User's Guide

For
CabinLink 6

Document Number USR102078
Rev F

TABLE OF CONTENTS

LIST OF FIGURES

REVISION HISTORY

Rev	Description	Date	Contributor
Draft	Initial Draft	2022-10-13	J Mordacq
Rev A	Add more GUI Screens	2022-12-06	R Wolfe
Rev B	Add Use Case Examples, clean up GUI Screens	2023-04-13	R Wolfe
Rev C	Update mechanical drawings and pinout in section 2.9	2023-05-15	R Wolfe
Rev D	Added Log History 5.7, Self-Signed Certificate Config 7.1.3, Network Status 5.4, and System Health 5.8 Added DO-160G tested cable info to section 2.9	2023-05-23	R Wolfe
Rev E	Various updates to sections: 2.8, 3.1.2, 3.2.3, 8.2.6, 8.6.6 Added section 2.10	2023-08-16	R Wolfe
Rev F	Added section 2.8 Environmental Testing Performance Specifications, Appendix D Compliance Statements. Other sections shifted down. Updates to Figure 6, 8. Updated section 10 to include information on RS-232 connection.	2023-08-30	R Wolfe

1. Introduction

This document is the User's Guide for the Righthand Technologies CabinLink 6 Wireless Router and Access Point. The CL6 consists of a wireless router/access point line-replaceable unit (LRU) with RHT PN# 1024-200056 and an optional RaDome Antenna LRU with RHT PN# 1024-200057. This document describes the device's usage, installation, and configuration options.

1.1 References

Document Tite: ICD102068_CabinLink_6_ICD
Document Name: RightHand Technologies CabinLink 6 Interface Control Document
Document Version: D
Document Path /URL:
http://repo2.righthandtech.local:7450/CabinLink6/Docs/blob/master/Process/Designs/ICD102068_CabinLink_6_ICD.docx

2. CabinLink 6 LRU Description

2.1 General Overview

The CL6 cabin systems LRU is designed to bring wireless networking capabilities to the light jet market, bridging cabin and aircraft wireless devices to interact with aircraft cabin system. It can also act as a wireless interface for passenger devices to access the Internet via an air/ground or satellite link (provided by an external system). The CL6 may act as just a wireless access point to provide wireless access to the cabin system and may also act as a router between the cabin system and another external network (such as internet connectivity through a Satcom system). It can also act as a range extender to repeat the wireless signal from a router to expand its coverage. The CL6 supports Wifi 6 (IEEE 802.11ax) and legacy wireless modes. It supports both 2.4GHz and 5GHz wireless bands, and has five wired ethernet ports.

2.2 Physical Description

The CL6 device brings out all of the I/O interfaces used in flight, which include: (1) +28V Power and Return, (3) Address Straps, (2) RF kill discrete inputs, (2) discrete outputs for power enable and wireless enable status, (4) SMA connectors supporting dual band WIFI antennas, (4) 1000 Mbps Ethernet Port, (1) 2500 Mbps Ethernet Port, and (1) 10-32 Chassis Ground. An additional RS-232 port is available only for debug and is not used in flight.

The antenna module has (4) SMAs that connect to the CL6's SMAs through four SMA cables. Four #8-32 x 3/8" stainless steel, Phillips Pan head with Nylon patch screws are used to mount the antenna to the CL6 and, normally, (4) 4" SMA cables (Rht Pn# 3600-200242) connect the LRUs.

An overview of the CL6 with the antenna attached and without can be seen below.

Figure 1 - CL6 with and without attached antenna

2.3 Input Power

The CL6 is designed to operate with 28 VDC aircraft power and to withstand surge voltage up to 100 V. The CL6 has reverse input power protection and an input over current limit set to 6.9 Amps. It also has internal short-circuit protection through the use of a Texas Instruments TPS2493PW hot-swap controller and Infineon BSC360N15NS3G 150 V, 33 A N-Channel MOSFET. All internally-generated power supply voltage rails have short circuit protection integrated into their associated regulators.

2.4 ESD Protection

The CL6 has been designed with ESD protection on all input and output circuits attached to connectors J1, J2, J3, J4, J5, and ETH0 through ETH4.

2.5 Electromagnetic Interference Protection

The CL6 chassis has been designed to provide an electrical seal around the internal circuitry and cables with a direct metal-to-metal connection of all connector faces to chassis. External interconnecting cables use metal-enclosed back shells with improved EMI immunity.

2.6 Electrical and Thermal Safety Protection

The CL6 has the following electrical and thermal protection features. These features are fully hardware-controlled and require no software for operation.

- Input hot-swap controller
  - Power-on occurs only when input voltage is within the range of 18 to 33 VDC.
- Input thermal protection
  - Power-on occurs only when the internal ambient temperature is between -35 °C and 90 °C. In addition, there is about 5°C degrees of hysteresis returning from these extremes.

2.7 Setting IP Address with Switches

The CL6 determines its IP address per the following table (where 1 = asserted = ground). If the user wants to use IP configuration defined in a configuration file, the address straps are disconnected and the user must modify the IP address for the 'lan' in /etc/config/network settings.

If the CL6 will obtain IP addresses from a DHCP Server, the address straps are connected to ground.
Otherwise, set address straps per the following table.

First 3 bytes: Obtained from /etc/config/network (configured IP address) Last byte: from straps.

IP Strap 2	IP Strap 1	IP Strap 0	Address
0	0	0	Per config file
0	0	1	X.X.X.1
0	1	0	X.X.X.2
0	1	1	X.X.X.3
1	0	0	X.X.X.4
1	0	1	X.X.X.5
1	1	0	X.X.X.6
1	1	1	Via DHCP Client

Figure 2 - IP Strapping options

2.8 Environmental Testing Performance Specifications

Environment Condition	DO-160G Section	Test Category	Requirements/Comments
Temperature	Section 4	A2	Normal Operating Temperature Range: -15 ℃ TO +70 ℃
Altitude	Section 4	A2	+15,000 FT
Decompression	Section 4	A2	+55,000 FT
Overpressure	Section 4	A2	Test level: 180kP
Temperature Variation	Section 5	B	(5 ℃ / MIN)
Touch Temperature	-	PER ARINC 628 / PART 7, SECTION B4.6.2	Test at 30 ℃ Ambient Aluminum <= 51.1 ℃ Stainless Steel <= 52.9 ℃ Acrylic <= 60.1 ℃, Plastics <= 59.0 ℃. If touch temperature exceeded, should be protected from contact and provide easily-visible placard warning.
Humidity	Section 6	A	95% RH @ 50℃
Operational Shock	Section 7	B	
Crash Impulse Shock	Section 7	B	20g/11ms
Crash Sustained	Section 7	B	18 G
Vibration	Section 8	S	Curve C
RAT	N/A	N/A	By analysis
Windmilling	N/A	N/A	Use DO-160G sine sweep to show compliance
Explosive Atmosphere	Section 9	N/A	Not Required
Waterproofness	Section 10	W	
Fluids Susceptibility	Section 11	F	Test Fluids Classes: Cleaning Fluids, Disinfectant, Fire Extinguishing Agent.
Sand and Dust	Section 12	N/A	Not Required
Fungus Resistance	Section 13	F	
Salt Spray	Section 14		
Icing	Section 24	N/A	Not Required
Max and Min Voltage at Temp	N/A	N/A	20 VDC @ -15°C, 32.2 VDC @ +70°C
Power on at -50°C	N/A	N/A	

Figure 3 – Environmental Test Performance

Electrical / EMI Condition	DO-160G Section	Test Category	Requirements/Comments
Magnetic Effect	Section 15	A	
Power Input	Section 16	ZXI	All equipment shall withstand momentary losses of power as follows: • For interruption over time periods ranging from 0 to 50 ms: no resulting degradation of performance; particularly microprocessor based equipment will continue their computation cycles with no effect on input acquisitions and output emissions. • For interruption over time periods ranging from 50 to 150 ms: degradations of performance are acceptable and the equipment shall return to the previous operating mode without external action within 5 s (warm start). • For interruption over time periods ranging from 150 to 250 ms: degradations of performance are acceptable and the equipment shall return to a pre-defined operating mode without external action within 1 min (cold start).
Voltage Spikes	Section 17	A	
Audio Frequency Susceptibility	Section 18	Z	
Induced Signal Susceptibility	Section 19	AW	Note: Electric Fields into Equipment not applicable to the Antenna LRU
RF Susceptibility Radiated & Conducted	Section 20	RR	
RF Emissions Radiated	Section 21	P or Q	The test shows noncompliance for CAT P or Q, then CAT M shall be acceptable
RF Emissions Conducted	Section 21	P or Q	
Lightning Induced Susceptibility	Section 22	A2E2XX	Cable bundle single and multiple stroke test (XXE3XX or XXG3XX or XXJ3XX) is considered representative enough to predict the equipment behavior under Pin test level 2 (A2XXXX).

Lightning Direct Effects	Section 23	N/A	Not Required
Electrostatic Discharge (ESD)	Section 25	A	
X Radiation	N/A	N/A	By analysis

Figure 4 – Electrical/EMI Test Performance

2.9 CL6 Wiring Configuration

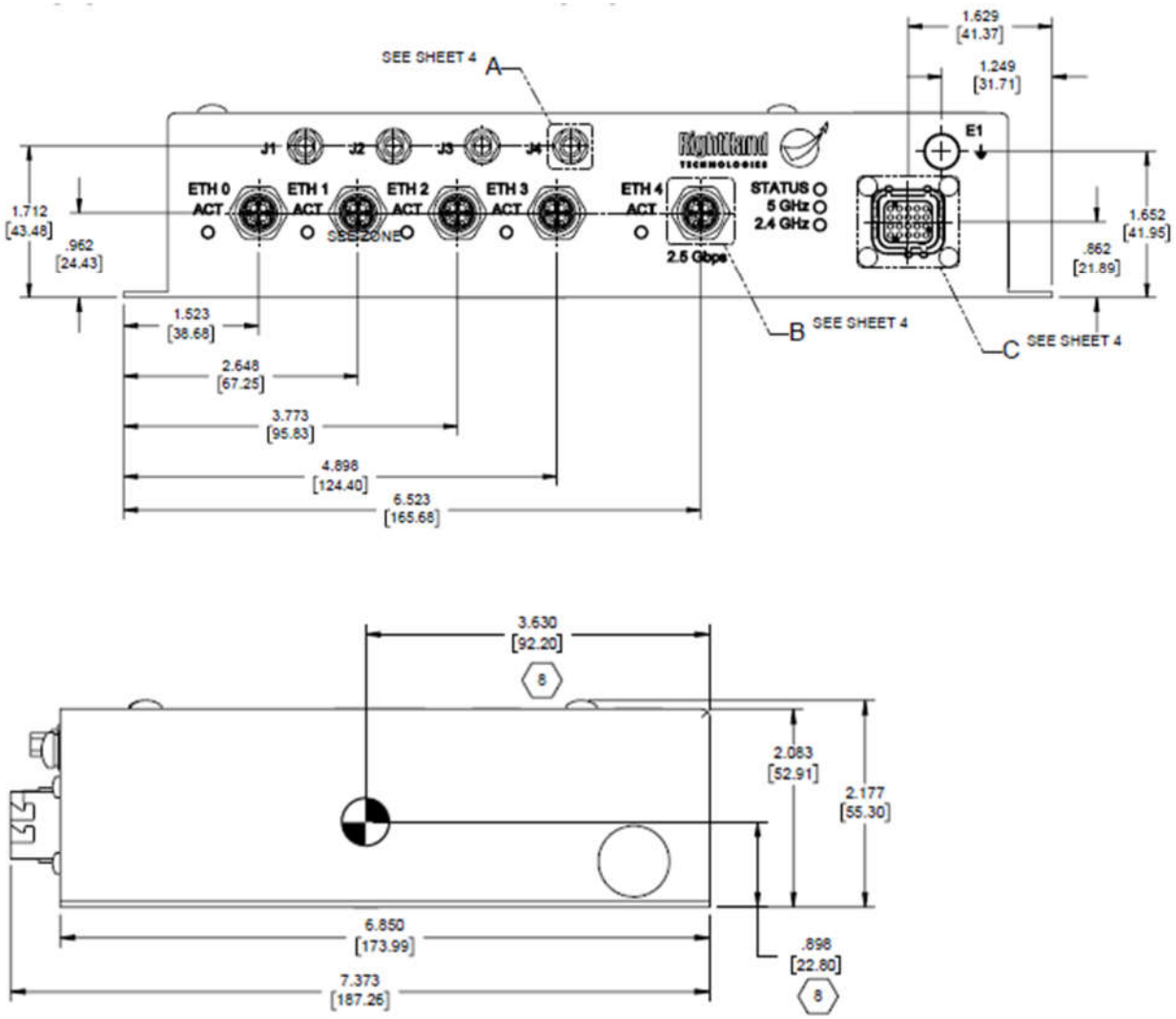
The CL6 has the following ports on the face.

