Morse Micro
reaching farther™

MM6108 - OpenWrt 2.5

Web GUI User Guide

March 2024

Author: Matthew Forgie

Table of Contents

1 Overview

Thank you for choosing to evaluate Morse Micro 802.11ah HaLow for use in your application. This guide will get you started using the kit and evaluating the 802.11ah technology. It is primarily intended for users of the web UI but will mention other configuration methods for reference.

The Morse Micro Web UI provides a graphical method of viewing and modifying the device configuration, in particular the operating mode and HaLow radio parameters. The interface is available on EKH01 and EKH03 evaluation kits, and is based on the standard LuCI interface of OpenWrt.

Section 2 of this document provides a brief description on how to set up the hardware and outlines the basic scenarios that might be used for evaluation. Section 3 explains how to configure a system for the first time using the Morse Micro Web UI. Section 4 and 5 describes how to test the performance of Wi-Fi HaLow by using Wavemon and iPerf. Section 8 has a description of some of the available GUI screens & tools, and Section 9 provides advanced configuration tips that are not usually required but may be useful in some situations. Section 10 describes the configuration architecture, and how UI configuration is passed through the system to effect changes. Section 11 provides some troubleshooting advice for common problems.

Throughout this document, references to 'AP' imply a Wi-Fi Access Point and references to 'STA' imply a Wi-Fi station.

2 Device Setup

A brief description of the hardware and browser set-up is included below for configuration via the Web GUI, along with a description of the standard test setup scenarios.

2.1 EKH01

- **microSD card** - this contains the device firmware.
- **Status LEDs** - the red LED indicates power, and the green LED indicates SD card activity.
- **USB Type-C** - USB-C port for supplying power to the EKH01. The kit includes an AC adapter that converts mains power to 5V for the EKH01 via the USB-C connector.
- **Micro HDMI** - Micro HDMI display outputs for EKH01
- **Headphone Jack** - not typically used.

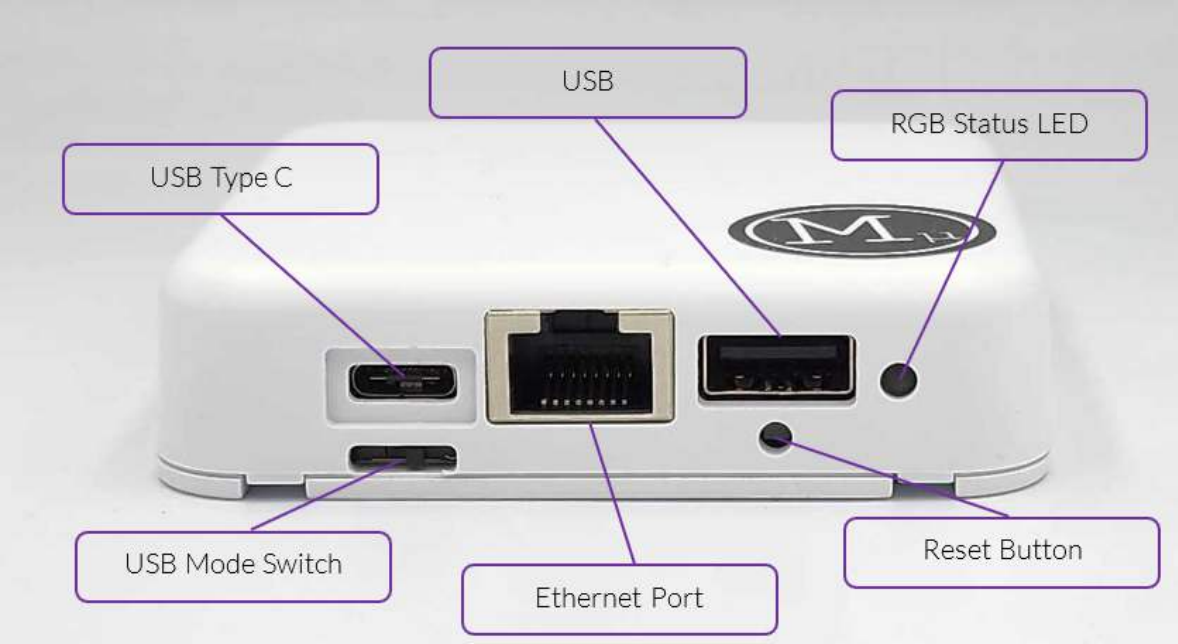
- **USB Ports** - USB-A ports for connecting peripherals and USB to serial adapter. Any of these ports can be used for serial console access, but note the cable must be plugged in at boot time to be detected. The serial console operates at 115,200 bps 8N1 by default.
- **Ethernet** - Ethernet port for either a LAN connection (e.g. a laptop) or an upstream WAN connection (e.g. gateway router).
- **(Optional) Camera** - the device may include a camera depending on the kit version ordered.

2.1.1 Basic setup

1. Connect the antenna to the RF connector on top of the unit.
2. Optional - connect an RJ45 Ethernet cable to the Ethernet port if required.
3. Optional - connect a USB-serial cable to any of the USB ports if required for debugging. This is not usually required.
4. Once power is applied, it should take the device around 60 seconds to boot up and be operational.

2.2 EKH03

- **USB Type-C** - Powers the board and can function as an Ethernet-to-USB adapter if the USB mode switch is in the left position.
- **USB** - this port can be used for connecting peripheral devices to the EKH03.
- **RGB Status LED** - this is a multi-color LED that is used to indicate the status of the device (see below in 'Basic Setup' for details).
- **USB Mode Switch** - Select whether to use the USB-C or Ethernet port for LAN connection. Direction of the switch point the selected prot to use (*left* - USB-C for Ethernet *right* - Ethernet port for Ethernet)
- **Ethernet port** - Ethernet port for either a LAN connection (e.g. a laptop) or an upstream WAN connection (e.g. gateway router).
- **Reset button** - this can be used to reset the device. Pressing and holding the button for 10 seconds will trigger a full factory reset of the device, returning it to the factory default configuration. Further details in section 3.8 on DPP push button.
- **2.4 GHz Wi-Fi** - by default, the EKH03 will bring up a 2.4 GHz Wi-Fi access point which is bridged to the Ethernet interface.



2.2.1 Basic setup

1. Connect the provided antenna to the port shown above.
2. A USB-C to USB-A cable is provided in the kit, this can be used to connect the EKH03 to a suitable power source to power the EKH03 via the USB-C port. For example, many laptops can deliver sufficient power over USB, or a phone charger can be used.
3. Once the device is powered, the RGB LED will display the boot status of the device:
    a. Solid yellow indicates that the bootloader is running.
    b. Flashing green indicates that Linux is booting.
    c. Solid green indicates that the device is fully booted.
    d. Red indicates that the device has failed to boot, contact support for advice on troubleshooting further.
    e. After pressing the button:
        i. Flashing yellow/green indicates that DPP is running.
        ii. Flashing red for 5 seconds indicates that DPP failed.
        iii. Flashing blue indicates a reboot is in progress. Fast blue flashing indicates a factory reset.

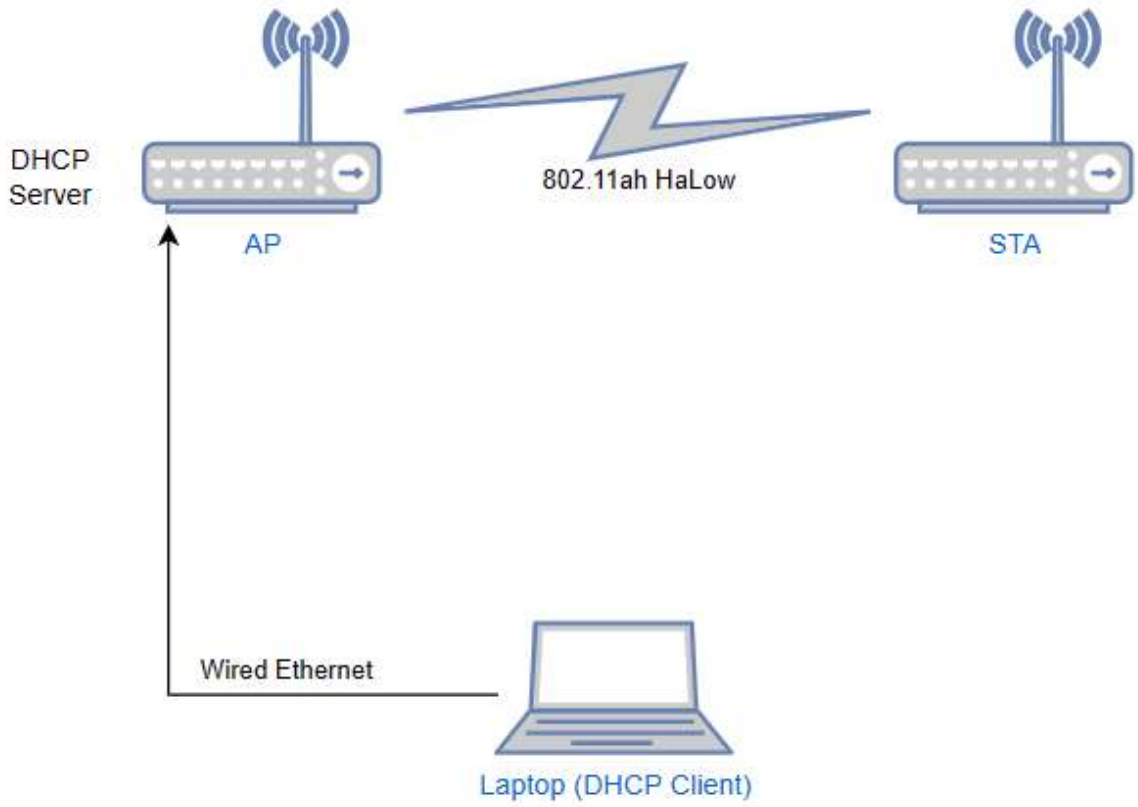
2.3 Browser support

The Web GUI has been tested and verified to work with the following browsers:

- Google Chrome
- Firefox
- Microsoft Edge
- Apple Safari

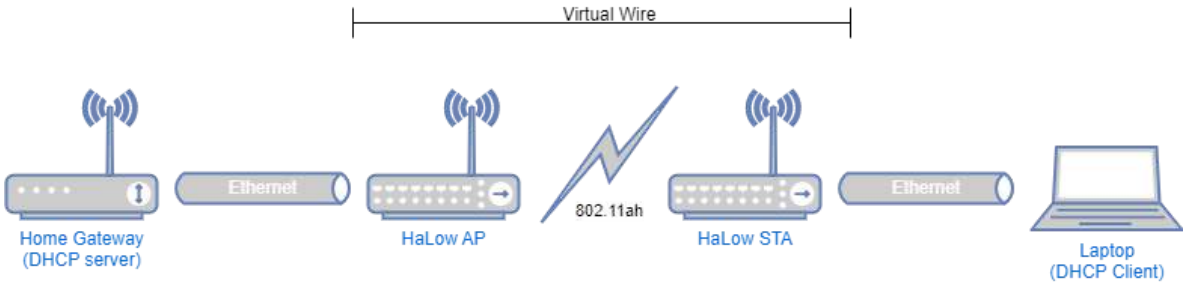
2.4 Standard setup scenarios

2.4.1 Standalone Access Point with client devices



This is the configuration that is typically used to do standalone testing of a HaLow connection e.g. range testing. It is also useful in closed network scenarios, where connected devices do not need access to external networks such as the Internet. The key here is that the traffic will only go between the AP and STA and need not go any further. If you're not sure which setup to use, start with this one.

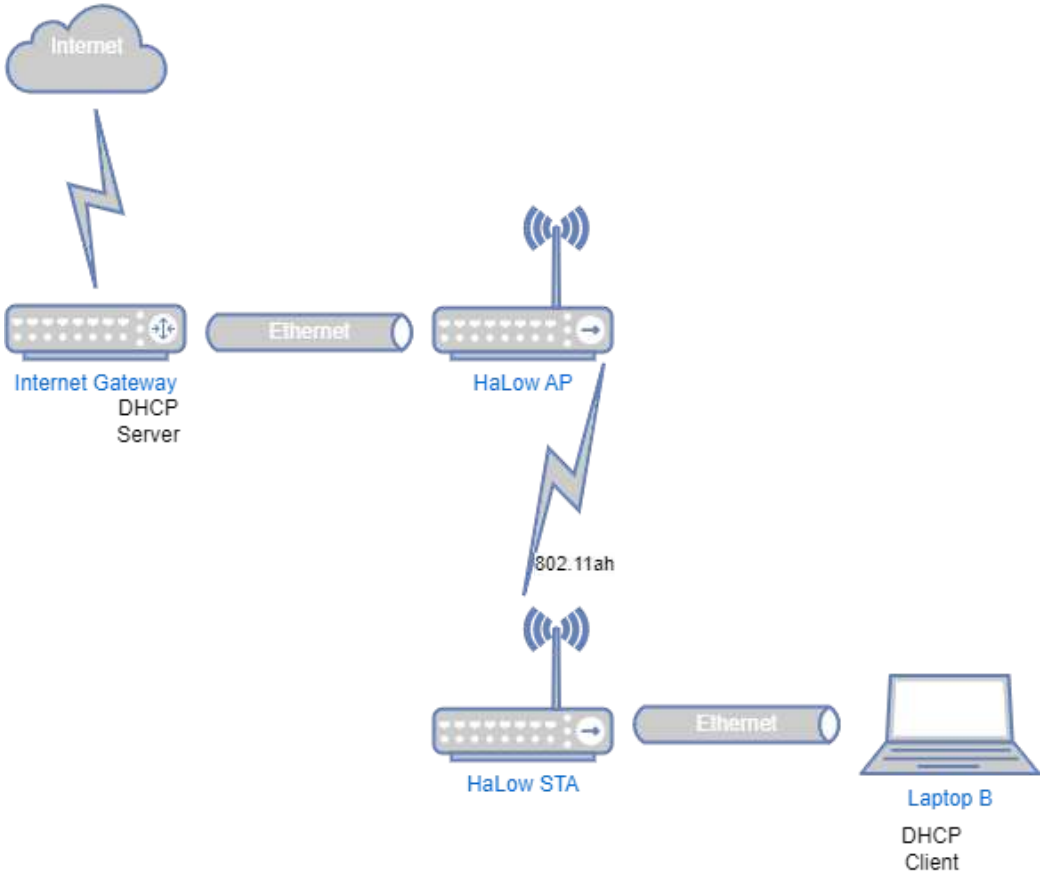
2.4.2 Using HaLow as a 'virtual wire' (Layer 2 bridge)



In this scenario, the use of HaLow is transparent to the rest of the devices in the network. The HaLow link is used as a means of providing a 'virtual' Ethernet connection between two points where it may not be practical to run a physical cable.

This scenario is useful as a simple way to test HaLow with real-world traffic by introducing it into an existing network without having to adjust the configuration of the non-HaLow devices.

2.4.3 Non-standalone Access Point with routing



This scenario is a more complicated version of the above, where rather than using bridging to simplify the setup, each device is a router with its own DHCP server and local network. This allows for a more complex network setup, but is more difficult to set up. It is also robust in that if the HaLow links goes down, the station will still have an IP address and the UI will be reachable.

This scenario is useful for evaluating the HaLow device's ability to handle traffic flows at Layer 3, which places more load on the CPU. Unless you have a good reason to want to do this, bridging is an easier and better way to go.

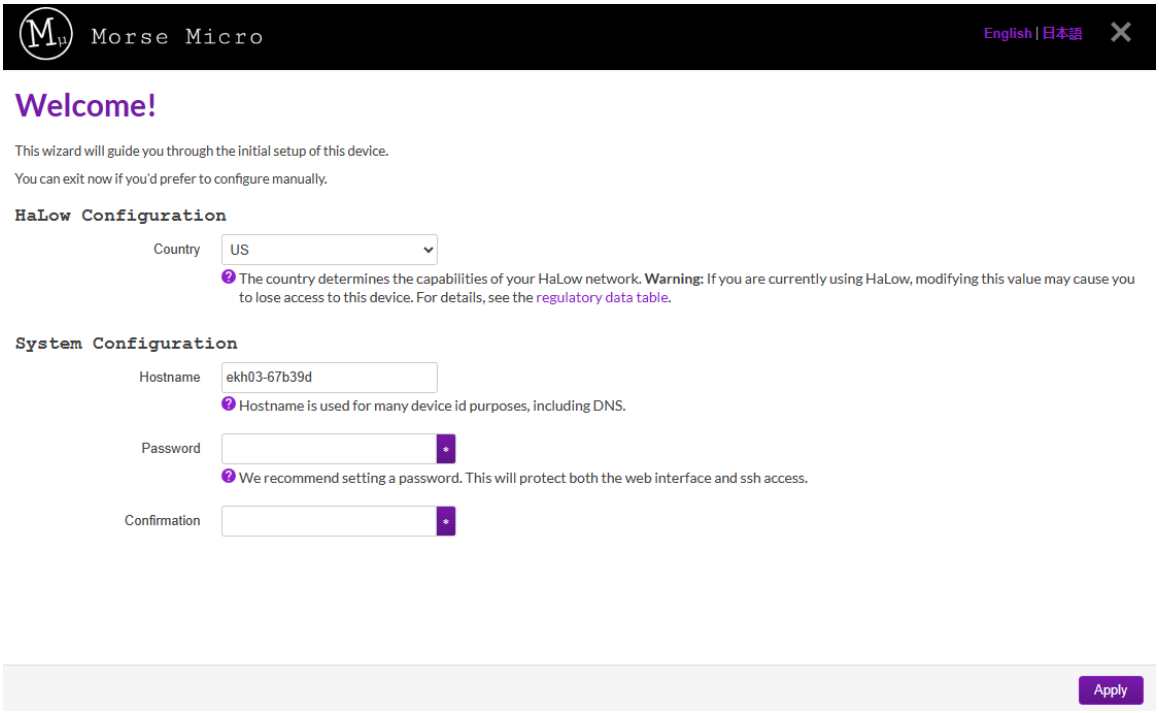
3 Configuration of Operating Modes

Evaluation kits are dispatched in a default configuration, and the assumption of this guide is that the devices will be used starting in this state. If the devices have been used previously you may need to reset the device back to a default state before following the below steps. See Chapter 3.6 for details on how to reset to default configuration.

Since the 2.3.x release of OpenWrt a configuration wizard has been included in the UI to aid with quick setup of devices. This guide now focuses on using the configuration wizard, but it is also possible to use the standard configuration pages in the UI to set up the device.

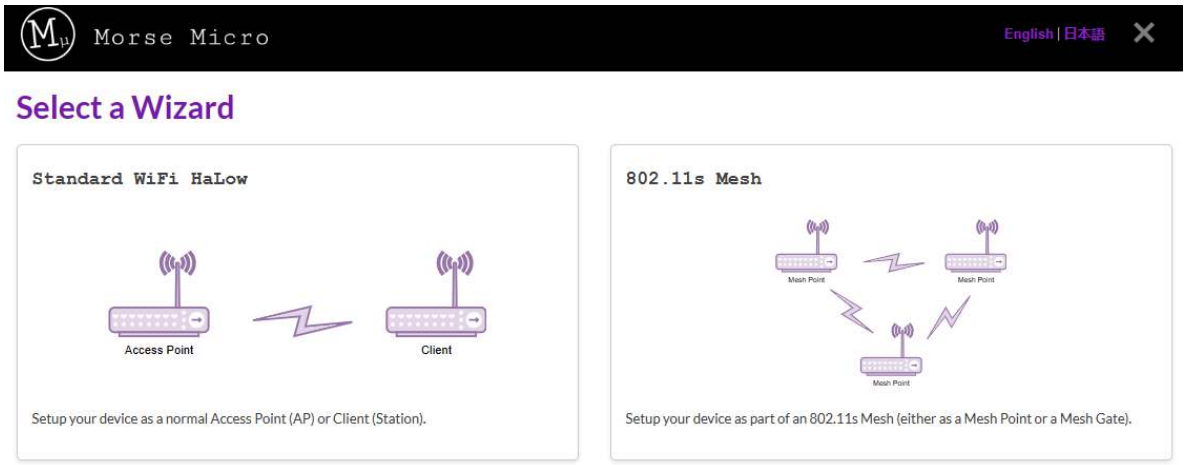
3.1 Initial Setup

1. Connect your laptop to the Morse Micro HaLow device via an Ethernet cable.
2. Ensure that the Ethernet interface on the laptop is configured as a DHCP client (this is usually default, so often no change is required).
3. Open a web browser and go to the following address: http://10.42.0.1
4. Select the **Country** (for regulatory requirements) and optionally a unique **Hostname** for the device and a **Password** (which controls SSH and web access):



5. Click **Apply** in the bottom right.

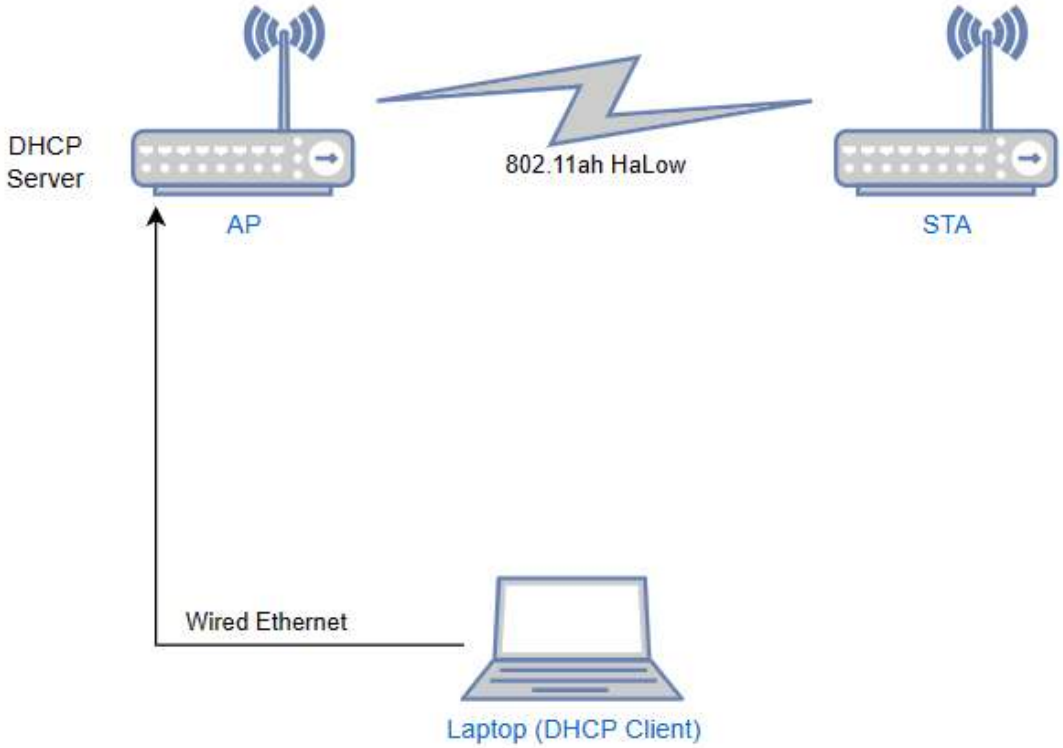
The next screen will present an option to configure the device either as a standalone AP/STA or as part of an 802.11s mesh. For first time users, the standard Wi-Fi HaLow wizard is the best option to start with. Mesh configuration allows multiple APs to be linked in order to provide an even wider coverage area. Other mesh options are available in the standard UI, for example EasyMesh (see Chapter 6).



