# MM6108 - OpenWrt - Web GUI

User Guide

## Wi-Fi HaLow Configuration Interface

# 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 6 has a description of all the available GUI screens and tools and Section 7 provides advanced configuration tips that are not usually required but may be useful in some situations.

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

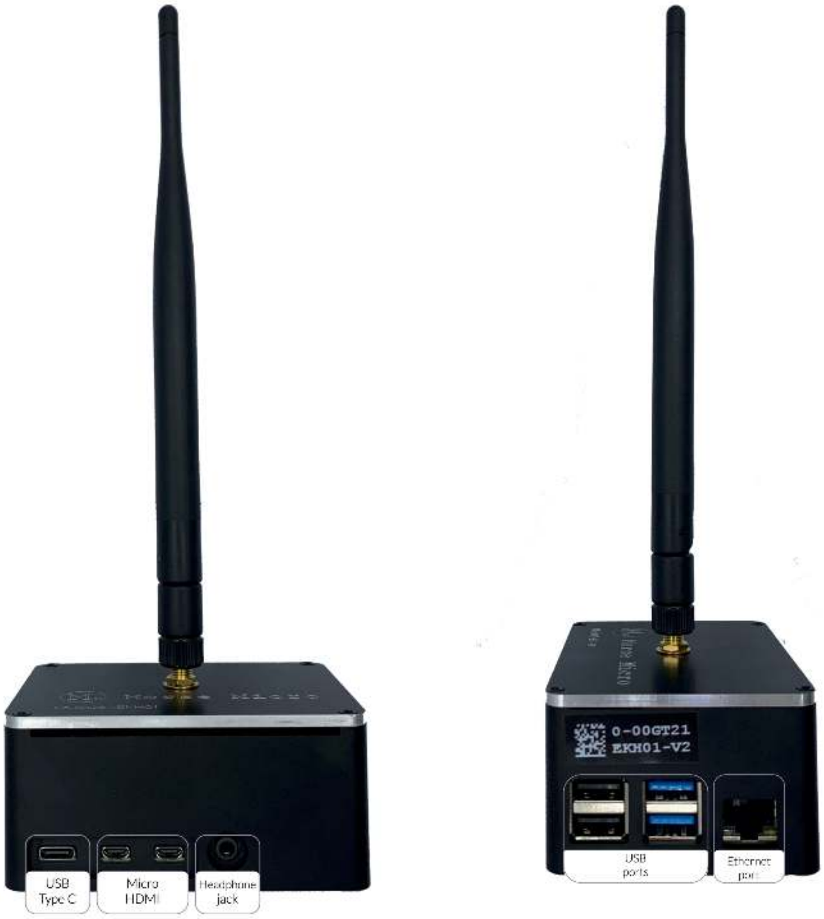
# 2 Device setup

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

- Ethernet - Ethernet port for either a LAN connection (e.g. a laptop) or an upstream WAN connection (e.g. gateway router).

- 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.
- USB Type C - Type 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.



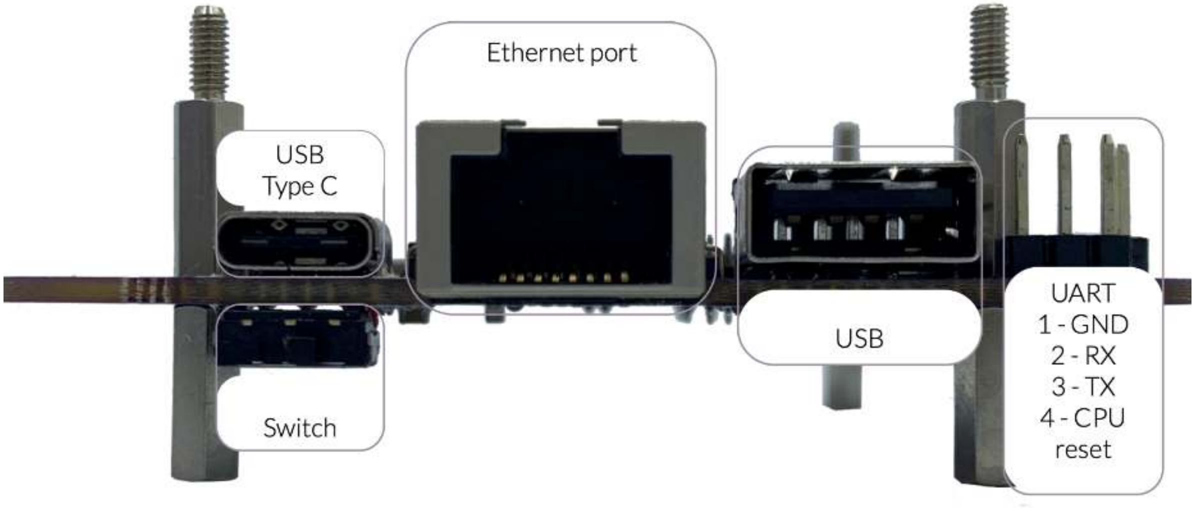
## 2.2 Basic setup

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.

## 2.3 EKH03

- USB-C - Powers the board and can function as an Ethernet-to-USB adapter
- Ethernet - Ethernet port for either a LAN connection (e.g. a laptop) or an upstream WAN connection (e.g. gateway router).
- Switch - Select whether to use micro-USB or Ethernet port for LAN connection. Direction of the switch point the selected port to use (*left* - micro-USB *right* - Ethernet port)
- USB - USB port that can be used for connecting peripherals to the EKH03
- UART - Serial console connection to the board, which operates at 115,200 bps 8N1 by default
- CPU - Jumper to reset the CPU



### 2.3.1 Basic setup

1. An AC adapter is included in the kit that should be connected to the Micro-USB connector on the EKH03.
2. Optional - seconds to boot up and be operational.

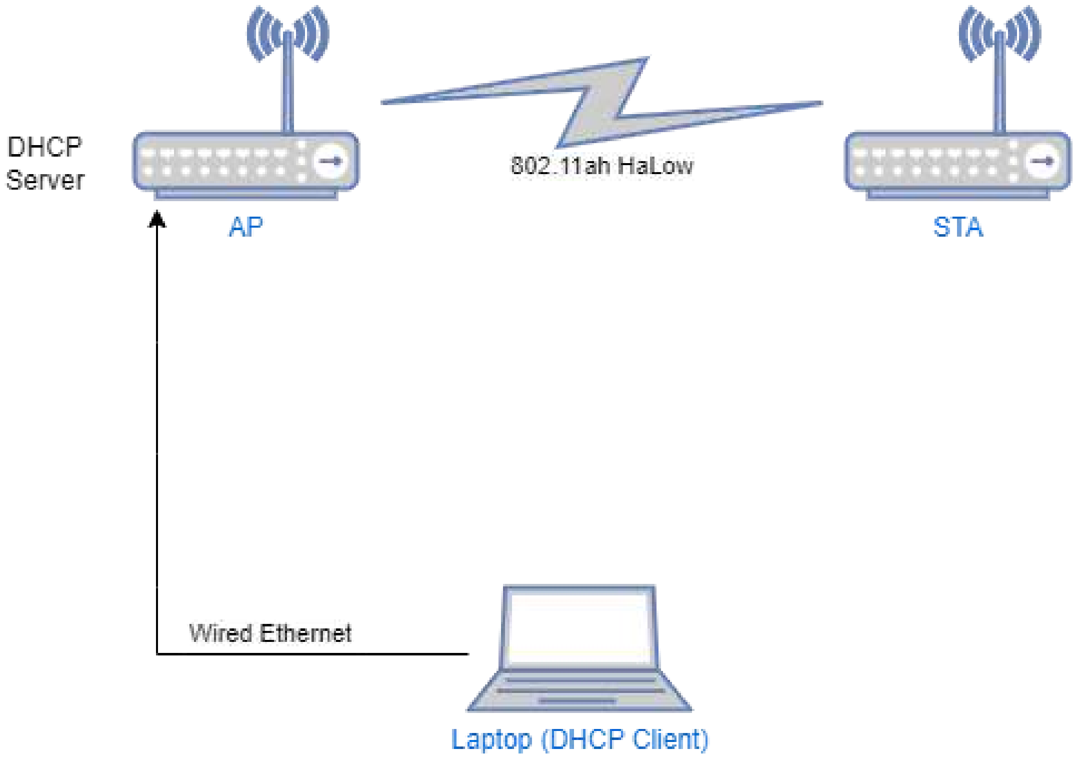
## 2.4 Browser configuration

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

- Google Chrome
- Firefox
- Microsoft Edge
- Apple Safari

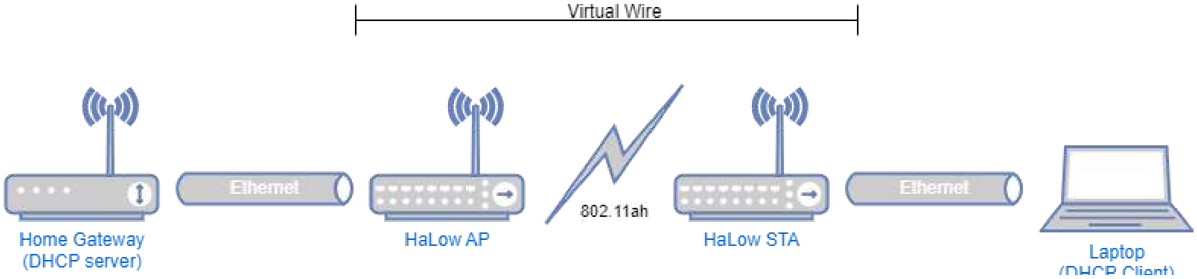
## 2.5 Standard setup scenarios

### 2.5.1 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.

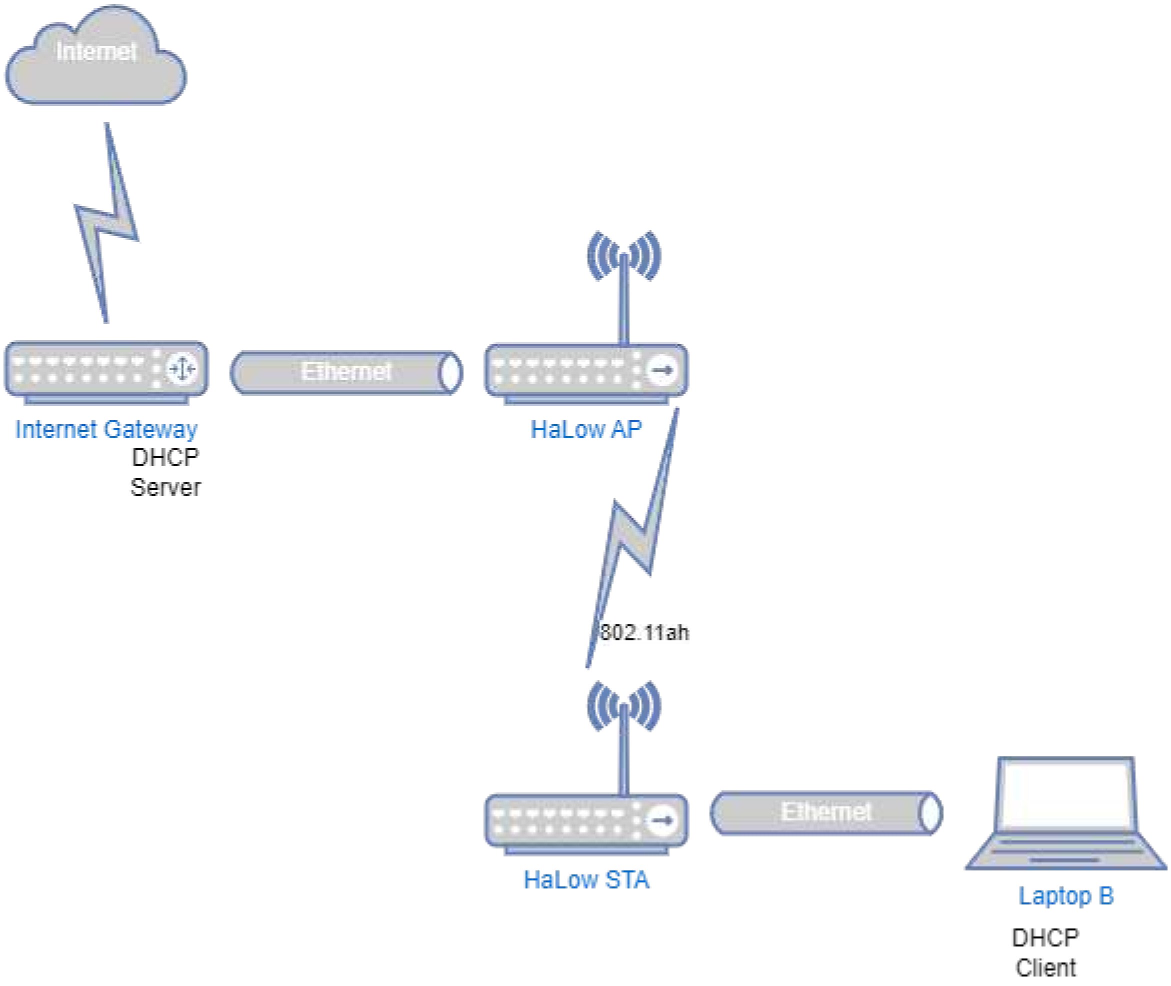
### 2.5.2 Using HaLow as a 'virtual wire' (Layer 2 bridge)



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.

### 2.5.3 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.

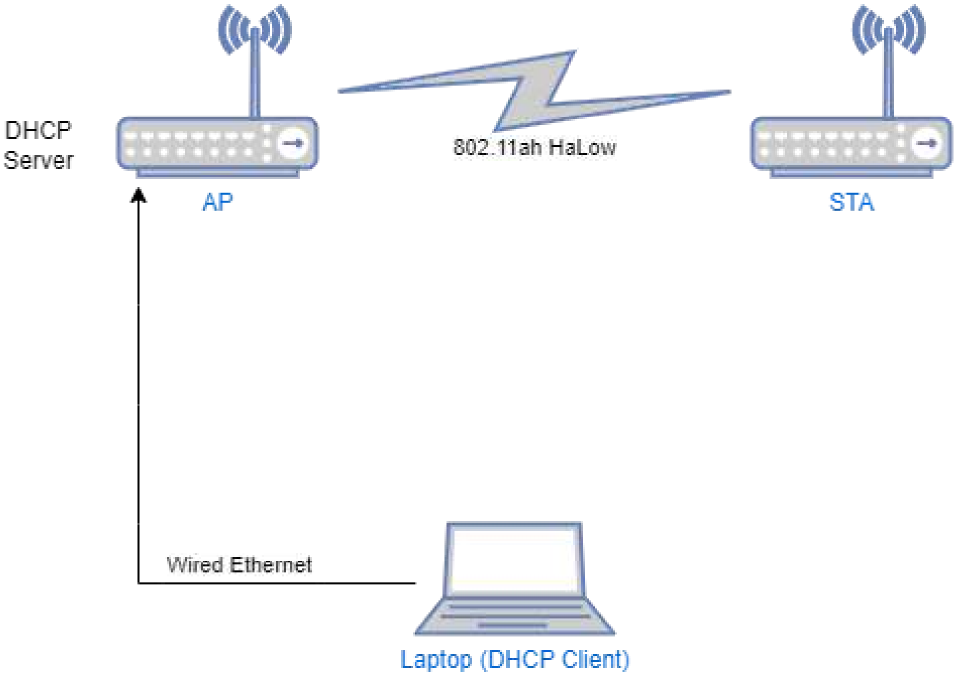
This scenario is useful for evaluating the HaLow device's ability to handle traffic flows at Layer 3, which places more load on the CPU.  Unless you have a good reason to want to do this, bridging is an easier and better way to go.

# 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 3.4 for details on how to reset to default configuration.

## 3.1 Standalone AP and STA

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

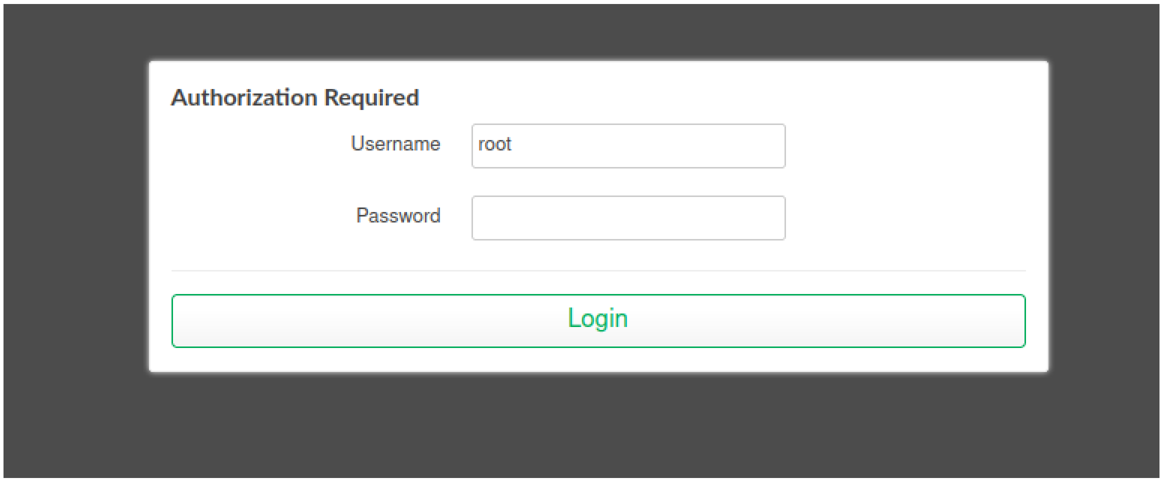


### 3.1.1 Laptop configuration

1. Connect your laptop to the AP or STA via an Ethernet cable.
2. Ensure that the Ethernet interface on the laptop is configured as a DHCP client (this is usually default, so likely no change required).
3. Open a web browser and go to the following address: http://10.42.0.1

### 3.1.2 Access point configuration

1. Follow the steps in the basic setup, and connect an Ethernet cable between the laptop and the access point.
2. In the browser setup above, there will be a prompt to login, the default username is *root* and no password is set. Click the 'Login' button to login to the configuration interface.