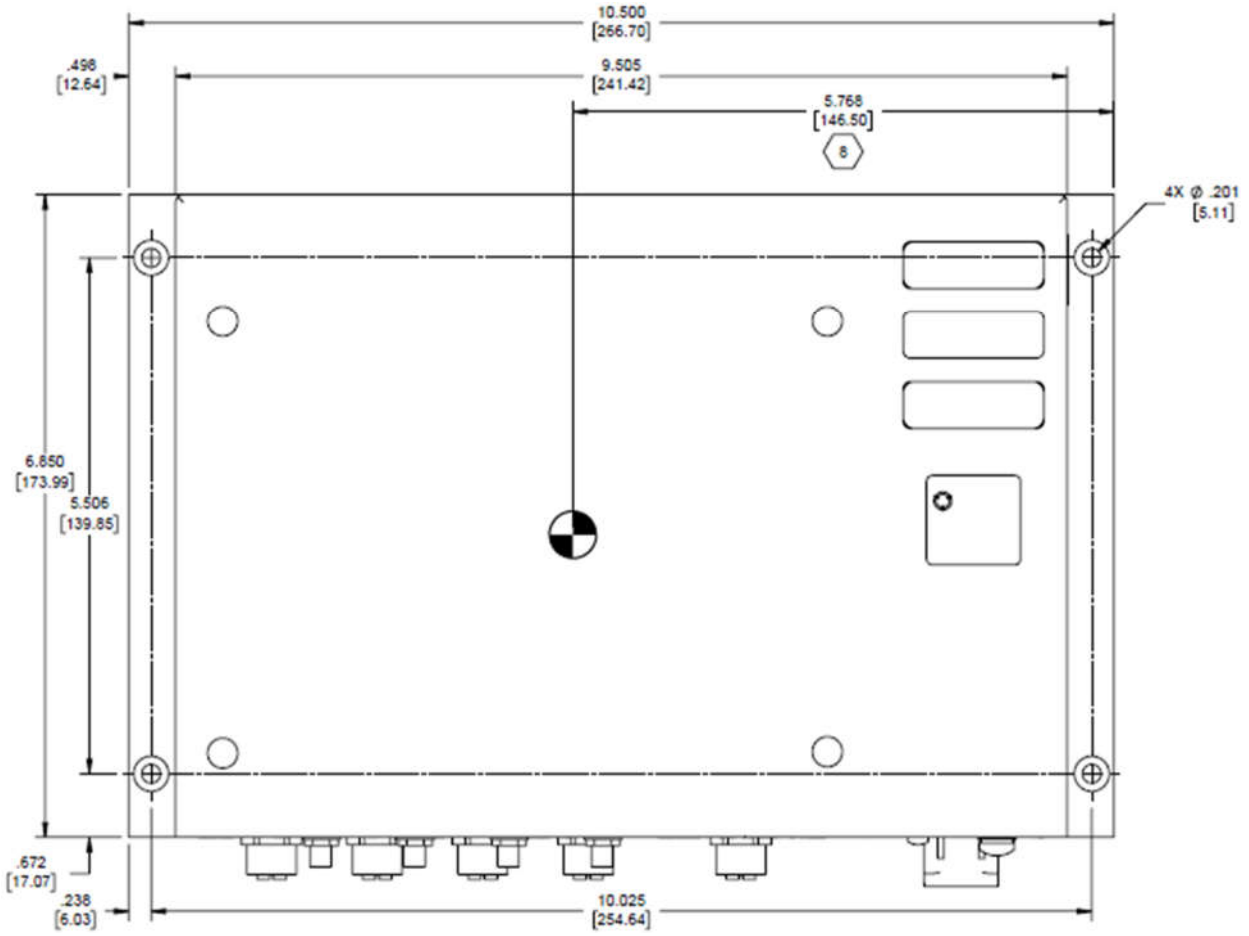
Figure 5 - CL6 Ports

J1 to J4	SMA connectors to the Antenna ports
ETH0 to ETH3	10/100/1000 Ethernet ports
ETH4	2.5G Ethernet port
J5	Connector for 28DC Power, Ground and Discreet inputs and outputs
E1	Ground wire

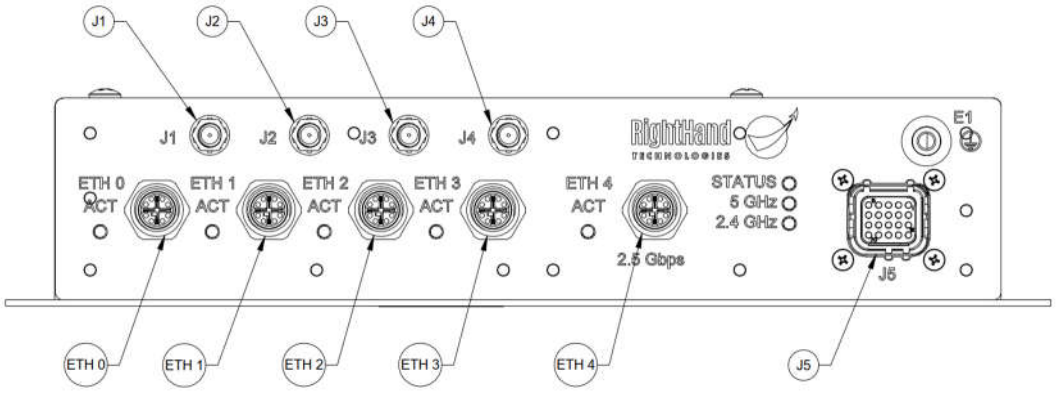
2.10 CL6 Installation

General




10.500
[266.70]
.496
[12.64]
9.505
[241.42]
5.768
[146.50]
B
4X Ø .201
[5.11]
6.850
[173.99]
5.506
[139.85]
.672
[17.07]
.238
[6.03]
10.025
[254.64]

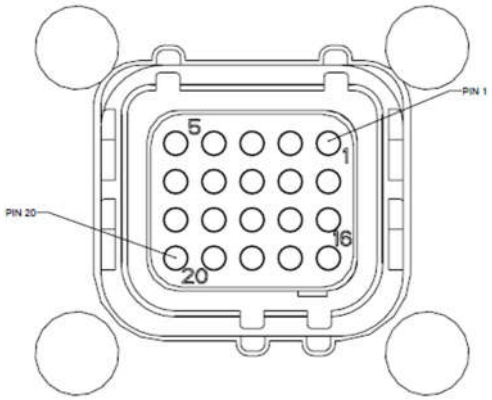
Connector Information



CONNECTOR	CONNECTOR OR EQUIVALENT	GENDER	LOCKING MECHANISM	MATING CONNECTOR OR EQUIVALENT
J1	SMA	FEMALE	Mating SMA connectors assembled using HUBER+SUHNER TORQUE WRENCH SMA/PC3.5 8MM (PN: 74_Z-0-0-21) which is factory calibrated with the required torque.	SMA PLUG
J2				
J3				
J4				
J5	TE CONNECTIVITY DMC-MD 24INS	FEMALE	Mating connector is equipped with self-locking mechanism.	TE CONNECTIVITY DMC-M 20-22 PN
E1	GROUND WIRE 16AWG	N/A	Use Screw #10-32 assembled using torque screwdriver (use 19 in.Lbs torque)	#10 RING TERMINAL
ETH0	AMPHENOL MSXS-08PFFR-SH7001	FEMALE	Mating connectors assembled using torque wrench (use 5.3 in.Lbs torque)	HARTING 21038811805
ETH1				
ETH2				
ETH3				
ETH4	AMPHENOL MSXS-08PFFR-SH7001	FEMALE	Mating connectors assembled using torque wrench (use 5.3 in.Lbs torque)	HARTING 21038811805

Figure 6 - Connection Information

CONNECTOR PINOUT – J5



PIN	SIGNAL NAME
1	PWR_EN
2	FACT_RESET
3	GND
4	DIS_IN_1
5	DIS_IN_2
6	GND
7	SPARE0
8	SPARE1
9	GND
10	GND
11	RS232 TX*
12	RS232 RX*
13	IP_STRAP_0
14	IP_STRAP_1
15	IP_STRAP_2
16	DIS_OUT_1
17	DIS_OUT_2
18	CHAS
19	+28V_RTN
20	+28V_IN
* FOR LAB/MAINTENANCE USE ONLY. NOT CONNECTED ON AIRCRAFT	

Figure 7 - J5 Connector Pin Configuration

See Figure 9 and Figure 10 for DO-160G tested cable specifications.

PIN	SIGNAL NAME	SIGNAL DESCRIPTION	Direction	GROUND	OPEN	Standard
1	PWR_EN	Power Enable	Input	Power ON	Power Off	ARINC 763A Sections 2.10.6, 6.4.1
2	FACT_RESET*	Factory Reset	Input	Reset CL6	CL6 normal operation	ARINC 763A Sections 2.10.6, 6.4.1
3	GND	Ground				
4	DIS_IN_1	2.4GHz RF Enable/Disable	Input	2.4GHz Radios Enable	2.4GHz Radios Disable	ARINC 763A Sections 2.10.6, 6.4.1
5	DIS_IN_2	5GHz RF Enable/Disable	Input	5GHz Radios Enable	5GHz Radios Disable	ARINC 763A Sections 2.10.6, 6.4.1
6	GND	Ground		-	-	-
7	SPARE0	Spare0/Test line	Input	-	-	-
8	SPARE1	Spare1/Test line	Input	-	-	-
9	GND	Ground		-	-	-
10	GND	Ground		-	-	-
11	RS232 TX**	Console Serial Port		-	-	-
12	RS232 RX**	Console Serial Port		-	-	-
13	IP_STRAP_0	IP Strap 0	Input	1 See Section 2.7	0 See Section 2.7	ARINC 763A Sections 2.10.6, 6.4.1
14	IP_STRAP_1	IP Strap 1	Input	1 See Section 2.7	0 See Section 2.7	ARINC 763A Sections 2.10.6, 6.4.1
15	IP_STRAP_2	IP Strap 2	Input	1	0	

				See Section 2.7	See Section 2.7	ARINC 763A Sections 2.10.6, 6.4.1
16	DIS_OUT_1	Power state on	Output	Power ON	Power OFF	ARINC 763A Sections 2.10.7, 6.4.2
17	DIS_OUT_2	Wireless status 2.4 & 5 GHz on	Output	All Radios Operational	At least one radio not operational	ARINC 763A Sections 2.10.7, 6.4.2
18	CHAS	Chassis Ground	-	-	-	-
19	+28V_RTN	+28V Power Return	Return	-	-	-
20	+28V_IN	+28V Power Input	Input	-	-	-

* - The Factory Reset input should never be grounded unless a factory reset of the WAP is required