The following sections assume that the standard Wi-Fi HaLow wizard has been selected.

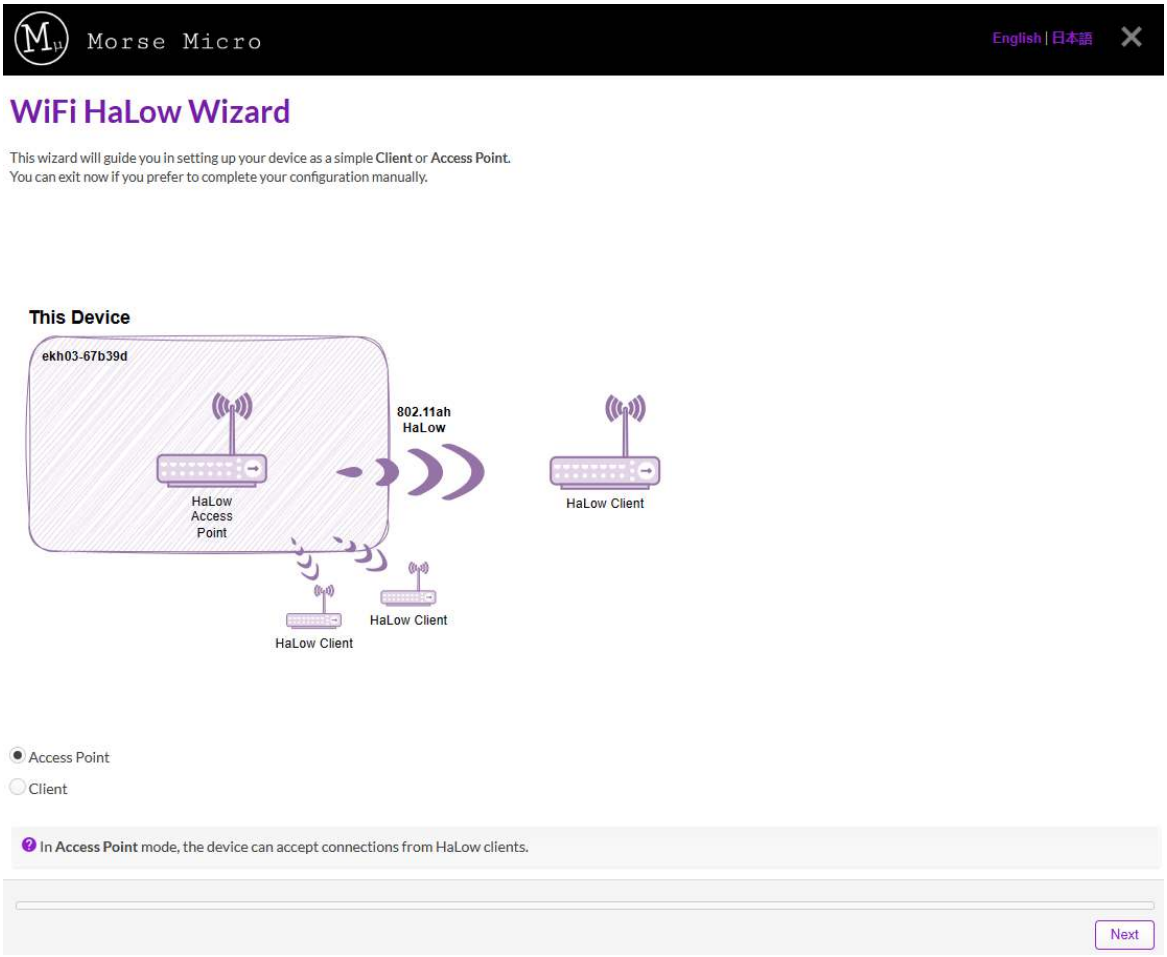
3.2 Standalone AP and STA

This section outlines how to configure the AP and STA per the scenario defined in 2.5.1.



3.2.1 Access Point configuration

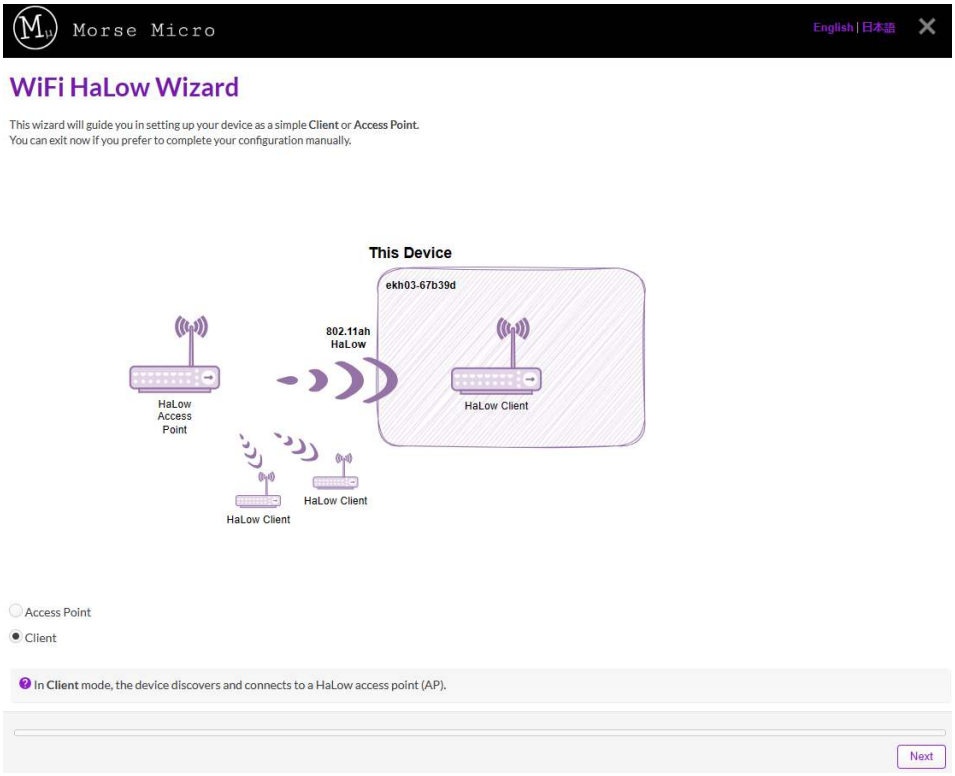
1. Follow the steps in 3.1 to connect to the device and set the region at http://10.42.0.1
2. For **Mode** selection, choose Access Point:



3. Click the **Next** button at the bottom right to go to the next page.
4. On the following pages:
    a. **Setup HaLow Network - AP** has a default SSID/passphrase of MorseMicro/12345678; you can change this if you wish. Bandwidth & Channel can be left as default. Then click **Next**.
    b. **Upstream Network** should be *None*. Click **Next**.
5. You can then **Apply** your configuration on the final page.

3.2.2 Station/Client configuration

1. Disconnect your laptop from the Ethernet interface of your AP (from section 3.2.1 above) so that its IP address doesn't clash with the client IP.
2. Follow the steps in 3.1 to connect to the device and set the region.
3. For the **Mode** selection, choose 'Client' and then click **Next**.



4. On the **Connect to a HaLow Network** page, choose 'Manual credentials' and then **Scan** to find the SSID you entered for your AP. Then enter the passphrase from above, and click **Next.**
5. For the **Traffic Mode**, select 'Bridge' and click **Next**.
6. Turn off the 2.4 GHz **EnableAccess Point** toggle if standard Wi-Fi access is not needed. Click **Next.**
7. Once you have saved the configuration (by clicking 'Apply'), you should disconnect your laptop from the Station and connect it to the AP. You can return to the Station's admin interface by inspecting the **Active DHCP Leases** on the **Status** page of the AP's admin interface.

3.2.3 (Optional) Add upstream Internet connectivity

In many situations it is helpful to have an upstream connection to the Internet. The following steps outline how to connect the AP to an upstream router that will provide Internet access to the HaLow devices.

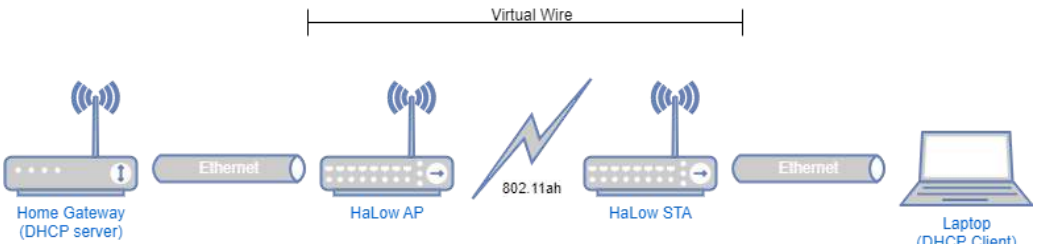
It assumed the upstream gateway provides the following:

- DHCP server to allocate an address to the AP Wired Interface
- DNS server will be provided via an option in the DHCP offer
- A gateway address will be assigned via the DHCP offer

1. Connect your laptop to your device as in 3.1, and go to its admin interface (usually http://10.42.0.1).
2. If the wizard does not come up because you've already configured your device, go to **Morse > Setup Wizard** in the top menu.
3. On the **Upstream Network** page, choose *Ethernet*, and set the **Traffic Mode** to *Router*.
4. Apply the configuration on the final page.
5. Use an Ethernet cable to connect your AP to your existing network.
6. To access the device's admin interface again, you can access 192.168.1.1 over the HaLow link or you will need to determine the address allocated by your network's DHCP server. See section 3.6 for how to reset your device if you lose access.

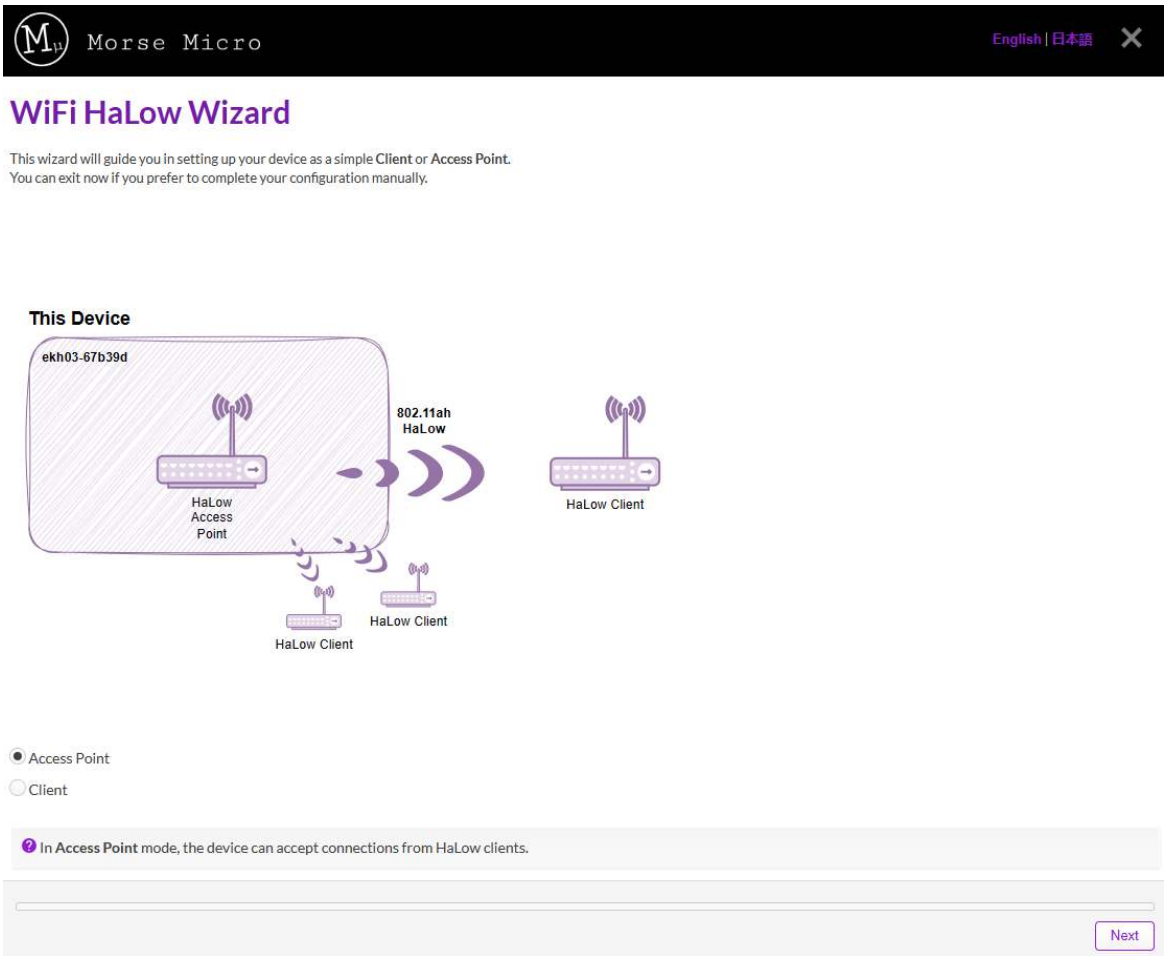
3.3 'Virtual Wire' - Layer 2 bridging

This section outlines how to configure the AP and STA per the scenario defined in 2.5.2.



3.3.1 Access Point configuration

1. Follow the steps in 3.1 to connect to the device and set the region at http://10.42.0.1
2. For **Mode** selection, choose Access Point:



3. Click the **Next** button at the bottom right to go to the next page.
4. On the following pages:
    a. **Setup HaLow Network - AP** has a default SSID/passphrase of MorseMicro/12345678; you can change this if you wish. Bandwidth & Channel can be left as default. Then click **Next**.
    b. **Upstream Network** should be *Ethernet*. Selecting Ethernet will show a new option for **Traffic Mode** which should set to *Bridge*. Click **Next**.
5. You can then **Apply** your configuration on the final page.

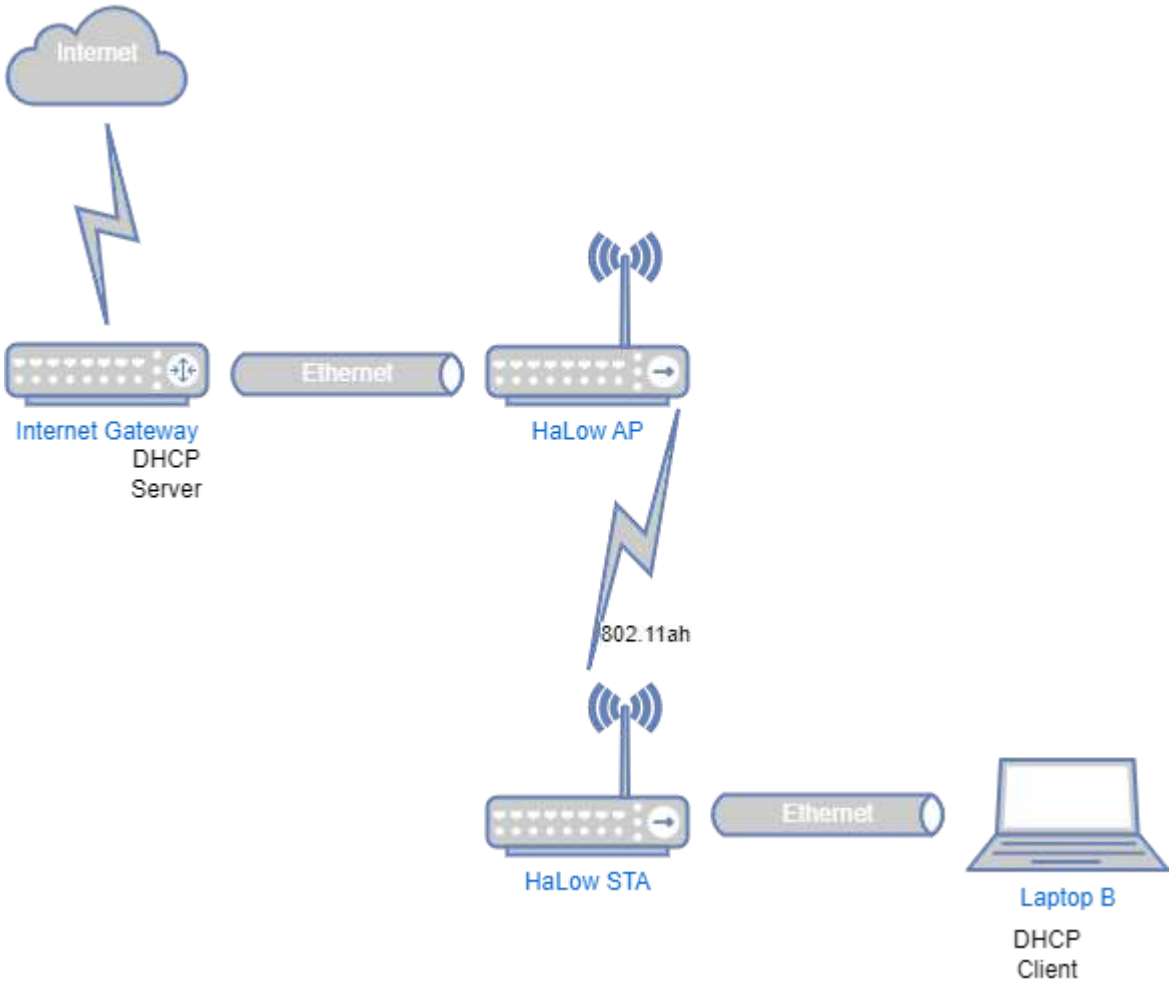
To access the device's admin interface again, you will need to check the IP address allocated by your network's DHCP server. See section 3.6 for how to reset your device if you lose access.

3.3.2 Station/Client configuration

Follow the instructions in 3.2.2. Once you've saved your configuration, however, your station's IP address will be allocated by your network's DHCP server and will be accessible on that network.

3.4 Non-standalone AP with routing

This section outlines how to configure the AP and STA per the scenario defined in 2.5.3.



3.4.1 Access Point configuration

Follow 3.2.1 and 3.2.3 exactly to configure an *Access Point* with **Uplink** set to *Ethernet* and **Device Mode** set to *Router*.

3.4.2 Station configuration

Follow the STA configuration for the scenario in 3.1, but for **Device Mode** choose *Extender* instead of *Bridge*.

3.5 Setting a custom static IP

By default, devices configured as an AP are reached via 10.42.0.1 on the Ethernet interface and 192.168.1.1 on the HaLow interface. If the two interfaces are bridged together, they will both use the same 192.168.1.x/24 subnet and the device will be reached on 192.168.1.1 via both interfaces.

In simple topologies this default setup is often sufficient, however in setups with multiple APs it can become necessary to configure custom static addresses to ensure each device has a unique IP address. Static IP addresses can also be useful to ensure that devices configured as STAs always are reachable at the same address, particularly when many similar STAs are on a given HaLow network. DHCP, which is the default on Ethernet and HaLow interfaces, will assign different addresses to STAs each time otherwise.

To configure a static IP address on either the Ethernet or HaLow interface, browse in the UI to the **Morse->HaLow Config** in the top menu.

3.6 Reset the device to default configuration

This section outlines how to get the device back to a default configuration in different situations. From 2.4.4 onwards, all firmware releases use SquashFS with an overlay which allows a full factory reset to be achieved by wiping the overlay.

3.6.1 Access to web UI is available

In this scenario, you can login to the device and go to the 'System -> Backup/Flash Firmware' page. Choose the option "Reset to defaults", and the device will reset the configuration and reboot.