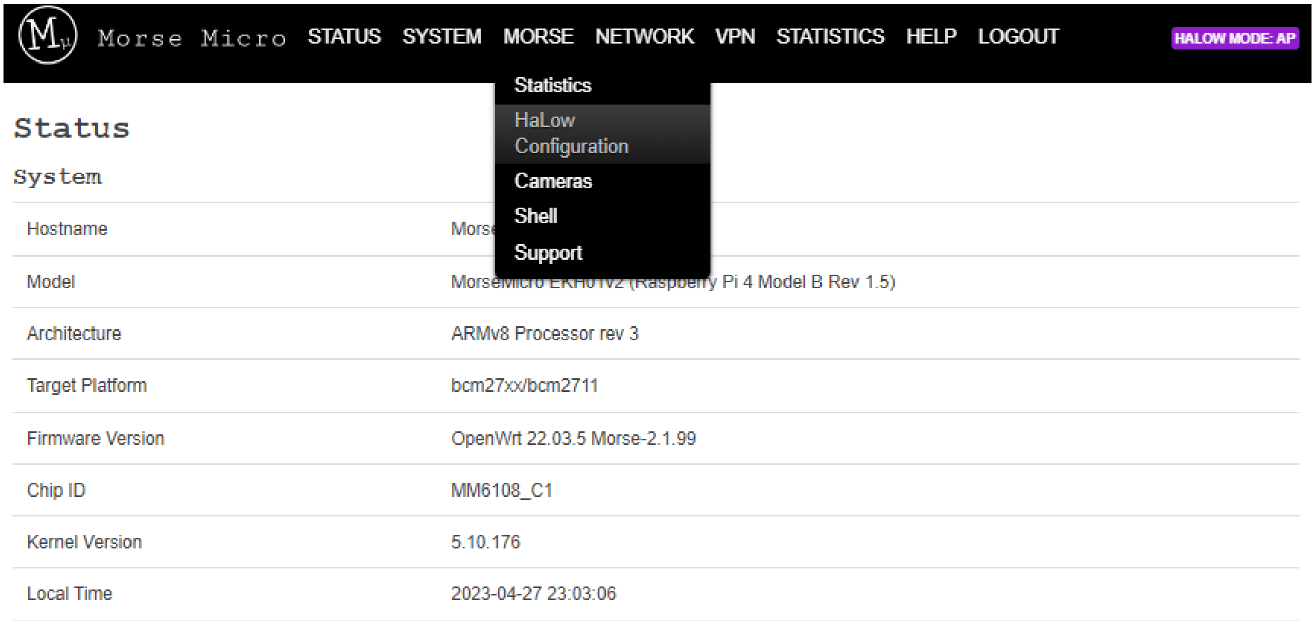


Authorization Required

Username: root

Password:

3. Using the top navigation menu, browse to 'Morse -> HaLow Configuration' page.

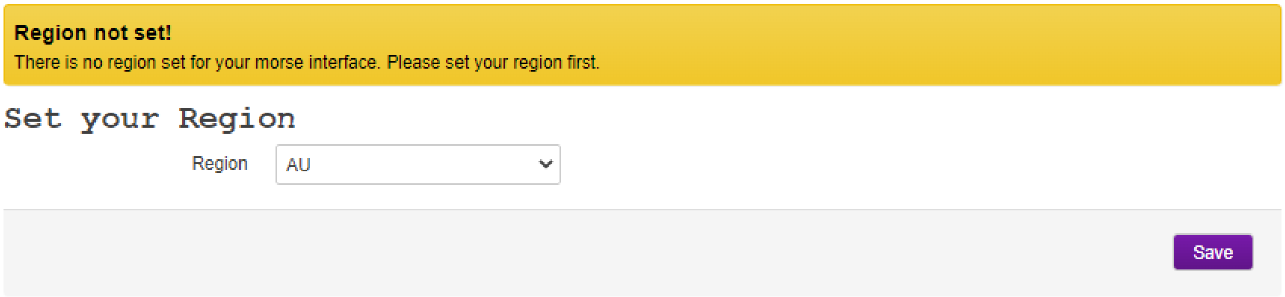


Status

System

| | |
|---|---|
| Hostname | Morse |
| Model | MorseMicro EKH01V2 (Raspberry Pi 4 Model B Rev 1.5) |
| Architecture | ARMv8 Processor rev 3 |
| Target Platform | bcm27xx/bcm2711 |
| Firmware Version | OpenWrt 22.03.5 Morse-2.1.99 |
| Chip ID | MM6108_C1 |
| Kernel Version | 5.10.176 |
| Local Time | 2023-04-27 23:03:06 |

4. Select your desired region from the Region option first and then click 'Save':

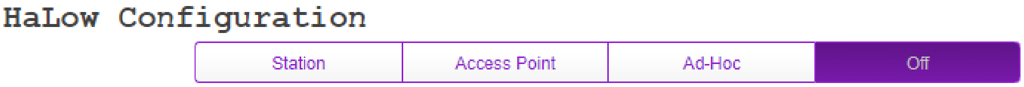


**Region not set!**
There is no region set for your morse interface. Please set your region first.

Set your Region

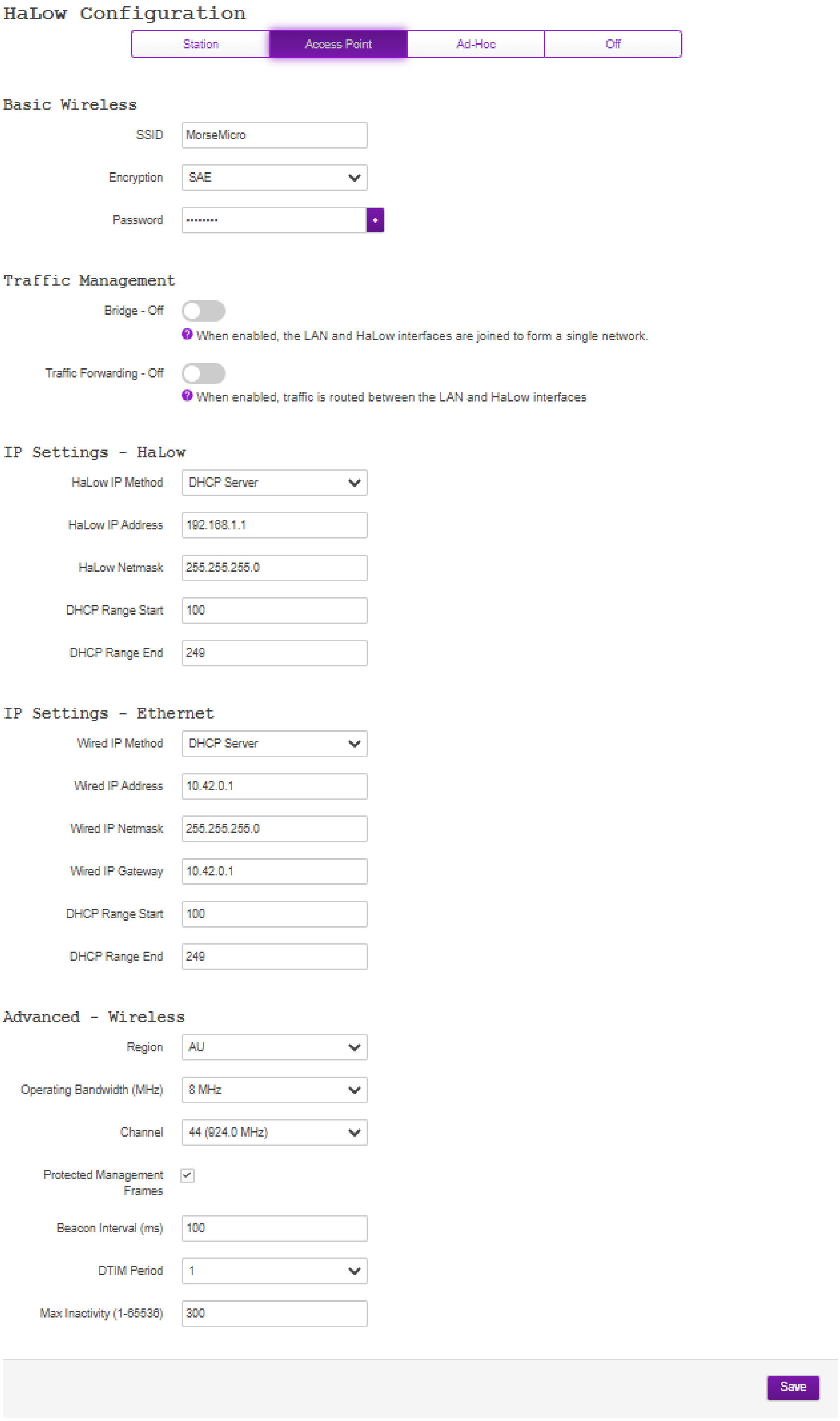
Region: AU

5. Select 'Access Point' and configure as desired.



HaLow Configuration

The defaults will work to quickly get a test connection going, but should not be considered secure for production use.  For the first scenario only the basic wireless section should be updated, the rest can be left as default (see image below).



## HaLow Configuration

### Basic Wireless

| | |
|---|---|
| SSID | MorseMicro |
| Encryption | SAE |
| Password | •••••••• |

### Traffic Management

| | |
|---|---|
| Bridge - Off | ○ |
| | When enabled, the LAN and HaLow interfaces are joined to form a single network. |
| Traffic Forwarding - Off | ○ |
| | When enabled, traffic is routed between the LAN and HaLow interfaces |

### IP Settings - HaLow

| | |
|---|---|
| HaLow IP Method | DHCP Server |
| HaLow IP Address | 192.168.1.1 |
| HaLow Netmask | 255.255.255.0 |
| DHCP Range Start | 100 |
| DHCP Range End | 249 |

### IP Settings - Ethernet

| | |
|---|---|
| Wired IP Method | DHCP Server |
| Wired IP Address | 10.42.0.1 |
| Wired IP Netmask | 255.255.255.0 |
| Wired IP Gateway | 10.42.0.1 |
| DHCP Range Start | 100 |
| DHCP Range End | 249 |

### Advanced - Wireless

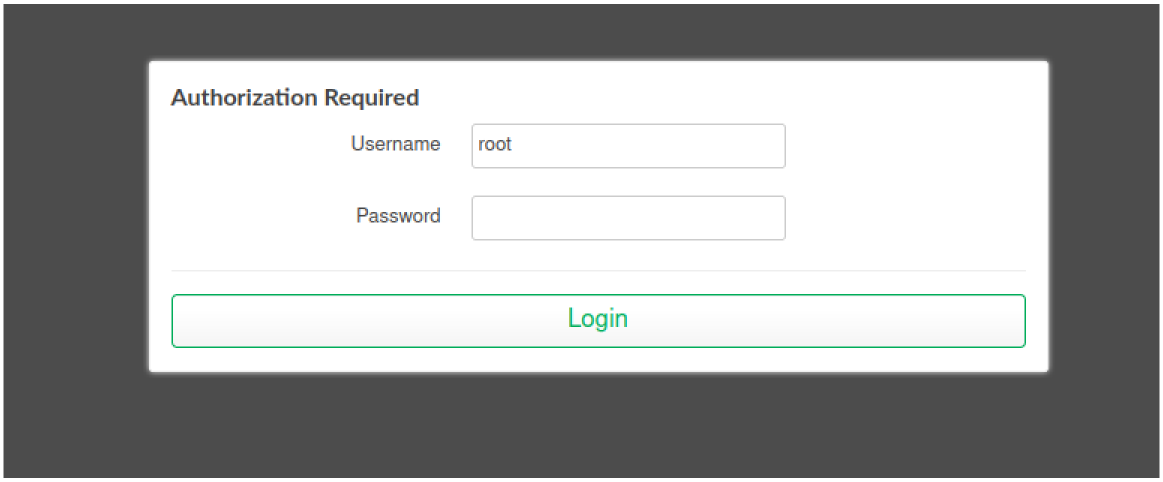
| | |
|---|---|
| Region | AU |
| Operating Bandwidth (MHz) | 8 MHz |
| Channel | 44 (924.0 MHz) |
| Protected Management Frames | ☑ |
| Beacon Interval (ms) | 100 |
| DTIM Period | 1 |
| Max Inactivity (1-65535) | 300 |

6. Click ‘Save’ to apply the configuration and bring up the router.

### 3.1.3 Station configuration

1. Follow the steps in the basic setup, and connect an Ethernet cable between the laptop and the station(STA).

2. Open a browser and go to http://10.42.0.1. There will be a prompt to login, the default username is *root* and no password is set. Click the ‘Login’ button to login to the configuration interface.

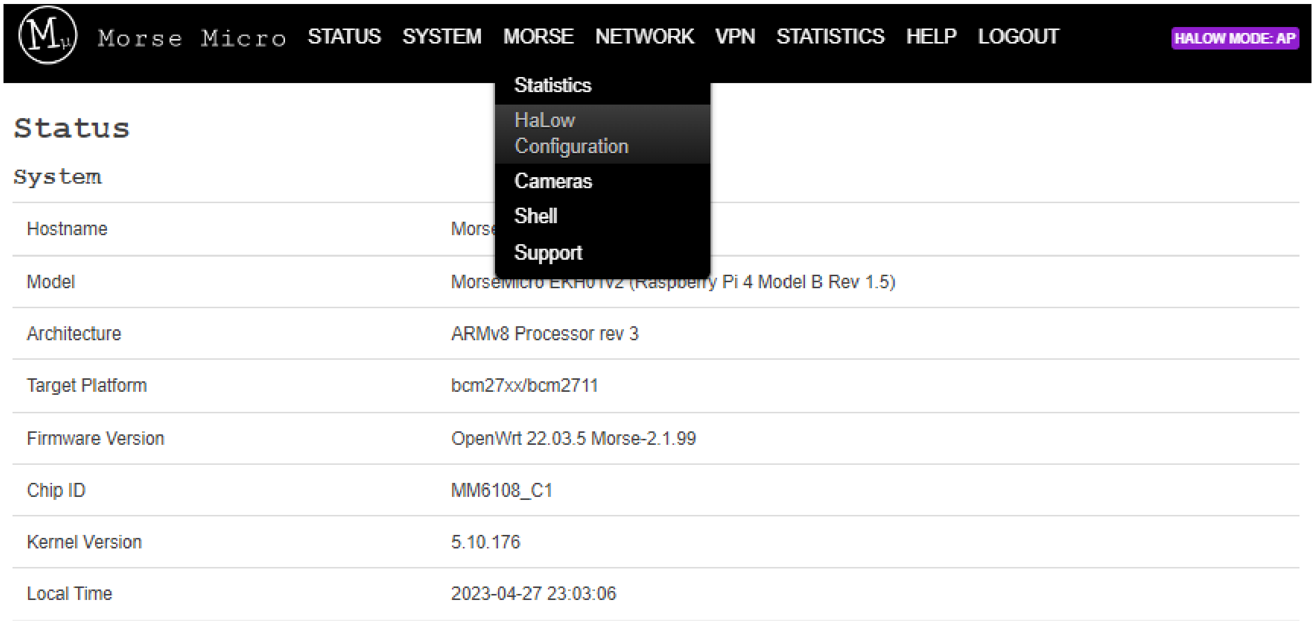


Authorization Required

Username: root

Password:

3. Using the top navigation menu, browse to 'Morse -> HaLow Configuration' page.

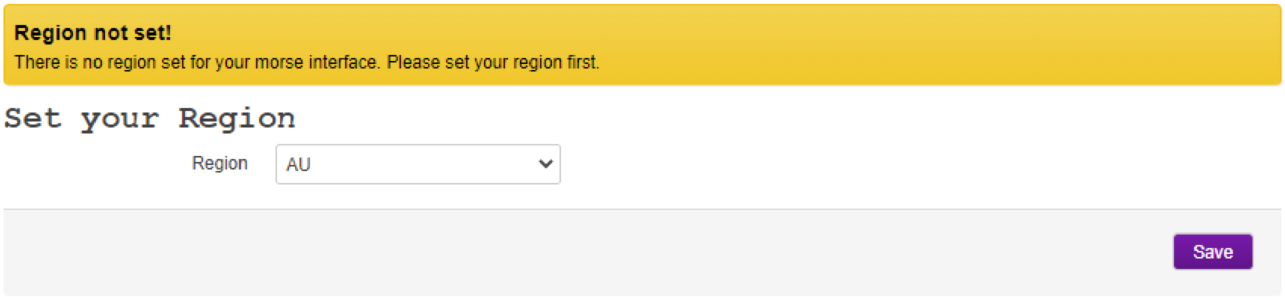


## Status

### System

| | |
|---|---|
| Hostname | Mors |
| Model | MorseMicro EKH01V2 (Raspberry Pi 4 Model B Rev 1.5) |
| Architecture | ARMv8 Processor rev 3 |
| Target Platform | bcm27xx/bcm2711 |
| Firmware Version | OpenWrt 22.03.5 Morse-2.1.99 |
| Chip ID | MM6108_C1 |
| Kernel Version | 5.10.176 |
| Local Time | 2023-04-27 23:03:06 |

4. Select your desired region from the Region option first and save.



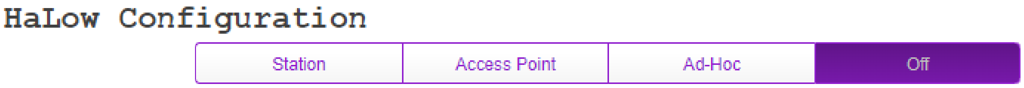
**Region not set!**

There is no region set for your morse interface. Please set your region first.