** FOR LAB/MAINTENANCE USE ONLY. NOT CONNECTED ON AIRCRAFT

Figure 8 - J5 Connector Pin Information

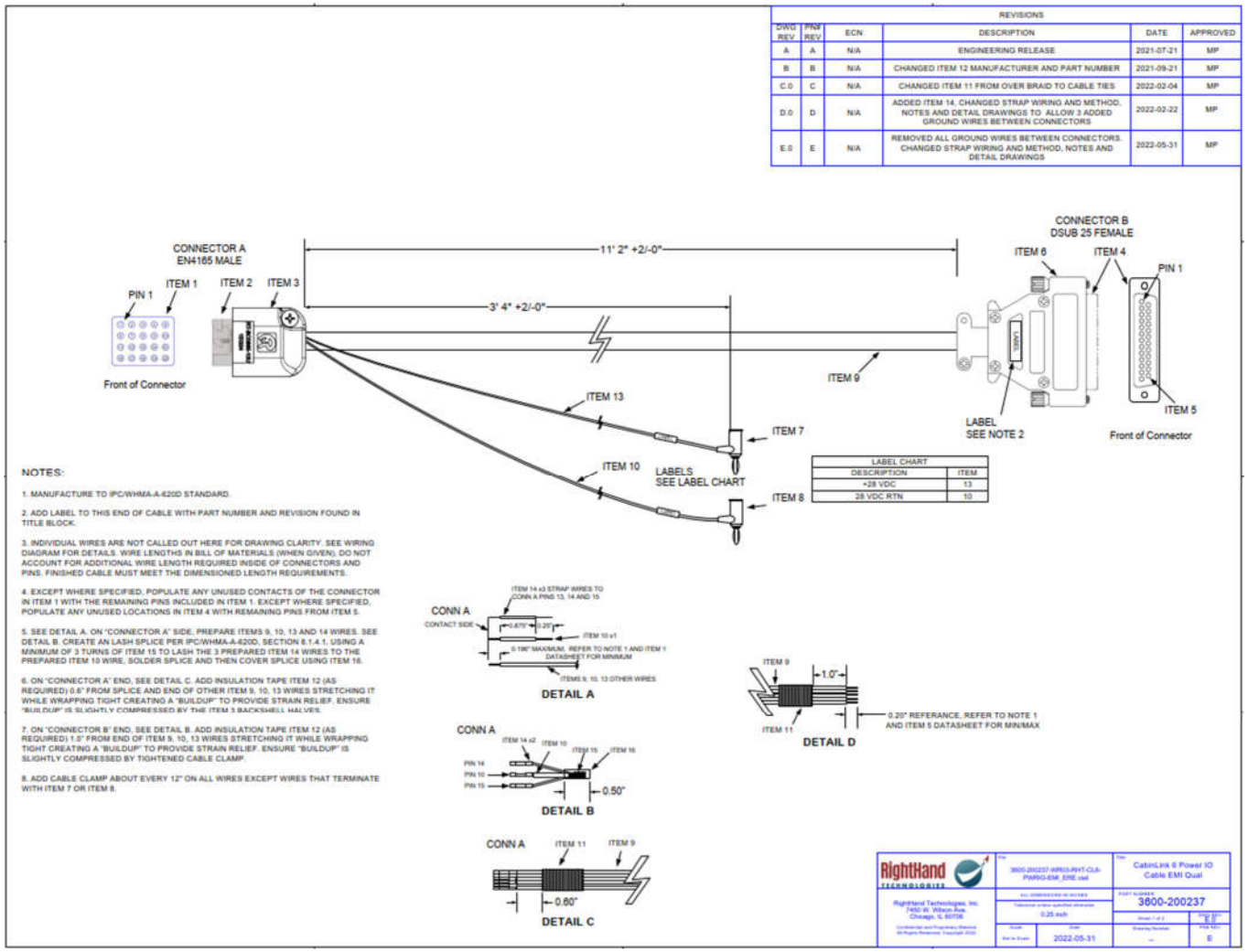
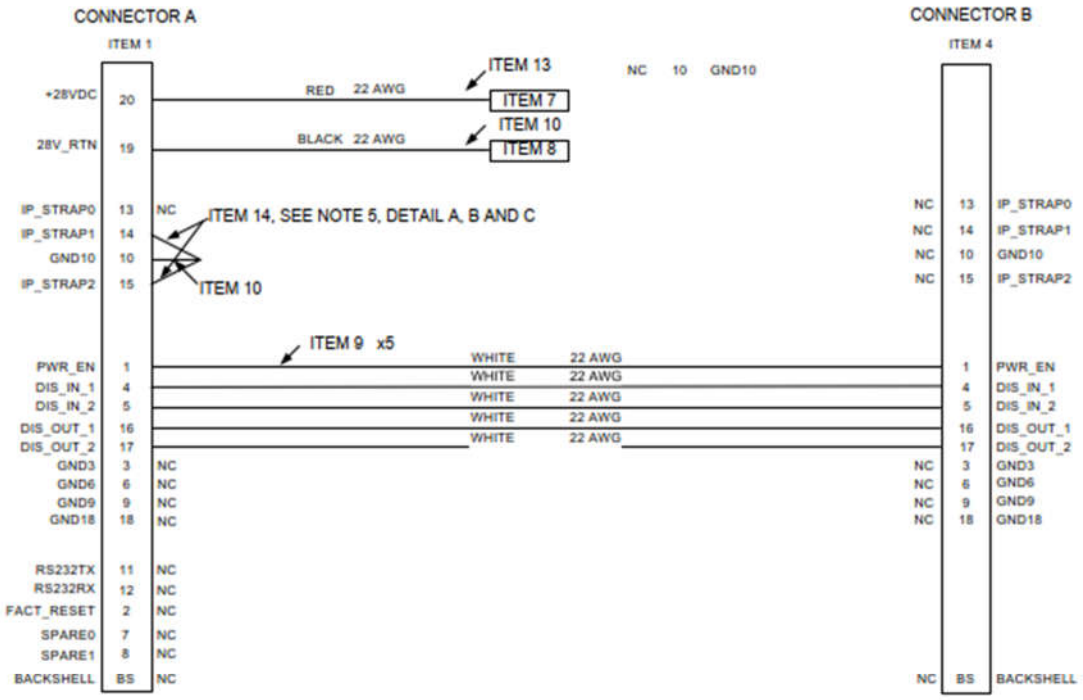


Figure 9 – DO-160-Tested Cable Specification for J5

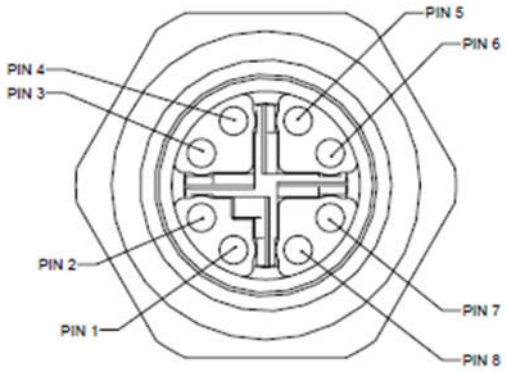


BILL OF MATERIALS

ITEM #	DESCRIPTION	MFG	PN / MIL#	QTY.
1	EN4165 20 POS CONN WITH 22 AWG MALE PIN CONTACTS	TE CONNECTIVITY	DMC-M 20-22 PN	1
2	EN4165 N KEY PLUG	TE CONNECTIVITY	DMC-MD 20 N	1
3	EN4165 EMI BACKSHELL	RUSSTECH ENGINEERING	RT-BC0865-10U	1
4	DSUB 25M STANDARD DENSITY FEMALE CONNECTOR	POSITRONICS	RD25S00000	1
5	DSUB FEMALE CONTACT PIN 22 AWG	POSITRONICS	FC6020D2	25
6	EMI HOOD DSUB SHELL WITH JACKSCREWS	POSITRONICS	D25000GE0	1
7	BANANA PLUG RED	POMONA ELECTRONICS	1825-2	1
8	BANANA PLUG BLACK	POMONA ELECTRONICS	1825-0	1
9	WIRE STRANDED 22 AWG PTFE WHITE		MIL 16878/4	AR
10	WIRE STRANDED 22 AWG PTFE BLACK		MIL 16878/4	AR
11	CABLE TIE, NYLON, NATURAL, 3.9 INCH, ROHS COMPLIANT	PANDUIT	PLT1M	10
12	LOW DUROMETER SELF FUSING SILICONE TAPE 0.020 x 0.5" x 36 FT	ROWE INDUSTRIES	GL20B67100	AR
13	WIRE STRANDED 22 AWG PTFE RED		MIL 16878/4	AR
14	WIRE STRANDED 24 AWG PTFE BLACK		MIL 16878/4BEE	AR
15	BUSS BAR WIRE 26 AWG	ALPHA	299/1 SV005	AR
16	HEATSHRINK, 3:1, 1/8"	QUALTEK	Q2-F3X-1/8-01	0.5"

Figure 10 - DO-160-Tested Cable Specification for J5

CONNECTOR PINOUT – ETH0, ETH1, ETH2, ETH3, ETH4



PIN	SIGNAL NAME
1	ETH n BI_DA +
2	ETH n BI_DA -
3	ETH n BI_DB +
4	ETH n BI_DB -
5	ETH n BI_DD +
6	ETH n BI_DD -
7	ETH n BI_DC -
8	ETH n BI_DC +

Figure 11 - J5 Connector Pin Configuration

See Figure 12 for DO-160G tested cable specification.

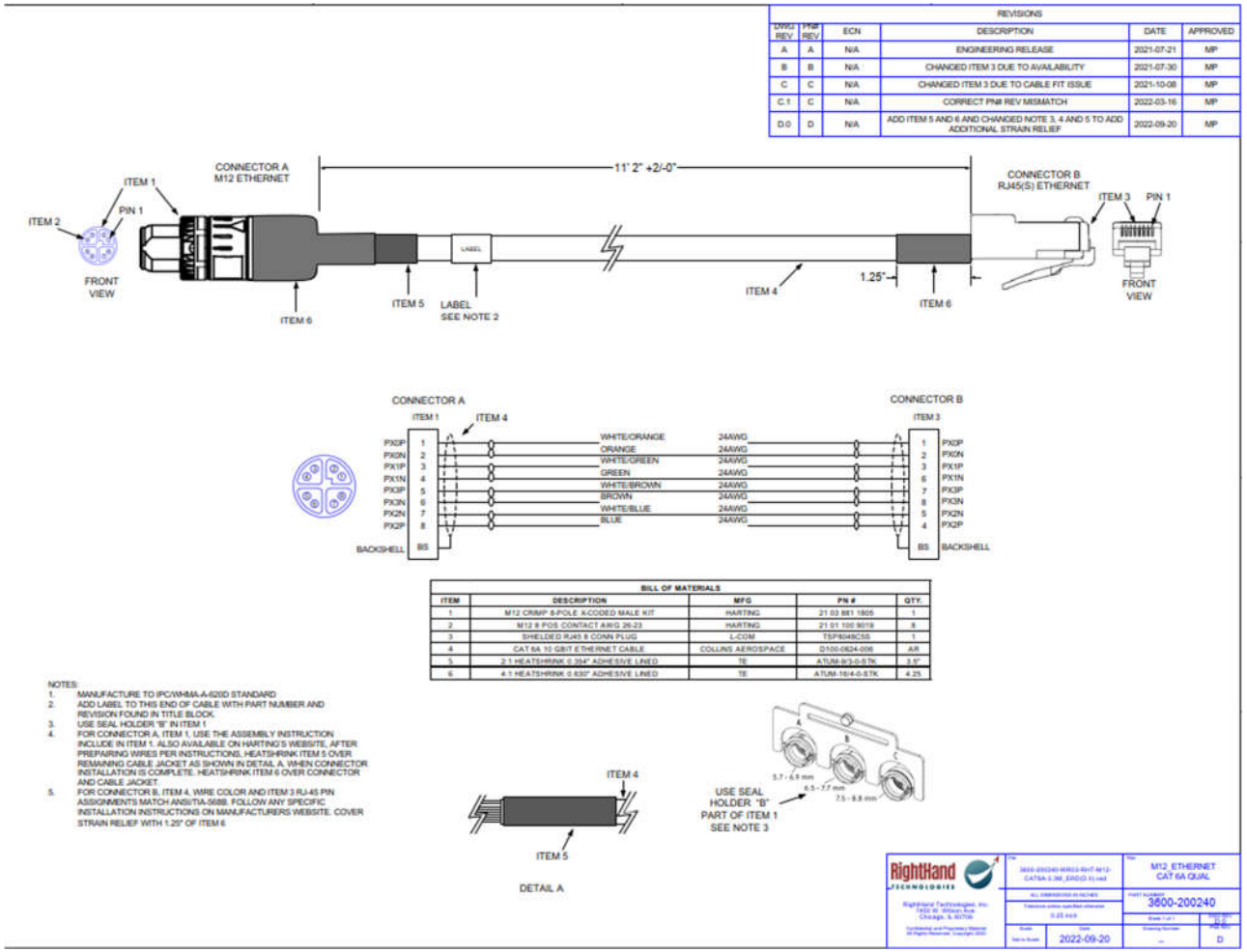


Figure 12 - DO-160-Tested Cable Specification for ETH0 thru ETH4

Ground Connection Information

Install ground wire with a #10 ring terminal to the ground point, E1 with the following

- Screw, #10-32, 0.5 inch, Phillips, Pan Head (RHT 3200-200112 or equivalent)
- Split Lock Washer, Mil. Spec, #10 (RHT 3200-200115 or equivalent)
- External-Tooth Lock Washer, #10 (RHT 3200-200114 or equivalent)

See Figure 13 for DO-160G tested cable specification.