3.6.2 SSH access is available

In this scenario, you can login to the device via ssh (ssh root@ipaddress) and run the following command at the prompt:

```
# firstboot && reboot
```

3.6.3 No network access - EKH01

This scenario can occur when the IP address of the device has been changed, and it is not obvious what the address is. The quickest method here is to remove the SD card and write a new firmware to it using a program such as Balena Etcher to write the SD card from a laptop.

3.6.4 No network access (Option 1) - EKH03

This scenario can occur when the IP address of the device has been changed, and the user is unable to identify it via a lease list on their DHCP server. Using a suitable object, press and hold the reset button, shown in section 2.3, for more than 10 seconds to reset the device to factory defaults. After releasing the button, the device should reboot, which will be indicated by the LED on the device. It may take a few seconds, after releasing, for the device to reboot.

3.6.5 No network access (Option 2) - EKH03

This scenario requires using a serial console cable to access the device. The basic setup section of this guide shows the location of the UART header on the EKH03 PCB, and a 3.3V TTL serial USB cable can be used to connect a computer to this port. Once connected, a suitable terminal emulator program will be needed to connect to it, such as PuTTY in Windows or picocom in Linux.

Once connected to the serial console, run the following command to reset the configuration:

```
# firstboot && reboot
```

3.7 Using DPP QR code

Device provisioning protocol (DPP) provides a simple process to onboard stations into an existing wireless network. Station devices are provisioned by scanning a QR code with a "configurator" device already associated with the network.

3.7.1 On the AP

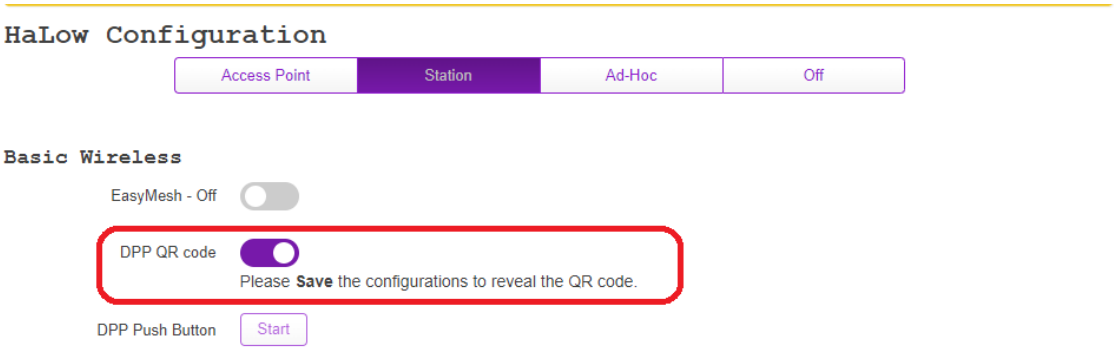
No explicit action is required to enable DPP in AP mode. Simply set your device to work as an AP with SAE security.

Note that if you are using 802.11s mesh, this does not by default include AP functionality, and the hostapd process will not be started. The hostapd process is required for DPP to function. It is possible to run 802.11s Mesh with an AP, this mode is known as a 'Mesh Gate' - see Chapter 3.9.2 for details.

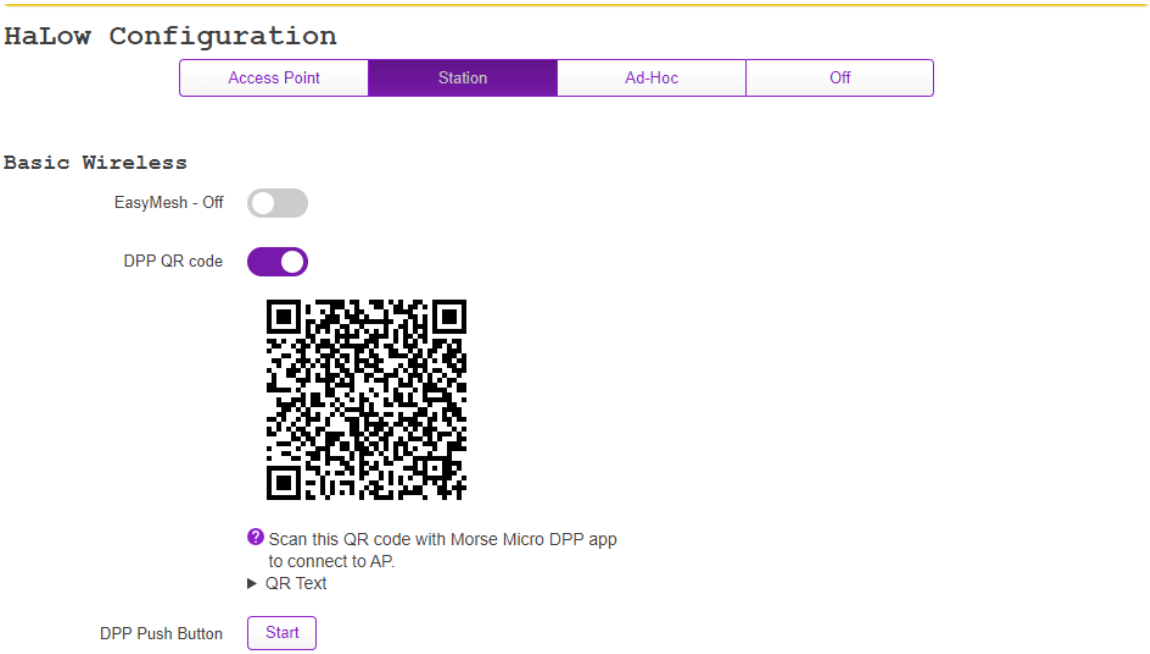
The credentials for the AP DPP configurator are set in /etc/dppd/auth_secrets.txt, you will be asked for these in the mobile app after selecting the AP to provision a device to. The default username/password is **morse/HaLow**.

3.7.2 On the STA

To enable DPP through the web UI, after setting your Device as a station, switch DPP on and save. The Page will prompt you to save, so the QR code can be shown.



After saving the configurations, the QR code will be shown.



To start provisioning, use the Morse Micro DPP app on the phone to scan the QR code.

NOTE: (For the 2.4.4 release) The DPP QR code is not persistent on EKH01 devices and will change if updating the image without keeping configs or flashing the image to the microSD card using a computer.

After a successful provision, the DPP switch will turn off and SSID, key, and encryption will be set automatically.

3.7.3 Using the Morse Micro App

To prepare a phone to act as a configurator - a device which scans and sends provisioning information to the AP - follow the steps below.
IMPORTANT NOTE: In order to use the Morse Micro App, you'll need a HaLow AP connected to the same network as your phone.

To download the Morse Micro DPP application for:

Apple iOS (needs authorization):

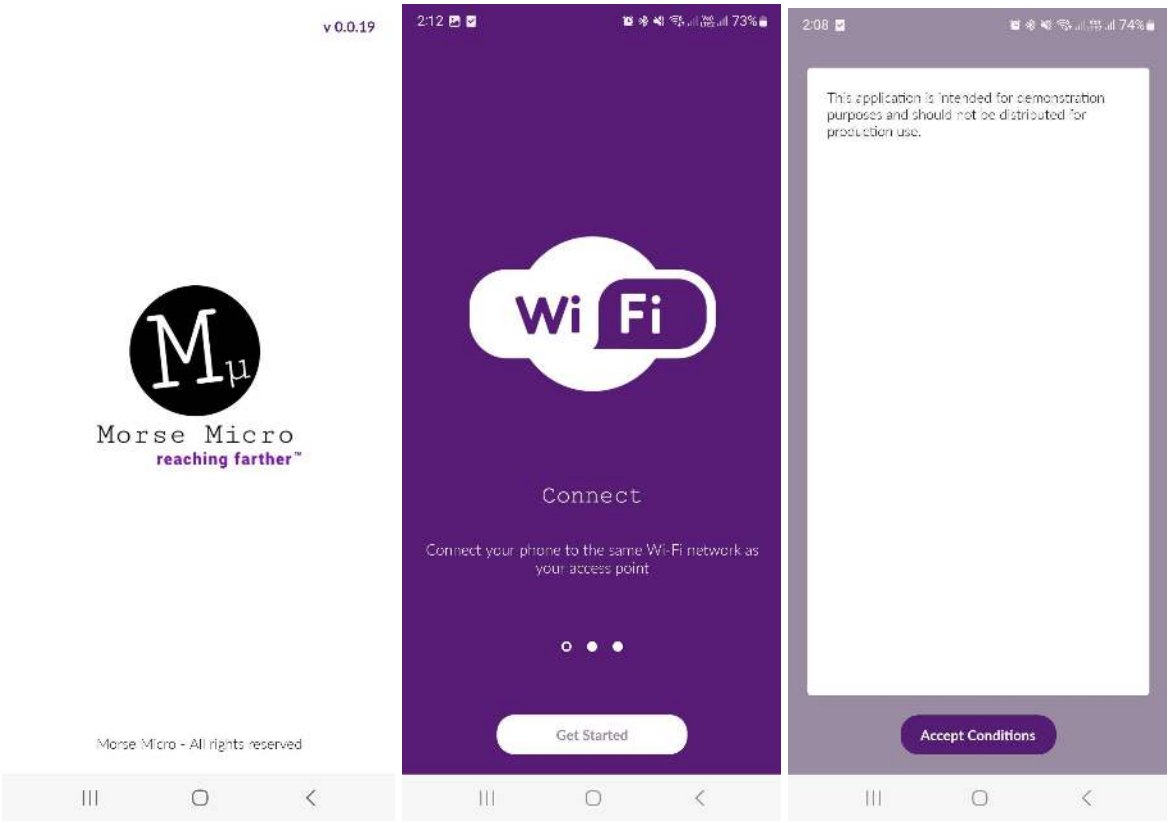
https://testflight.apple.com/join/LnXpFMPj

Android, use the link below:
https://app.bitrise.io/app/26fcf521506b532d/build/fb927766-2eaa-425f-a2b2-19f1342b432d/artifact/ce4e33d57257f294/p/bd9fd36d28dc80f5edef30ade4899720

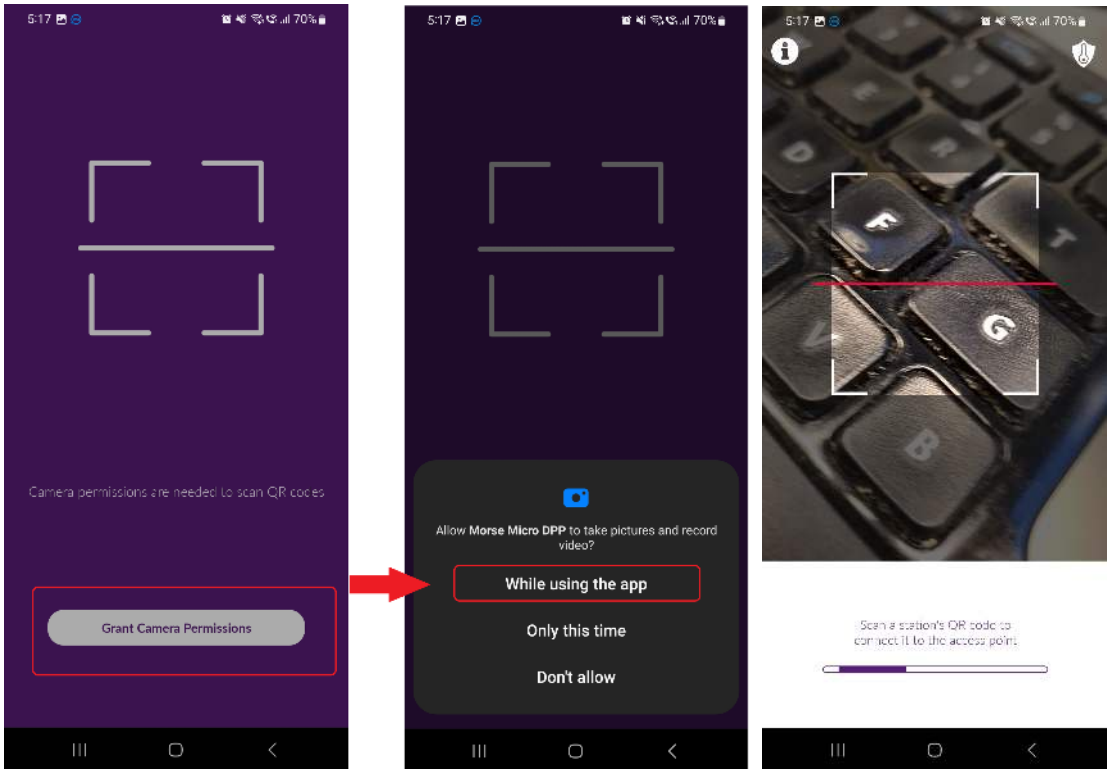
or scan this QR code with your phone:

and proceed until you install the app on your phone.

After the app is installed, open the app - if it is the first time running the app you will see a welcome/tutorial screen otherwise it will go straight to the 'Accept Conditions' screen. Click 'Get Started' if needed, and then 'Accept Conditions' to begin using the app.



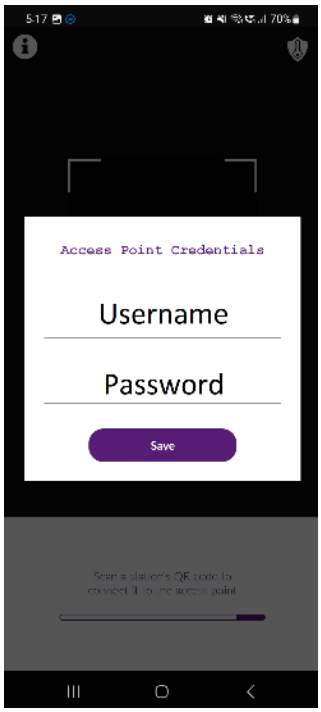
When prompted, grant the application access to your camera, so it can read QR codes.



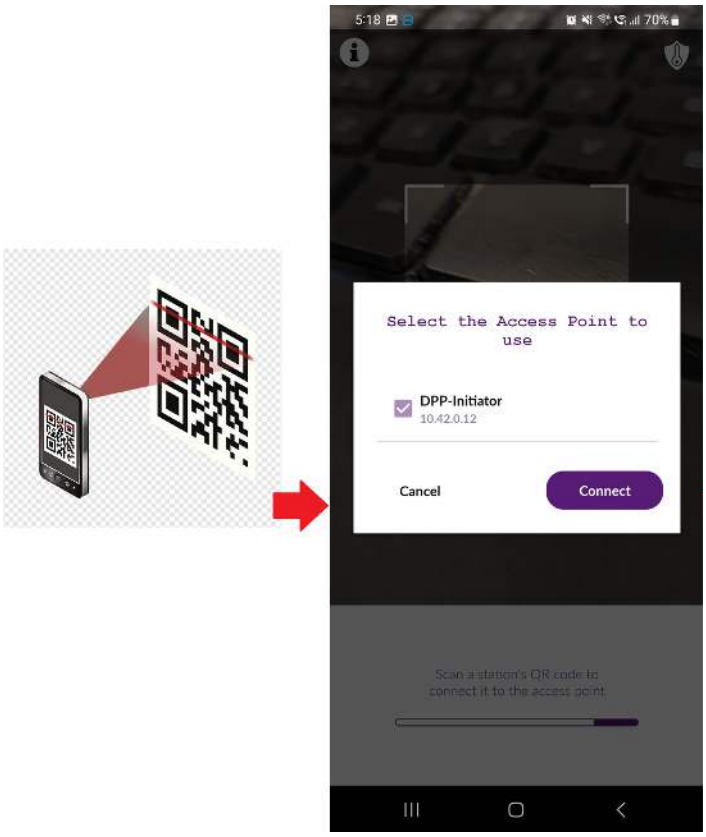
When you see the screen on the right (above), your app is ready to capture a QR code from the device to be provisioned.

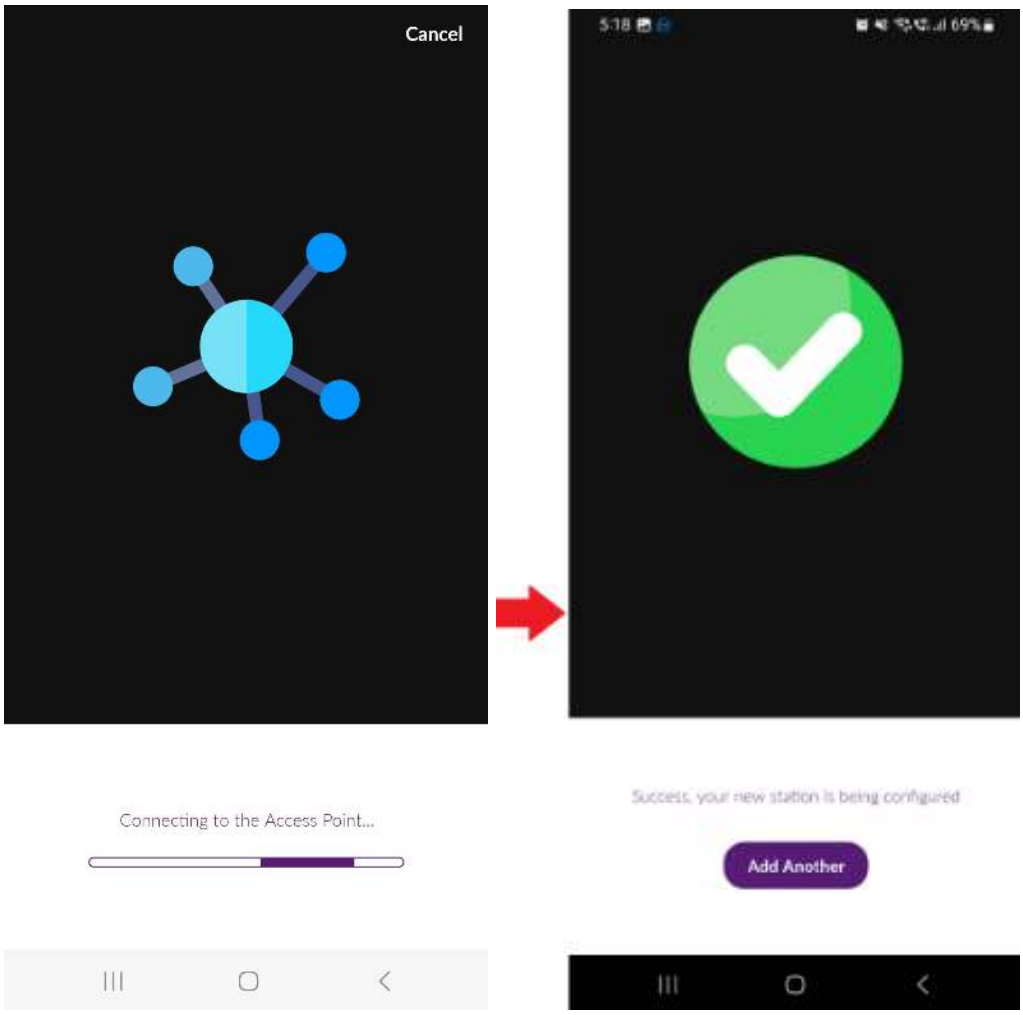
Before capturing a QR code, set up the credentials for accessing the AP by clicking the icon in the top right corner that looks like a key on a shield. You will need to enter the username and password of the DPP server on the AP.

The current default username is **morse** and the password is **HaLow**.



Point the camera to the QR code to scan it. When you scan a station's QR code, the app will show you a dialog with a list of available DPP servers on your network. Select the desired AP and tap on “Connect”.



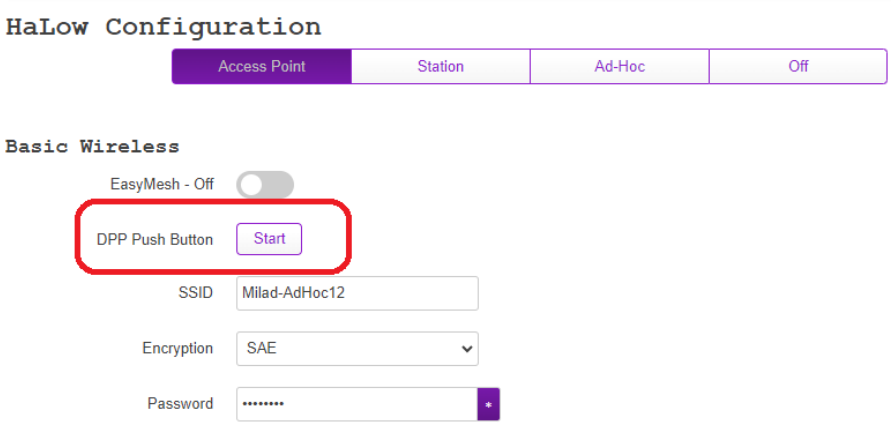


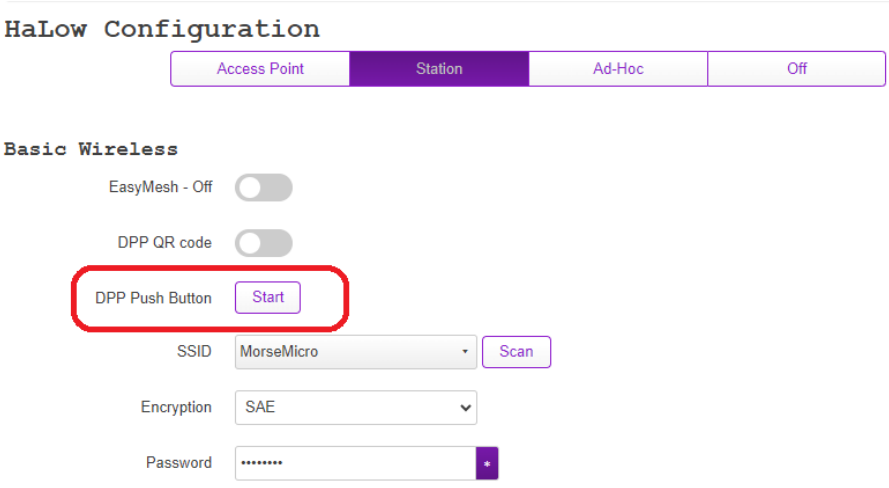
At the end the confirmation screen will be shown. To provision additional devices, click on “Add Another” to go back to the QR scanner .