## Set your Region

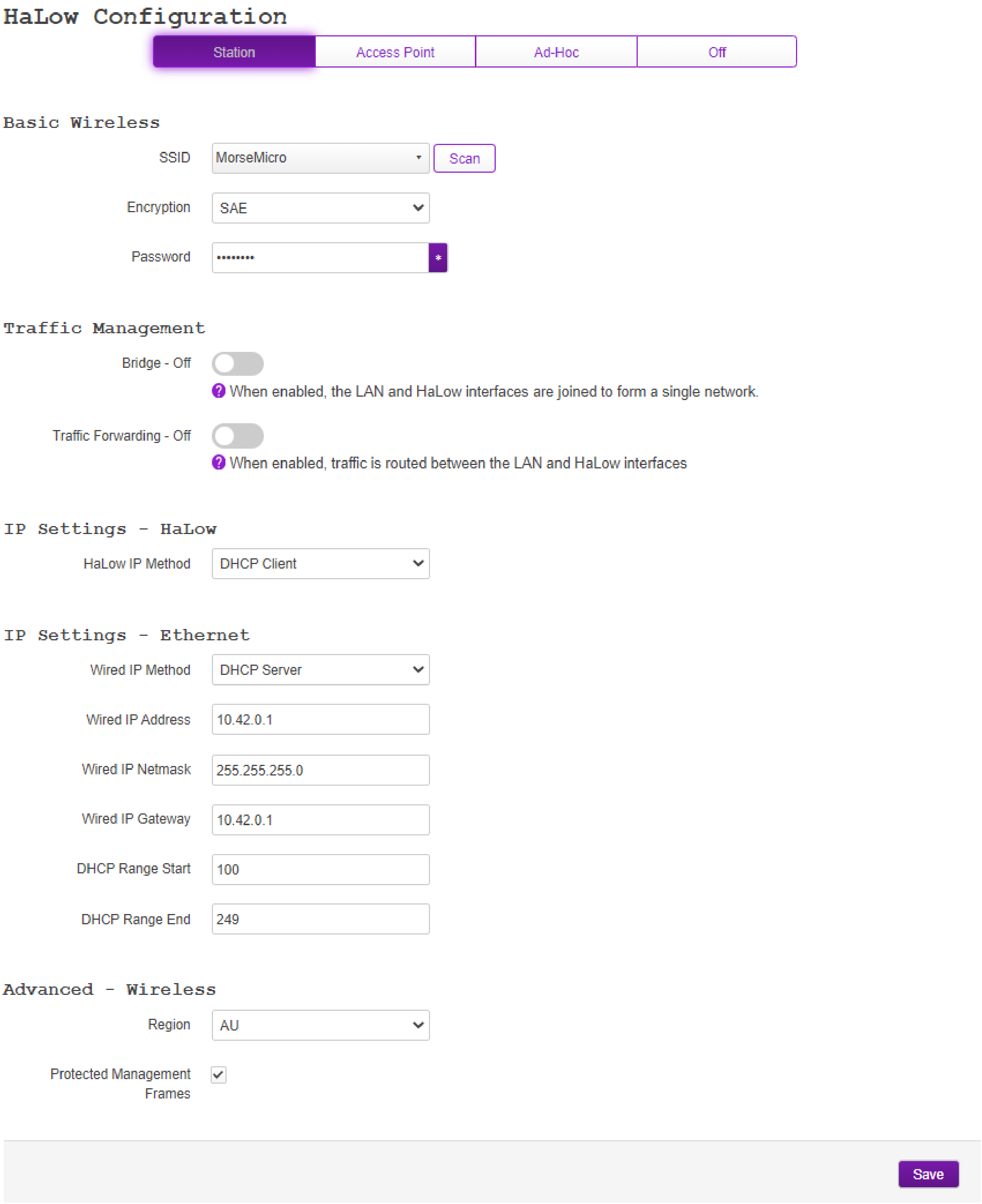
Region: AU

5. Select the 'Station' option and configure as desired.



## HaLow Configuration

The scan button can be used to populate the dropdown with available SSIDs, and choose an appropriate encryption and password. The defaults will work to quickly get a test connection going, but should not be considered secure for production use. See below screenshot as a reference for default settings:



HaLow Configuration

Station | Access Point | Ad-Hoc | Off

Basic Wireless

SSID: MorseMicro ▾ Scan

Encryption: SAE

Password: ••••••••

Traffic Management

Bridge - Off

When enabled, the LAN and HaLow interfaces are joined to form a single network.

Traffic Forwarding - Off

When enabled, traffic is routed between the LAN and HaLow interfaces

IP Settings - HaLow

HaLow IP Method: DHCP Client

IP Settings - Ethernet

Wired IP Method: DHCP Server

Wired IP Address: 10.42.0.1

Wired IP Netmask: 255.255.255.0

Wired IP Gateway: 10.42.0.1

DHCP Range Start: 100

DHCP Range End: 249

Advanced - Wireless

Region: AU

Protected Management Frames ☑

6. For this scenario, settings can be left as default. Note the key ones are:
   - HaLow IP Method = DHCP client
   - Wired IP Method = DHCP Server
   - Wired IP Address = 10.42.0.x
     (Note this defaults to 10.42.0.1 which is the same address as AP, so this should be assigned a different IP address, e.g 10.42.0.2.)

7. Click ‘Save’ to apply the configuration and bring up the station.

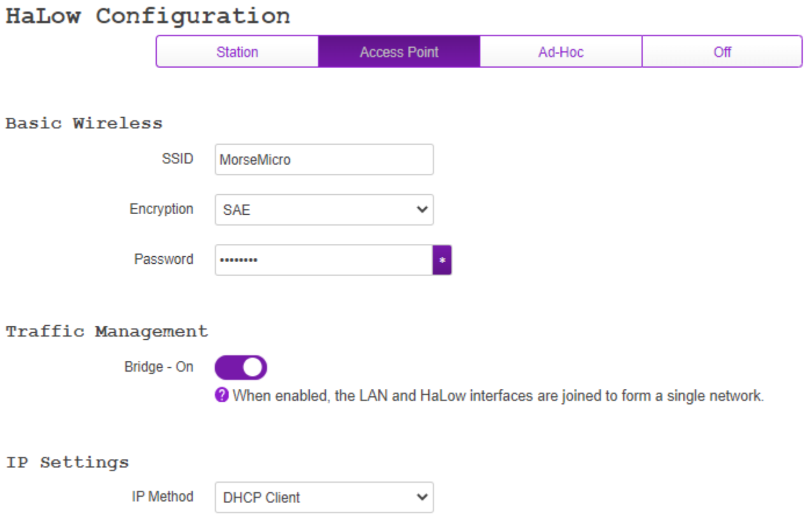
### 3.1.3 (Optional) Add upstream Internet connectivity

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:

- A 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

Make the following changes on the AP in the HaLow configuration page to enable it to reach the Internet via the upstream gateway:

1. Change the Wired IP Method to “DHCP client”
2. In the Traffic Management section, configure Bridge to ‘on’



HaLow Configuration

Basic Wireless

SSID: MorseMicro

Encryption: SAE

Password: ••••••••

Traffic Management

Bridge - On

When enabled, the LAN and HaLow interfaces are joined to form a single network.

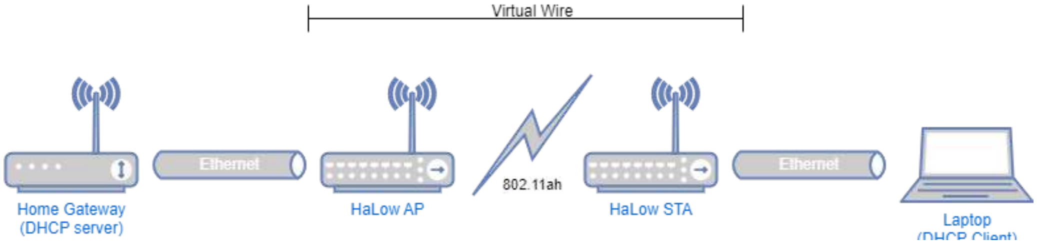
IP Settings

IP Method: DHCP Client

The impact of this is that all the HaLow STAs connected to the AP will now receive addresses from the upstream gateway, including the AP itself.

## 3.2 ‘Virtual Wire’ - Layer 2 bridging

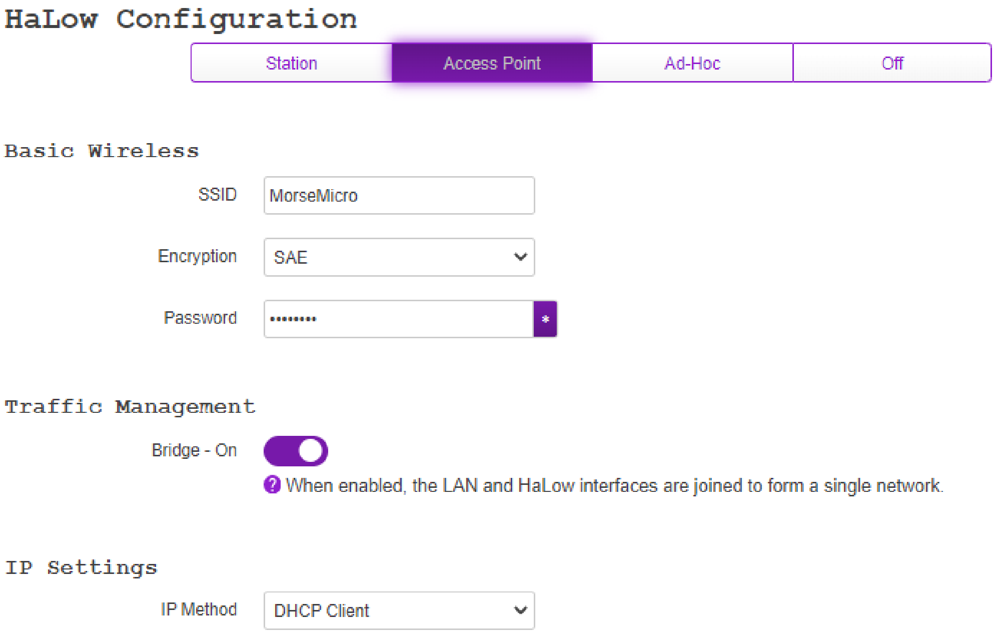
This section outlines how to configure the AP and STA per the scenario defined in 2.5.2.



### 3.2.1 Access point configuration

Same as above in 3.1, but make the following additional changes:

1. Enable bridge mode:



**HaLow Configuration**

**Basic Wireless**

SSID: MorseMicro

Encryption: SAE

Password: ••••••••

**Traffic Management**

Bridge - On

When enabled, the LAN and HaLow interfaces are joined to form a single network.

**IP Settings**

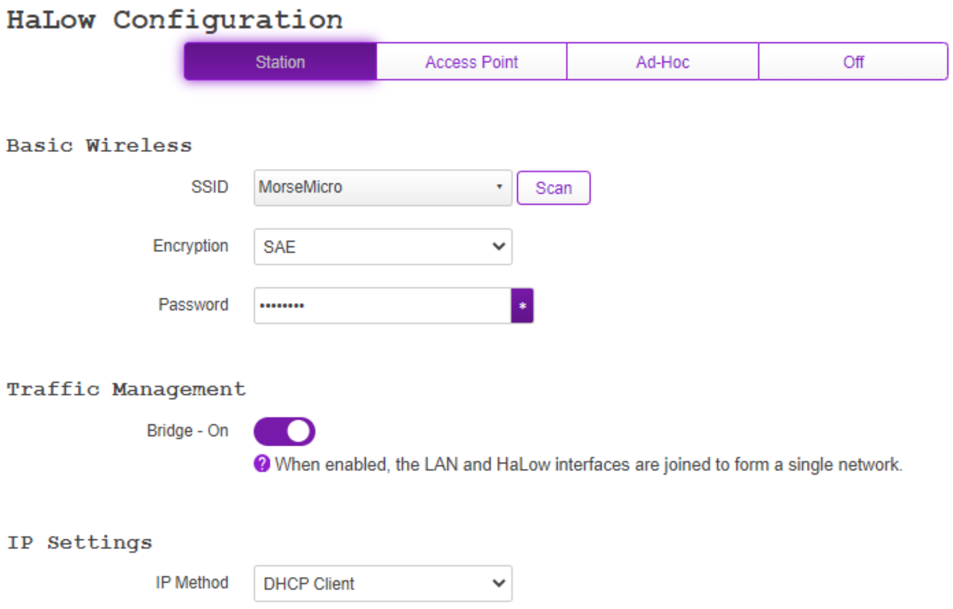
IP Method: DHCP Client

2. (Optional) Change the IP Method to ‘DHCP Client’ so that the bridge will receive an IP address from the DHCP server. This will be helpful for reconfiguring later if needed.

### 3.2.2 Station configuration

Same as above in 3.1, but take the additional following steps:

1. Enable ‘Bridge Mode’:



**HaLow Configuration**

Station | Access Point | Ad-Hoc | Off

**Basic Wireless**

SSID: MorseMicro (Scan)

Encryption: SAE

Password: ••••••••

**Traffic Management**

Bridge - On

When enabled, the LAN and HaLow interfaces are joined to form a single network.

**IP Settings**

IP Method: DHCP Client

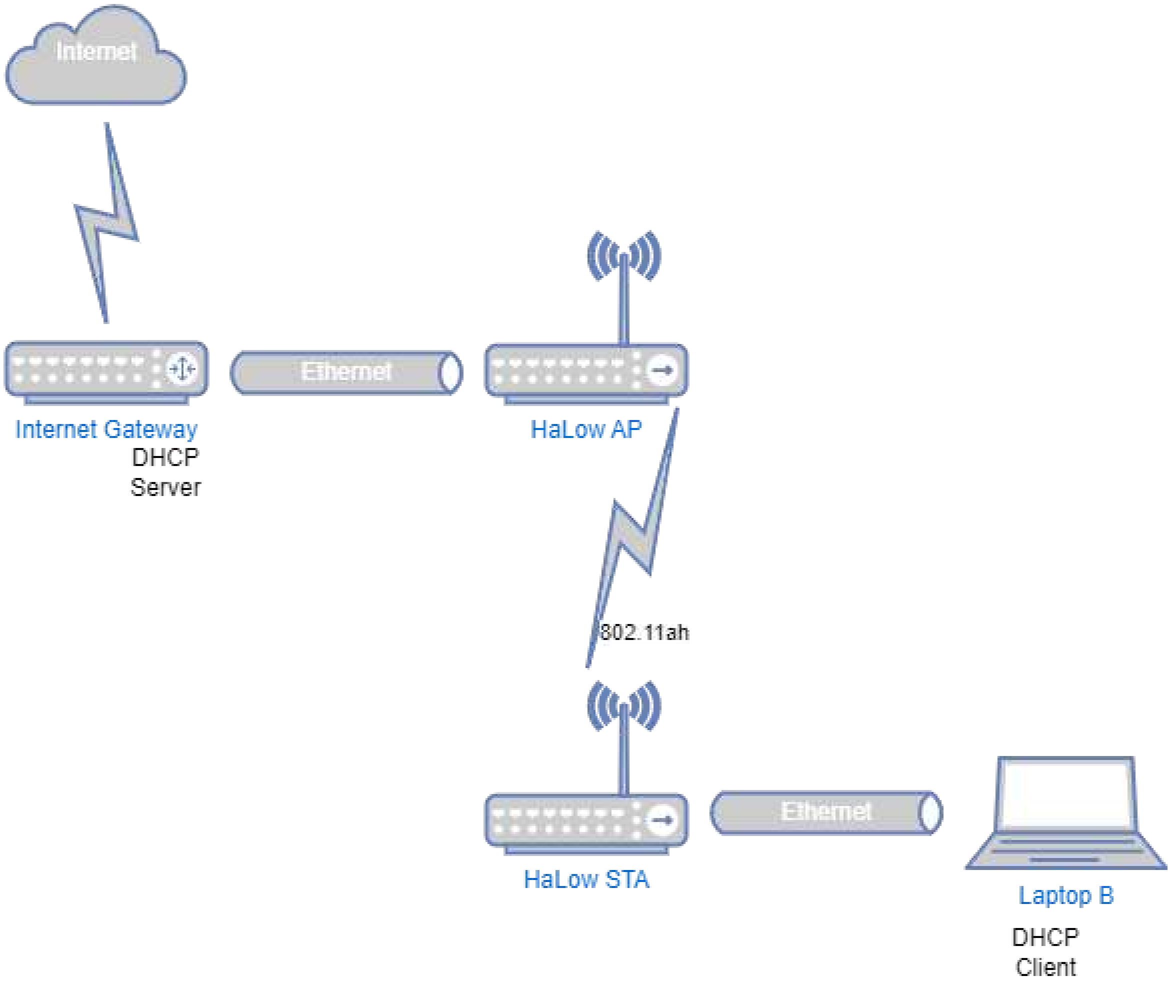
2. (Optional) Select the IP Method to be ‘DHCP Client’ so that it can receive an address from the DHCP server (if one exists). Doing this will ensure that the web interface can be reached for reconfiguring the device at a later time.

### 3.2.3 Laptop configuration

No additional configuration beyond what is specified in section 3.1 above.

## 3.3 Non-standalone AP with routing

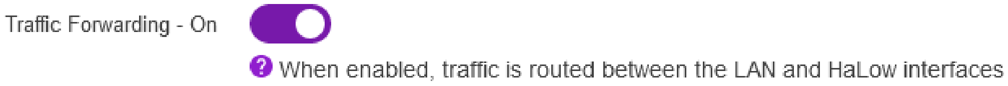
This section outlines how to configure the AP and STA per the scenario defined in 2.5.3.



### 3.3.1 Access point configuration

Similar to 3.1, but make the following additional changes:

1. Turn traffic forwarding on



Traffic Forwarding - On

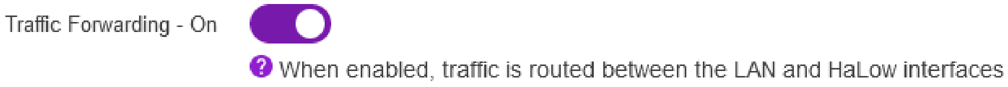
When enabled, traffic is routed between the LAN and HaLow interfaces

2. Set 'HaLow IP Method' to be DHCP server
3. Set 'Wired IP Method' to be DHCP client

### 3.3.2 Station configuration

Follow the STA configuration for the scenario in 3.1, but make the following additional changes:

1. Turn traffic forwarding on



Traffic Forwarding - On

When enabled, traffic is routed between the LAN and HaLow interfaces

2. Set 'HaLow IP Method' to DHCP client
3. Set 'Wired IP Method' to DHCP server
4. Set the 'Wired IP Gateway' to the same 'Wired IP Address'

### 3.3.3 Laptop configuration

No additional configuration beyond what is specified in section 3.1 above.

## 3.4 Reset the device to default configuration

This section outlines how to get the device back to a default configuration in different situations. Note that a full-factory reset is not possible with ext4-based firmware, which only performs a reset of key configuration files. To ensure a full-factory reset, please use a squashfs-based firmware image.