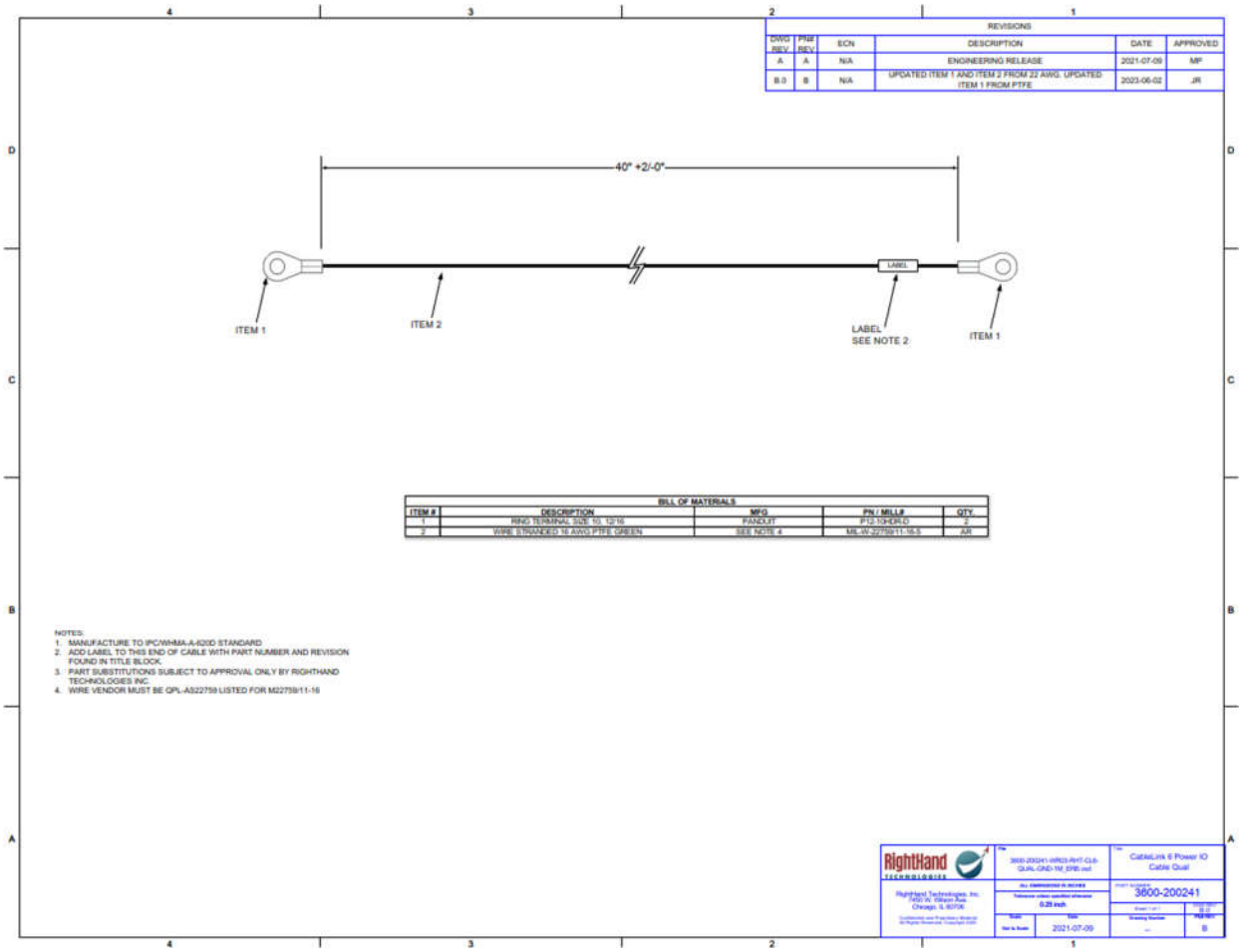


Figure 13 - DO-160-Tested Cable Specification for ground wire

2.11 Antenna and Cable Information

Collins 441-2199-100 (RightHand Tech 1024-200049) Antenna Information	
Antenna Type	4-Element Omni-directional
Connector	SMA Female Socket
Maximum Gain in 2.4GHz	3.6dBi
Maximum Gain in 5GHz	5.75dBi

Figure 14 – Antenna Information

Cable Information	
Minimum Cable Length	4''
Maximum Cable Length	Per Maximum Cable Loss
Maximum Cable Loss	9 dB
Allowable Antenna Type	To be used only with: Collins 441-2199-100 (RightHand Tech 1024-200049)
Maximum Cable Loss Difference	Any Note: All regulatory and performance testing performed with cables with a maximum of 0.5 dB of cable loss difference.

Figure 15 – Cable Information

2.12 LED Port Indicators

Each port has an LED indicator to the left of the port. The blinking pattern of the LEDs is defined in the table below.

ETH0 to ETH3 – 10/100/100 Ethernet port
LEDs OFF – no link
Green LED ON – 1 Gbps link
Yellow LED ON – 10/100 Mbps link
LED BLINKING – activity
ETH4 – 2.5G Ethernet port
LEDs OFF – no link
Green LED ON – 2.5/1 Gbps link
Yellow LED ON – 10/100 Mbps link
LED BLINKING – activity
Power Status LED
LEDs OFF – power off
Green LED ON – power on/operational
Yellow LED ON – power on/booting
5 GHz Radio LED
Green LED ON: 5 GHz radio is up/operational
Yellow LED ON: 5 GHz radio is down/off
LEDs OFF: 5 GHz radio is off/not fully booted.
2.4 GHz Radio LED
Green LED ON: 2.4 GHz radio is up/operational
Yellow LED ON: 2.4 GHz radio is down/off
LEDs OFF: 2.4 GHz radio is off/not fully booted.

Figure 16 - LED Port Indicators

3. Configuring the CabinLink 6 - Quick Start Guide

The CL6 can be configured to operate in several network modes. It can operate as a router, access point, and range extender. The CL6 may act as just a wireless access point to provide wireless access to the cabin system. It can also act as a router between the cabin system and another external network (such as internet connectivity through a Satcom system). It can also act as a range extender to repeat the wireless signal from a router to expand its networks coverage.

Multiple LRU configurations allow for mesh operation, which allows for better wireless coverage with multiple connectivity points in a cabin environment. If one of the non-primary LRUs goes offline, wireless clients seamlessly connect to other LRUs in the mesh. Clients seamlessly switch and authenticate between LRUs depending on which LRU gives them the best signal.

The CL6 can be configured to operate in these modes via the GUI (see CabinLink 6 GUI Configuration) or through command line. See 10 for using SSH connections to access the command line interface.

These wireless configurations are kept in configuration files that can be copied, uploaded, and downloaded through the Configuration Management page in the GUI (see System – Configuration Management).

Below are six use cases for the CL6. These use cases include operating as an Access Point, Wireless Router, Multiple Wireless Access Points, Multiple Routers with VLAN support, Access Point with Range Extender/Wireless Mesh, and Multiple Wireless Access Points with Load Balancing.

Use Case	**Corresponding configuration files**
Access Point	uc1_example_AP
Wireless Router	uc2_example_RTR
Multiple Wireless Access Points	uc3_example_multiAP_qos_1 uc3_example_multiAP_qos_2
Multiple Routers with VLAN support	uc4_example_multiRTR_VLAN4 uc4_example_multiRTR_VLAN5
Access Point with Range Extender/Wireless Mesh	uc5_example_multiAP_wds_master uc5_example_multiAP_wds_re
Multiple Wireless Access Points with Load Balancing	uc6_example_multiWAP_lb_primary uc6_example_multiWAP_lb_secondary

3.1 CL6 Access Point Configuration

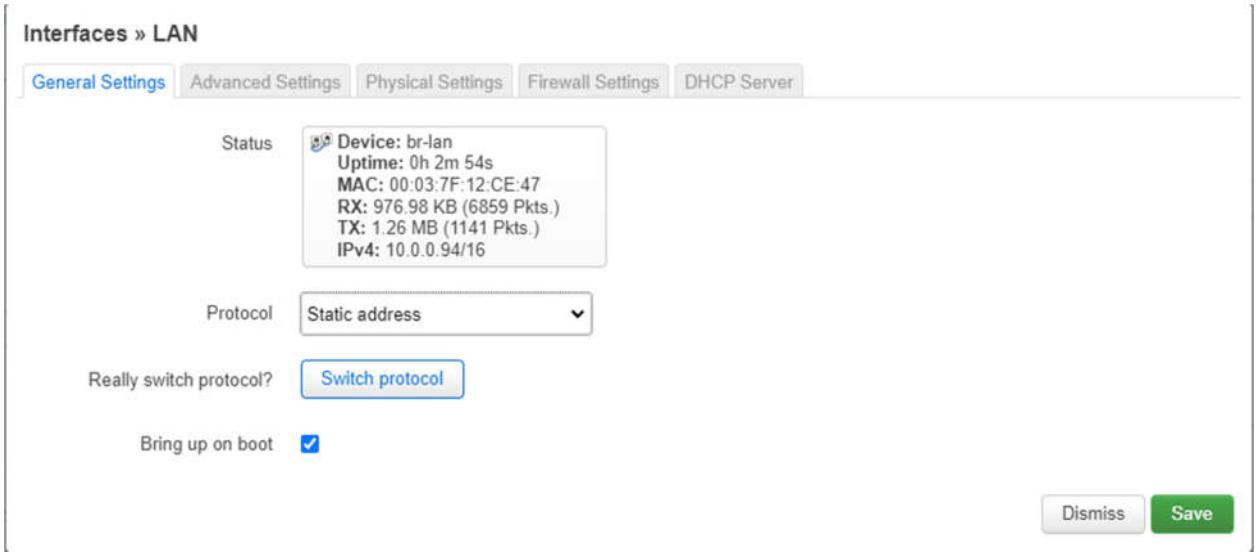
In this case, a third-party router is responsible for network setup, with the wireless access point acting as an access point only (layer two functions only). The wireless access point is connected to the third-party router via a Gigabit-Ethernet link (GE) to any of its LAN ports and serves wireless clients over WiFi.