Note: Once this process is completed, it means the device has been provisioned but not necessarily connected yet. Check the station list on the AP to verify the device has connected.

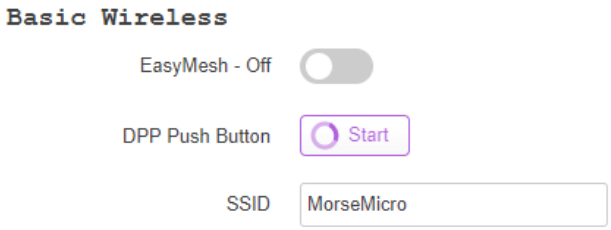
3.8 Using DPP push button

To utilize DPP (Device Provisioning Protocol) using the push button, simply set your device as an Access Point or Station and save the configurations and wait until the page reloads. Then press the Start button in front of the “DPP Push Button” on the Access Point and Station at the same time. Please note that the Start button will be disabled if you’ve changed from another mode to your current mode without saving your configurations.





After initiating the DPP process, the Start button will change to disabled with busy indication.

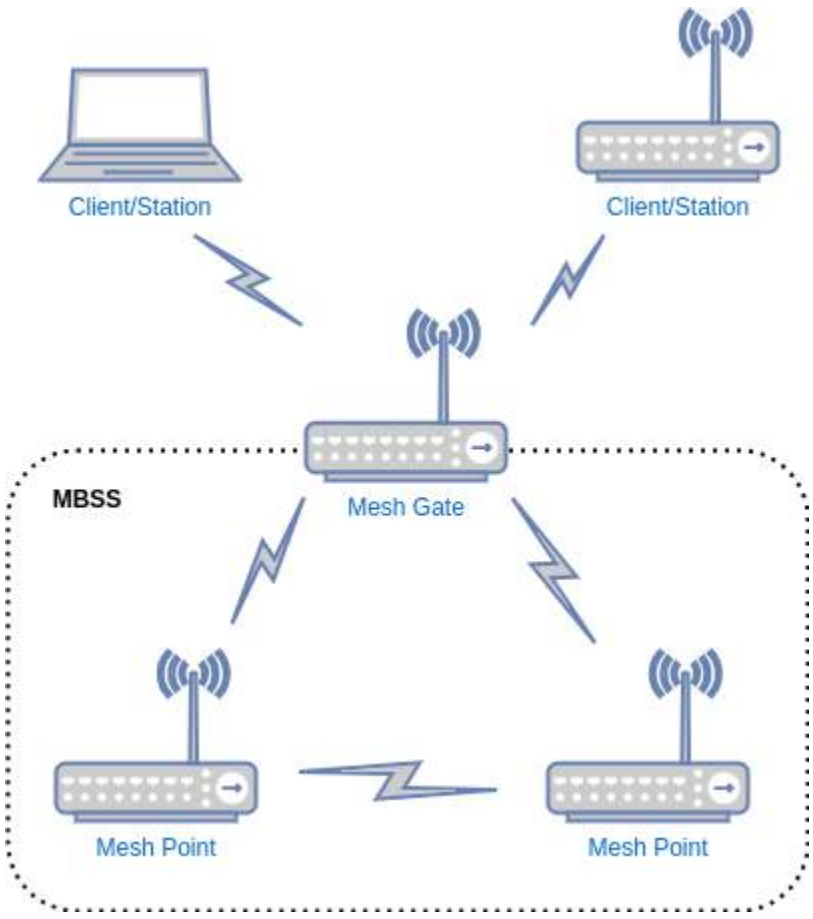


Please note that the Start button will stay in a busy state until you refresh the page or the DPP timeout elapses (100 seconds). Even in case of a successful provisioning, the buttons on both the Access Point and Station will stay in the busy state.

On the EKH03 the physical 'reset' button on the device can also be used for DPP. Pushing the button for less than 2 seconds will start the DPP push button process, if the device has been configured as an Access Point or Station. The RGB status LED will indicate that the DPP push button process is running, see the EKH03 setup section for details.

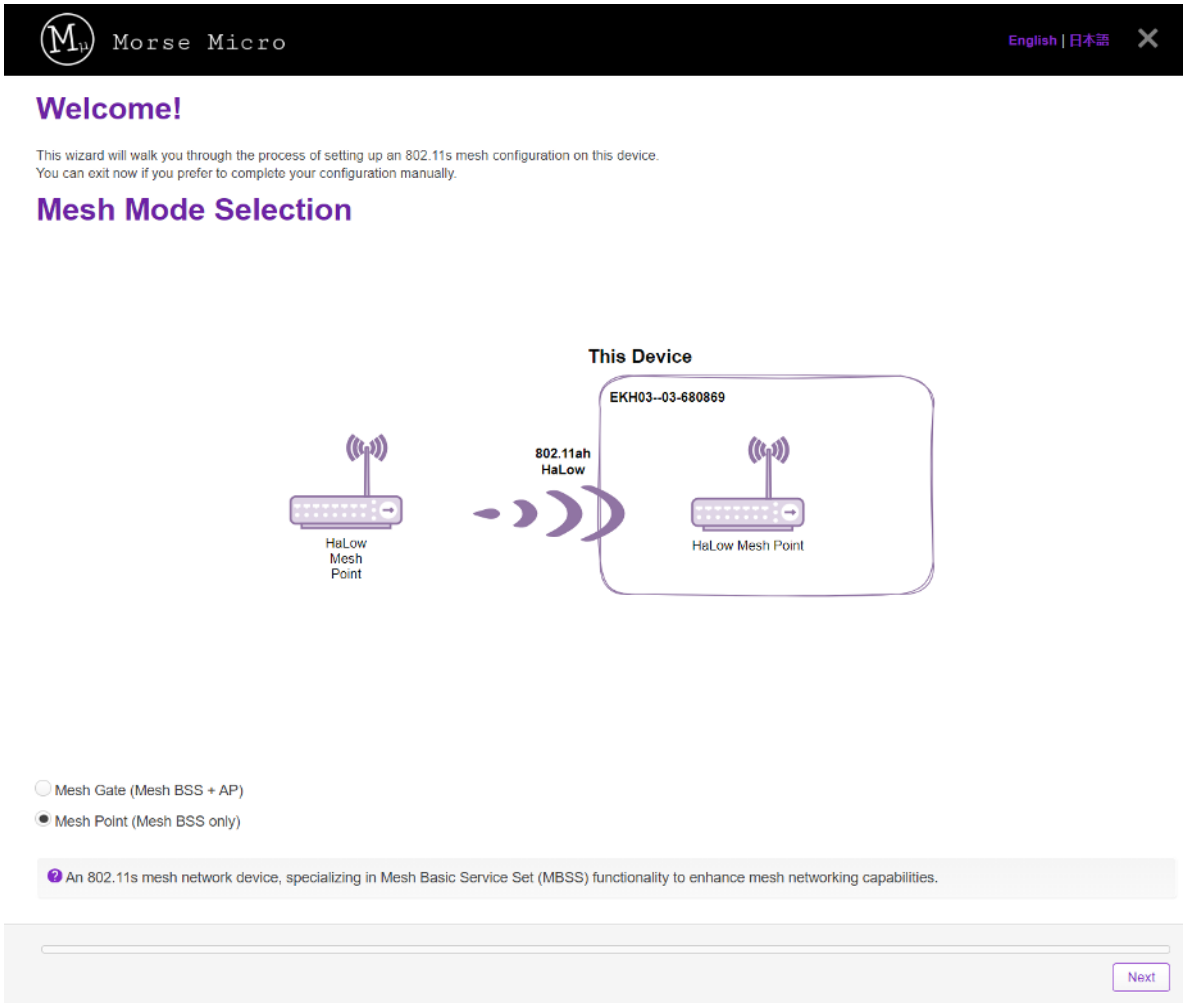
3.9 802.11s Mesh Configuration

802.11 mesh networks aim to increase coverage and range by establishing peer-to-peer links between the various neighbor mesh STAs in the mesh topology. Only mesh capable devices can join the mesh BSS (MBSS) or make use of the mesh functionality provided by the MBSS. Interaction with non-mesh capable devices is handled via mesh gateways (potentially co-located with a non-mesh AP).



3.9.1 Mesh STA / Mesh Point configuration

1. As a prerequisite, ensure that your device is configured with the appropriate region and a channel. Refer to steps in 3.1 to connect to the device and set the region.
2. Once you decide to configure your device as a Mesh Point, navigate to the **Morse > 802.11s Mesh Setup Wizard** in the top menu.
3. Follow the steps in For **Mode Selection**, choose 'Mesh Point' and then click **Next**.

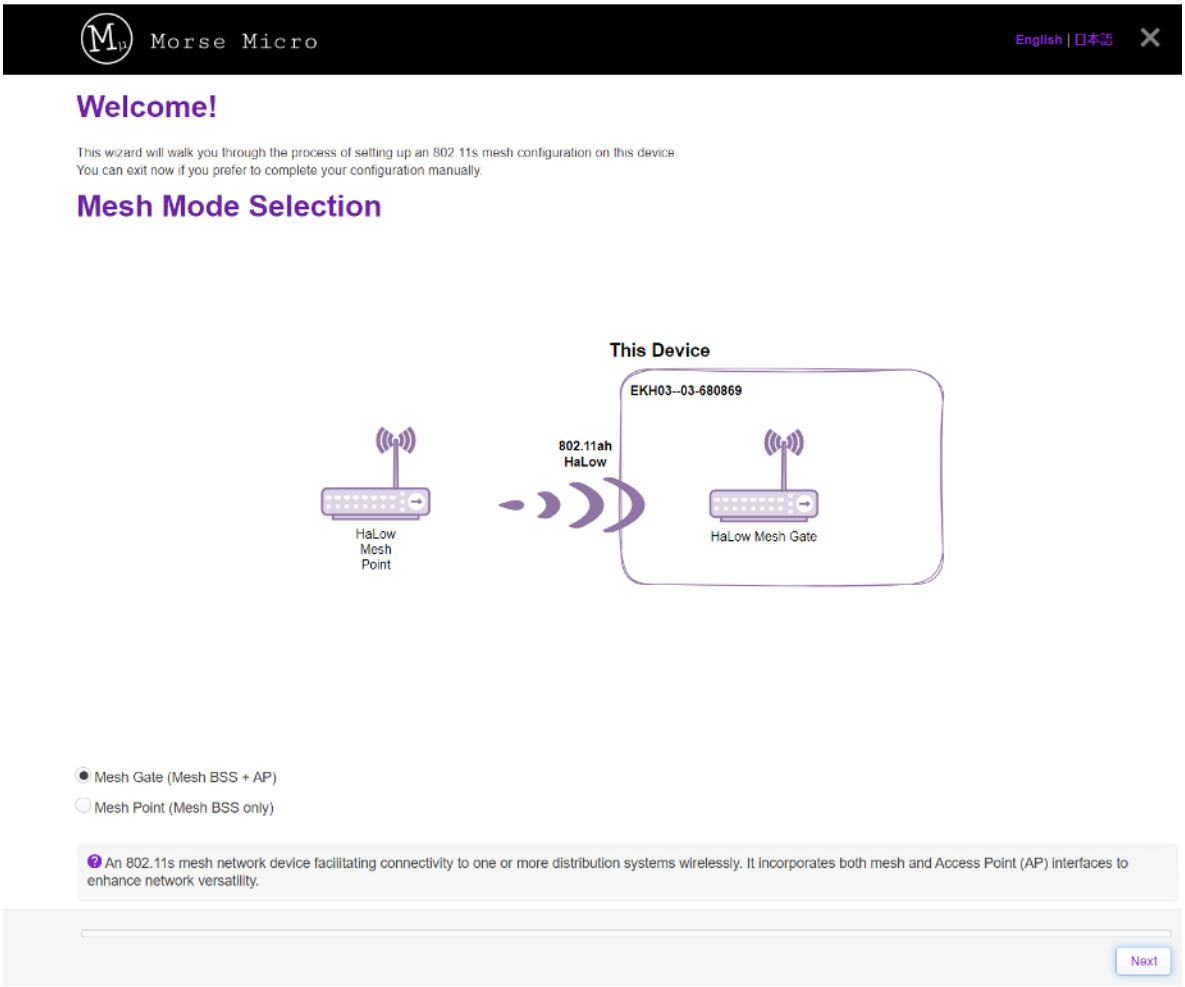


4. On the **Setup Mesh Network -** set an appropriate Mesh ID, encryption and passphrase. Then click **Next**.
5. For the **Traffic Mode**, select 'Bridge' and click **Next**.
6. After saving the configuration (by clicking 'Apply'), disconnect your laptop from the Mesh Point and connect it either to the Mesh Gate or another Mesh Point to integrate it into the

Mesh Network and obtain an IP address for the device. To access the Mesh Point's admin interface again, navigate to the **Status** page of the Mesh Gate's admin interface and inspect the **Active DHCP Leases**.

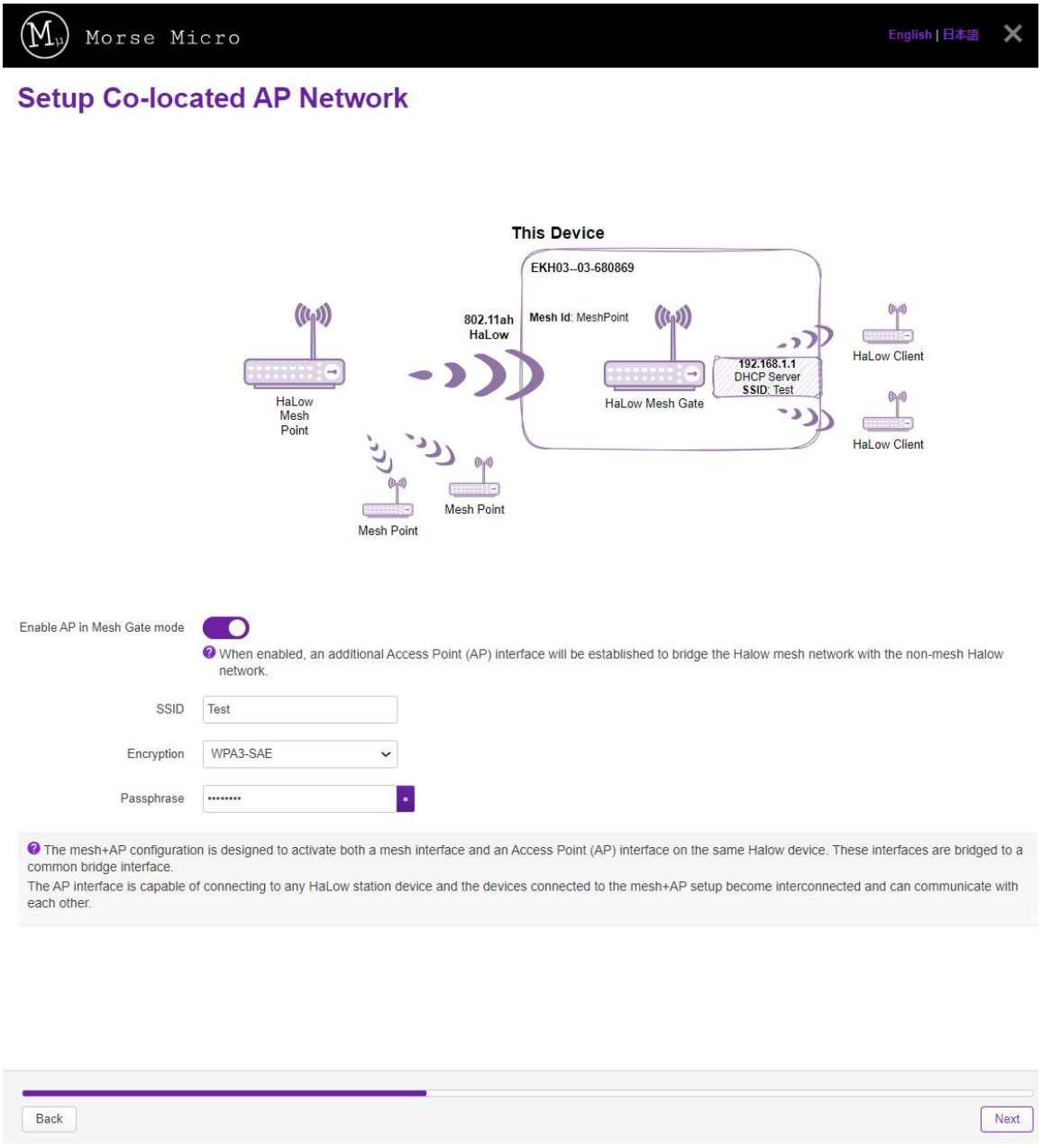
3.9.2 Mesh Gate configuration

1. As a prerequisite, ensure that your device is configured with the appropriate region and a channel. Refer to steps in 3.1 to connect to the device and set the region.
2. Once you decide to configure your device as a Mesh Gate, navigate to the **Morse > 802.11s Mesh Setup Wizard** in the top menu.
3. For **Mode Selection**, choose Mesh Gate:



4. Click the **Next** button at the bottom right to go to the next page.
5. On the **Setup Mesh Network -** set an appropriate Mesh ID, encryption and passphrase. Then click **Next**.
6. For a Mesh Gate, you have the option to set up an additional Access Point interface (**Co-located AP**) alongside the Mesh interface to extend the HaLow network if needed. On the **Setup Co-located AP Network** page, if you enable the AP, then ensure to fill in the SSID, encryption and password for that interface. Please note, that this AP interface

that is created is always bridged with the Mesh interface in the Mesh Gate mode.Then click **Next**.



7. On the following page, **Upstream Network** should be *None*. Click **Next**.
8. You can then **Apply** your configuration on the final page.

3.9.3 (Optional) Add upstream Internet connectivity in Mesh Gate mode

Typically a Mesh Gate is a device that provides access to one or more distribution systems, via the wireless medium for the mesh basic service set (MBSS). Hence it is helpful to have an upstream connection to the Internet. The following steps outline how to connect the Mesh Gate to an upstream router that will provide Internet access to the HaLow devices.

It assumed the upstream gateway provides the following:

- DHCP server to allocate an address to the Mesh Gate's Wired Interface
- DNS server will be provided via an option in the DHCP offer
- A gateway address will be assigned via the DHCP offer

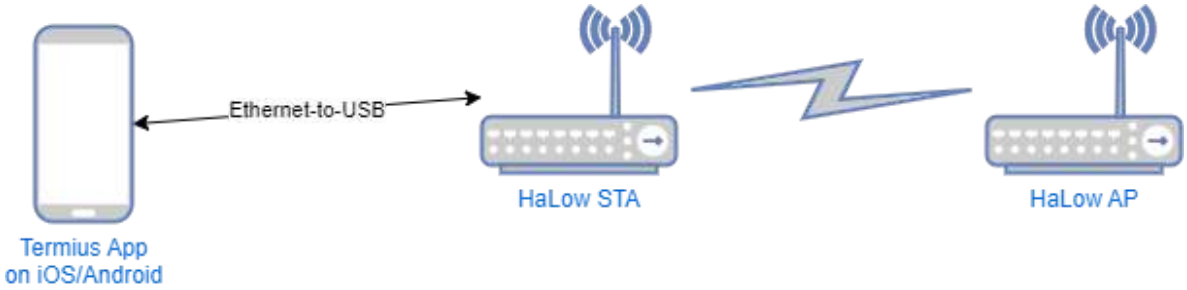
1. Connect your laptop to your device as in 3.1, and go to its admin interface (usually http://10.42.0.1).
2. Go to **Morse > 802.11s Mesh Setup Wizard** in the top menu.
3. On the **Upstream Network** page, choose *Ethernet*, and set the **Traffic Mode** to *Router*.
4. Apply the configuration on the final page.
5. Use an Ethernet cable to connect your Mesh Gate to your existing network.
6. To access the device's admin interface again, you can access 192.168.1.1 over the HaLow link or you will need to determine the address allocated by your network's DHCP server. See section 3.6 for how to reset your device if you lose access.