### 3.4.1 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.

### 3.4.2 No access to the web UI - 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.

### 3.4.3 No access to the web UI - EKH03

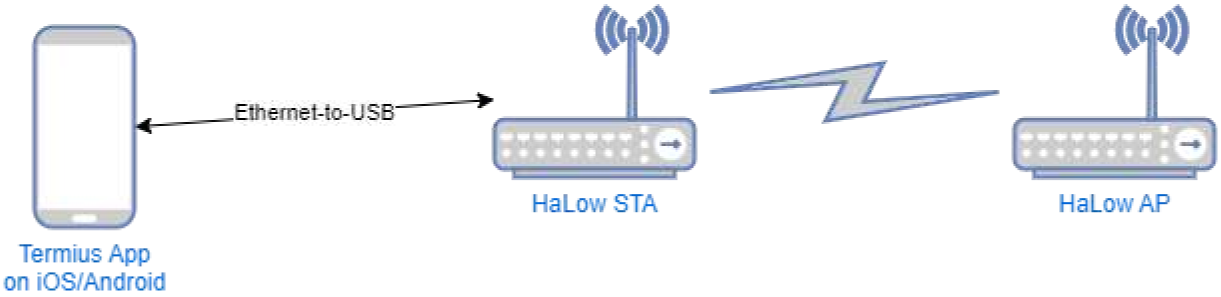
This scenario requires using a serial console cable to access the device. The basic setup section of this guide shows the location of the UART header on the EKH03 PCB, and a 3.3V TTL serial USB cable can be used to connect a computer to this port. Once connected, a suitable terminal emulator program 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:

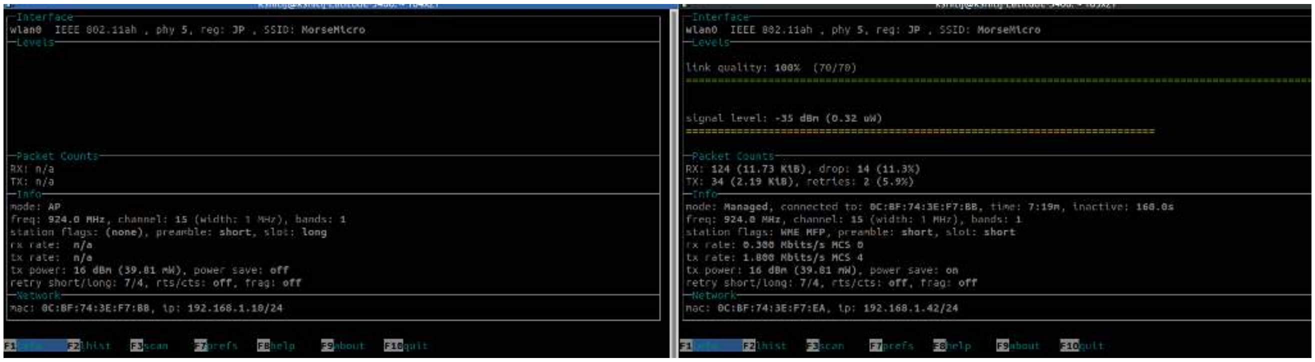
```
/morse/scripts/factory_reset.sh
```

# 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:



```
-Interface-
wlan0  IEEE 802.11ah , phy 5, reg: JP , SSID: MorseMicro
-Levels-







-Packet Counts-
RX: n/a
TX: n/a
-Info-
mode: AP
freq: 924.0 MHz, channel: 15 (width: 1 MHz), bands: 1
station flags: (none), preamble: short, slot: long
rx rate:  n/a
tx rate:  n/a
tx power: 16 dBm (39.81 mW), power save: off
retry short/long: 7/4, rts/cts: off, frag: off
-Network-
mac: 0C:BF:74:3E:F7:B8, ip: 192.168.1.10/24

F1       F2lhist   F3scan    F7prefs   F8help    F9about   F10quit
```

```
-Interface-
wlan0  IEEE 802.11ah , phy 5, reg: JP , SSID: MorseMicro
-Levels-

link quality: 100%  (70/70)
==========================================================================================


signal level: -35 dBm (0.32 uW)
==========================================================================

-Packet Counts-
RX: 124 (11.73 KiB), drop: 14 (11.3%)
TX: 34 (2.19 KiB), retries: 2 (5.9%)
-Info-
mode: Managed, connected to: 0C:BF:74:3E:F7:B8, time: 7:19m, inactive: 168.0s
freq: 924.0 MHz, channel: 15 (width: 1 MHz), bands: 1
station flags: WME MFP, preamble: short, slot: short
rx rate: 0.300 Mbits/s MCS 0
tx rate: 1.800 Mbits/s MCS 4
tx power: 16 dBm (39.81 mW), power save: on
retry short/long: 7/4, rts/cts: off, frag: off
-Network-
mac: 0C:BF:74:3E:F7:EA, ip: 192.168.1.42/24

F1       F2lhist   F3scan    F7prefs   F8help    F9about   F10quit
```

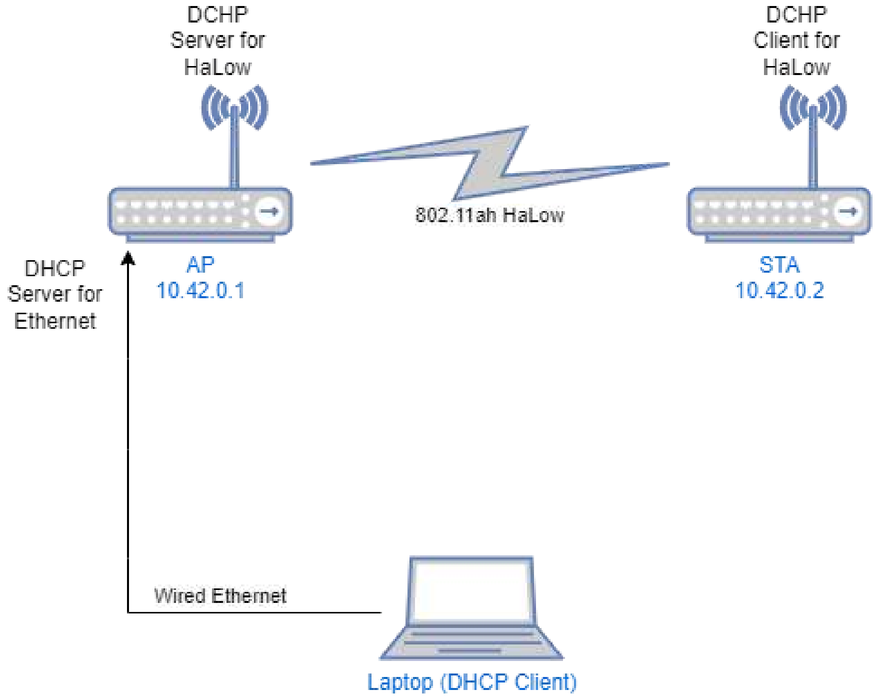
Note that pt will ping 192.168.1.2 by default, but an alternate address can be provided as an argument to the script, e.g. “pt 1.2.3.4”.

# 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.

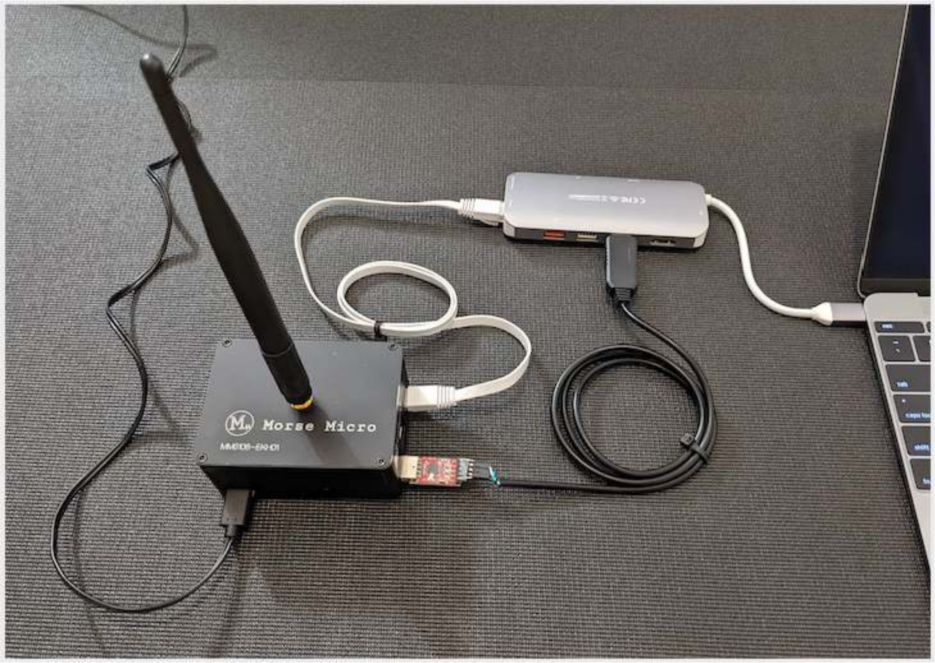
The following guide outlines how to run iPerf traffic between two devices connected via HaLow. In the diagram below, there are two devices, AP and STA, which may be any of the available evaluation kits (EKH01, EKH03).

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 to the Morse Micro device *(EKH01 only)*. Connect an Ethernet cable from your PC to the RJ45 of the Morse Micro device. Connect a USB-C power cable to the Morse Micro AP device and optionally connect the USB/UART dongle for a console, then power the unit on. Wait ~60 seconds to allow the device to start up.



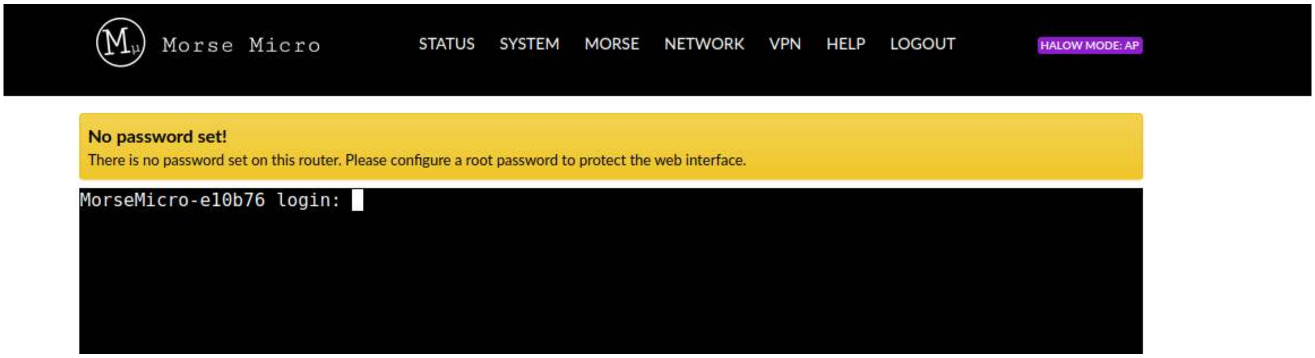
2. In a web browser on the laptop, navigate to the web UI of the device (http://10.42.0.1 by default).

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

3. Navigate to the ‘HaLow Configuration’ page under the ‘Morse’ menu in the top navigation bar. 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 |

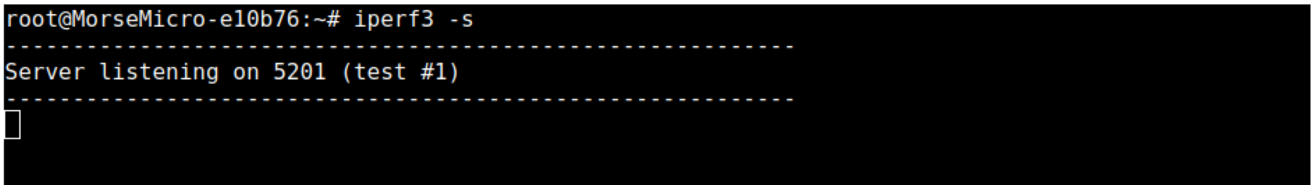
4. Navigate to the ‘Shell’ page under the MORSE menu in the top navigation bar. Note the credentials will be the same as used to login to the web UI.



**No password set!**
There is no password set on this router. Please configure a root password to protect the web interface.

```
MorseMicro-e10b76 login:
```

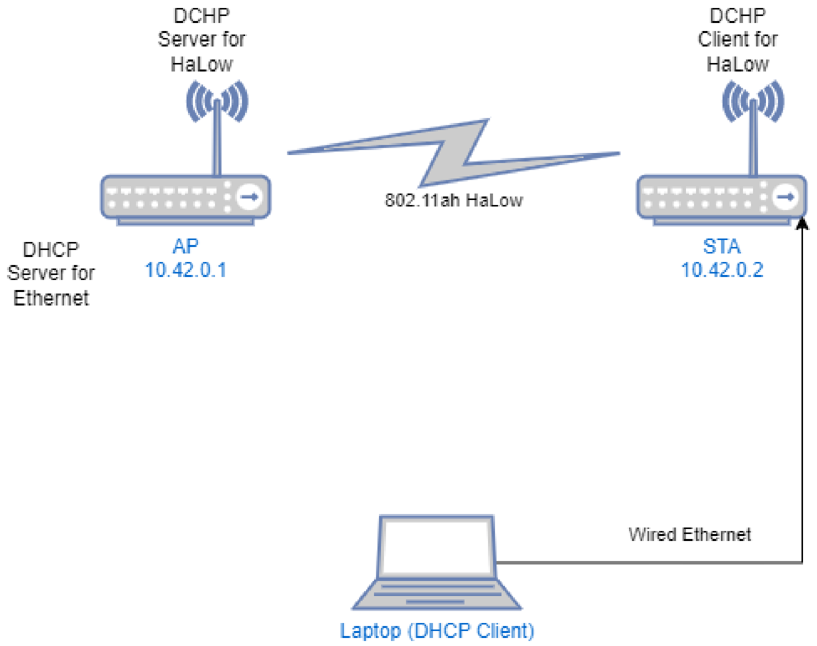
5. Type ‘iperf3 -s’ and press enter to launch the iperf3 server.



```
root@MorseMicro-e10b76:~# iperf3 -s
-----------------------------------------------------------
Server listening on 5201 (test #1)
-----------------------------------------------------------
```

6. Remove the Ethernet cable from your PC.

## 5.2 STA configuration

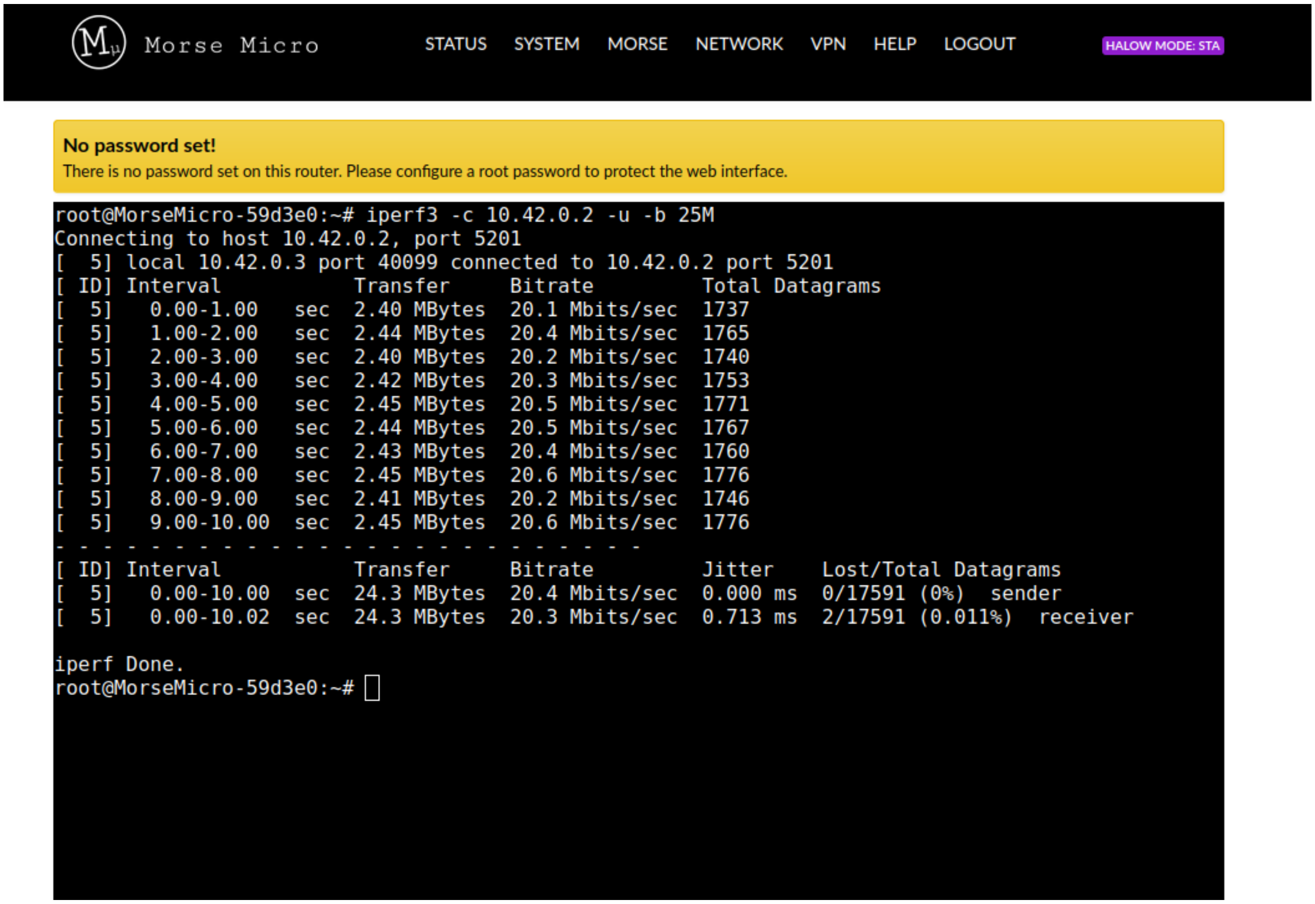


1. Connect an antenna *(EKH01 only)* and an Ethernet cable from your PC to the RJ45 of the Morse Micro device that is the STA. Connect a USB cable for power and optionally the USB/UART cable for a console then power the unit on. Allow ~60 sec for start up.
2. In a web browser on the laptop, navigate to the web UI of the device (http://10.42.0.1 by default).
3. Navigate to the 'Station Configuration' page under the MORSE menu in the top navigation bar. 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 |

4. Navigate to the 'Shell' page under the MORSE section in the UI navigation menu.

5. 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.



**No password set!**
There is no password set on this router. Please configure a root password to protect the web interface.

```
root@MorseMicro-59d3e0:~# iperf3 -c 10.42.0.2 -u -b 25M
Connecting to host 10.42.0.2, port 5201
[  5] local 10.42.0.3 port 40099 connected to 10.42.0.2 port 5201
[ ID] Interval           Transfer     Bitrate         Total Datagrams
[  5]   0.00-1.00   sec  2.40 MBytes  20.1 Mbits/sec  1737
[  5]   1.00-2.00   sec  2.44 MBytes  20.4 Mbits/sec  1765
[  5]   2.00-3.00   sec  2.40 MBytes  20.2 Mbits/sec  1740
[  5]   3.00-4.00   sec  2.42 MBytes  20.3 Mbits/sec  1753
[  5]   4.00-5.00   sec  2.45 MBytes  20.5 Mbits/sec  1771
[  5]   5.00-6.00   sec  2.44 MBytes  20.5 Mbits/sec  1767
[  5]   6.00-7.00   sec  2.43 MBytes  20.4 Mbits/sec  1760
[  5]   7.00-8.00   sec  2.45 MBytes  20.6 Mbits/sec  1776
[  5]   8.00-9.00   sec  2.41 MBytes  20.2 Mbits/sec  1746
[  5]   9.00-10.00  sec  2.45 MBytes  20.6 Mbits/sec  1776
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  5]   0.00-10.00  sec  24.3 MBytes  20.4 Mbits/sec  0.000 ms  0/17591 (0%)  sender
[  5]   0.00-10.02  sec  24.3 MBytes  20.3 Mbits/sec  0.713 ms  2/17591 (0.011%)  receiver

iperf Done.
root@MorseMicro-59d3e0:~# 
```

# 6 EasyMesh

## 6.1 Theory of Operation

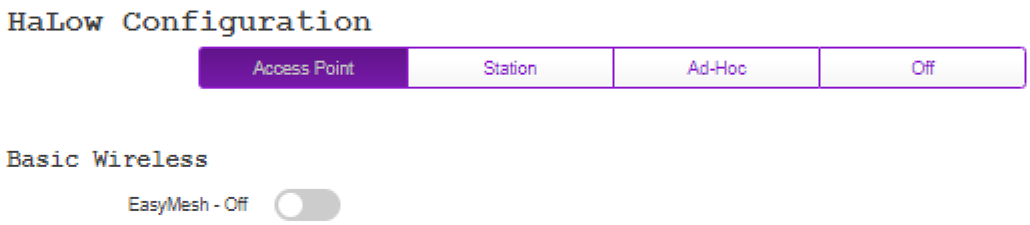
EasyMesh is a Wi-Fi branded, standards-based solution for meshing together access points to provide an extended coverage area (but with reduced bandwidth available to stations). EasyMesh forms a tree structure with one controller at the root that controls the mesh network, and agent APs that connect 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 Configuration

### Access Point Controller

Navigate to the 'Morse->HaLow Configuration' page in the UI. Select 'access point' mode, and then turn on the EasyMesh toggle at the top of the page.