To use this configuration, start by connecting the IP address straps to ground (See Setting IP Address with Switches). This will allow the CL6 to get an IP address via DHCP. Navigate to System → Configuration Management and select uc1_example_AP from the Current Configuration dropdown. After doing so, click the "Set as Current Config" button and then click the "Apply Current Config to System" button. Wait about 1 minute for configuration to apply to the wireless access point and then reboot the unit. You may lose connection to the GUI since the CL6 will get an IP via DHCP from the third-party router. The IP address of the CabinLink 6 can be determined by issuing the "arp -a" command on a computer connected to the DHCP enabled network. The CabinLink 6 will have a MAC address starting with '00:1A:9C:14'

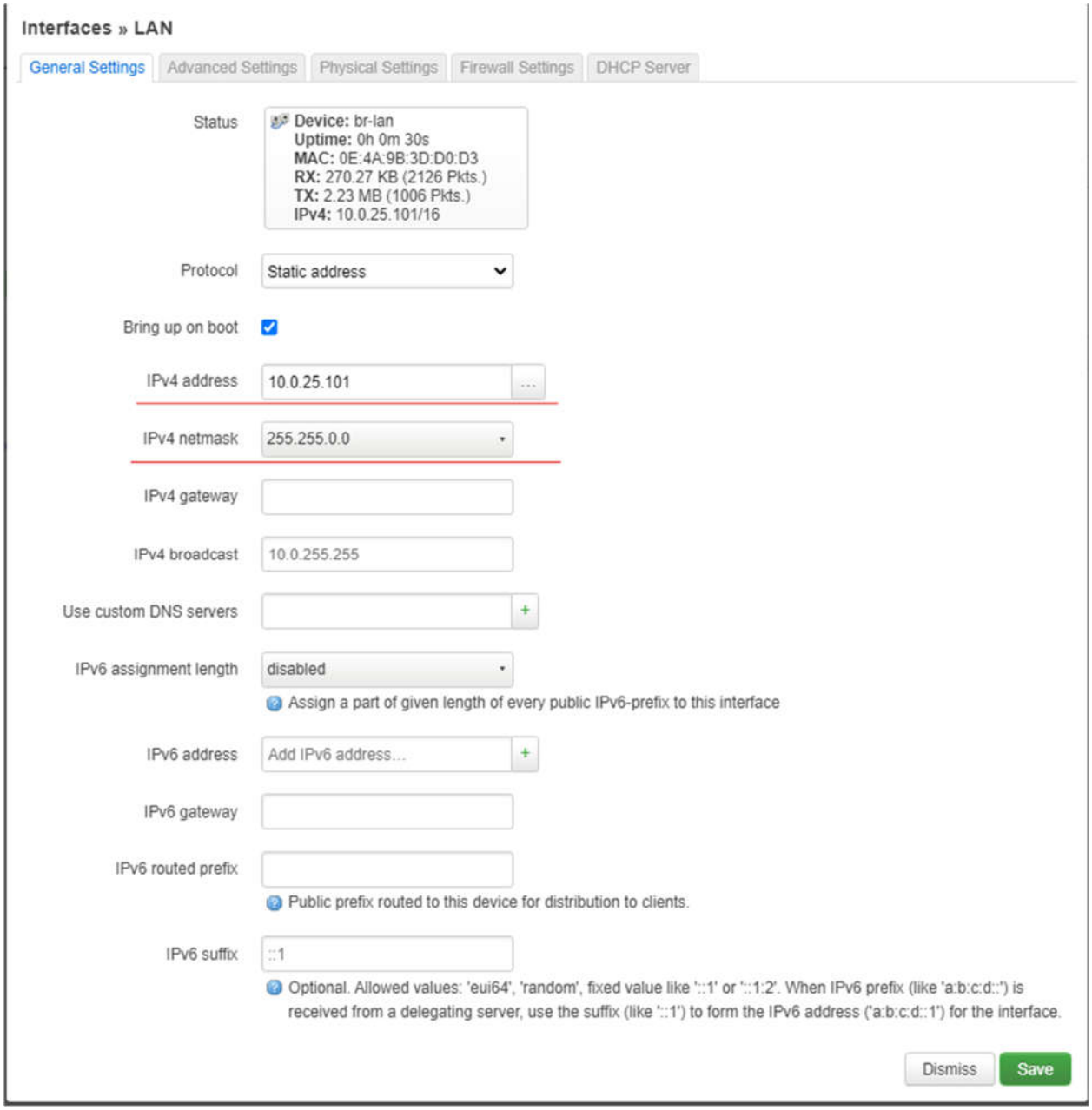
3.1.1 CL6 Access Point Configuration – Changing the IP address

The wireless access point can also be configured to use a static address. To do so, disconnect the IP address straps to allow the IP address to be set from the configuration file (See Setting IP Address with Switches). Next, navigate to Network → Interfaces and click "Edit" on the LAN interface.

Next, select static address from the Protocol dropdown and click the "Switch Protocol" button.



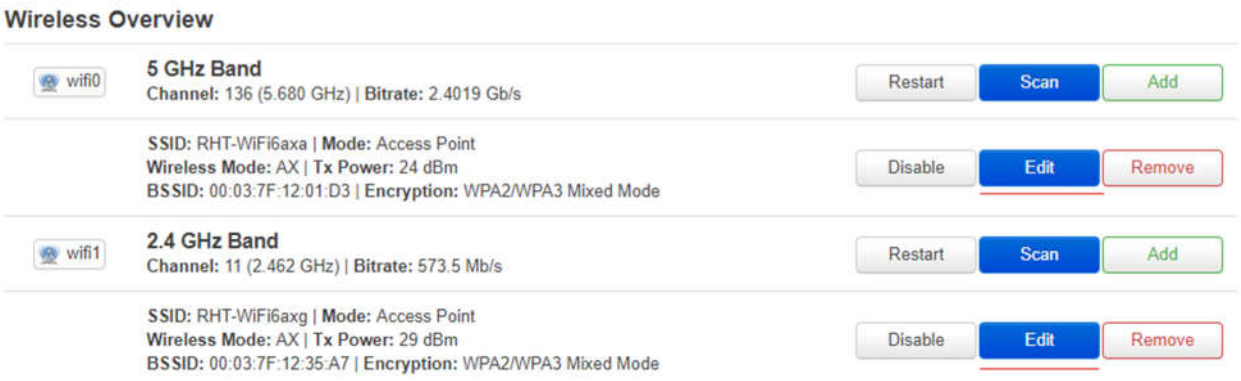
You will need to fill in the IPv4 address and IPv4 netmask fields. You must use an unused IP address compatible with the router's subnet and outside of its DHCP pool to avoid conflicts.



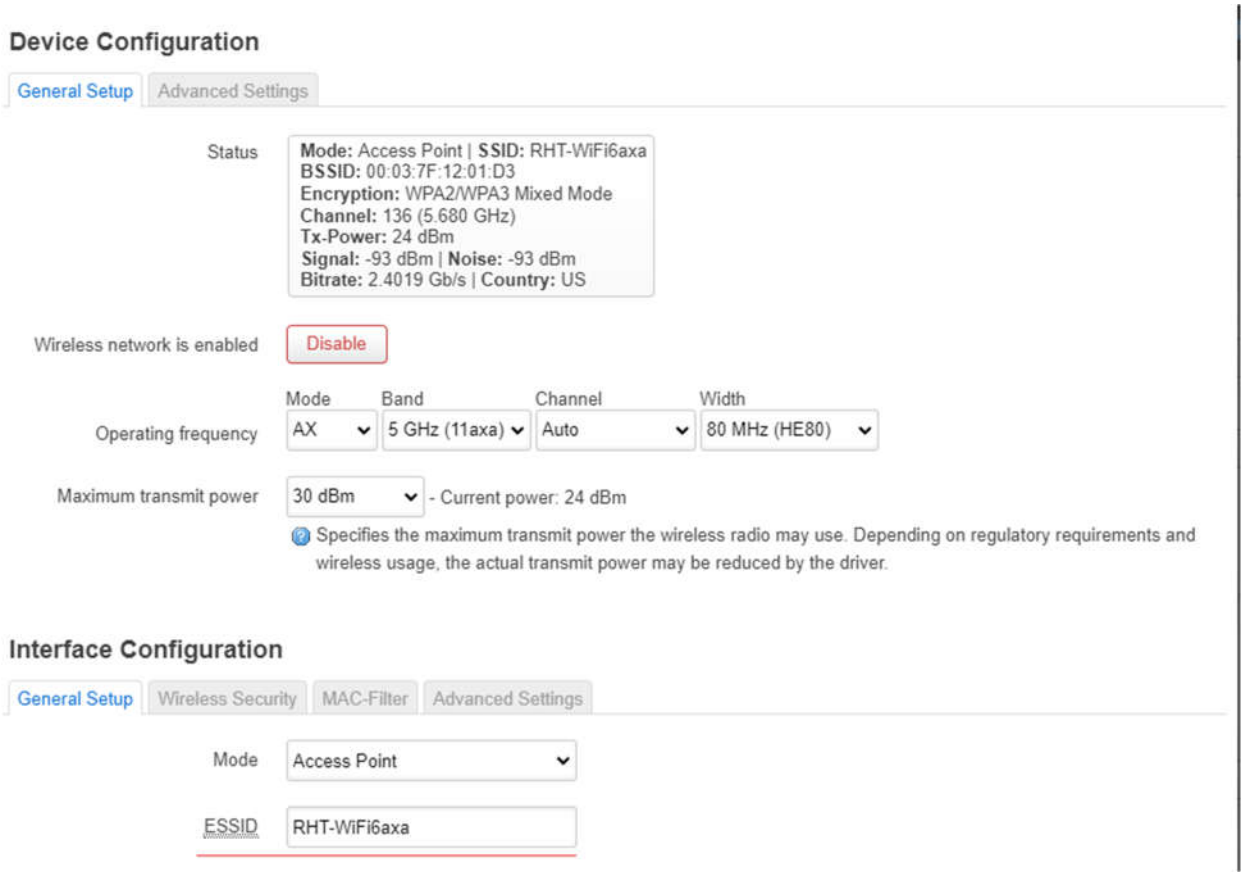
After these fields are populated, Save and apply your changes. With the IP address straps disconnected (See Setting IP Address with Switches), the wireless access point will now use the IP address you provided. Information on how to configure the rest of the settings on this page can be found in 8.1.

3.1.2 CL6 Access Point Configuration – Changing the SSID

To change the SSID for the network, start by navigating to Network → Wireless.