3.9.4 Additional 802.11s Mesh settings

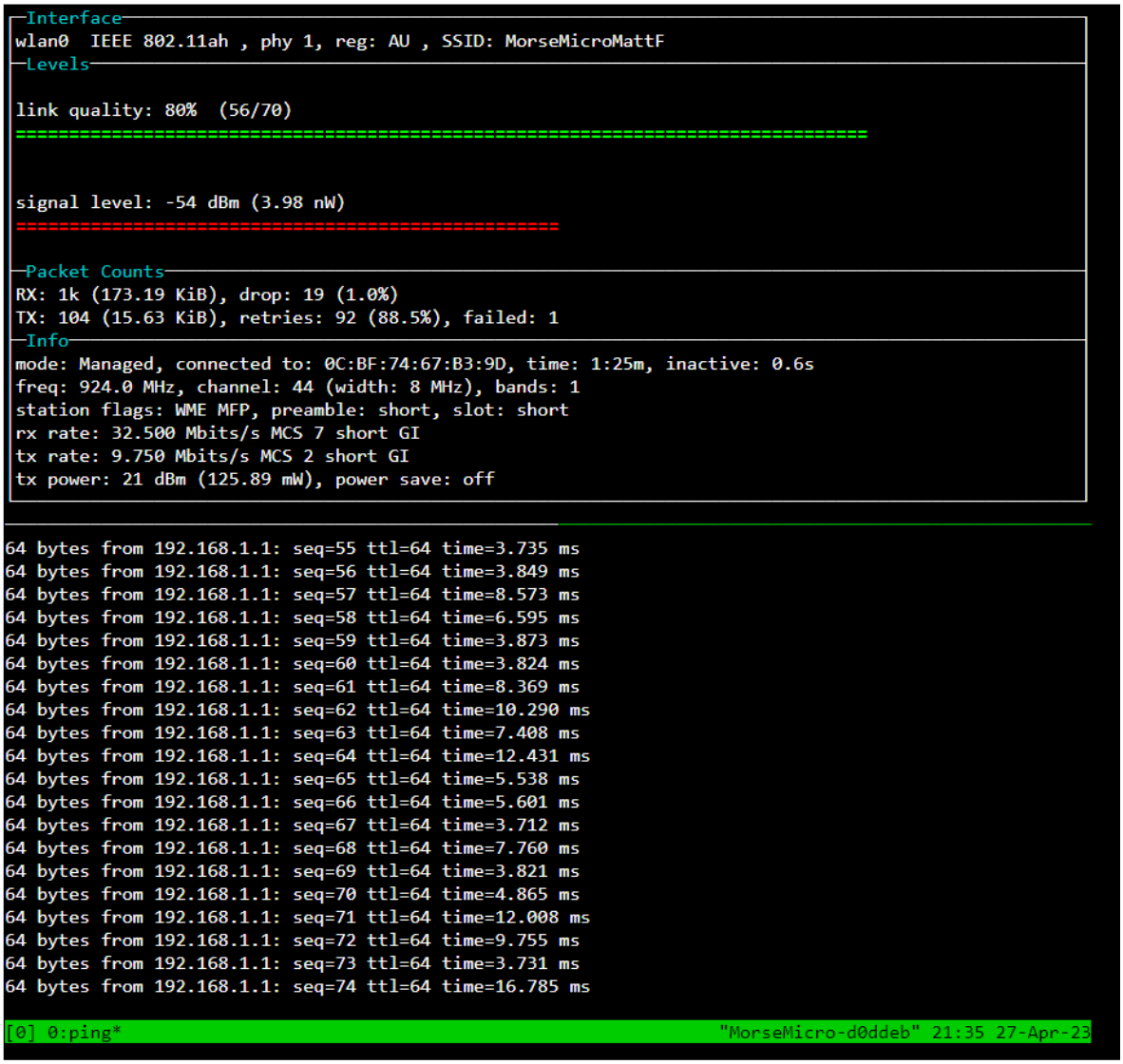
1. In addition to configuring the 802.11s Mesh settings through the wizard, you can access further options by navigating to the **Network > Wireless** page. Click on "**Edit**" next to the Mesh Interface to access and adjust the advanced mesh settings available in this section.
2. If you decide to enable B.A.T.M.A.N for the Mesh Interface in Mesh Gate mode, remember to include the AP interface (if it exists) in the same network. You can achieve this by adding the same network name to the AP interface in Network > Wireless > Edit (AP) > Interface Configuration > Network.
3. If you need to change the HaLow IP address while in 802.11s Mesh Gate/Mesh Sta mode, follow these steps:
    1. Go to the **Network > Wireless page**.
    2. Click "**Edit**" next to the Mesh Interface.
    3. Under **Interface Configuration**, locate the **Network** name in the General setup tab.
    4. Navigate to **Network > Interfaces** and select "**Edit**" next to the corresponding network name.
    5. Modify the **IPv4 address** as needed, then save the changes.

4 Wavemon and Ping Testing

Wavemon provides a powerful way to quickly check the performance and quality of a HaLow connection in the field. All that is required is a mobile phone, HaLow AP and HaLow STA (with a suitable power supply), and a USB-Ethernet cable to connect the mobile to one of the HaLow devices. The diagram below shows how to setup the equipment:



To run wavemon, the mobile device will need to be able to run a SSH session (e.g. using Termius for Android/iOS). Once a SSH session has been started, run the command 'pt' from the command line interface (CLI), and wavemon plus a ping test will be started, see below for a screenshot of how it should appear:



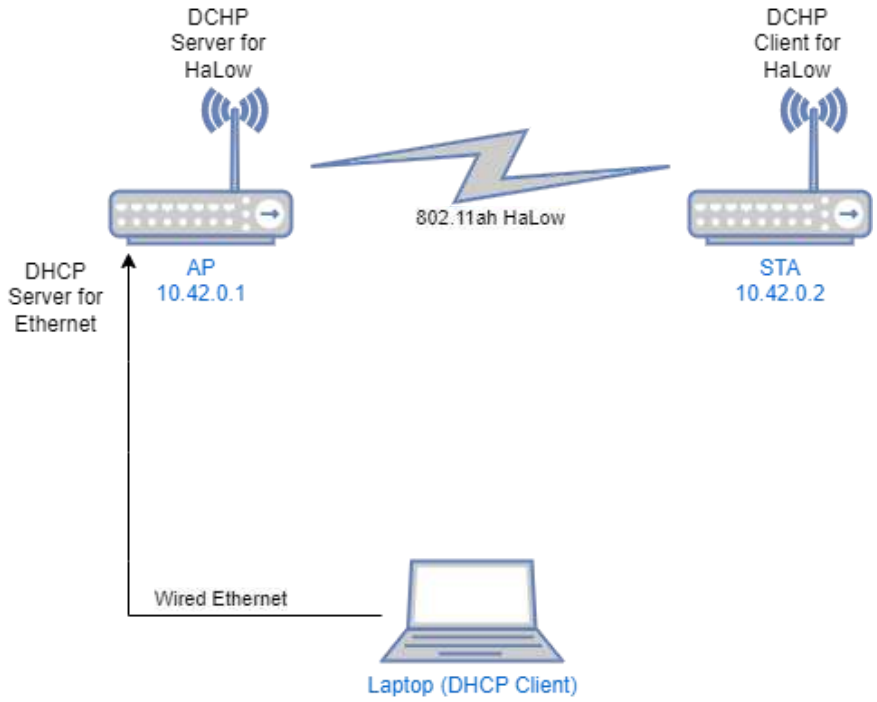
Note that pt will ping 192.168.1.1 by default, but an alternate address can be provided as an argument to the script, e.g. “pt 1.2.3.4”.

5 Setting up iPerf traffic testing

iPerf testing provides a tool for analysing the quality of HaLow connections by sending a stream of traffic and measuring the speed, throughput and latency.

The following guide outlines how to run iPerf traffic between two devices connected via HaLow. In the diagram below, there are two devices, AP and STA, which may be any of the available evaluation kits (EKH01, EKH03).

In this setup the AP will also be the iPerf server, and the STA will be the iPerf client.



5.1 AP configuration

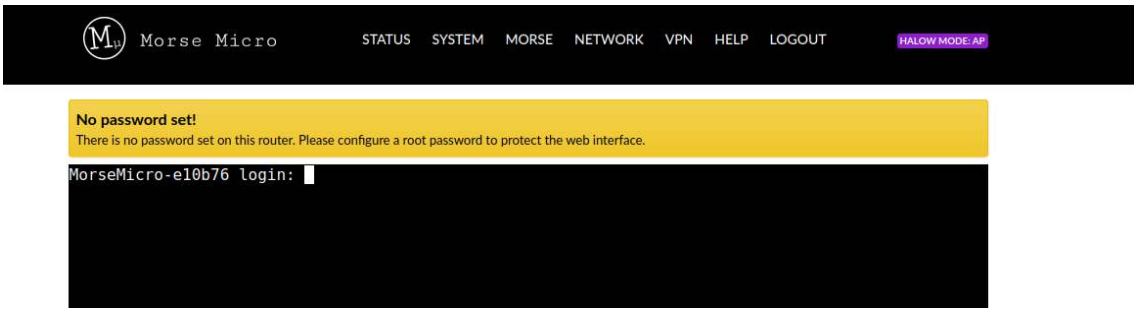
1. Connect an antenna (if applicable).
2. Connect an Ethernet cable from your PC to the RJ45 port of the Morse Micro device.
3. Connect a USB-C power cable to the Morse Micro AP device.
4. Power the unit on and wait ~60 seconds to allow the device to start up.
5. In a web browser on the laptop, navigate to the web UI of the device (http://10.42.0.1 by default). Close the wizard (click 'X' on the top right) if it's enabled.

   Note: If DHCP client mode is enabled on the Ethernet port, it will be assigned an IP address via DHCP from the upstream device.

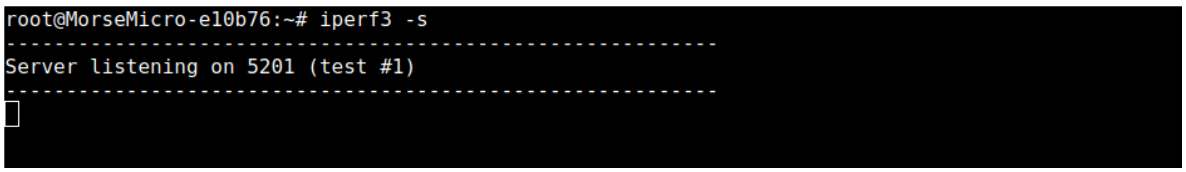
6. Navigate to the **Morse->HaLow Config** page in the top menu of the UI. Select 'Access Point' and configure the following settings (the rest can remain as default):

Configuration item	Value
Region	AU (or as appropriate)
Wired IP address	10.42.0.1 (default)
Enabled HaLow DHCP server	Enabled

7. Navigate to the 'Shell' page under the MORSE menu in the top navigation bar. Note the credentials will be the same as used to login to the web UI.

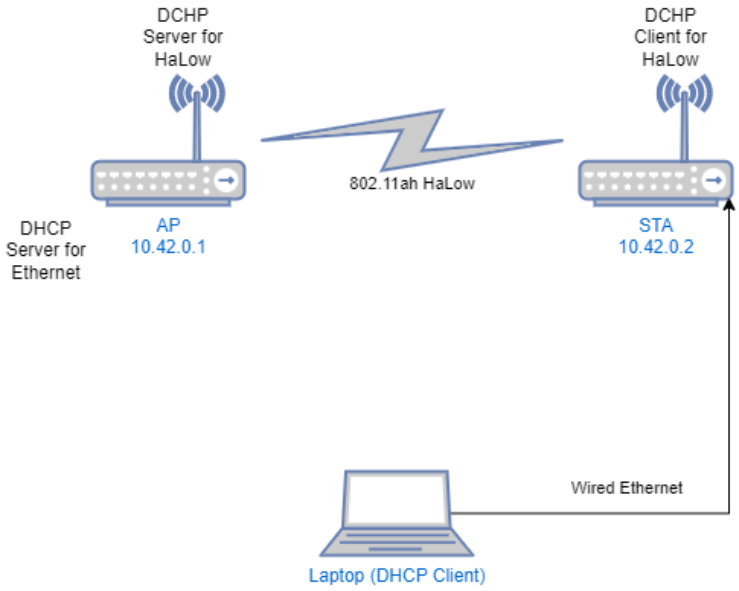


8. Type ‘iperf3 -s’ and press enter to launch the iperf3 server.



9. Remove the Ethernet cable from your PC. **Warning:** the server will only run for a short amount of time, so you must do the client setup and iperf3 below immediately. If you wish to keep the server running indefinitely, start the iPerf server within **tmux** (included in the image).

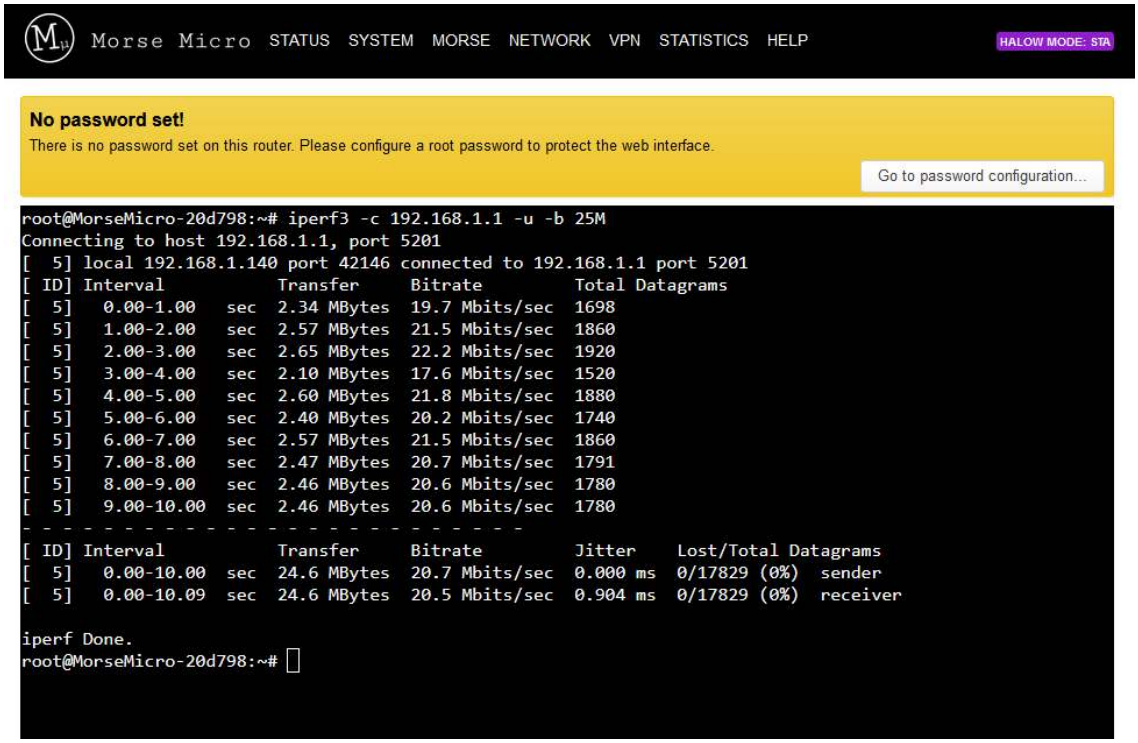
5.2 STA configuration



1. Connect an antenna (if applicable).
2. Connect an Ethernet cable from your PC to the RJ45 port of the Morse Micro device.
3. Connect a USB-C power cable to the Morse Micro AP device.
4. Power the unit on and wait ~60 seconds to allow the device to start up.
5. In a web browser on the laptop, navigate to the web UI of the device (http://10.42.0.1 by default). Close the wizard (click 'X' on the top right) if it's enabled.
6. Navigate to the **Morse->HaLow Config** page in the top menu. Select 'Station' and configure the following settings (the rest can remain as default):

Configuration item	Value
Region	AU (or as appropriate)
Wired IP Address	10.42.0.2
SSID/Encryption/Password	Matching the config on the AP
HaLow IP Method	DHCP

7. Navigate to the 'Shell' page under the MORSE section in the UI navigation menu.
8. Type 'iperf3 -c IP_ADDR -u -b 25M' where IP_ADDR is the IP address of the other side of the HaLow link and press enter to launch the iperf3 client. The STA will connect as an iperf3 client to the server running on the AP to run traffic between them.



5.3 Web user interface

You can also run iPerf in server and client mode via the web UI. This can be accessed from the top menu in UI by browsing to **Network -> Diagnostics**.

6 EasyMesh

6.1 Theory of Operation

EasyMesh is a Wi-Fi branded, standards-based solution for meshing together access points to provide an extended coverage area (but with reduced bandwidth available to stations). EasyMesh forms a tree structure with a controller at the root that controls the mesh network, and agent APs that connect both upstream towards the controller and downstream towards stations. Stations are agnostic to mesh, and continue to connect to the closest AP as usual.

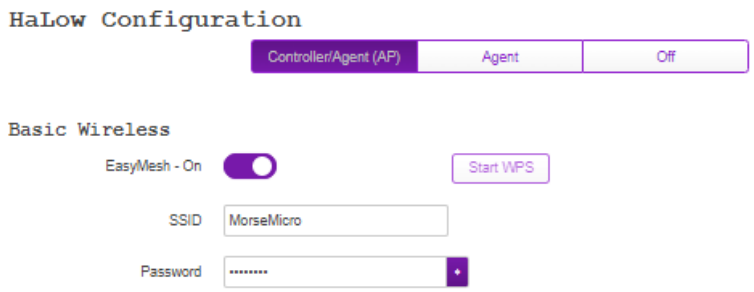
The current implementation supports up to 4 agents in addition to the controller, with at most 2 agents between the controller and a station.

6.2 EasyMesh Configuration

6.2.1 Access Point Controller

Navigate to the **Morse->HaLow Config** page in the top menu of the UI. Select 'Access Point' mode, and then turn on the EasyMesh toggle at the top of the page.

The page will display a new set of configuration specific to EasyMesh:

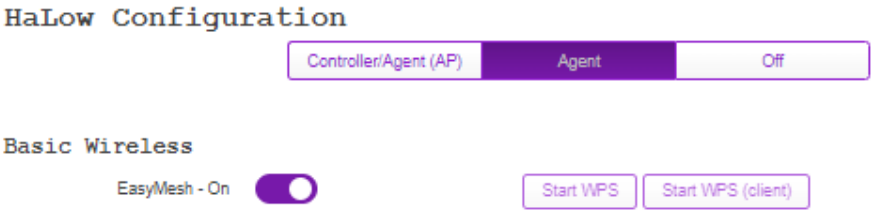


From here, select 'Controller' and configure the remaining settings as per a normal access point. When a new access point agent is being added to the mesh, the 'Start WPS' button can be used to initiate the agent onboarding process.

6.2.2 Access Point Agent

Navigate to the **Morse->HaLow Config** page in the top menu of the UI. Select 'Access Point' mode, and then turn on the EasyMesh toggle at the top of the page.

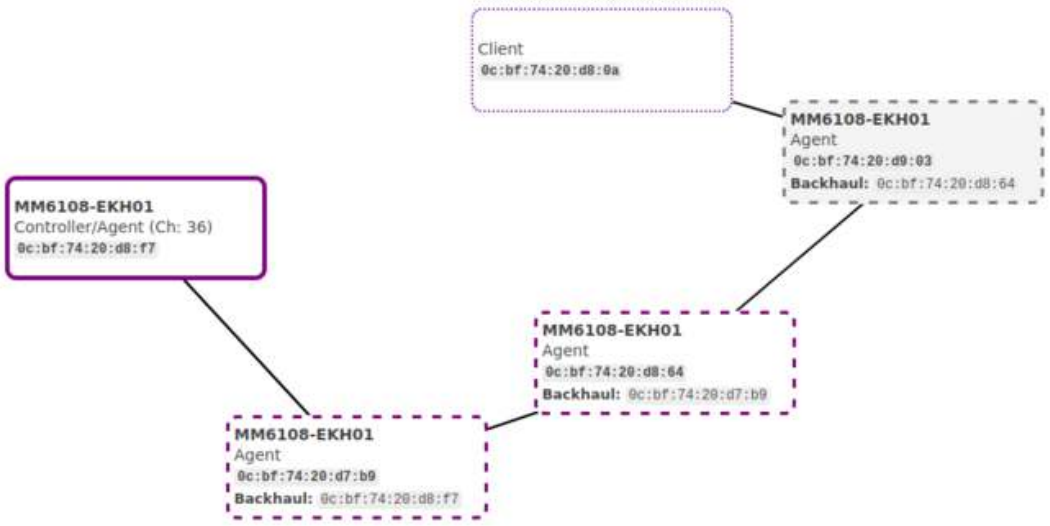
The page will display a new set of configuration specific to EasyMesh:



From here, select 'agent', and configure the remaining settings as per a normal access point. Click 'save' to apply the settings. When the agent is ready to be added to the mesh, the 'Start WPS (client)' button can be used to initiate the agent onboarding process.

6.3 EasyMesh Status

To confirm that EasyMesh has been enabled and is working, status information is available on the 'Status -> Overview' page, with a diagram showing the current topology:



For a controller, you'll also see a summary of the current connection map:

EasyMesh

Management mode	Multi-AP-Controller-and-Agent
Operating mode	Gateway
Agent operational	yes

```
Start conn map
Found 1 devices
Device[1]: name: GW_MASTER, mac: 0e:bf:74:cb:29:27, ipv4: 10.84.0.1
        RADIO[1]: mac: 0c:bf:74:cb:29:27, ch: 44, freq: 924MHz, bw: 8 Mhz
```

Logs are also available from 'Status -> System Logs' when EasyMesh is enabled. If these are not visible, you may need to logout of the frontend due to caching.