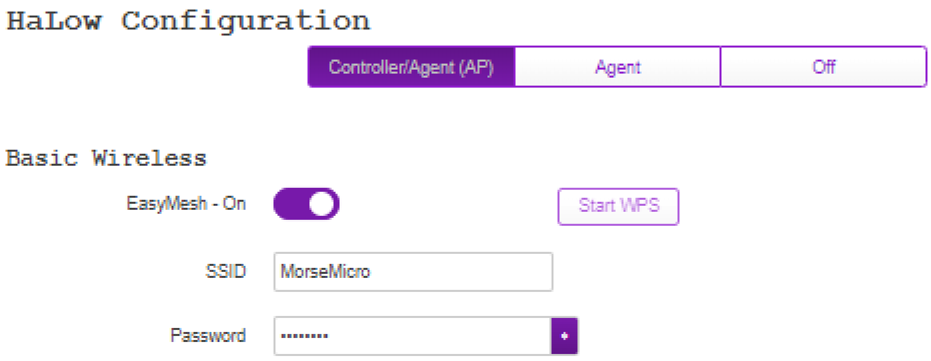


HaLow Configuration

Basic Wireless

EasyMesh - Off

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



HaLow Configuration

Basic Wireless

EasyMesh - On

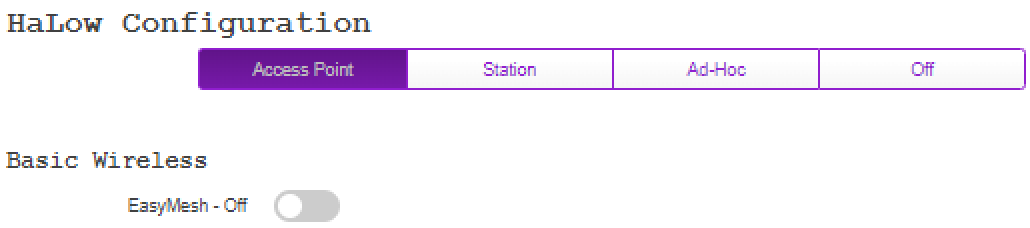
SSID: MorseMicro

Password: ••••••••

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.

### Access Point Agent

Navigate to the 'Morse->HaLow Configuration' page in the UI. Select 'access point' mode, and then turn on the EasyMesh toggle at the top of the page.



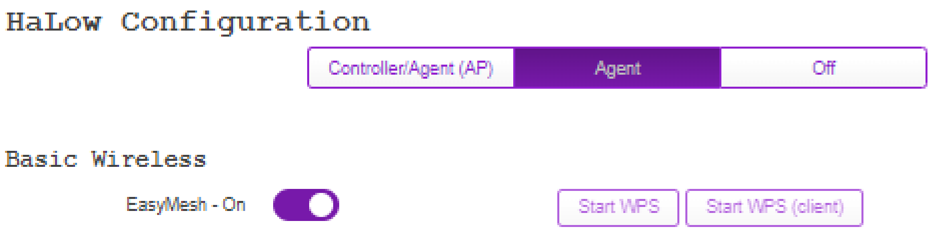
HaLow Configuration

Access Point | Station | Ad-Hoc | Off

Basic Wireless

EasyMesh - Off

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



HaLow Configuration

Controller/Agent (AP) | Agent | Off

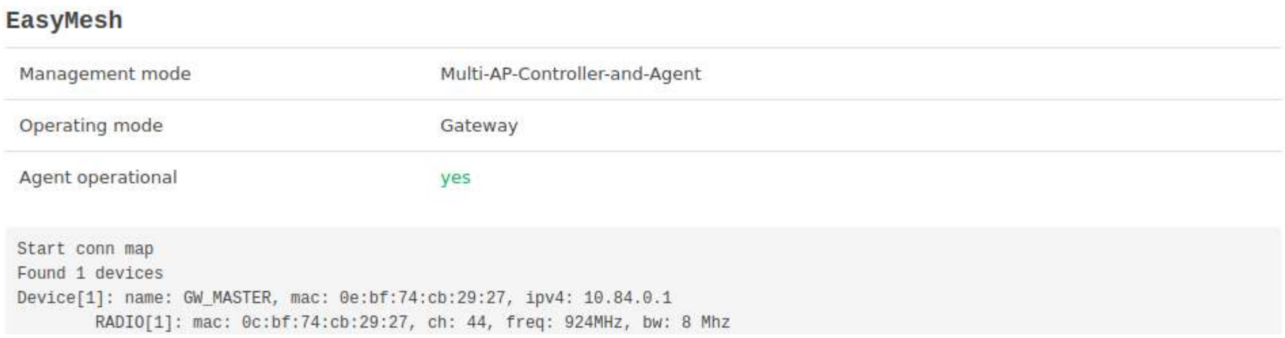
Basic Wireless

EasyMesh - On

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

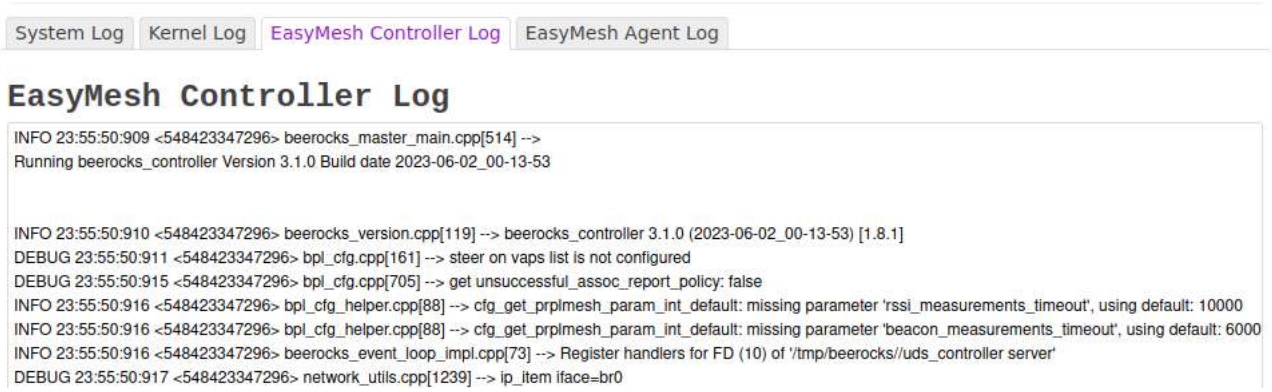


EasyMesh

| | |
|---|---|
| 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.



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:** Video streaming is currently only available for the EKH01s and does not support EKH03s.

## 7.1 Setting up

### Access Point

Setup the access point as a virtual wire (section 3.2) and set a static IP address.

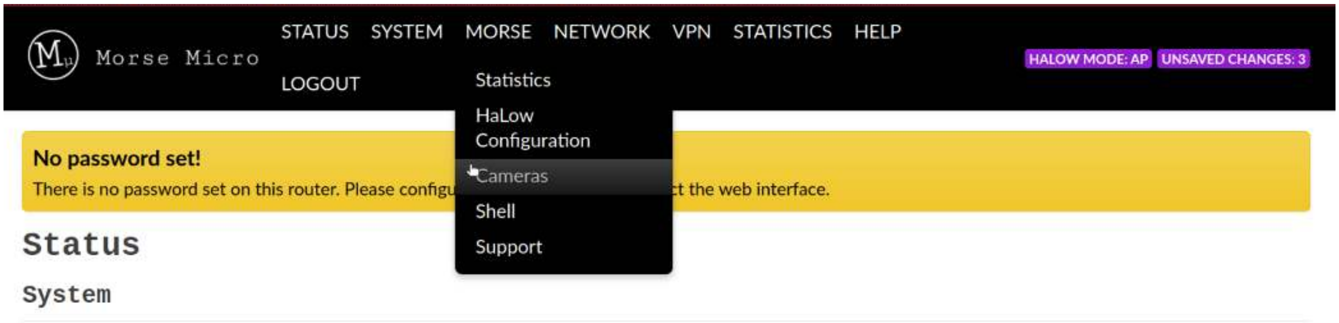
### Stations

Setup stations as standalone devices (section 3.1). Note that stations with an attached camera use a different firmware; the firmware should have '-camera' in the filename.
**WARNING:** If you're using this firmware, it's **not** designed to be used in bridge mode on the stations; if you wish to use it in bridge mode, the ONVIF server configuration needs to be changed via the command line:

```
uci set rpos.core.interface=lan
uci commit
/etc/init.d/rpos restart
```

## 7.2 Getting Video Stream

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

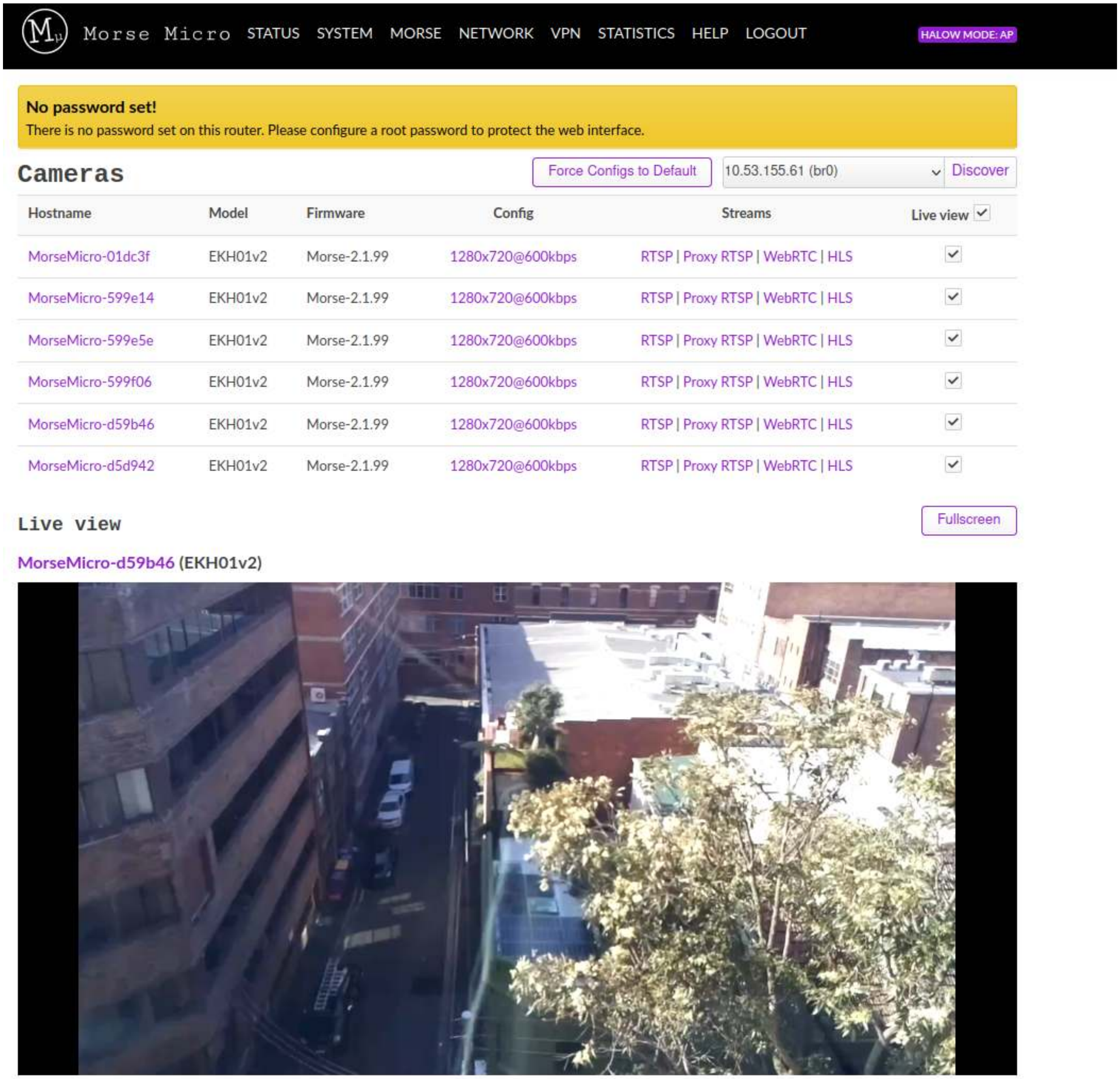


No password set!

There is no password set on this router. Please configu… …t the web interface.

In the camera section the AP will automatically discover all EKH01 devices with cameras. 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.



**No password set!**
There is no password set on this router. Please configure a root password to protect the web interface.

**Cameras**

| Hostname | Model | Firmware | Config | Streams | Live view ☑ |
|---|---|---|---|---|---|
| MorseMicro-01dc3f | EKH01v2 | Morse-2.1.99 | 1280x720@600kbps | RTSP \| Proxy RTSP \| WebRTC \| HLS | ☑ |
| MorseMicro-599e14 | EKH01v2 | Morse-2.1.99 | 1280x720@600kbps | RTSP \| Proxy RTSP \| WebRTC \| HLS | ☑ |
| MorseMicro-599e5e | EKH01v2 | Morse-2.1.99 | 1280x720@600kbps | RTSP \| Proxy RTSP \| WebRTC \| HLS | ☑ |
| MorseMicro-599f06 | EKH01v2 | Morse-2.1.99 | 1280x720@600kbps | RTSP \| Proxy RTSP \| WebRTC \| HLS | ☑ |
| MorseMicro-d59b46 | EKH01v2 | Morse-2.1.99 | 1280x720@600kbps | RTSP \| Proxy RTSP \| WebRTC \| HLS | ☑ |
| MorseMicro-d5d942 | EKH01v2 | Morse-2.1.99 | 1280x720@600kbps | RTSP \| Proxy RTSP \| WebRTC \| HLS | ☑ |

**Live view**

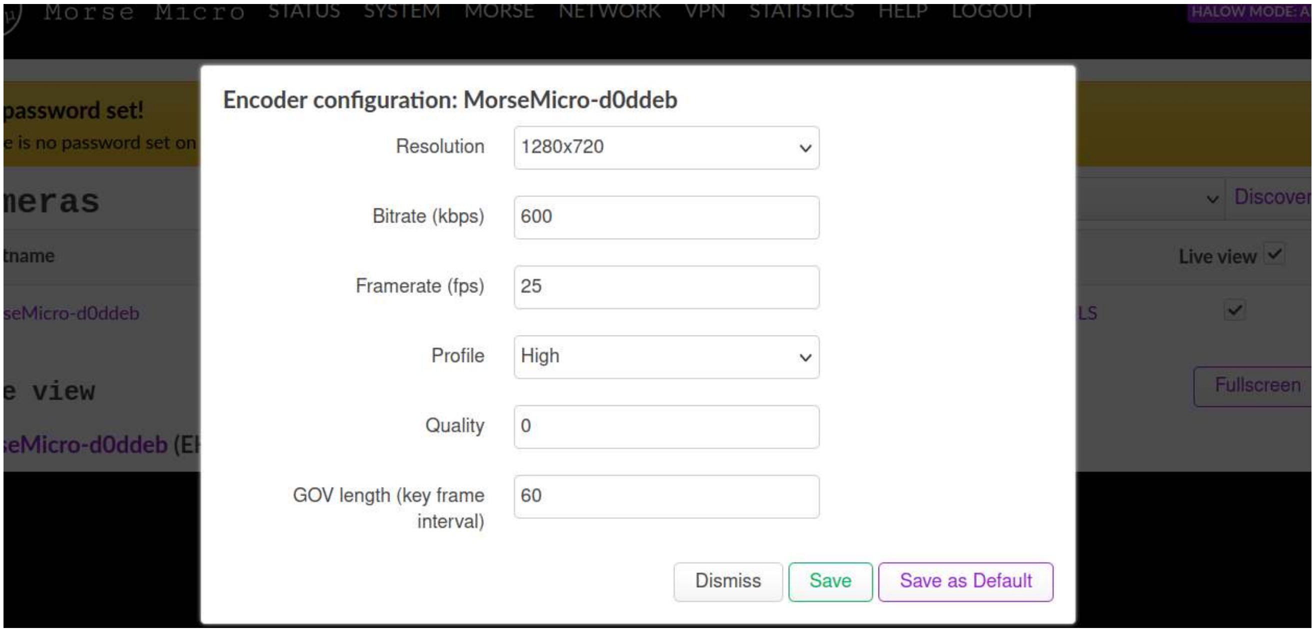
MorseMicro-d59b46 (EKH01v2)

## 7.2 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.

.