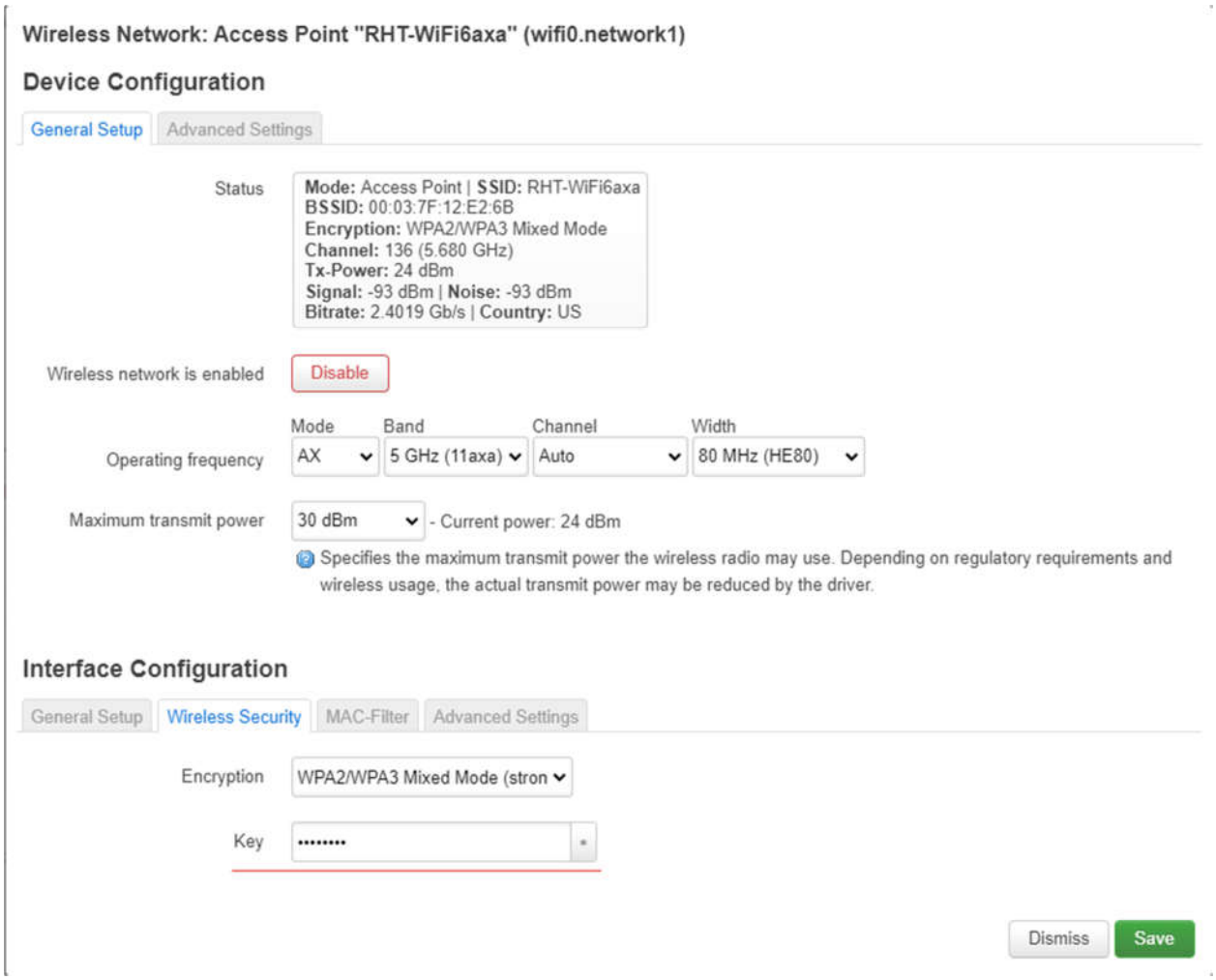
From this page, click edit on the wireless interface you want to change the SSID for.



Then, change the ESSID field to your desired SSID and save & apply your change. Each wireless interface can have their own unique SSID, or they can also share the same SSID. The maximum allowed number of SSIDs per radio is 16.

3.1.3 CL6 Access Point Configuration – Changing the Wi-Fi Password

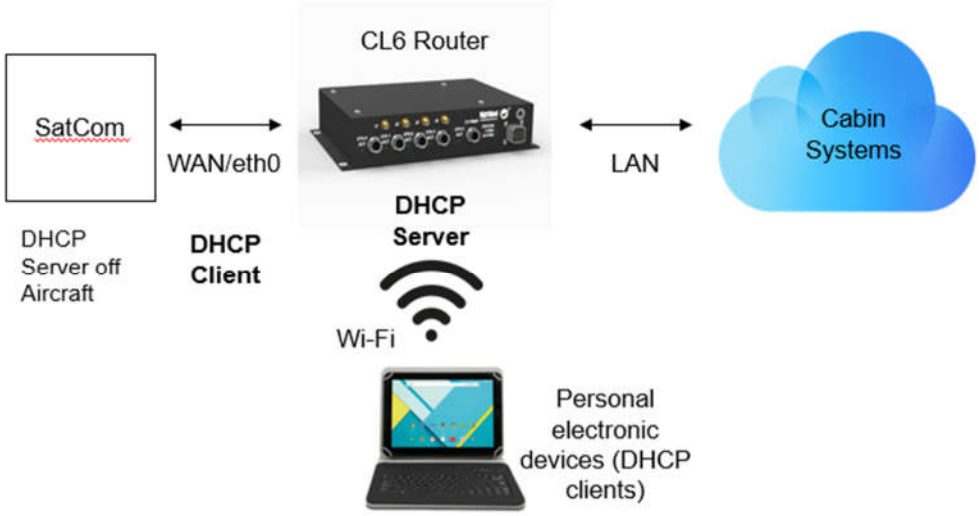
To change the password for your WiFi, click the wireless security tab on the same page.



Changing the value in the "Key" field will change the password for your WiFi. You can also change the wireless encryption type from this page by selecting an encryption type from the "Encryption" dropdown. Information on how to configure the rest of the settings on this page can be found in 8.2.

3.2 CL6 Wireless Router Configuration

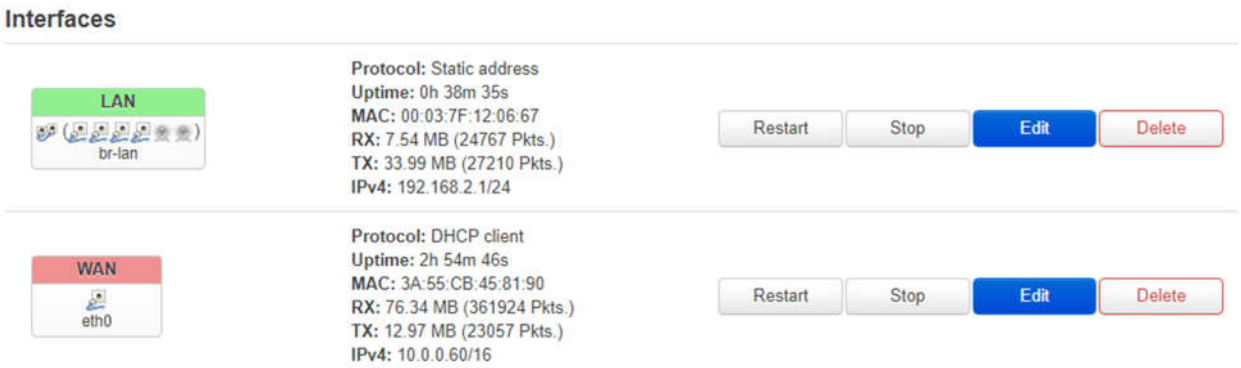
In this case, the CL6 acts as a layer three router. The ETH0 interface is configured as the WAN port and connects to the aircraft satellite/internet provider's system. In this example the WAN is configured as a DHCP client. ETH1 through ETH4 and the wireless interfaces are bridged as the virtual interface br-lan and share a static IP address assignment. The CL6 acts as a DHCP server on the br-lan interface.



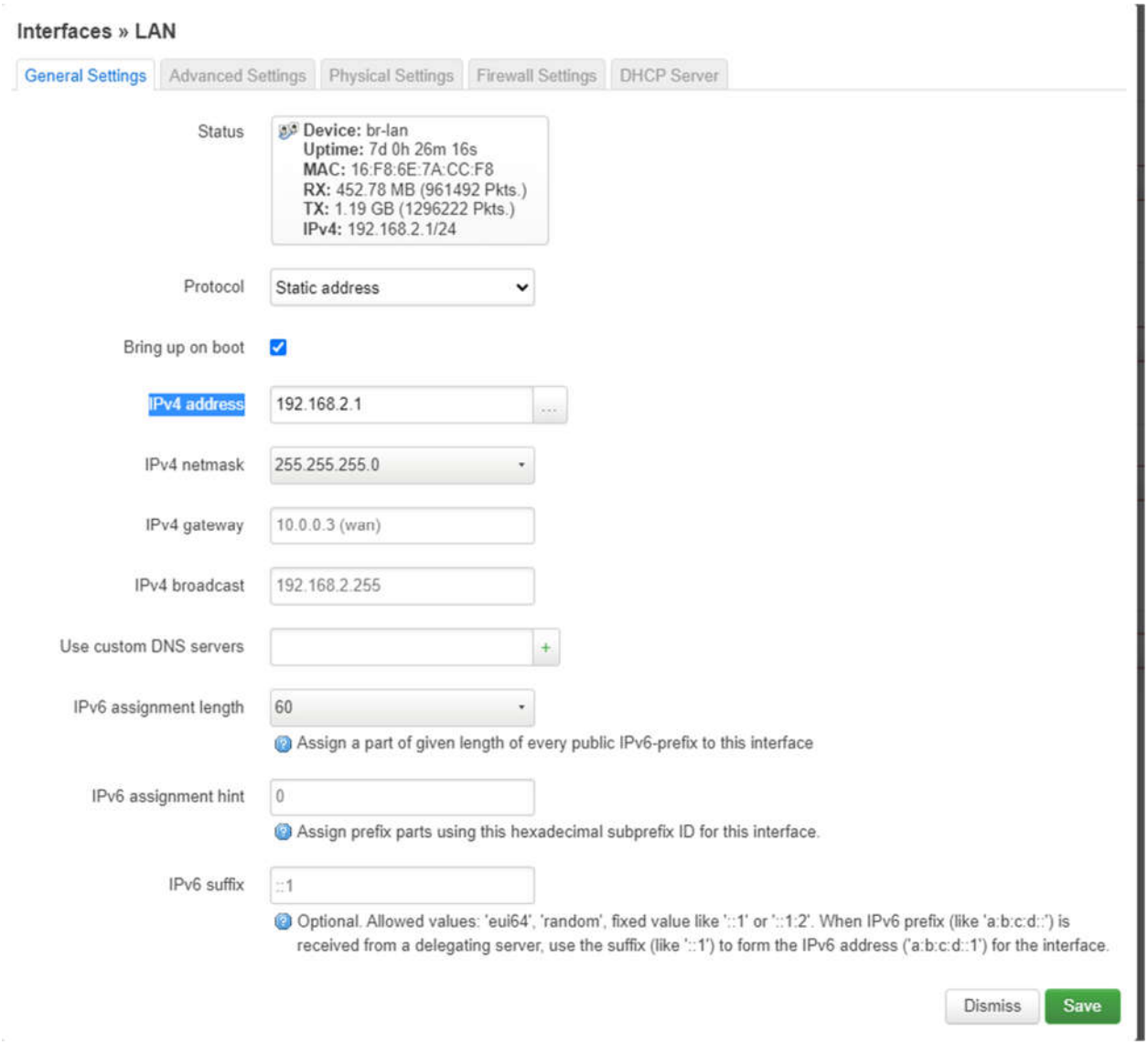
To use this configuration, disconnect the IP address straps to allow the IP address to be set from the configuration file (See Setting IP Address with Switches). Navigate to System → Configuration Management and select uc2_example_RTR from the Current Configuration dropdown. After doing so, click the "Set as Current Config" button and then click the "Apply Current Config to System" button. Wait about 1 minute for configuration to apply to the CL6 and then reboot the unit. The IP address will change to 192.168.2.1, enter this into a browser search bar to access the GUI.

3.2.1 CL6 Wireless Router Configuration – Changing LAN IP address

To change the IP address of the Access Point, navigate to Network → Interfaces and click edit on the LAN interface.