System Log | Kernel Log | EasyMesh Controller Log | EasyMesh Agent Log

EasyMesh Controller Log

```
INFO 23:55:50:909 <548423347296> beerocks_master_main.cpp[514] -->
Running beerocks_controller Version 3.1.0 Build date 2023-06-02_00-13-53


INFO 23:55:50:910 <548423347296> beerocks_version.cpp[119] --> beerocks_controller 3.1.0 (2023-06-02_00-13-53) [1.8.1]
DEBUG 23:55:50:911 <548423347296> bpl_cfg.cpp[161] --> steer on vaps list is not configured
DEBUG 23:55:50:915 <548423347296> bpl_cfg.cpp[705] --> get unsuccessful_assoc_report_policy: false
INFO 23:55:50:916 <548423347296> bpl_cfg_helper.cpp[88] --> cfg_get_prplmesh_param_int_default: missing parameter 'rssi_measurements_timeout', using default: 10000
INFO 23:55:50:916 <548423347296> bpl_cfg_helper.cpp[88] --> cfg_get_prplmesh_param_int_default: missing parameter 'beacon_measurements_timeout', using default: 6000
INFO 23:55:50:916 <548423347296> beerocks_event_loop_impl.cpp[73] --> Register handlers for FD (10) of '/tmp/beerocks//uds_controller server'
DEBUG 23:55:50:917 <548423347296> network_utils.cpp[1239] --> ip_item iface=br0
```

7 Video Streaming

OpenWrt includes functionality to allow streaming video from cameras connected to stations back to the AP where it can be viewed within the web UI. This includes automatic discovery of cameras on the HaLow network where these are running the camera specific firmware (noted below in station configuration). This autodetection will work for any ONVIF compliant camera on the network supporting H.264 streams.

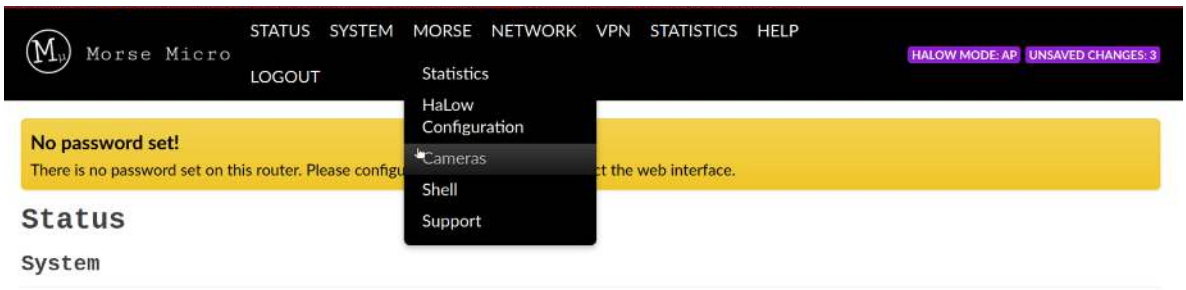
NOTE: When using the EKH03 as an AP, you view at most two live streams in the web UI at once. This is because of the CPU and memory requirements for proxying the streams.

7.1 Setting up

Follow Chapter 3 to configure your network, and determine the IP address of your AP.

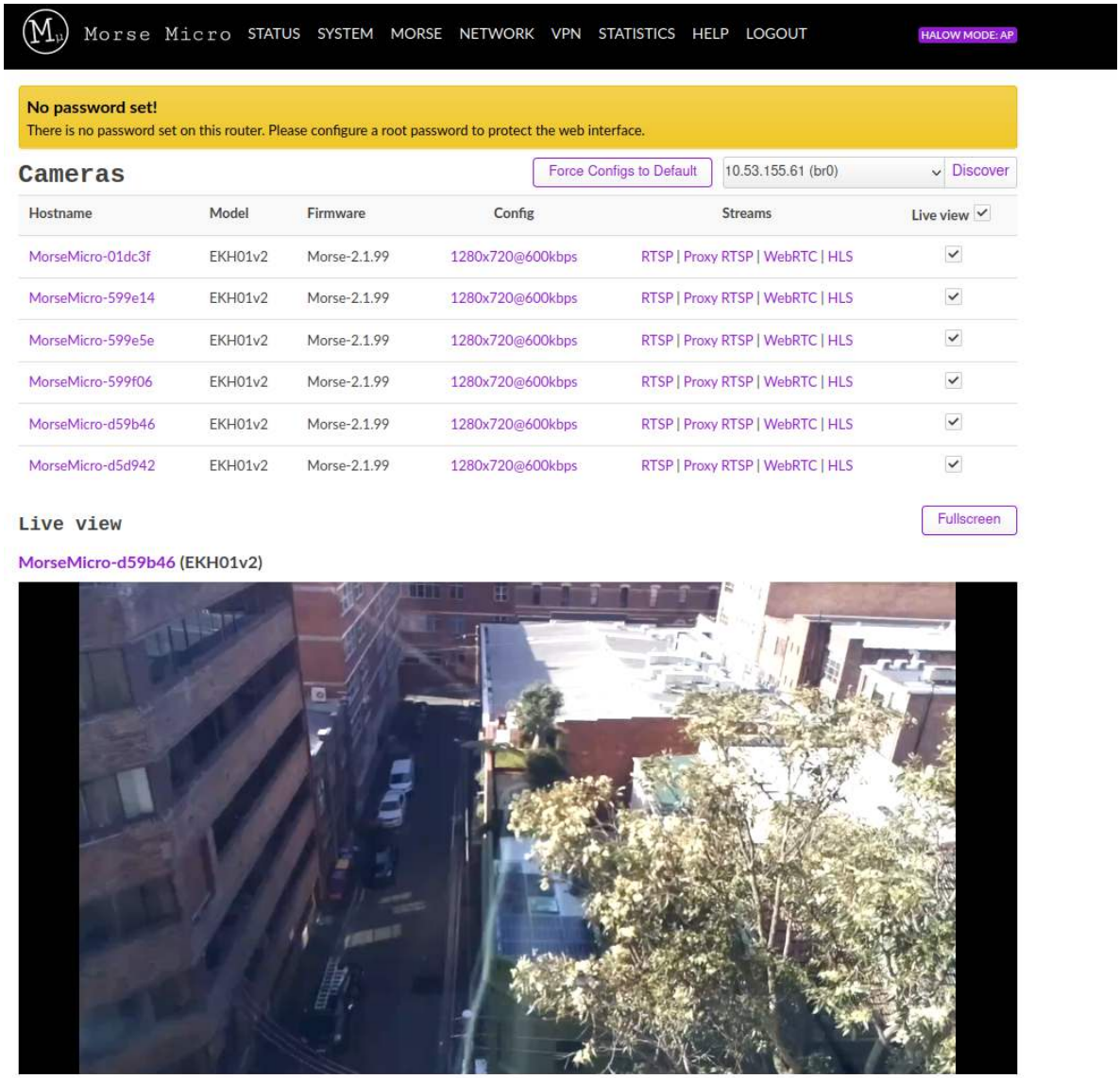
7.2 Getting Video Stream

In your browser navigate to web GUI of the access point and navigate to the 'Morse -> Cameras' section, shown below:



In the camera section the AP will automatically discover all ONVIF cameras on the network. Note that it will only scan the network attached to the interface listed on the top right, next to the 'Discover' button. After scanning it will automatically start streaming from the first 2 discovered cameras.

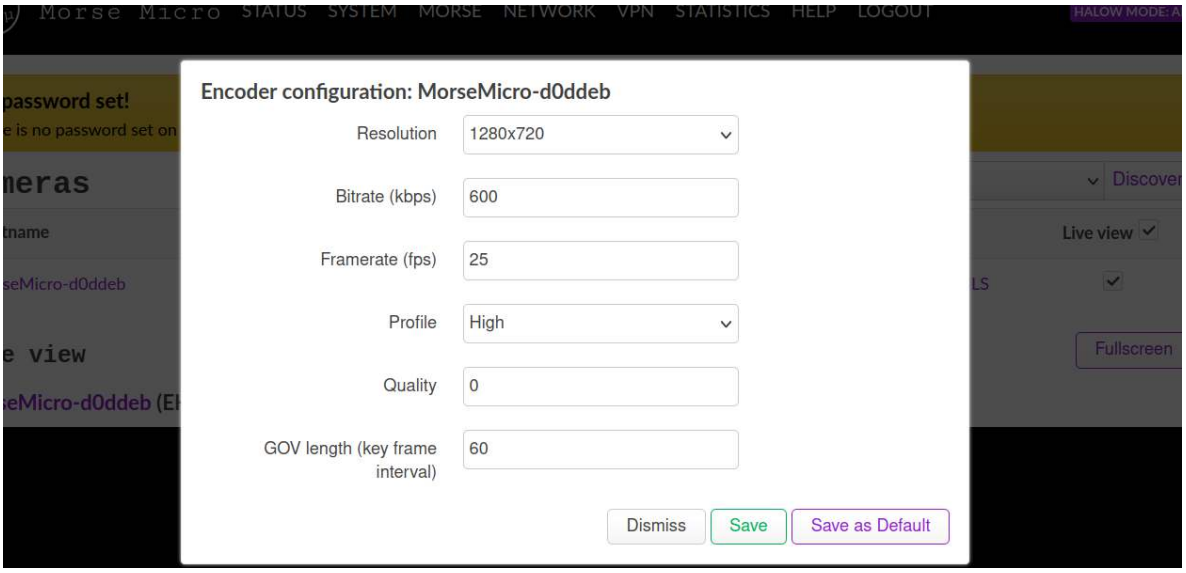
The checkboxes under the 'Live view' column are used to select which video streams should be displayed.



7.3 Configuration

The following fields are available for configuring video streaming:

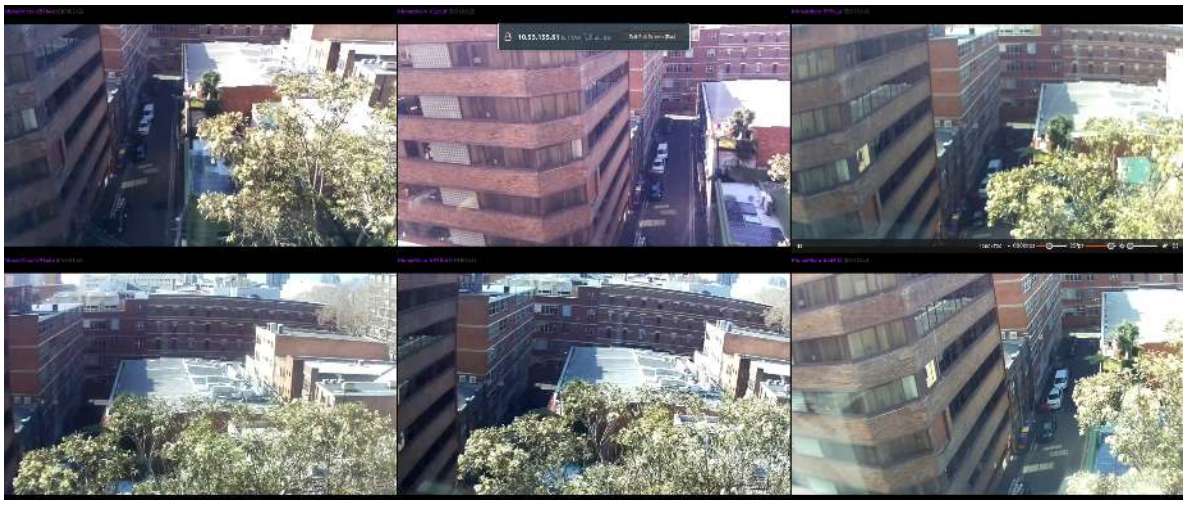
- **Force Configs to Default** - Changes all camera configurations to the default configuration. Hovering over the button displays the default configuration.
- **Discover** - Force the device to rediscover cameras on the selected interface.
- **Config** - Opens a window to modify the camera's configuration.



  - **Resolution** - Sets resolution of the camera
  - **Bitrate** - Sets bitrate of the video stream
  - **Framerate** - Sets framerate of the video stream
  - **Profile** - Sets the H264 profile
  - **Quality** - 0 for constant bitrate (CBR) and 1 for variable bitrate (VBR)
  - **GOV length** - Sets number frames between each I frame
  - **Save as Default** - Overrides the current default and sets the new default to your selected options.

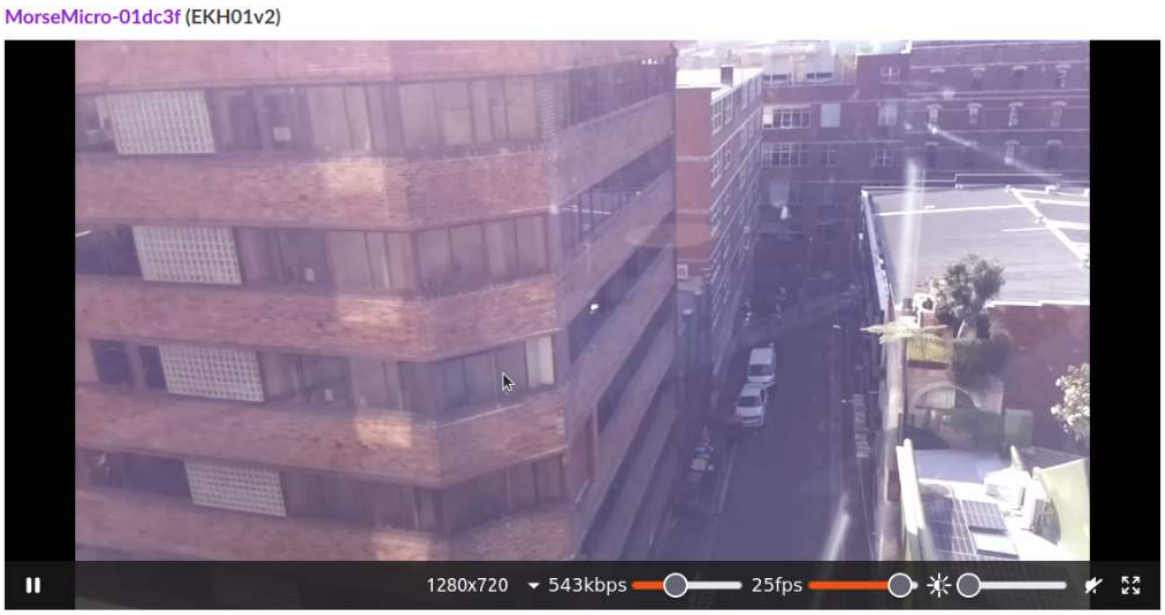
- **Streams** - Select the type of stream you want to view (this will open a new window to play the selected stream).
- **Live View** - Select whether to show a live stream on the page (via WebRTC).

- **Fullscreen** - Fullscreen view of all the currently enabled streams. To see a fullscreen view of an individual stream, hover over the stream to bring up the video controls. Full screen mode is shown below:



7.3.1 Live View

Cameras can also be configured from the live view window, that includes the resolution, bitrate, framerate and brightness.

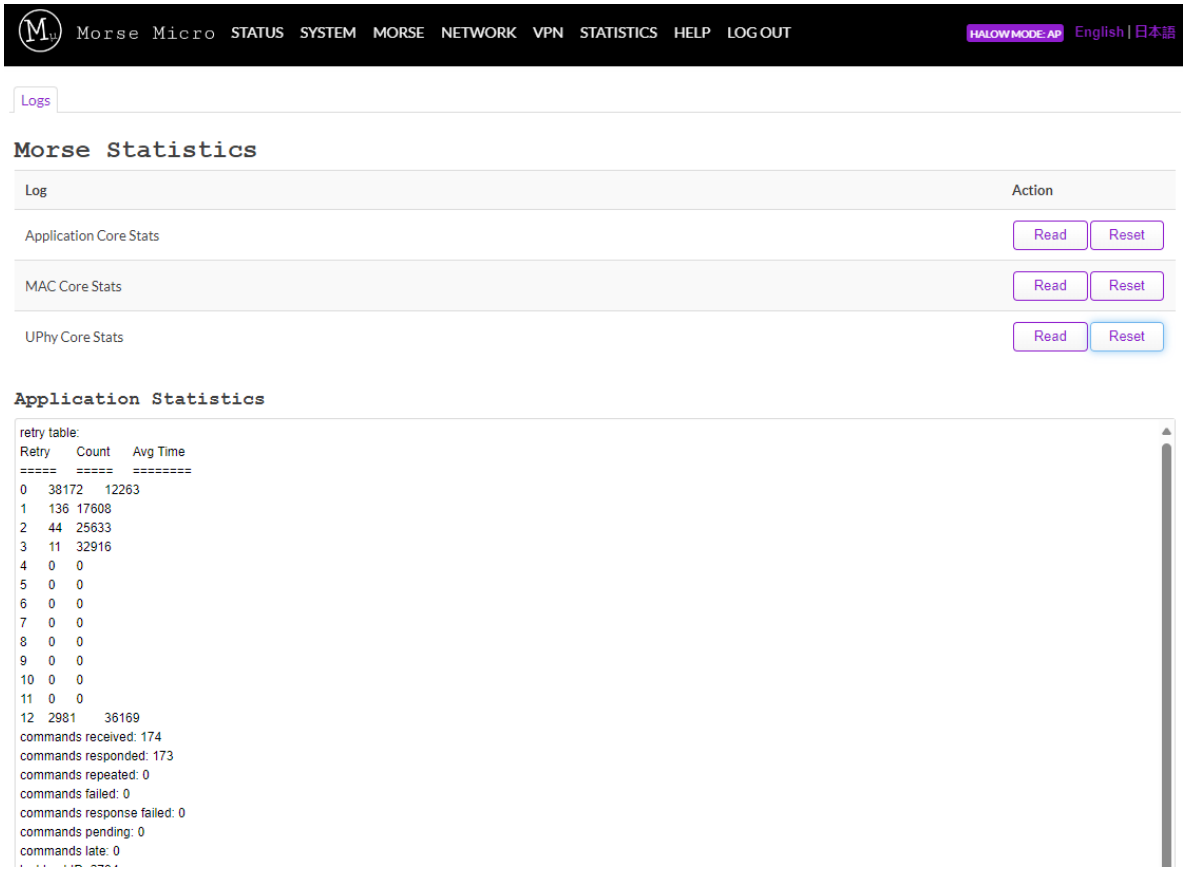


8 Page Descriptions

This section describes some of the pages available in the web UI.

8.1 Morse → Statistics

This page provides the ability to query statistics from each of the processor cores on the MM6108 chip. Select 'Read' to read out the current value of statistics for a given core, or 'Reset' to reset the statistics back to zero. The underlying information on this page is gathered via the morse_cli command, which can also be used to see this information from the CLI.



8.2 Status → Realtime Graphs → Wireless

The Realtime Graphs page displays animated graphs of HaLow statistics. The graphs show the last 3 minutes of data and update on a 3 second interval. The three graphs show signal strength, data rates, and MCS respectively.

8.3 Morse → HaLow Config

The **HaLow Config** page can be used to configure HaLow on the device in either Access Point, Station, or Ad-Hoc (IBSS) modes. Note that settings do not take effect until the 'Save' button at the bottom of the page is clicked.

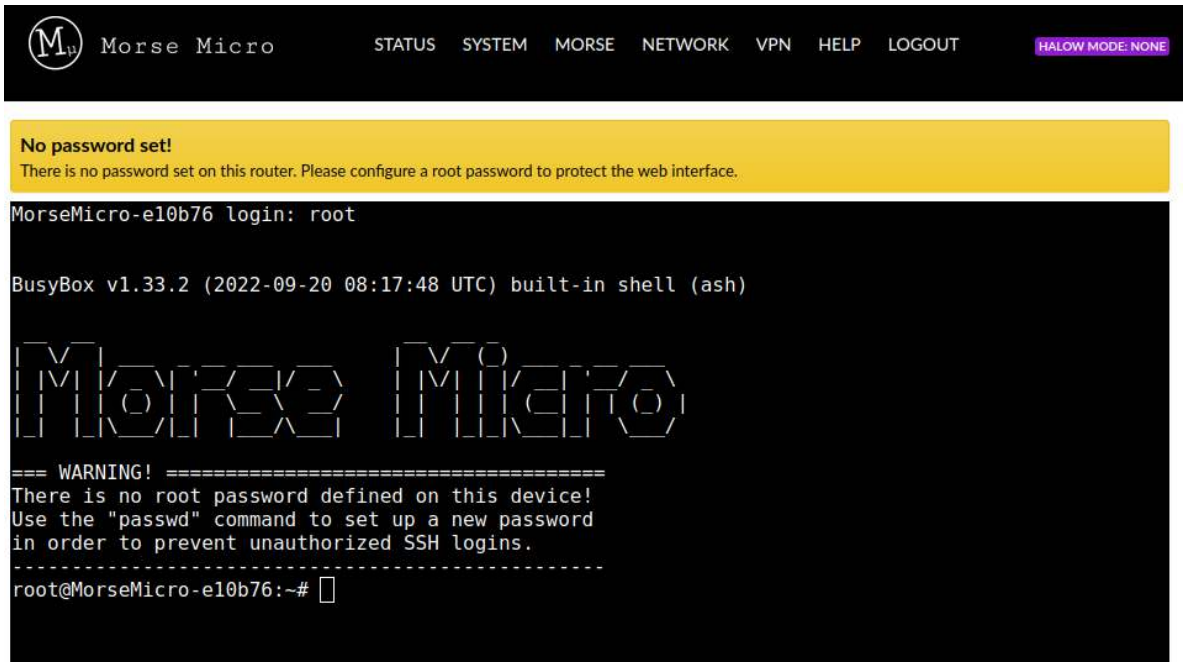
The following fields are available (only a subset of these is available for each mode):

- **Region** - Use this field to define which regulatory region you are using the HaLow device in. Based on this, restrictions on channel, bandwidth, power and duty cycle will be applied to ensure regulatory compliance. *See MM6108 Channels Guide for more information*. Only currently supported regions will be displayed in the drop-down list.
- **Mode** - This determines the mode of operation for the HaLow radio on the device and can be one of: Access Point, Station, Ad-Hoc(IBSS), or off (the radio is disabled).
- **SSID** - Configures the SSID to connect to. Initially the field will show the currently configured SSID. Clicking the 'Scan' button will cause the device to scan for visible HaLow networks and populate the dropdown with visible SSIDs, which can then be selected. If the SSID is not visible, it is possible to type in the name manually and press enter to set it.
- **Encryption** - Select the method used to encrypt data sent over the HaLow network. There are two methods currently available, OWE and SAE. OWE (Opportunistic Wireless Encryption) does not require a password to be set, and does not authenticate the station, but only ensures privacy between the station and the access point from other listening devices. SAE (Simultaneous Authentication of Equals) uses pre-shared passwords to set up a symmetric encryption that is well suited to mesh networks.
- **Password** - This field will be visible when SAE is selected as the encryption method (see above), and configures the password used to authenticate and set up encryption between this station and the access point.
- **Bridge** - Select to enable bridging mode between HaLow and Ethernet interfaces. This creates a single Layer 2 network for all Ethernet and HaLow devices connected to the station. This allows traffic to transit across the station transparently.
- **Traffic Forwarding** - This is similar to bridge mode above in that it allows traffic to be routed across the device while retaining separate networks on each interface. It provides greater control and flexibility but with additional complexity, so should be considered an advanced configuration only to be used when required.
- **HaLow IP Method** - When this is set to static it is possible to manually configure a specific IP address on the HaLow interface, along with the associated netmask and gateway. The other option is 'DHCP client' which will retrieve these settings from a DHCP server if available. It is generally preferable to use DHCP if possible. If using the static method, it is recommended to choose an IP address with 4th octet of 2 or above, so that 1 is available for the access point and potential address clashes are avoided.
- **HaLow IP Address** - This field will set a specific IP address to use for the HaLow interface. Only available if 'HaLow IP Method' is static.
- **HaLow Netmask** - The netmask to use on the HaLow interface. Only available if 'HaLow IP Method' is static.
- **HaLow Gateway** - The IP address of the upstream gateway to send all HaLow IP traffic to by default. Only available if 'HaLow IP Method' is static.