Encoder configuration: MorseMicro-d0ddeb

Resolution: 1280x720

Bitrate (kbps): 600

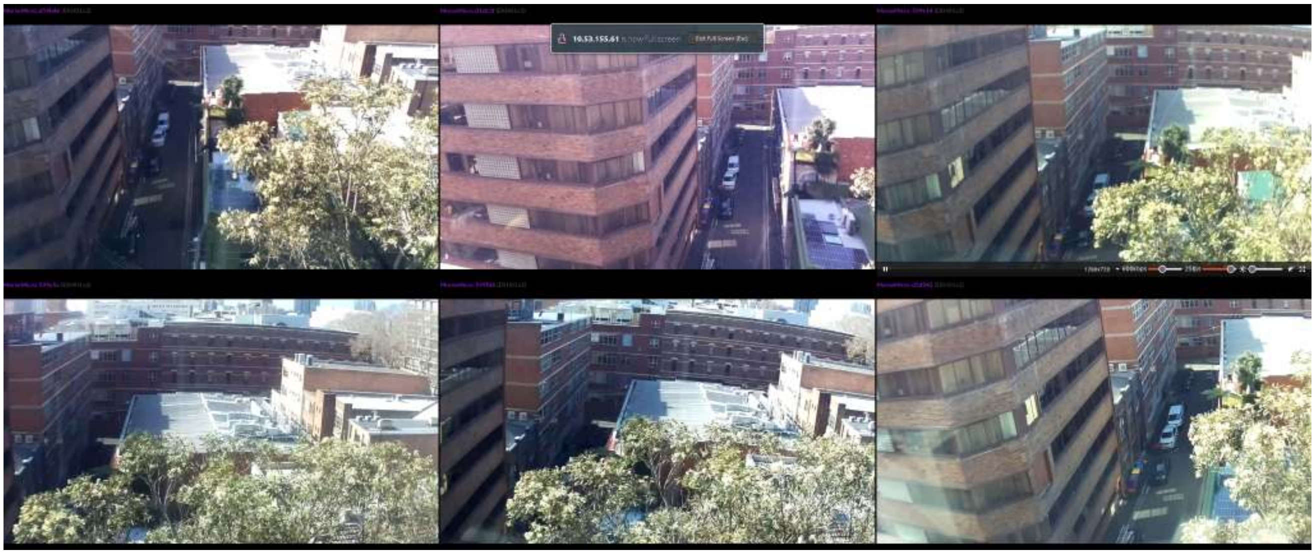
Framerate (fps): 25

Profile: High

Quality: 0

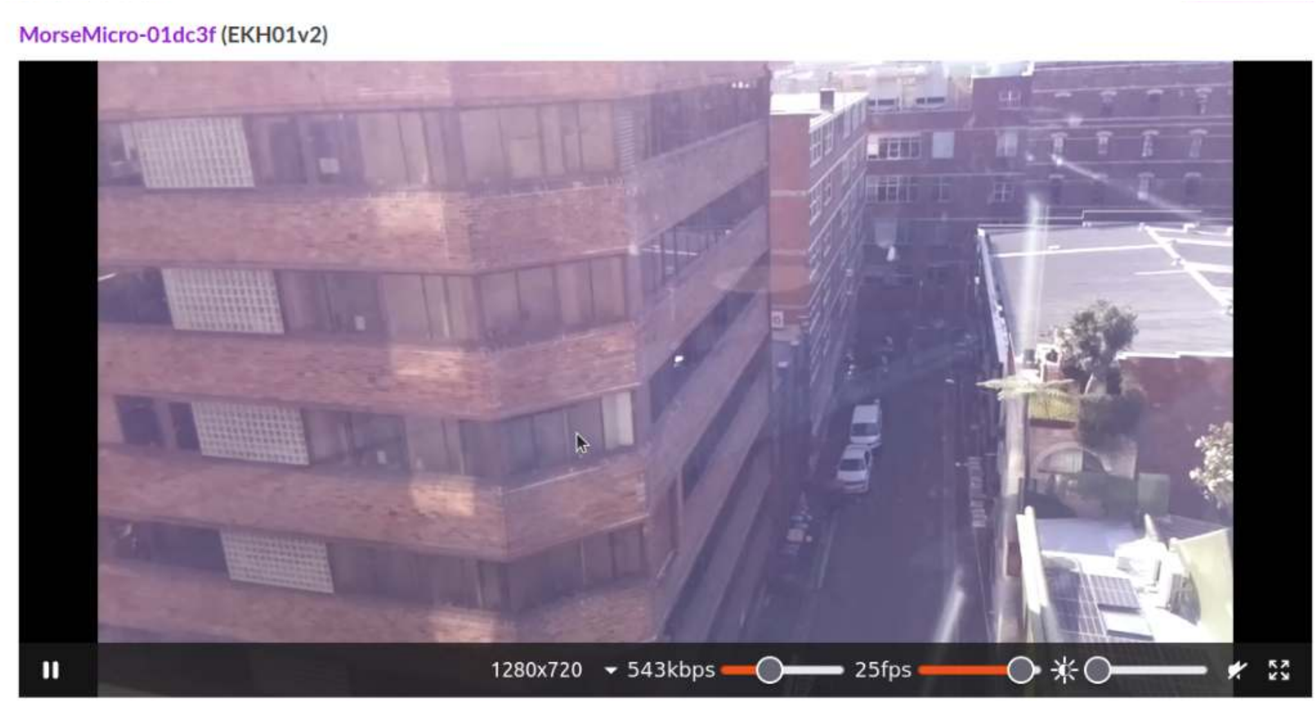
GOV length (key frame interval): 60

  - **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.



## Live View

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


MorseMicro-01dc3f (EKH01v2)

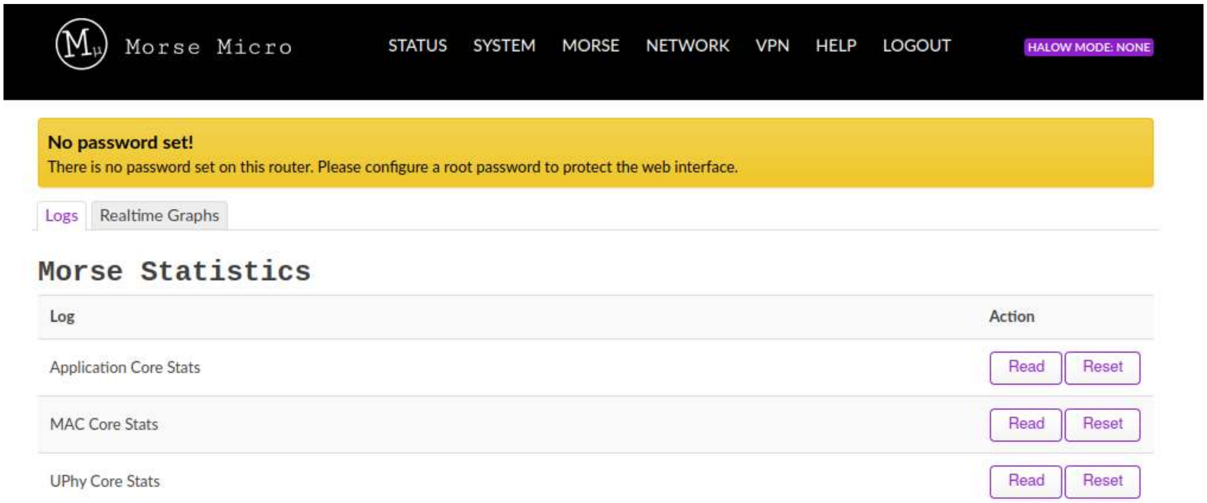
# 8 Page descriptions

## 8.1 MORSE -> Statistics

Provides the statistics for HaLow link including logs from the module and real-time graphs.

### 6.1.1 Logs

The Logs tab can be used to read or reset different sets of information from the stats command morsectrl tool. The read or reset buttons allow the user to choose whether to read or reset core statistics. The information is gathered from the morsectrl tool.



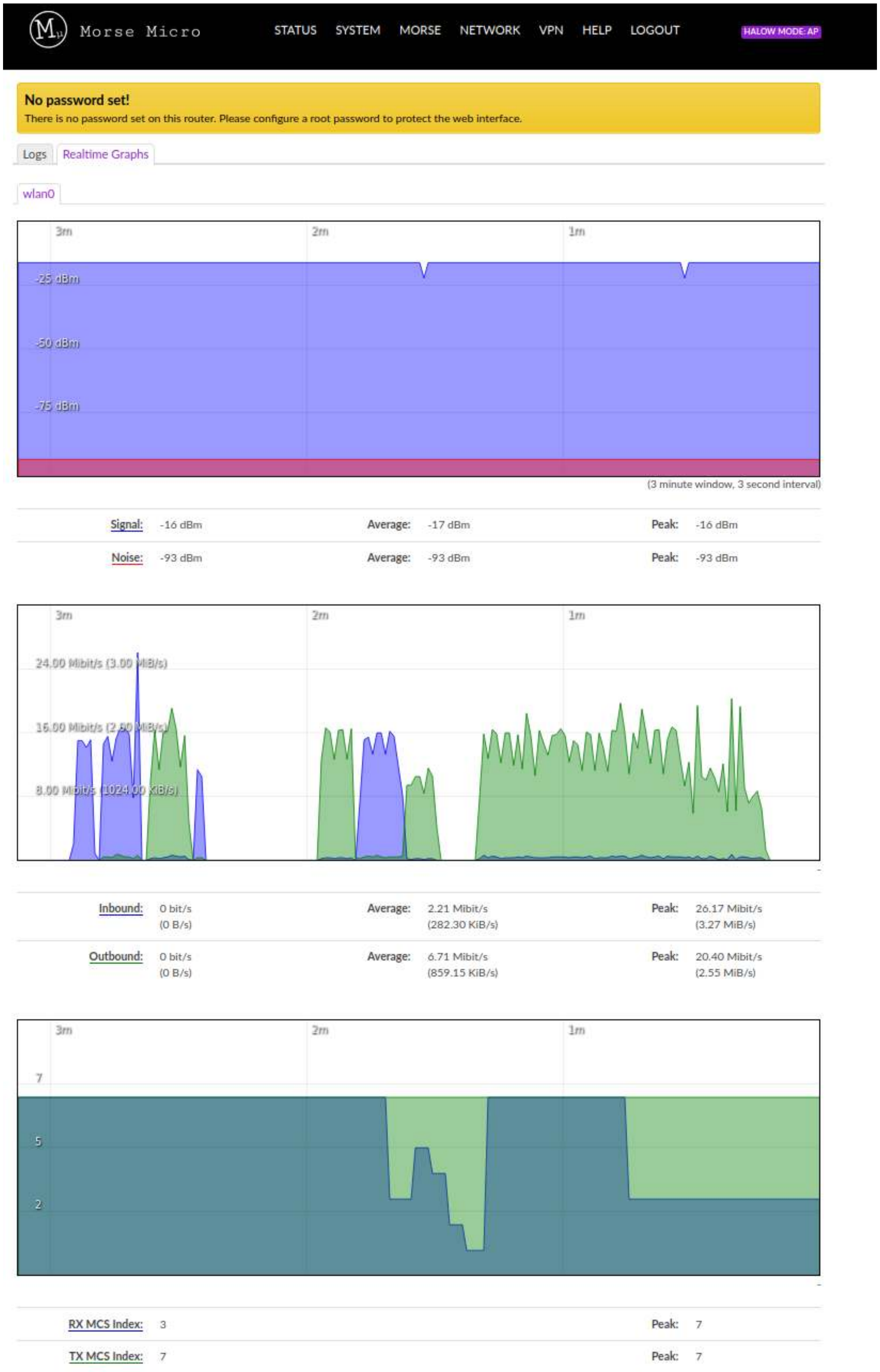
**No password set!**
There is no password set on this router. Please configure a root password to protect the web interface.

Morse Statistics

| Log | Action |
|---|---|
| Application Core Stats | Read Reset |
| MAC Core Stats | Read Reset |
| UPhy Core Stats | Read Reset |

### 6.1.2 Real-time Graphs

The Realtime Graphs page displays animated graphs of HaLow statistics. The graphs show the last 3 minutes of data and update on an interval that can be changed via the dropdown at the top of the page. The interval is set to 3 seconds by default and the dropdown provides options for 1-5 seconds. Changing the interval clears the data from the graphs.



**No password set!**

There is no password set on this router. Please configure a root password to protect the web interface.

(3 minute window, 3 second interval)

Signal: -16 dBm Average: -17 dBm Peak: -16 dBm

Noise: -93 dBm Average: -93 dBm Peak: -93 dBm

Inbound: 0 bit/s (0 B/s) Average: 2.21 Mibit/s (282.30 KiB/s) Peak: 26.17 Mibit/s (3.27 MiB/s)

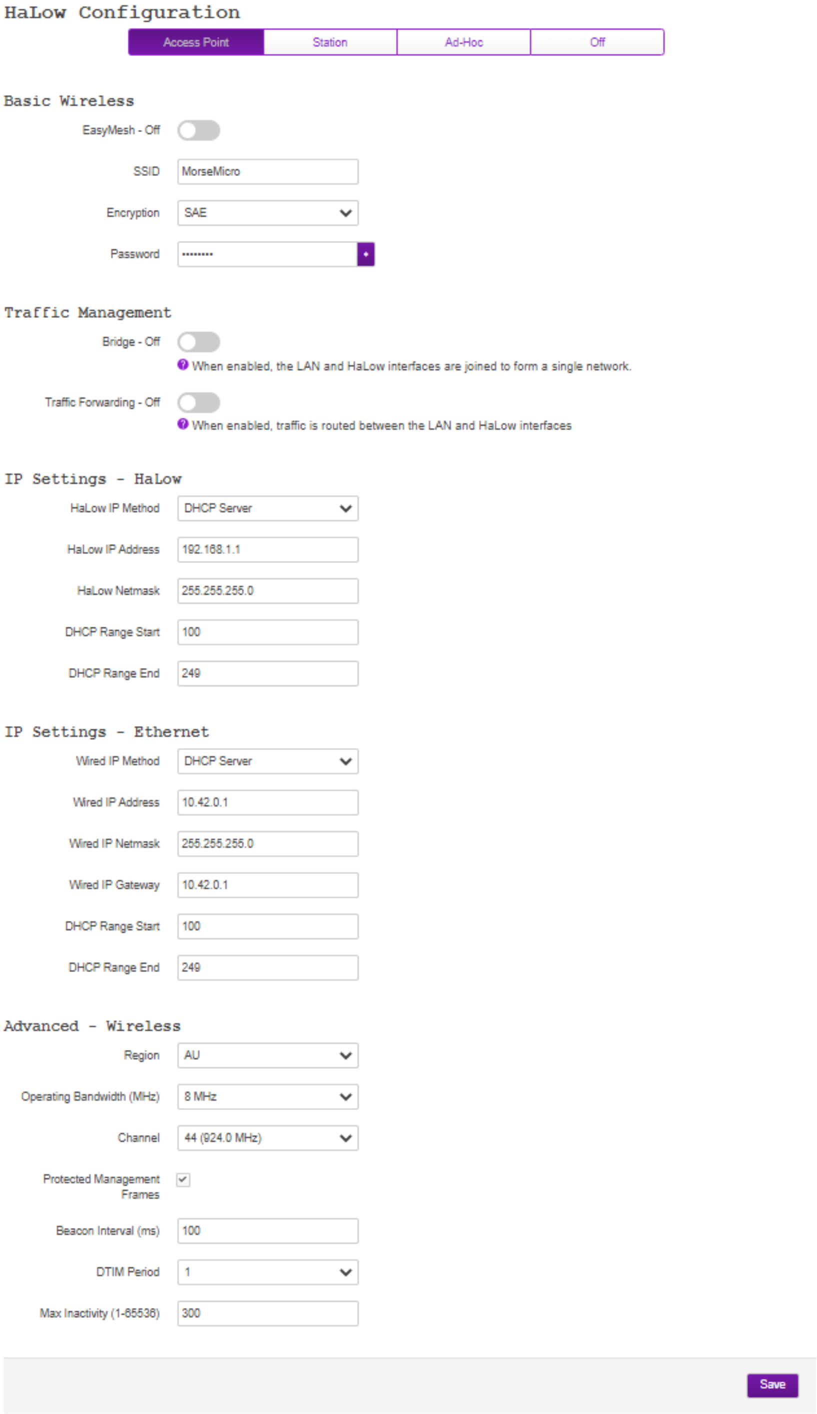
Outbound: 0 bit/s (0 B/s) Average: 6.71 Mibit/s (859.15 KiB/s) Peak: 20.40 Mibit/s (2.55 MiB/s)

RX MCS Index: 3 Peak: 7

TX MCS Index: 7 Peak: 7

# 8.2 MORSE -> HaLow Configuration

The ‘HaLow Configuration’ page can be used to configure HaLow on the device in either access point, station, ad-hoc (IBSS) modes.  Note that settings do not take effect until the ‘Save’ button at the bottom of the page is clicked.



HaLow Configuration

Basic Wireless

| | |
|---|---|
| EasyMesh - Off | ○ |
| SSID | MorseMicro |
| Encryption | SAE |
| Password | •••••••• |

Traffic Management

| | |
|---|---|
| Bridge - Off | ○ |
| | When enabled, the LAN and HaLow interfaces are joined to form a single network. |
| Traffic Forwarding - Off | ○ |
| | When enabled, traffic is routed between the LAN and HaLow interfaces |

IP Settings - HaLow

| | |
|---|---|
| HaLow IP Method | DHCP Server |
| HaLow IP Address | 192.168.1.1 |
| HaLow Netmask | 255.255.255.0 |
| DHCP Range Start | 100 |
| DHCP Range End | 249 |

IP Settings - Ethernet

| | |
|---|---|
| Wired IP Method | DHCP Server |
| Wired IP Address | 10.42.0.1 |
| Wired IP Netmask | 255.255.255.0 |
| Wired IP Gateway | 10.42.0.1 |
| DHCP Range Start | 100 |
| DHCP Range End | 249 |

Advanced - Wireless

| | |
|---|---|
| Region | AU |
| Operating Bandwidth (MHz) | 8 MHz |
| Channel | 44 (924.0 MHz) |
| Protected Management Frames | ☑ |
| Beacon Interval (ms) | 100 |
| DTIM Period | 1 |
| Max Inactivity (1-65536) | 300 |

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 doesn't 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

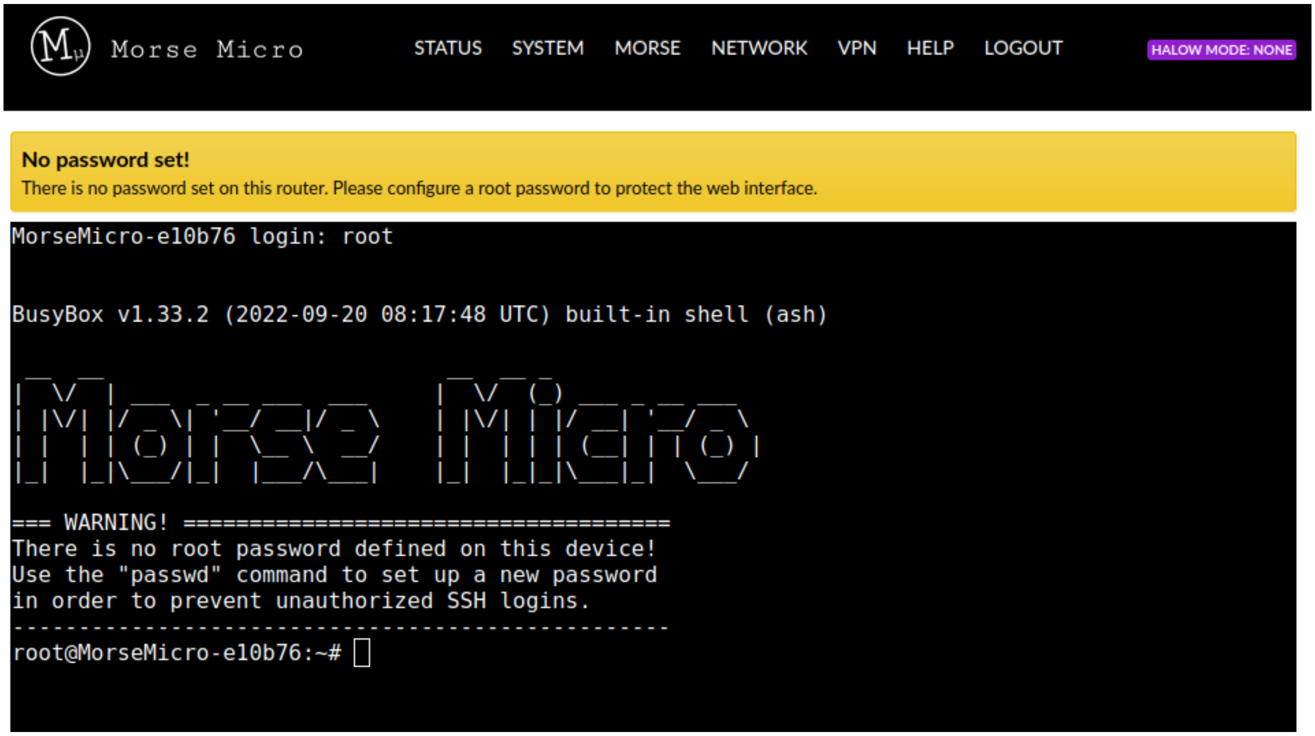
of 2 or above, so that 1 is available for the access point and potential address clashes are avoided.