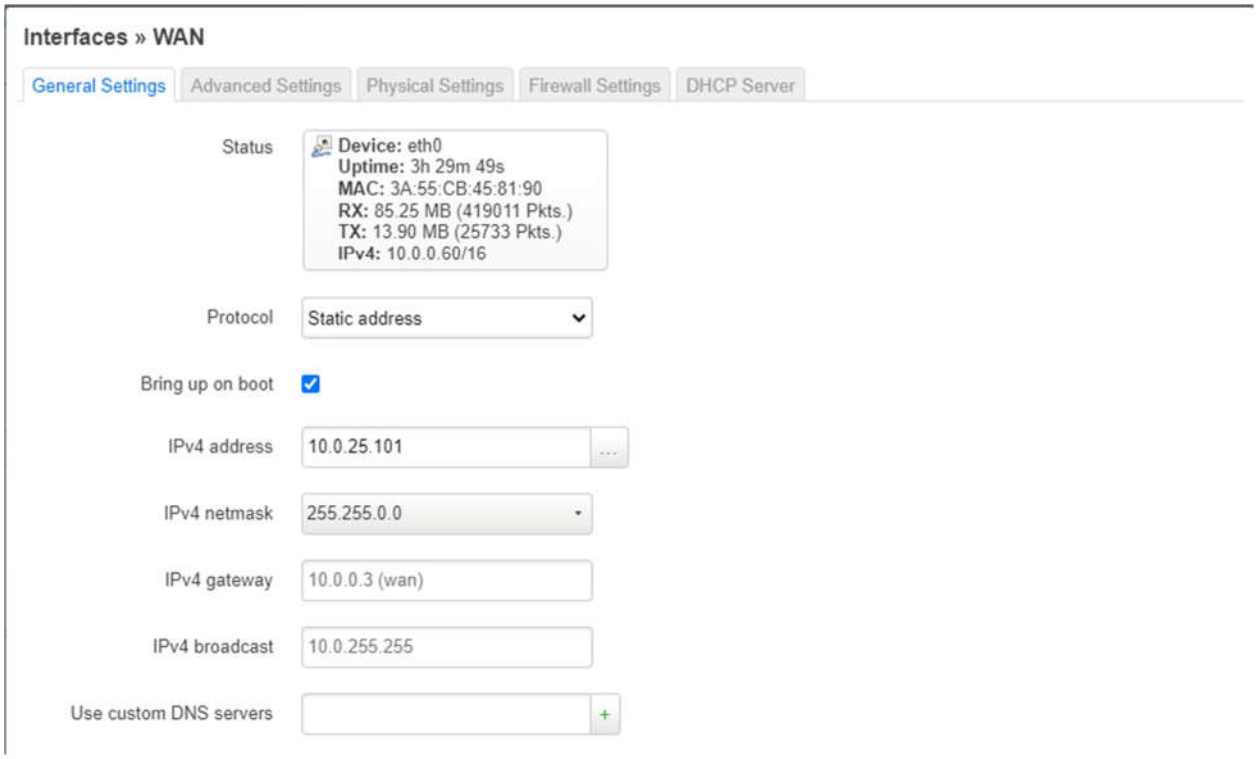
Under the General Settings tab, change the IPv4 address field to the desired IP address for the Access Point and click Save.



Information on how to configure the rest of the settings on this page can be found in 8.1.

3.2.2 CL6 Wireless Router Configuration – Assigning WAN a static IP address

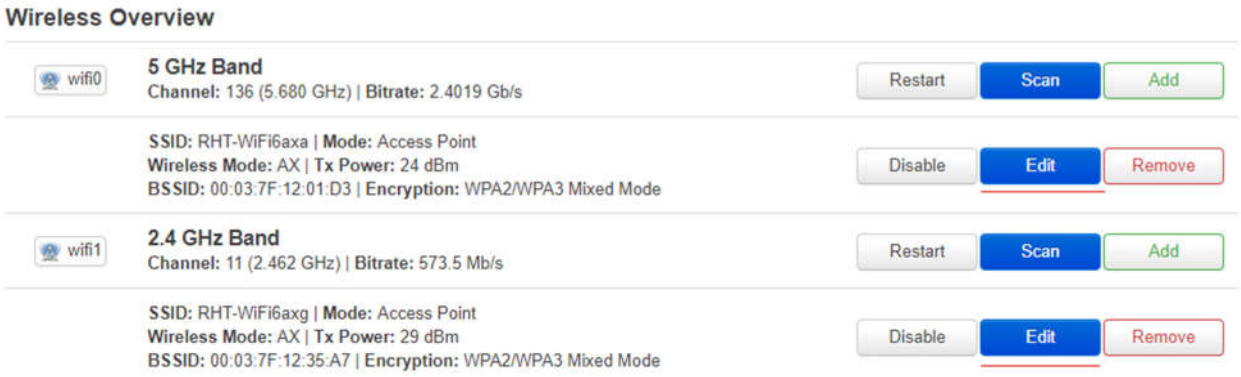
The WAN interface is configured as a DHCP client and gets its IP address from the DHCP server connected to ETH0. If you want to configure the WAN interface with a static IP address, navigate to Network → Interfaces and click edit on the WAN interface. Next, select static address from the Protocol dropdown and click the "Switch Protocol" button.



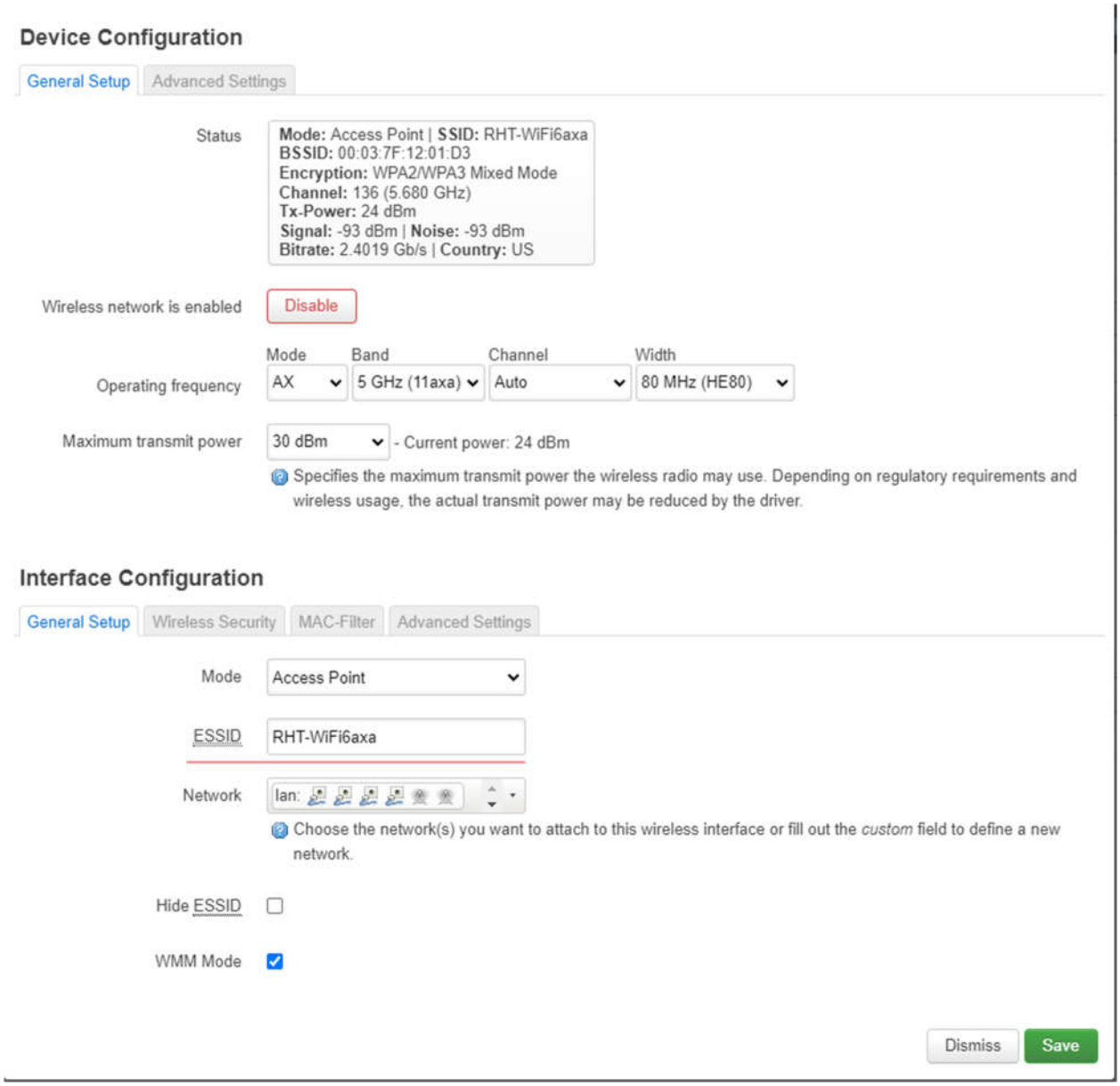
Configure the IPv4 address and IPv4 Netmask. It is recommended to use a valid, unused, IP address outside of the DHCP pool of the connected DHCP server to avoid address conflicts. After those fields are configured, click "Save & Apply". The WAN interface will now use its configured IP address.

3.2.3 CL6 Wireless Router Configuration – Changing the SSID

To change the SSID for the network, start by navigating to Network → Wireless.



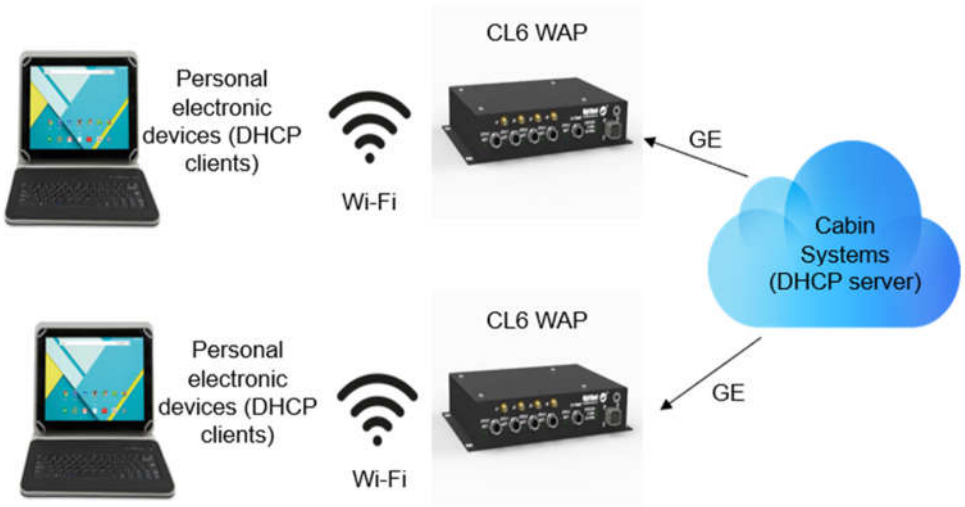
From this page, click edit on the wireless interface you want to change the SSID for.



Then, change the ESSID field to your desired SSID and save & apply your change. Each wireless interface can have their own unique SSID, or they can also share the same SSID. The maximum allowed number of SSIDs per radio is 16. Information on how to configure the rest of the settings on this page can be found in 8.2.

3.3 CL6 Multiple Wireless Access Points Configuration

In this case, there are multiple CL6's in the system. The CL6's act as access points (with layer two functions only).