- **Wired IP Method** - There are 3 methods available: DHCP Server (default), DHCP client, and Static address.
- **Wired IP Address** - The specific IP Address to assign to the wired interface when using the 'DHCP server' or 'Static' method.
- **Wired Netmask** - The netmask to use on the wired interface when using the 'DHCP server' or 'Static' method.
- **Wired Gateway** - Only available when using 'DHCP Server' or 'Static' methods. This sets the gateway address to forward all traffic that is not local to the station.
- **DHCP Range Start/End** - These define the first and last IP address that should be assigned by the DHCP server on the wired interface for incoming requests. The subnet is the same as the Wired IP address, with these fields setting the range based on the 4th octet of the IP address. It is usually safe to leave this as default, unless there is a need for a restricted or expanded number of addresses to be available.
- **Operating bandwidth** - The operating bandwidth to use for the HaLow network (dropdown is automatically populated based on the currently selected region).
- **Channel** - The frequency channel to use for the HaLow network (dropdown is automatically populated based on currently selected operating bandwidth)
- **Protected Management Frames** - enabling this feature provides additional protection for management frames used for things such as authentication, de-authentication, association, disassociation, beacons, and probes. By default management frames are sent unencrypted, but enabling this feature allows them to be encrypted and for forged frames to be detected, which is useful to prevent disconnect, honeypot, and evil-twin attacks.
- **Beacon Interval** - How often beacons should be broadcasted, measured in milliseconds.
- **DTIM Period** - The DTIM period to use, measured in number of beacon intervals. Based on this, the beacon will only include Delivery Traffic Indication Messages(DTIM) once per period.
- **Max inactivity** - The maximum amount of time the access point can be inactive, measured in seconds.

8.4 Morse → Shell

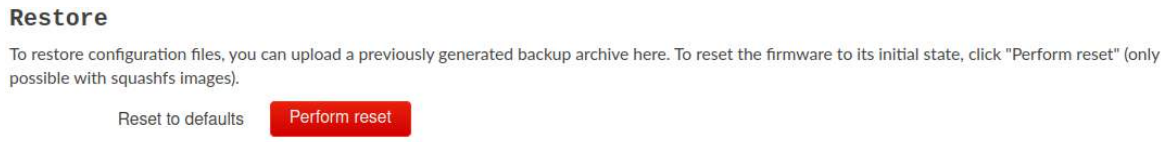
The Shell page allows the user to spawn a shell usable in the web browser. The shell can be hidden navigating to another page within the Web Interface.



8.5 System → Backup / Flash Firmware

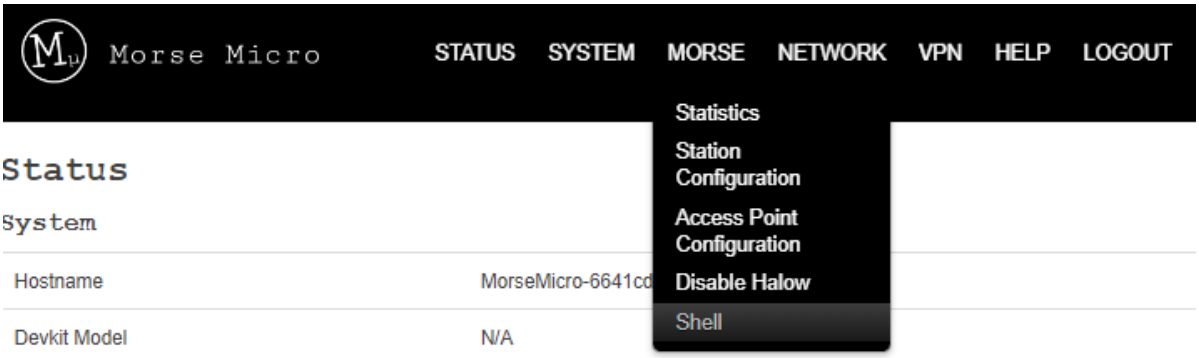
Perform reset button allows you to factory reset the device

Note: for EKH01 images using ext4 this will only reset the Morse Micro specific configurations; ext4 was only available for EKH01 in v2.2.2 and earlier.



9 Advanced Configuration

Some advanced configurations are useful to control HaLow behavior (particularly during certifications) and are documented here for convenience. Some may not be available via the web UI, but can be configured via the CLI if required. If unsure about whether to use these, it is best not to change the default unless advised by an FAE to do so.



The CLI is available from UI by navigating to the top menu and selecting 'Morse -> Shell'. For advanced users the CLI is available via SSH and serial console. The credentials are the same ones used to login to the web UI.

9.1 Disable AMPDU

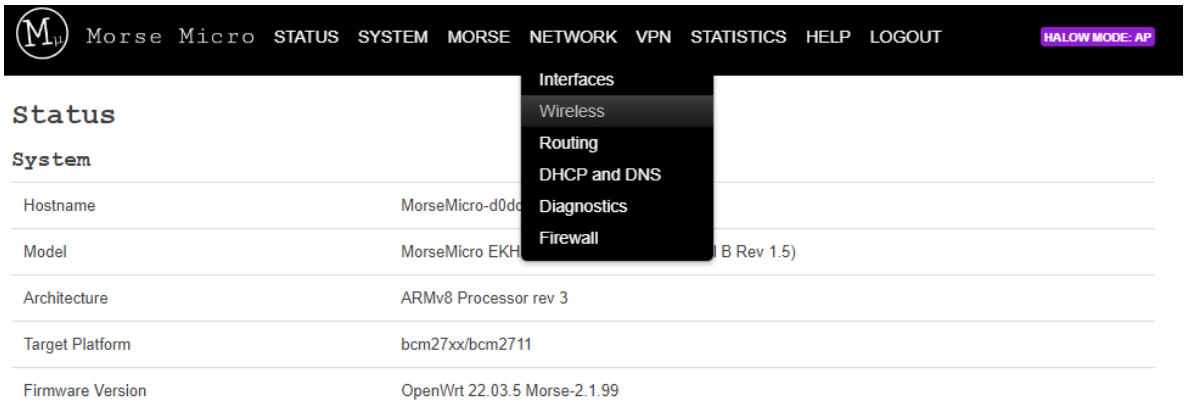
9.1.1 CLI

AMPDU can be disabled by running the following commands:

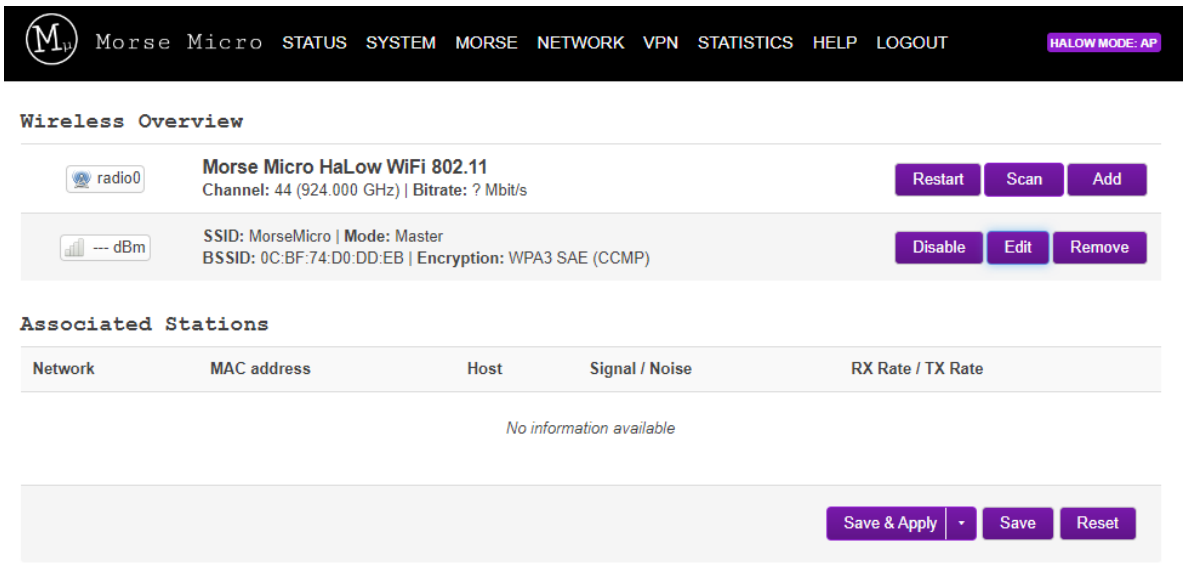
```
morse_cli -i wlan0 ampdu disable
```

9.1.2 Via UI

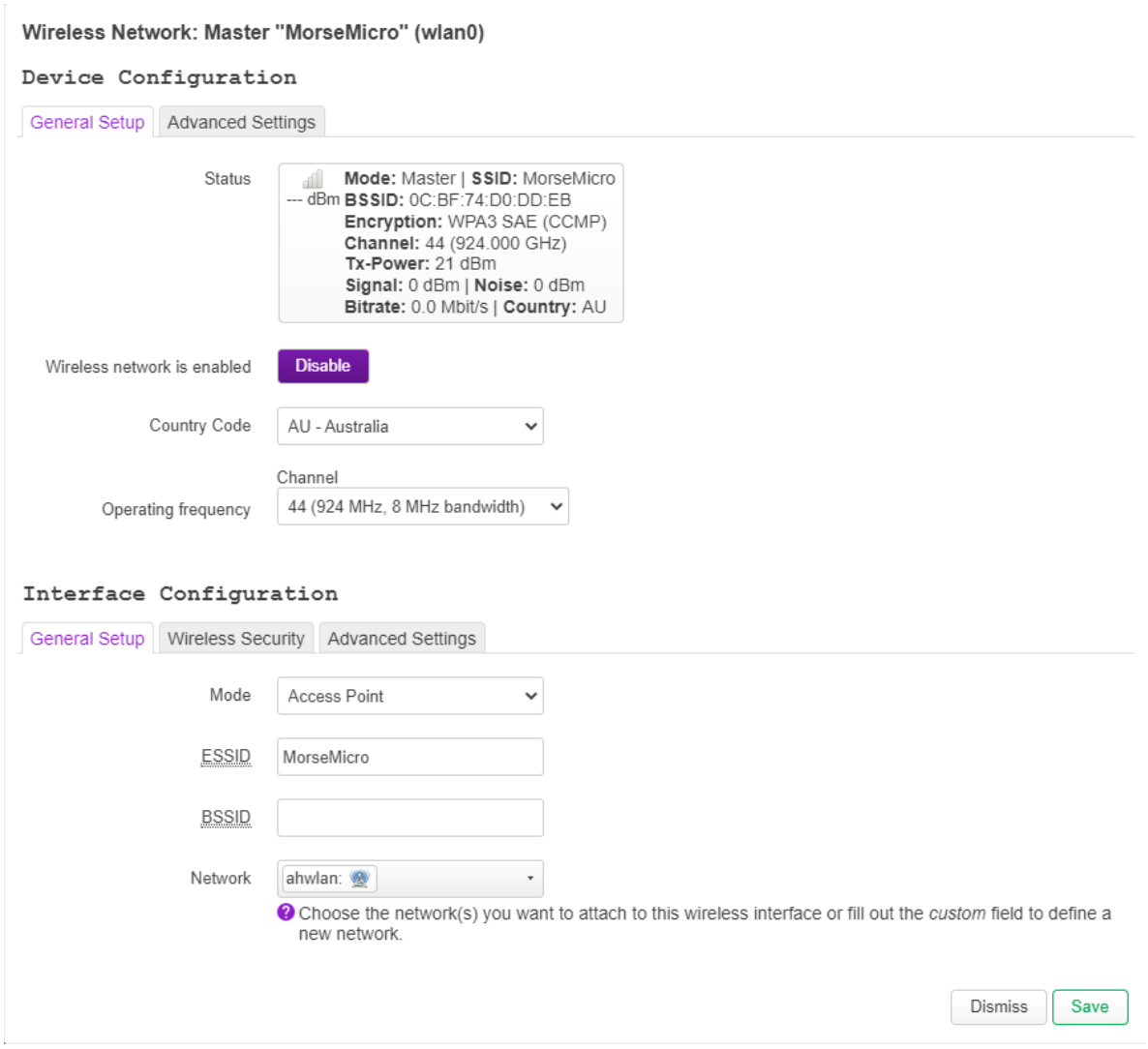
AMPDU can be configured in the advanced settings under the Network->Wireless menu:



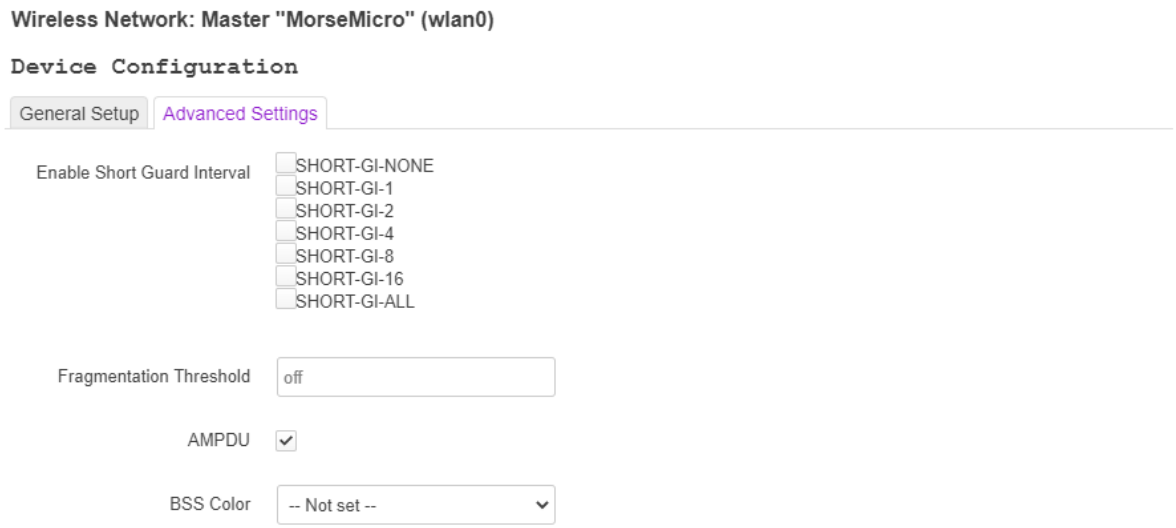
Select 'Edit' next to the HaLow network that is to be configured:



Select the 'Advanced Settings' tab in the Device Configuration section:



The untick the ‘AMPDU’ option to disable AMPDU:



9.2 Fragmentation Threshold

9.2.1 Via UI

In the same configuration section as above for AMPDU, there is an option for configuring the fragmentation threshold. To disable this feature enter 'off' into the field, otherwise the number of bytes beyond which fragmentation should occur.

9.2.2 Via CLI

The fragmentation threshold can be set with the `iw` tool:

```
iw phy <phyname> set frag <fragmentation threshold|off>
```

Where the <phyname> is provided by the iw list command, e.g.

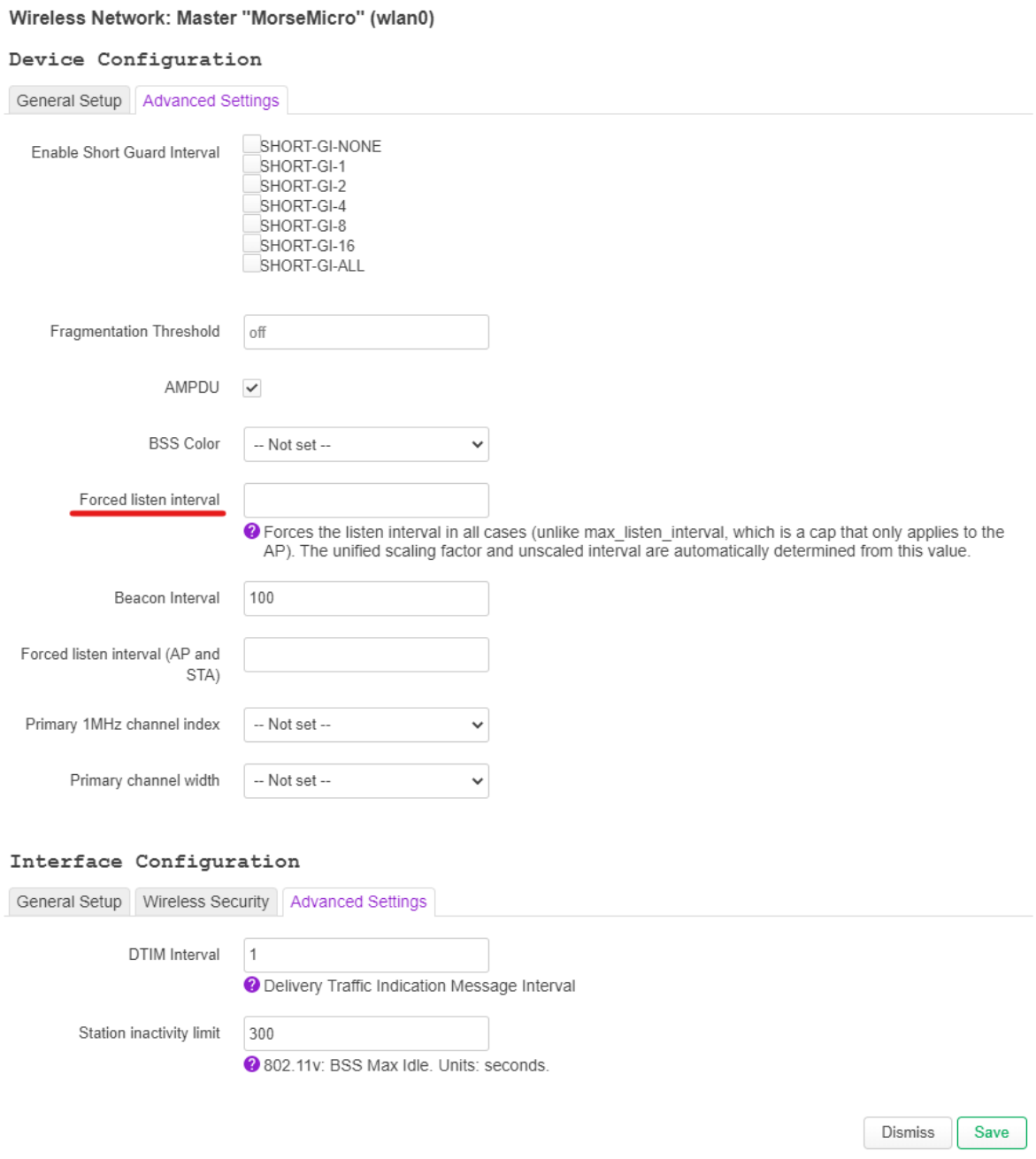
```
# iw list | grep Wiphy

Wiphy phy1
```

In this case, `phy1` is the `<phyname>`. The integer following phy enumerates every time the driver is (re)loaded.