- **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.

## 8.3 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.



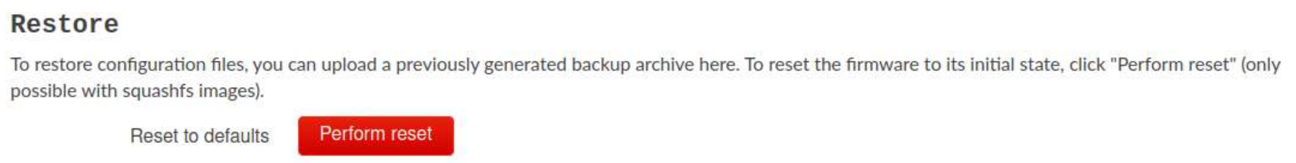
**No password set!**
There is no password set on this router. Please configure a root password to protect the web interface.

```
MorseMicro-e10b76 login: root


BusyBox v1.33.2 (2022-09-20 08:17:48 UTC) built-in shell (ash)

 __  __                       __  __ _
|  \/  | ___  _ __ ___  ___  |  \/  (_) ___ _ __ ___
| |\/| |/ _ \| '__/ __|/ _ \ | |\/| | |/ __| '__/ _ \
| |  | | (_) | |  \__ \  __/ | |  | | | (__| | | (_) |
|_|  |_|\___/|_|  |___/\___| |_|  |_|_|\___|_|  \___/

=== WARNING! =====================================
There is no root password defined on this device!
Use the "passwd" command to set up a new password
in order to prevent unauthorized SSH logins.
--------------------------------------------------
root@MorseMicro-e10b76:~# 
```

## 8.4 SYSTEM -> Backup / Flash Firmware

Perform reset button allows you to factory reset the device

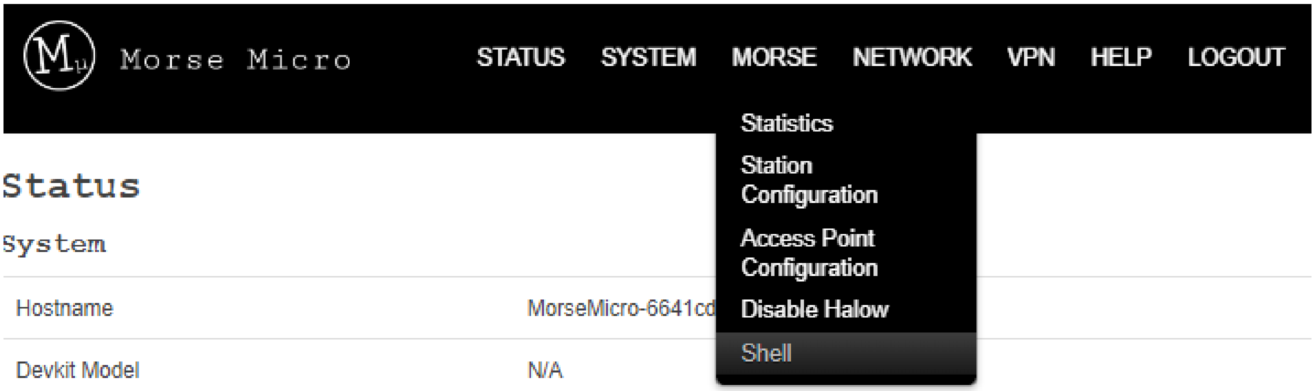
*Note* - for EKH01 this will only reset the Morse Micro specific configurations


Restore

To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

# 9 Advanced configuration

Some advanced configurations are useful to control HaLow behaviour (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.



Status

System

| | |
|---|---|
| Hostname | MorseMicro-6641cd |
| Devkit Model | N/A |

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

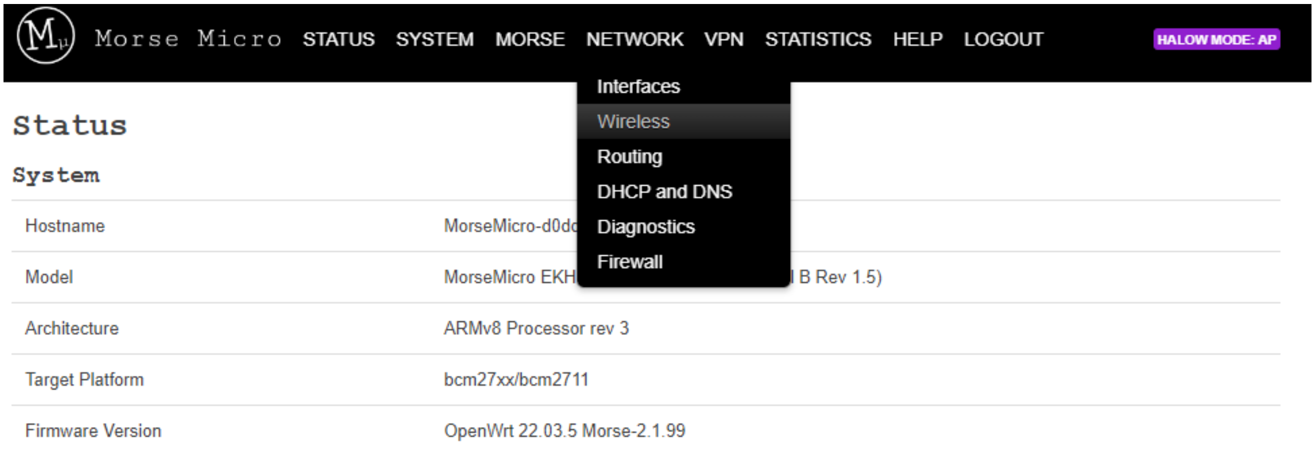
### CLI

AMPDU can be disabled by running the following commands:

```
morsectrl -i wlan0 ampdu disable
```

### Via UI

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

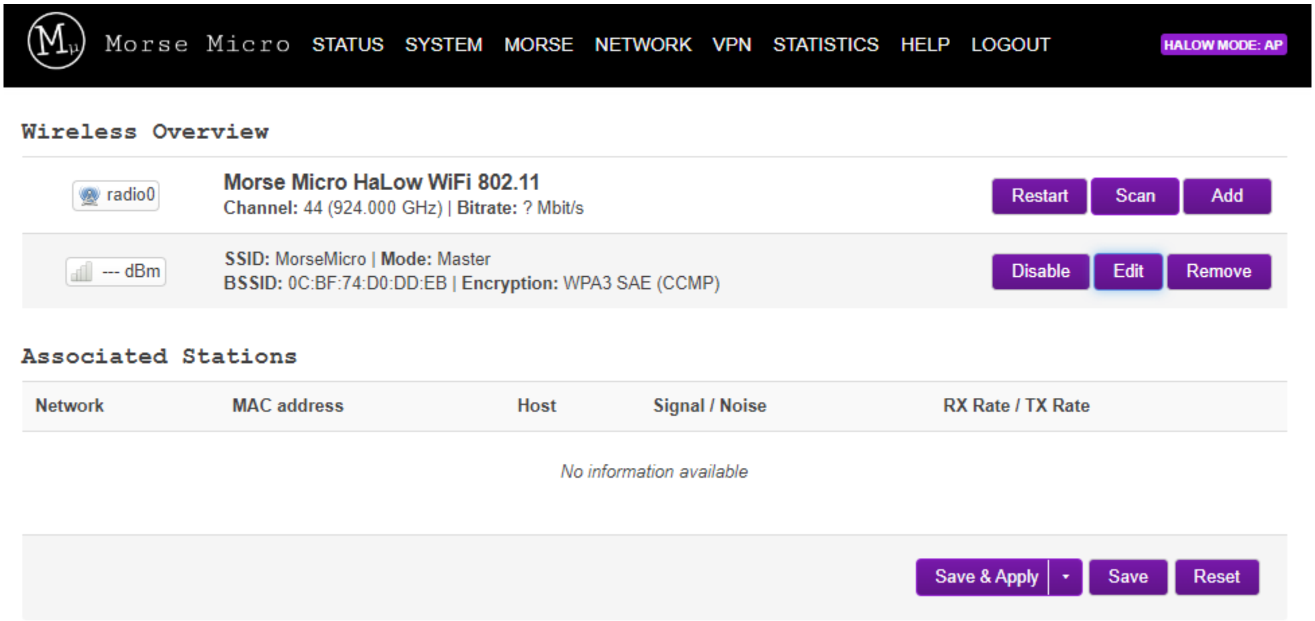


Status

System

| | |
|---|---|
| Hostname | MorseMicro-d0dc |
| Model | MorseMicro EKH … B Rev 1.5) |
| Architecture | ARMv8 Processor rev 3 |
| Target Platform | bcm27xx/bcm2711 |
| Firmware Version | OpenWrt 22.03.5 Morse-2.1.99 |

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



Wireless Overview

radio0 — **Morse Micro HaLow WiFi 802.11**
**Channel:** 44 (924.000 GHz) | **Bitrate:** ? Mbit/s

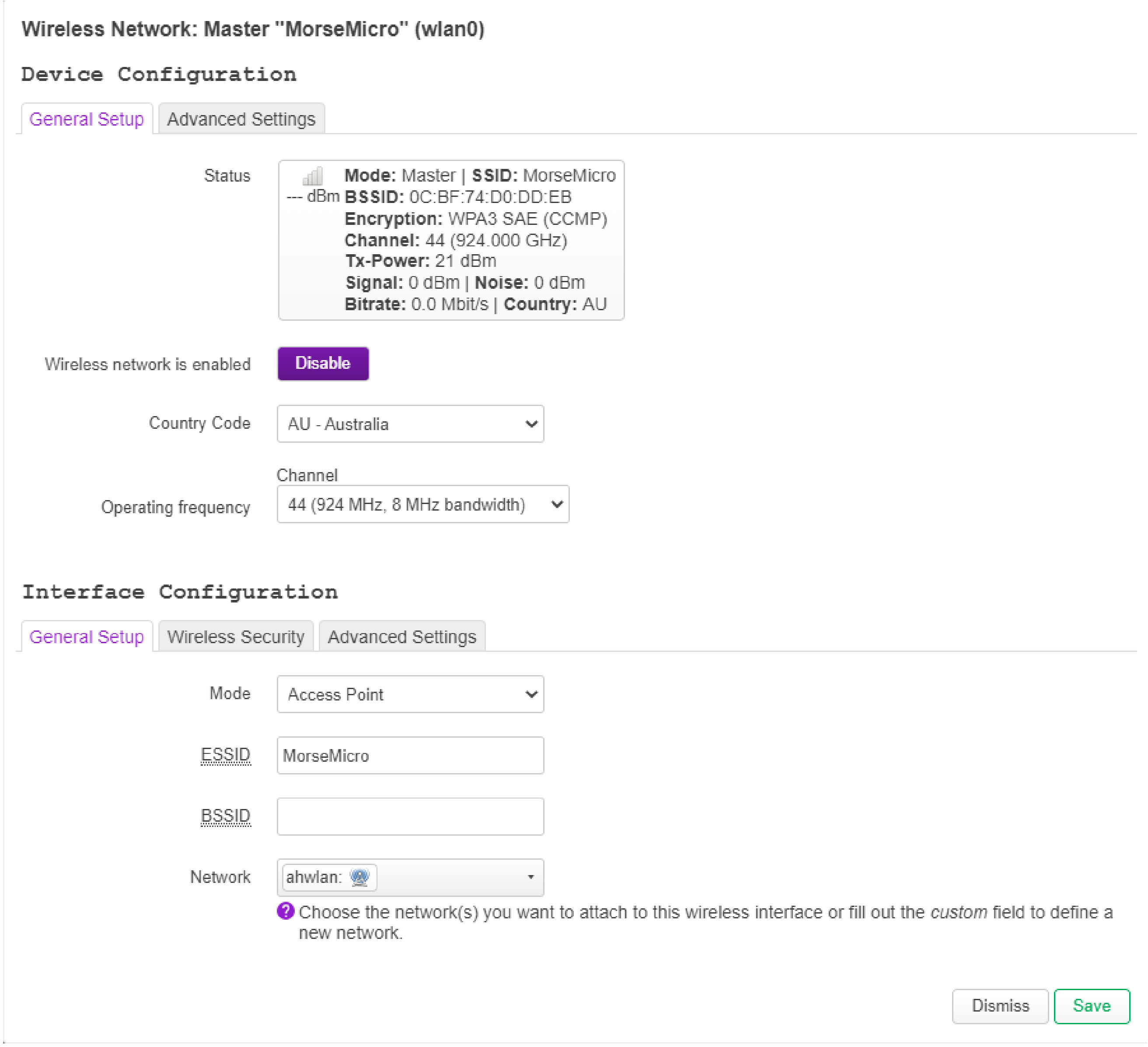
--- dBm — **SSID:** MorseMicro | **Mode:** Master
**BSSID:** 0C:BF:74:D0:DD:EB | **Encryption:** WPA3 SAE (CCMP)

Associated Stations

| Network | MAC address | Host | Signal / Noise | RX Rate / TX Rate |
|---|---|---|---|---|

*No information available*

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



Wireless Network: Master "MorseMicro" (wlan0)

Device Configuration

Status: --- dBm **Mode:** Master | **SSID:** MorseMicro
**BSSID:** 0C:BF:74:D0:DD:EB
**Encryption:** WPA3 SAE (CCMP)
**Channel:** 44 (924.000 GHz)
**Tx-Power:** 21 dBm
**Signal:** 0 dBm | **Noise:** 0 dBm
**Bitrate:** 0.0 Mbit/s | **Country:** AU

Wireless network is enabled: Disable

Country Code: AU - Australia

Operating frequency: Channel 44 (924 MHz, 8 MHz bandwidth)

Interface Configuration

Mode: Access Point

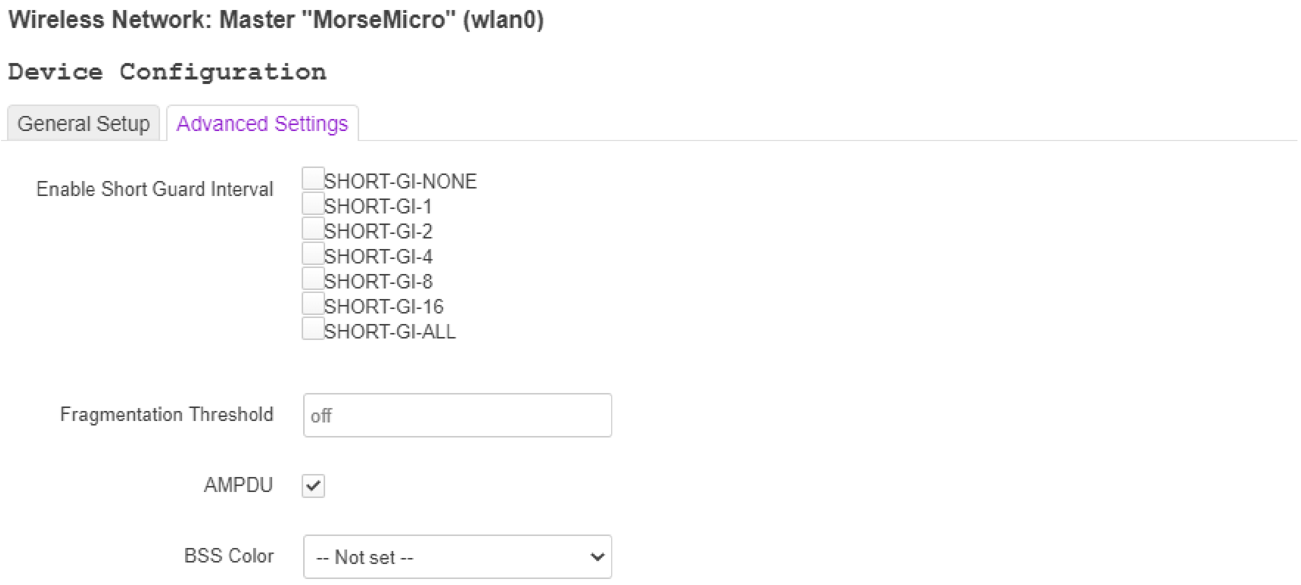
ESSID: MorseMicro

BSSID:

Network: ahwlan:

Choose the network(s) you want to attach to this wireless interface or fill out the *custom* field to define a new network.

