd. Corporate Headquarters

Level 8, 10-14 Waterloo Street, Surry Hills, NSW 2010, AUSTRALIA

Email: sales@morsemicro.com

Copyright © Morse Micro Pty. Ltd.