9.3 Unified Scaling Factor / Unscaled Interval

9.3.1 Via UI

Navigate to Network->Wireless and then choose 'edit' beside the HaLow network. Use the forced listen interval in Advanced Settings tab:



9.3.2 Via CLI

The UI and USF must be set together, with the morse_cli tool using the command:

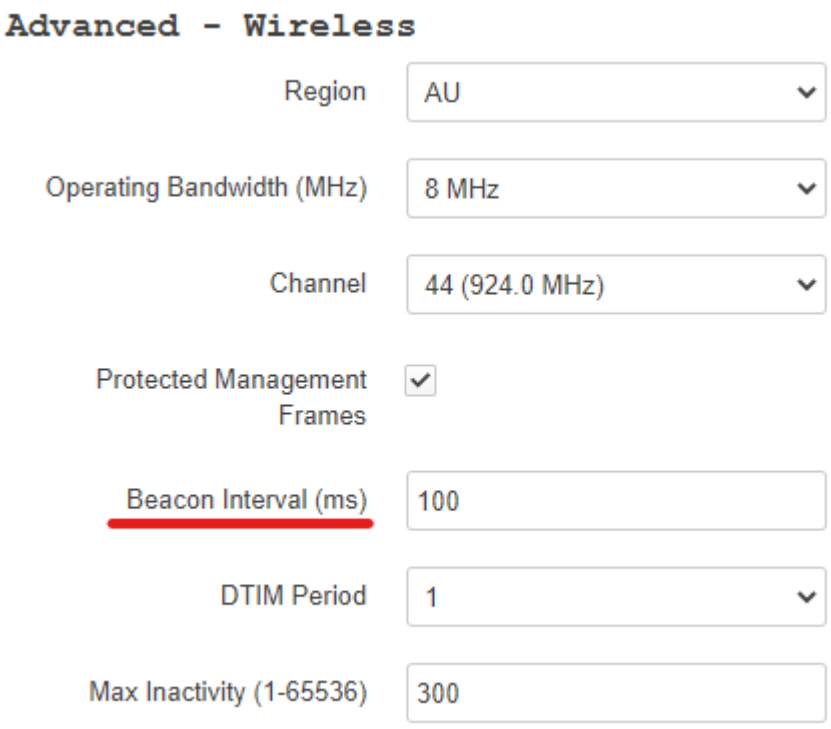
```
morse_cli -i wlan0 li <unscaled interval> <unified scaling factor>
```

Where `<unscaled interval>` multiplied by `<unified scaling factor>` must be less than or equal to the integer value 65536.

9.4 Beacon Interval

9.4.1 Via UI

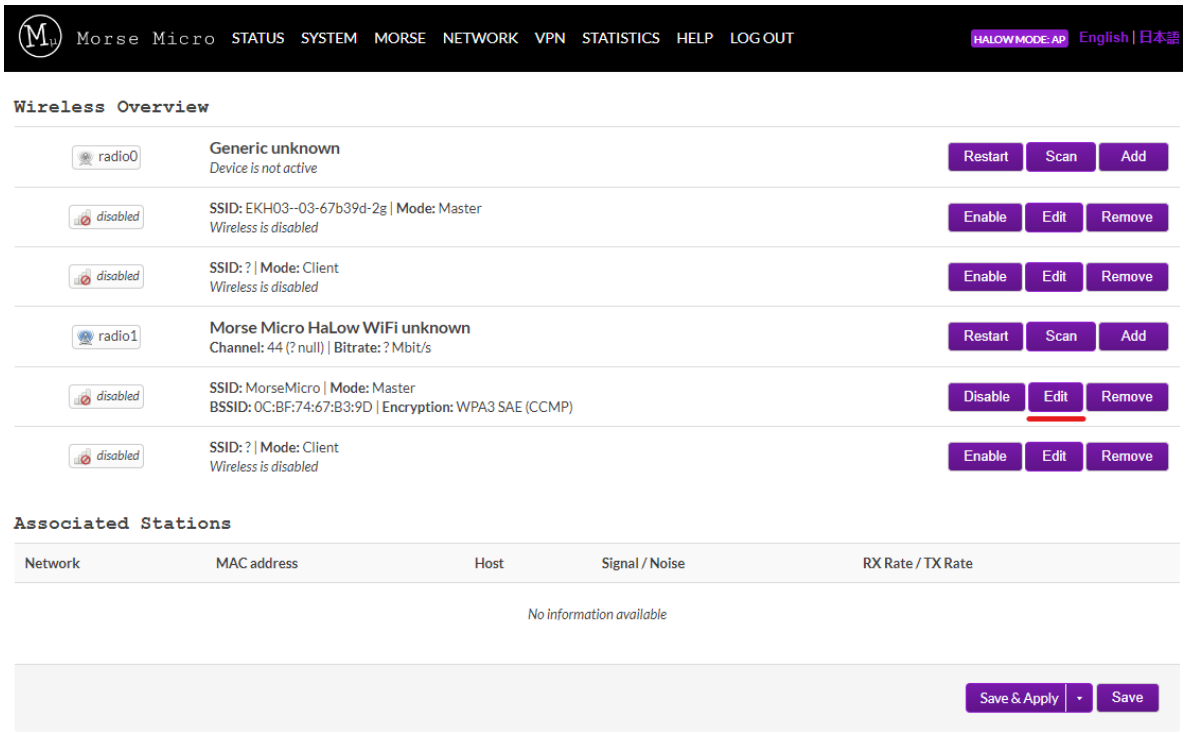
Beacon interval can be configured by navigating to **Morse->HaLow Config** and then in the 'Advanced - Wireless' section enter the beacon interval in milliseconds:



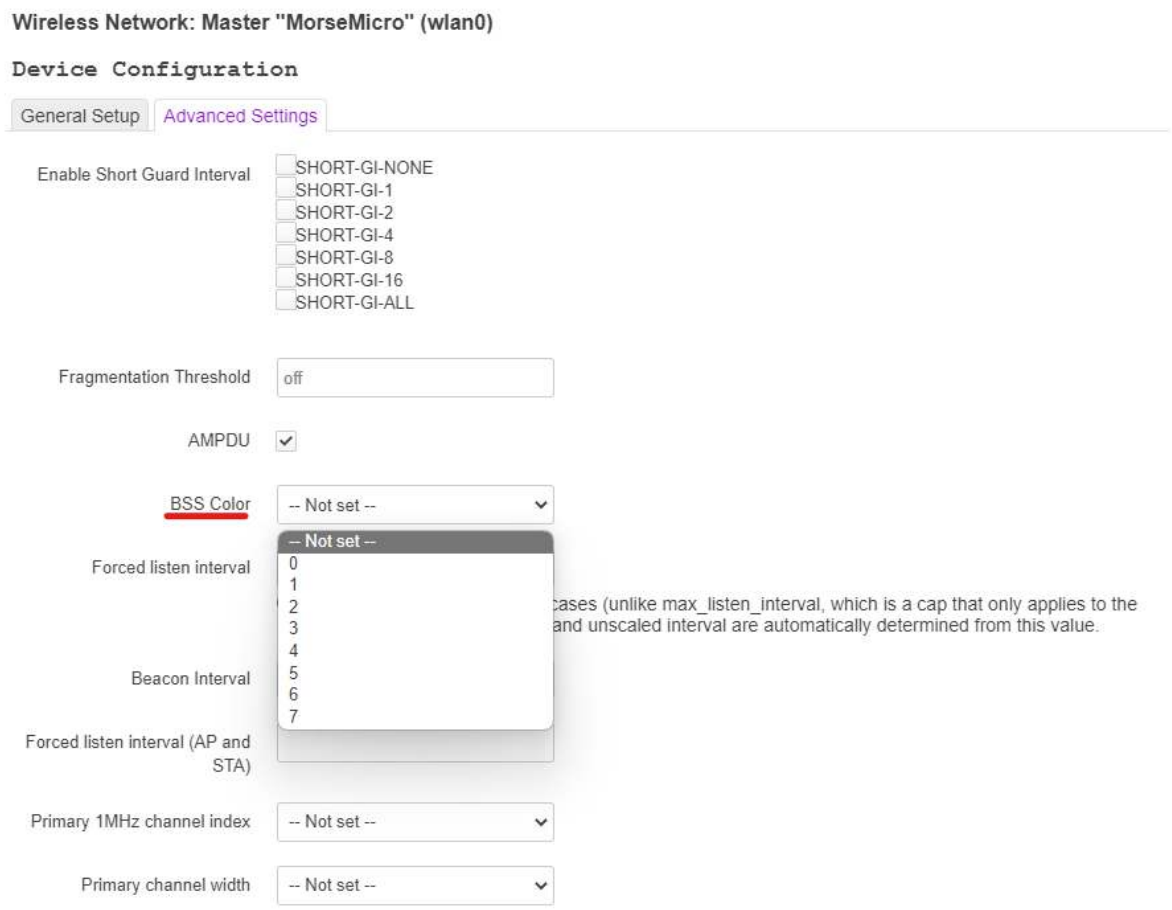
9.5 BSS Color

9.5.1 Via UI

Navigate to Network->Wireless, and click the 'edit' button beside the row with the HaLow SSID.



Click the 'Advanced Settings' tab at the top, and then the setting for BSS color can be seen and configured:



9.5.2 Via CLI

BSS color can be configured using the following command:

```
morse_cli -i wlan0 bsscolor <value>
```

Where `<value>` is a value from 0 to 7.

9.6 Other HaLow settings

Other advanced settings are available within the text files found at /etc/config/. Generic UCI options are defined in the OpenWrt documentation here: https://openwrt.org/docs/guide-user/network/wifi/basic.

9.7 morse_cli

`morse_cli` is a command line utility that allows you to control certain aspects of the radio behaviour. It replaces the `morsectrl` utility that was available in earlier releases, and has nearly identical functionality. For more details of its available options, please refer to the command help by running "`morse_cli -h`" from the CLI.

10 UI Configuration Architecture

This section outlines how changes to configuration in the UI are applied to the system.

From OpenWrt 2.0.2 onwards the Web UI configuration pages use the 'LuCI.uci' API to configure a standard, default set of UCI configuration sections which are stored in /etc/config/. To accelerate development from the old design based around a morse.conf file used in previous versions, the configuration pages implement a shim layer to consolidate and map the UCI sections and options to a JS object for native manipulation in the browser. Each page is configured to search for a particular set of fields in the JS object, and render them with the appropriate UI element.

The Morse configuration pages look for a small number of specific, hardcoded UCI sections in the network and DHCP configuration paths to greatly simplify more complicated network configurations such as bridge mode, DHCP/DNS servers, and so on. Utilising these different sections also allows storage of specific settings for "bridge mode", should it differ from the standalone configuration.

Removal of these sections will result in the Morse configuration page to no longer function correctly, and they will prompt the user to restore the missing configurations. Custom configurations can still be made using the more advanced, standard network and wireless pages provided by LuCI.

These required network sections (interfaces) are "lan", "privlan" and "ahwlan", with corresponding dhcp sections of the same names plus "_dns" suffixed sections.

- The "lan" interface is used for joining the ethernet and wireless network devices into the Morse bridge mode. Other devices added to this interface will also join the same bridge.
- The "privlan" interface is used to for a standalone ethernet configuration. By default, the ethernet device starts in this interface.
- The "ahwlan" interface is used for standalone HaLow device configuration. By default the HaLow device starts in this interface.

DHCP and firewall configurations can then be updated to configure the device for modes such as traffic forwarding and DHCP/DNS servers by changing references to these interfaces.

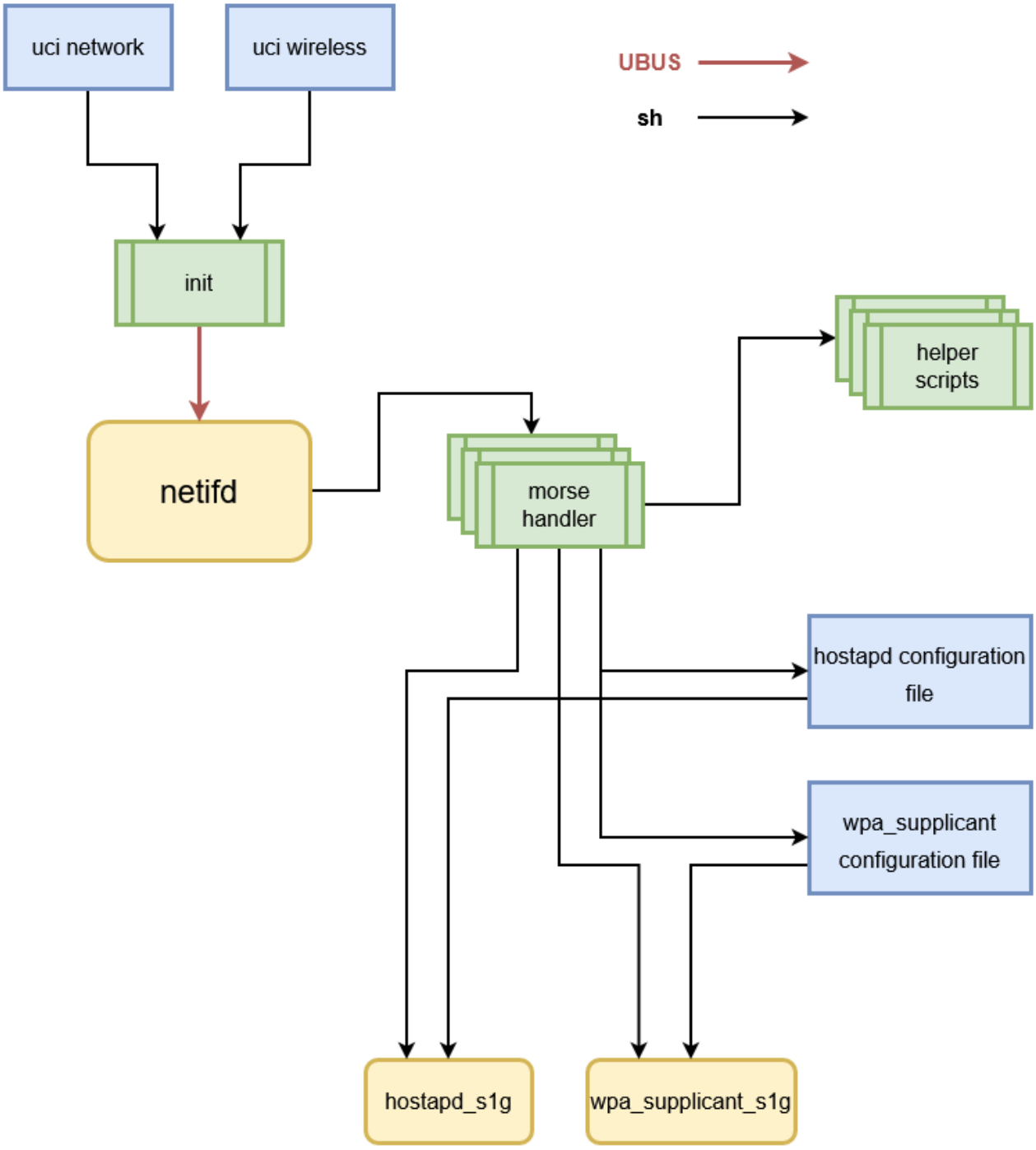
When a configuration change is saved the page will iterate over the fields available and set appropriate UCI configuration values for each changed field. UCI commands are sent via JSON-RPC API to a Ubus endpoint bound to the uhttpd server. Once all changed fields have been updated, the configuration is applied and UCI identifies which services it needs to reload. For the UI pages, this will be one or more of the following services: network, dnsmasq, or firewall.

The network service is the software daemon netifd. On a reload, this daemon examines changed UCI configuration and calls necessary handler scripts to bring up the affected component. In the case of a UCI wireless.wifi-device, netifd calls in wireless protocol handlers in /lib/netifd/wireless/*.sh. For MorseMicro HaLow devices, the UCI configuration will have type=morse, indicating to netifd to load /lib/netifd/wireless/morse.sh.

This protocol handler carries out the following:

- Parses the Morse type wifi-device in /etc/config/wireless
- Kills hostapd_s1g and wpa_supplicant_s1g
- Tears down the HaLow configured interface
- Unloads the morse driver modules
- Rebuilds any morse module parameters - e.g. region information
- Reloads the morse driver module
- Brings up the HaLow interface
- Creates appropriate hostapd or wpa_supplicant configuration files.
- Starts hostapd_s1g or wpa_supplicant_s1g as required.

The image below captures the execution flow of this process:



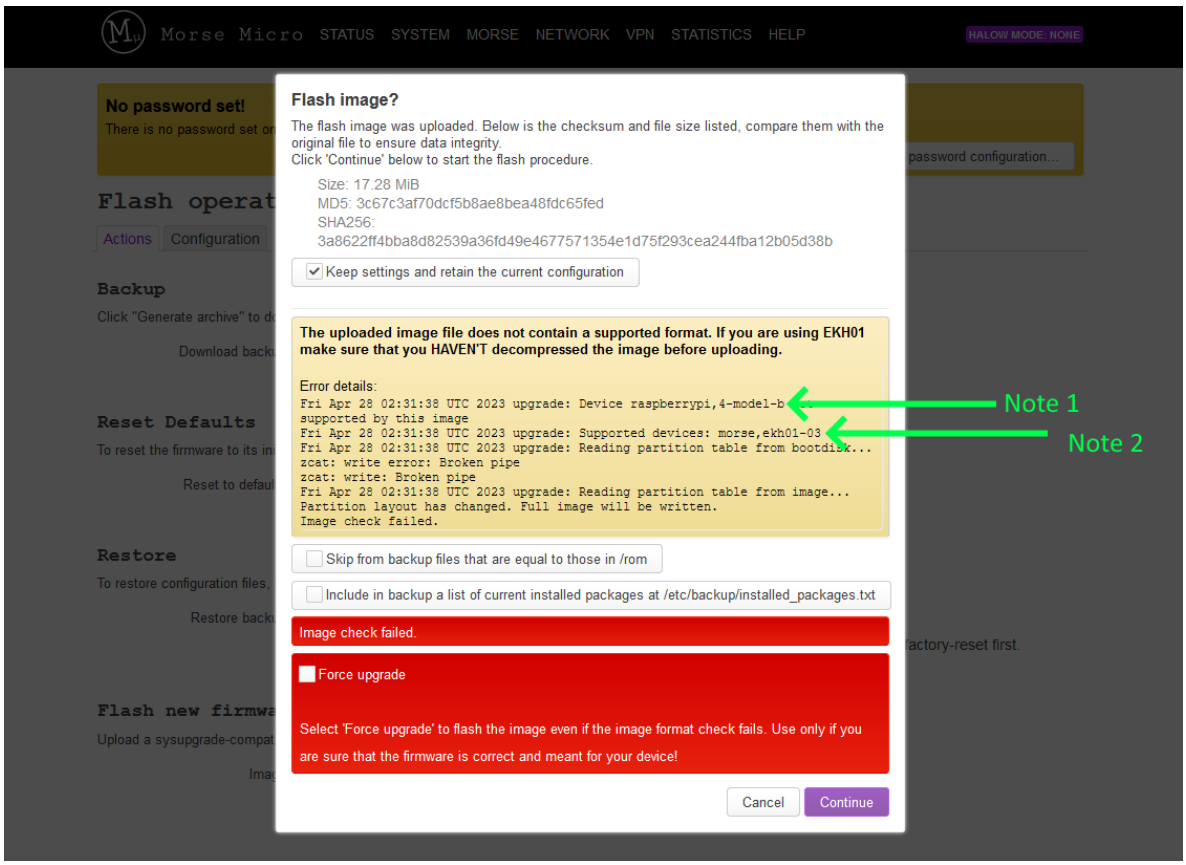
11 Troubleshooting

11.1 Updating firmware

Occasionally a platform name is updated, which can result in an error during upgrade e.g. “The uploaded image does not contain a supported format”(see below image). This is expected for the following upgrades:

- Updating an EKH01 from an image older than 2.3.3 to an image version 2.3.3 or higher.

Before proceeding, check that the “Supported devices:“ line matches the device revision; the device revision is printed on the case, and on a sticker on the case.



Note 1: This line describes the image currently running on the device.

Note 2: This line describes the image you are trying to install. Match the device name you see here to the information printed on your device.

When you have verified the image matches the device, click ‘Force Upgrade’ and continue. The warning will not be shown again for future upgrades.

12 Revision History

Release Number	Release Date	Release Notes
01	12/01/2021	• Initial release
02	12/02/2022	• Update for firmware release 1.3
03	04/03/2022	• IPERF Traffic Setup • Added Tools -> HaLow Firmware Upgrade
04	05/10/2022	• Updated for the LuCI interface • Added in EKH01
05	10/10/2022	• Improved formatting and reworded some sections for clarity. • Added UI Configuration architecture
06	20/10/2022	• Added example of how to run wavemon for basic HaLow testing
07	18/10/2022	Add description of key setup scenarios, and refactored configuration to match these. • Removed references to custom configurations, and manual configuration except where not available in UI. • Other general improvements
08	22/11/2022	• Updated device images
09	12/12/2022	• Updated formatting and cover page image
10	6/01/2023	• Updated for UCI configuration • Updated default IP address to 10.42.0.1
11	27/02/2023	• Correct some typos
12	02/06/2023	• Update for new HaLow configuration page • Update for new EasyMesh feature • Update for new Video UI feature • Update for adding Internet connectivity
13	03/11/2023	• General update and 1st release to Doc. Control
14	12/12/2023	• Updated for 2.4.4 release
15	7/03/2024	• Updated for 2.5.0 release

Release Number	Release Date	Release Notes
16	21/03/2024	• Updated for 2.5.2 release
17	28/03/2024	• Updated LED flash pattern for button presses (section 2.2.1)

Approvers: Chad O'Neill (VP of Applications), Matthew Forgie (Director of Software Applications).

Morse Micro
reaching farther™

Mouser Electronics

Authorized Distributor

Click to View Pricing, Inventory, Delivery & Lifecycle Information:

Morse Micro:

MM6108-EKH01-05US