The untick the 'AMPDU' option to disable AMPDU:



Wireless Network: Master "MorseMicro" (wlan0)

Device Configuration

Enable Short Guard Interval
□ SHORT-GI-NONE
□ SHORT-GI-1
□ SHORT-GI-2
□ SHORT-GI-4
□ SHORT-GI-8
□ SHORT-GI-16
□ SHORT-GI-ALL

Fragmentation Threshold: off

AMPDU ☑

BSS Color: -- Not set --

## 9.2 Fragmentation Threshold

### 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.

### 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
```

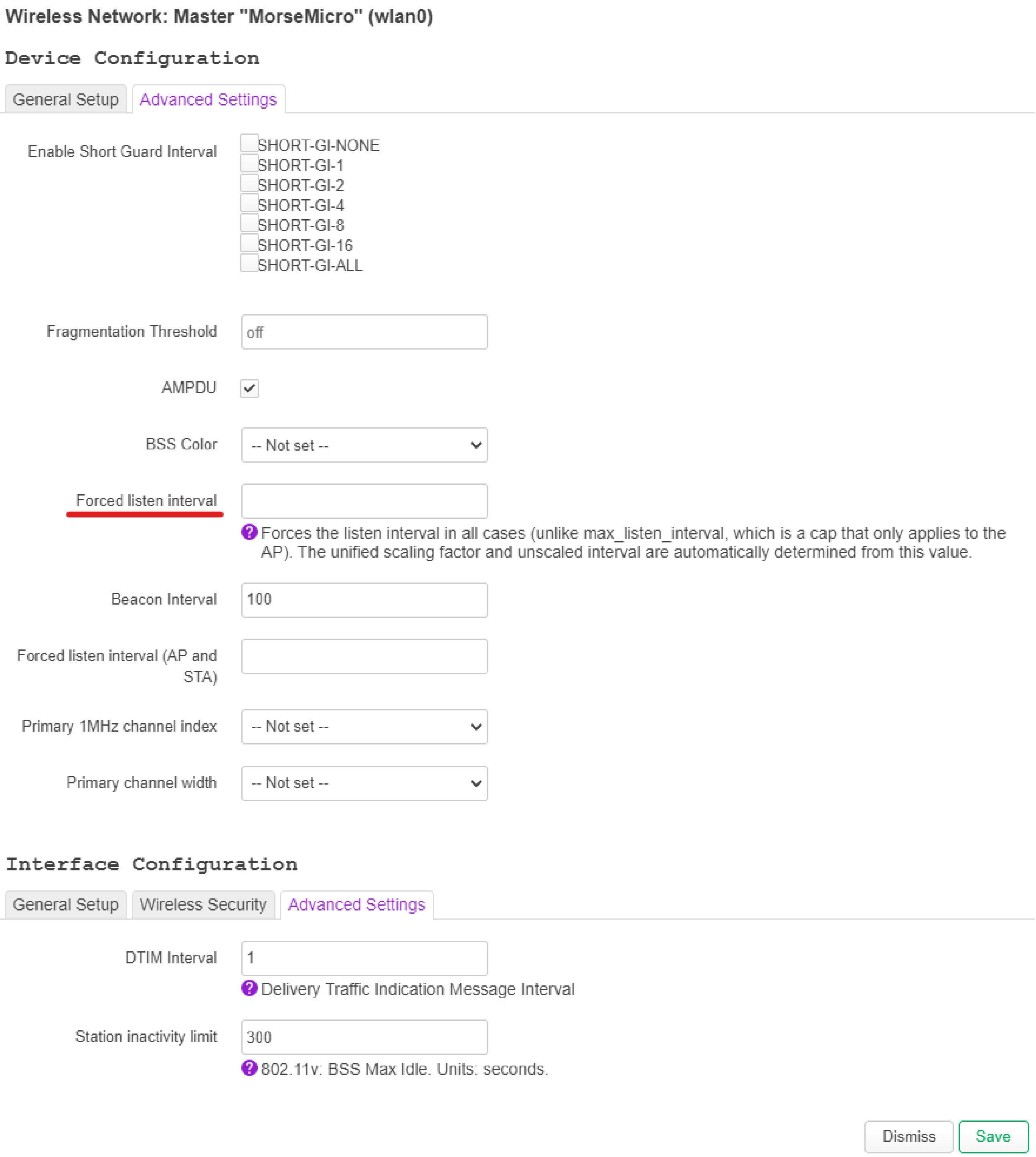
In this case, phy1 is the <phyname>. The integer following phy enumerates

every time the driver is (re)loaded.

## 9.3 Unified Scaling Factor / Unscaled Interval

### Via UI

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



**Wireless Network: Master "MorseMicro" (wlan0)**

**Device Configuration**

Enable Short Guard Interval
□ SHORT-GI-NONE
□ SHORT-GI-1
□ SHORT-GI-2
□ SHORT-GI-4
□ SHORT-GI-8
□ SHORT-GI-16
□ SHORT-GI-ALL

Fragmentation Threshold: off

AMPDU: ☑

BSS Color: -- Not set --

Forced listen interval:

Forces the listen interval in all cases (unlike max_listen_interval, which is a cap that only applies to the AP). The unified scaling factor and unscaled interval are automatically determined from this value.

Beacon Interval: 100

Forced listen interval (AP and STA):

Primary 1MHz channel index: -- Not set --

Primary channel width: -- Not set --

**Interface Configuration**

DTIM Interval: 1

Delivery Traffic Indication Message Interval

Station inactivity limit: 300

802.11v: BSS Max Idle. Units: seconds.

### Via CLI

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

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

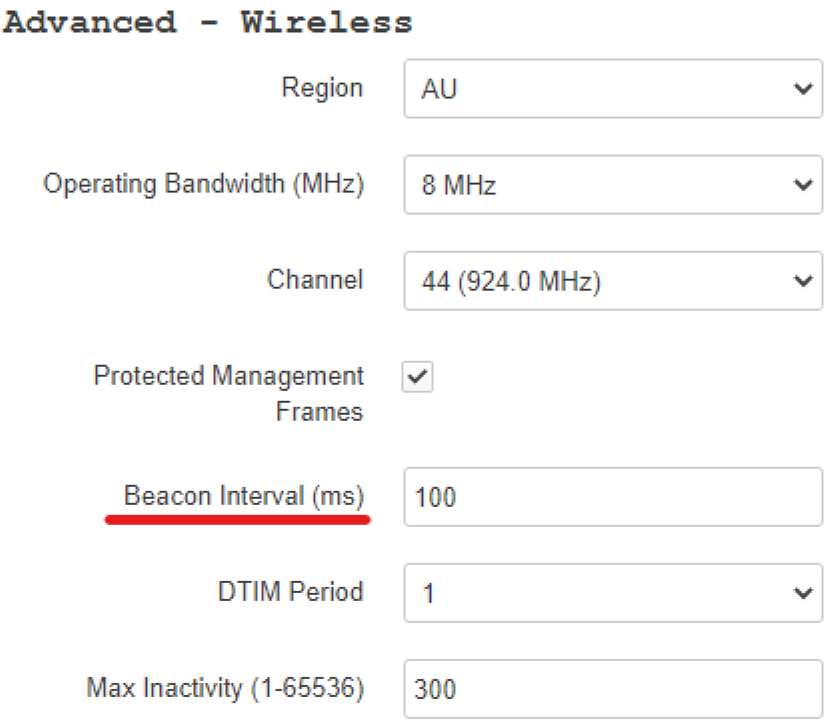
Where <unscaled interval> multiplied by <unified scaling factor> must be

less than or equal to the integer value 65536.

## 9.4 Beacon Interval

### Via UI

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



**Advanced - Wireless**

Region: AU

Operating Bandwidth (MHz): 8 MHz

Channel: 44 (924.0 MHz)

Protected Management Frames: ☑

Beacon Interval (ms): 100

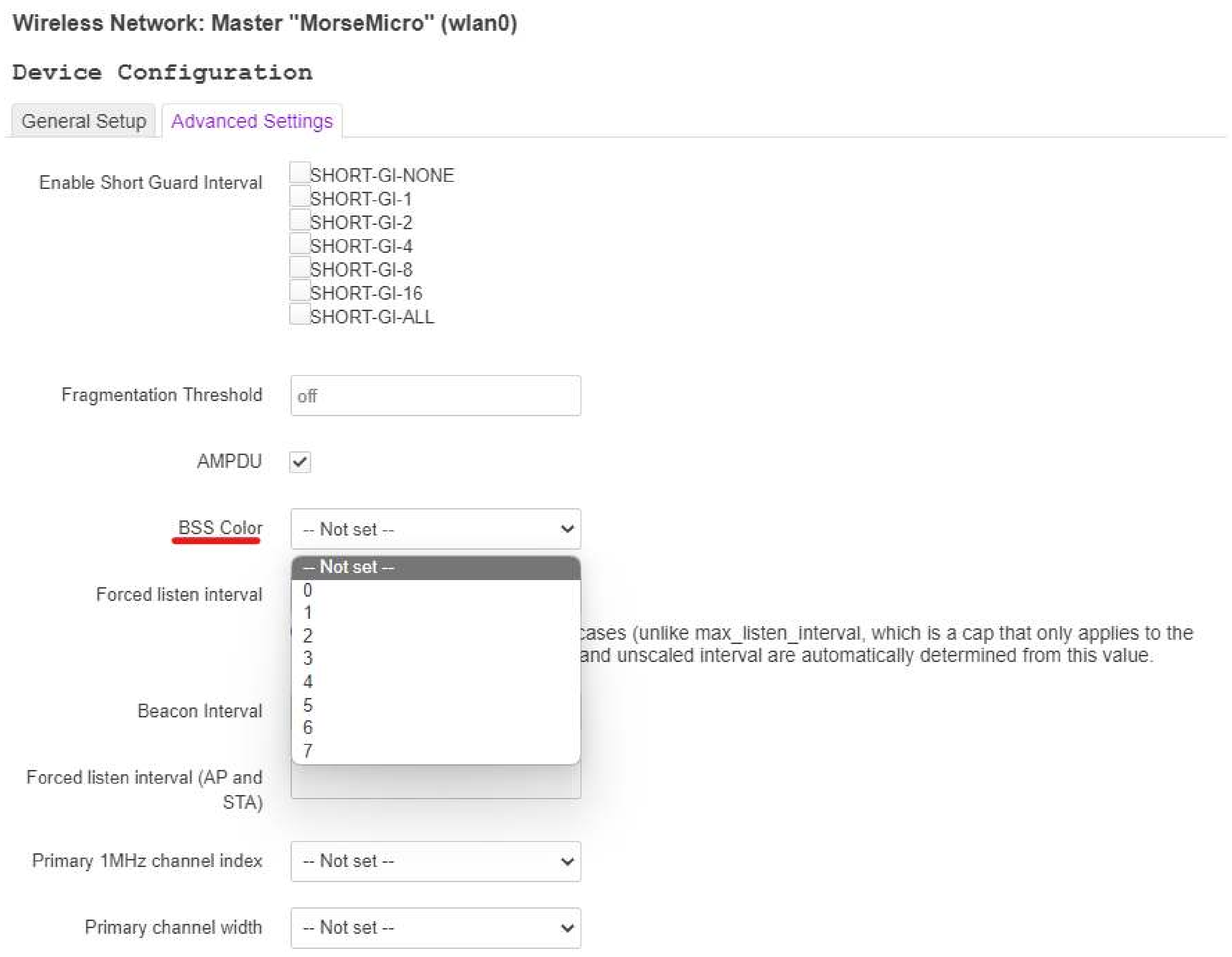
DTIM Period: 1

Max Inactivity (1-65536): 300

## 9.5 BSS Color

### Via UI

Navigate to Network->Wireless, and choose edit beside the HaLow network.  In the advanced settings tab at the top the setting for BSS color can be configured:



Wireless Network: Master "MorseMicro" (wlan0)

Device Configuration

Enable Short Guard Interval
□ SHORT-GI-NONE
□ SHORT-GI-1
□ SHORT-GI-2
□ SHORT-GI-4
□ SHORT-GI-8
□ SHORT-GI-16
□ SHORT-GI-ALL

Fragmentation Threshold: off

AMPDU: ☑

BSS Color: -- Not set --

-- Not set --
0
1
2
3
4
5
6
7

Forced listen interval

cases (unlike max_listen_interval, which is a cap that only applies to the
and unscaled interval are automatically determined from this value.

Beacon Interval

Forced listen interval (AP and STA)

Primary 1MHz channel index: -- Not set --

Primary channel width: -- Not set --

### Via CLI

BSS color can be configured using the following command:

```
Morsectrl -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 morsectrl

`morsectrl` is a command line utility that allows you to control certain aspects of the radio behaviour. For more details of its available options, please refer to the command help by running "`morsectrl -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 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.

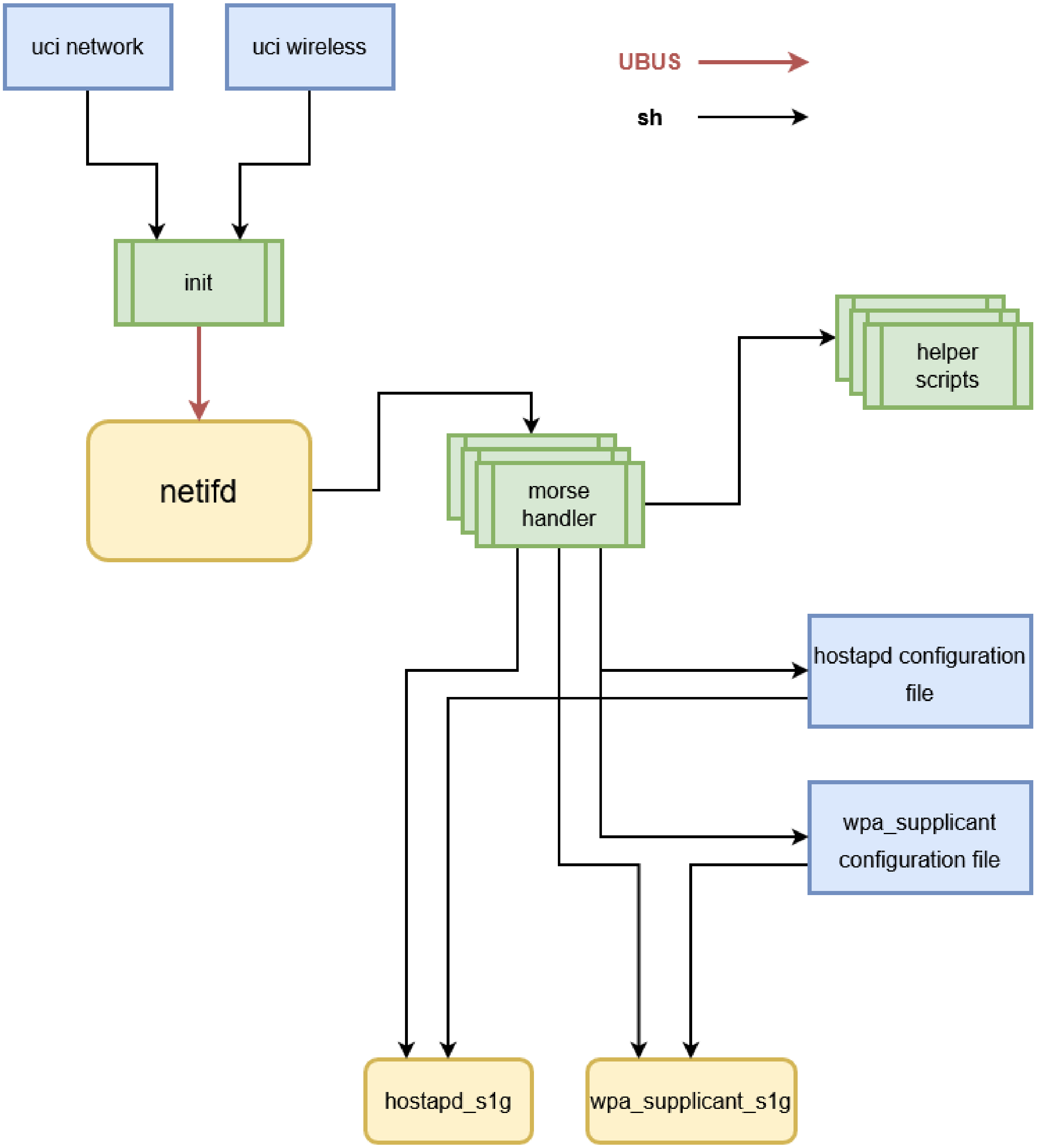
When a configuration change is saved the page will iterate over the fields available and set appropriate UCI configuration values for each changed field. UCI commands are sent via JSON-RPC API to a Ubus endpoint bound to the uhttpd server. Once all changed fields have been updated, the configuration 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:

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

The image below captures the execution flow of this process:



# 11 Revision history

| Revision Number | Release Date | Update Notes |
|---|---|---|
| 12 | June 2nd 2023 | ● Update for new HaLow configuration page<br>● Update for new EasyMesh feature<br>● Update for new Video UI feature<br>● Update for adding Internet connectivity |
| 11 | Feb 27th 2023 | ● Correct some typos |
| 10 | Jan 6th 2023 | ● Updated for UCI configuration<br>● Updated default IP address to 10.42.0.1 |
| 9 | Dec 12th 2022 | ● Updated formatting and cover page image |
| 8 | Nov 22nd, 2022 | ● Updated device images |
| 7 | Nov 18th, 2022 | ● Add description of key setup scenarios, and refactored configuration to match these.<br>● Removed references to custom configurations, and manual configuration except where not available in UI.<br>● Other general improvements |
| 6 | Oct 20th, 2022 | ● Added example of how to run wavemon for basic HaLow testing |
| 5 | Oct 10th, 2022 | ● Improved formatting and reworded some sections for clarity.<br>● Added UI Configuration architecture |
| 4 | Oct 5th, 2022 | ● Updated for the LuCI interface<br>● Added in EKH01 |
| 3 | Mar. 4th, 2022 | ● IPERF Traffic Setup<br>● Added Tools -> HaLow Firmware Upgrade |

| | | |
|---|---|---|
| 2 | Feb. 12th, 2022 | ● Update for firmware release 1.3 |
| 1 | Dec. 20th, 2021 | ● Initial release |

Morse Micro makes no warranty, representation, or guarantee regarding the information contained herein or the suitability of its products and services for any particular purpose, nor does Morse Micro assume any liability whatsoever arising out of the application or use of any product or circuit. The products sold hereunder and any other products sold by Morse Micro have been subject to limited testing and should not be used in conjunction with mission-critical equipment or applications. Any performance specifications are believed to be reliable but are not verified, and Buyer must conduct and complete all performance and other testing of the products, alone and together with, or installed in, any end-products. Buyer shall not rely on any data and performance specifications or parameters provided by Morse Micro. It is the Buyer's responsibility to independently determine suitability of any products and to test and verify the same. The information provided by Morse Micro hereunder is provided "as is, where is" and with all faults, and the entire risk associated with such information is entirely with the Buyer. Morse Micro does not grant, explicitly or implicitly, to any party any patent rights, licenses, or any other IP rights, whether with regard to such information itself or anything described by such information. Information provided in this document is proprietary to Morse Micro, and Morse Micro reserves the right to make any changes to the information in this document or to any products and services at any time without notice.

Morse Micro

reaching farther™

**Morse Micro Pty. Ltd. Corporate Headquarters**
Level 8, 10-14 Waterloo Street, Surry Hills, NSW 2010, Australia

USA: +1.949.501.7080
Australia: +61.2.905.45922
China: +86.571.229.30277
Email: sales@morsemicro.com