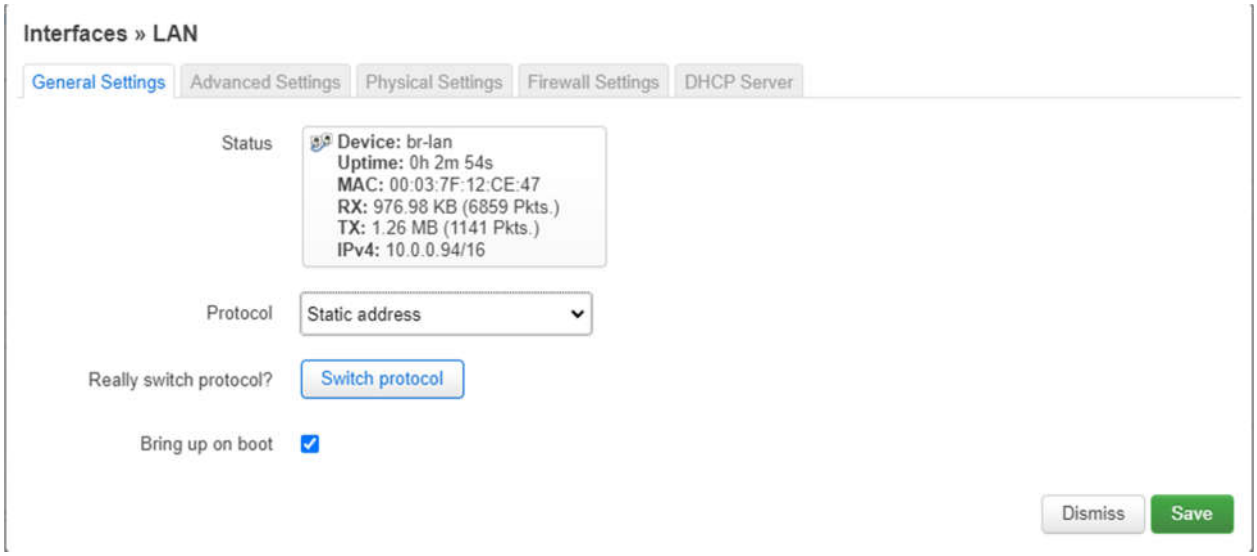
To use this configuration, navigate to System → Configuration Management on one of your CL6's and select "uc3_example_multiAP_qos_1" from the Current Configuration dropdown. After doing so, click the "Set as Current Config" button and then click the "Apply Current Config to System" button. Wait about 1 minute for configuration to apply to the CL6 and then reboot the unit. On the other CL6, navigate to System → Configuration Management and select "uc3_example_multiAP_qos_2" from the Current Configuration dropdown and follow the same procedure to apply the configuration. Both CL6's will receive an IP address through DHCP if the IP address straps are open/disconnected (i.e. use the configuration file) or all straps are asserted/grounded to force DHCP. The IP address of the each CabinLink 6 can be determined by issuing the "arp -a" command on a computer connected to the DHCP enabled network. The CabinLink 6's will have a MAC address starting with '00:1A:9C:14'

In this configuration, a WAN interface is not configured. Instead, ETH0 is added to the LAN port configuration. Neither of the CL6's run a DHCP server in this configuration. Instead, the DHCP service comes from the cabin systems.

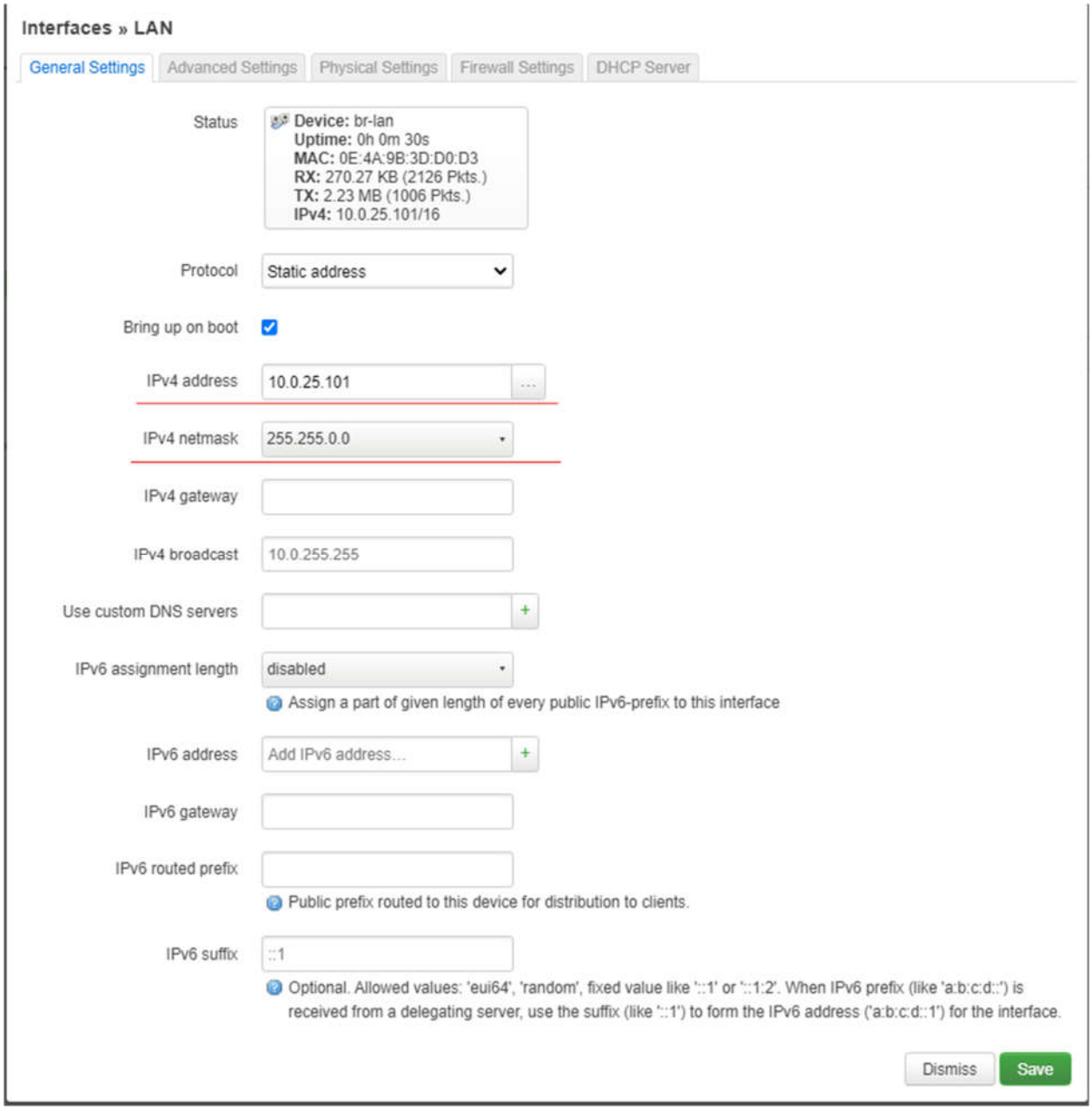
3.3.1 CL6 Multiple Wireless Access Points Configuration – Configuring a static IP on the LAN interface

The CL6 can also be configured to use a static address. To do so, either keep the IP address straps open to assign the address via configuration file, or configure the straps for a static IP assignment (See Setting IP Address with Switches). Navigate to Network → Interfaces and click "Edit" on the LAN interface.

Next, select static address from the Protocol dropdown and click the "Switch Protocol" button.



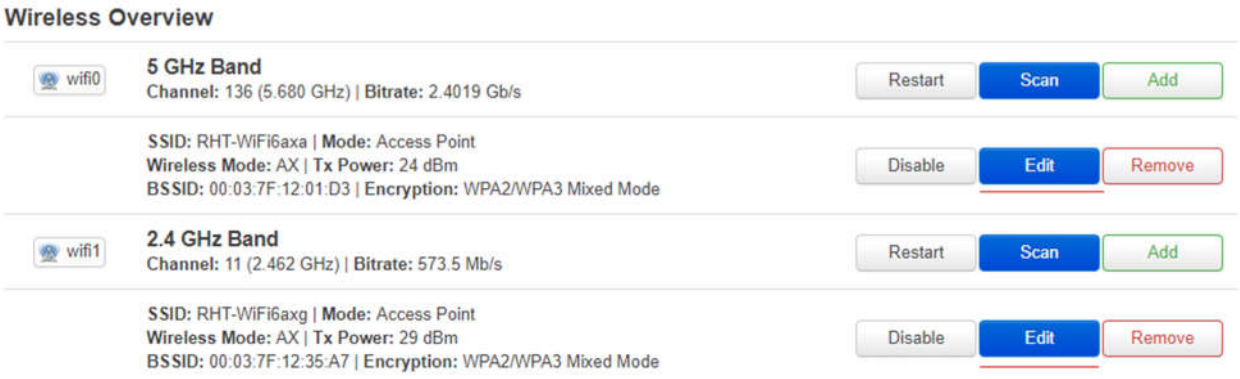
You will then need to fill in the IPv4 address and IPv4 netmask fields. It is recommended to use a valid, unused IP address outside of the DHCP IP address pool of the cabin system's DHCP server to avoid IP address conflicts.



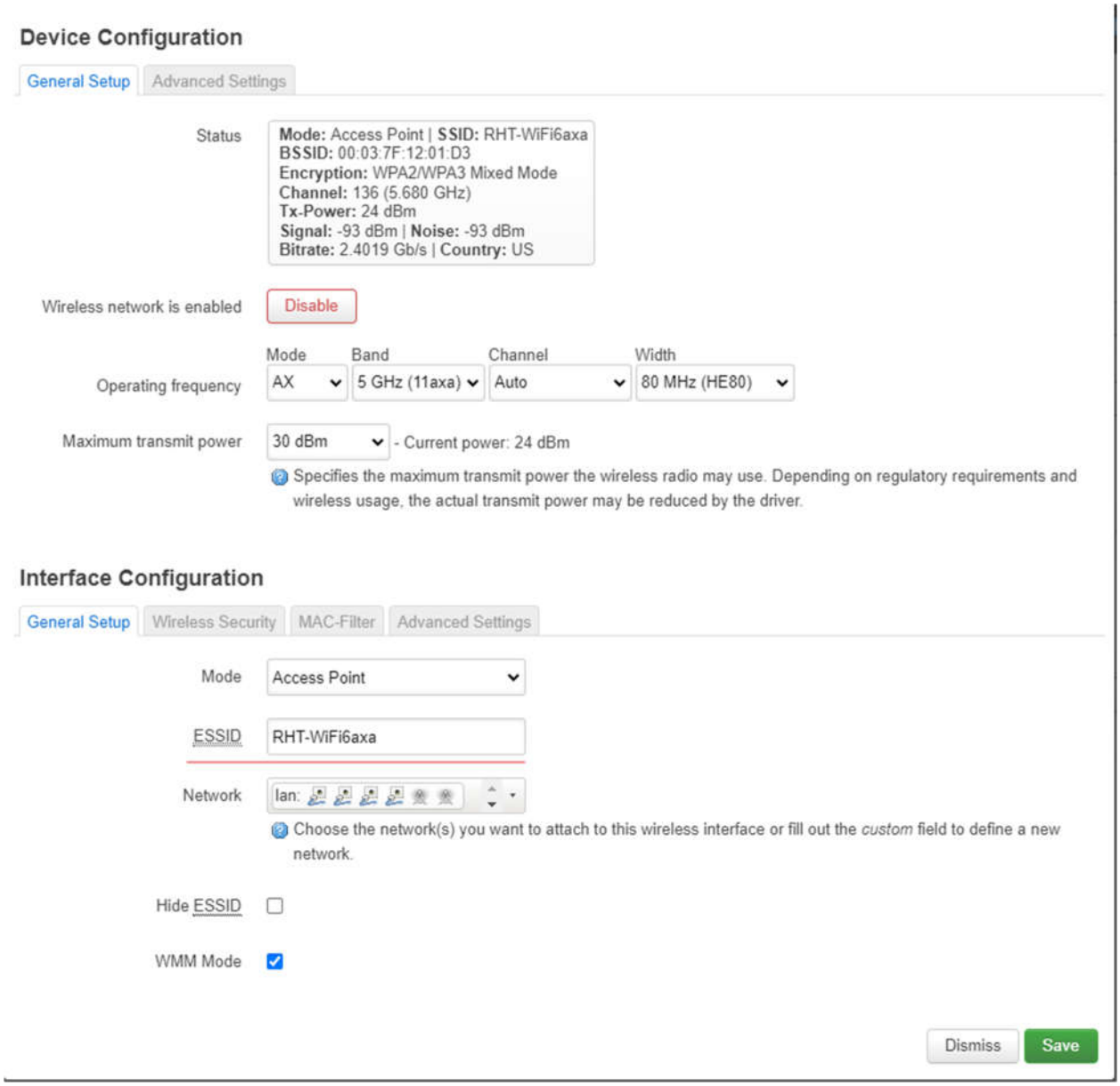
After these fields are populated, Save and apply your changes. The CL6 will now use the IP address you provided. Information on how to configure the rest of the settings on this page can be found in 8.1.

3.3.2 CL6 Multiple Wireless Access Points Configuration – Changing the SSID

To change the SSID for the network, start by navigating to Network → Wireless.



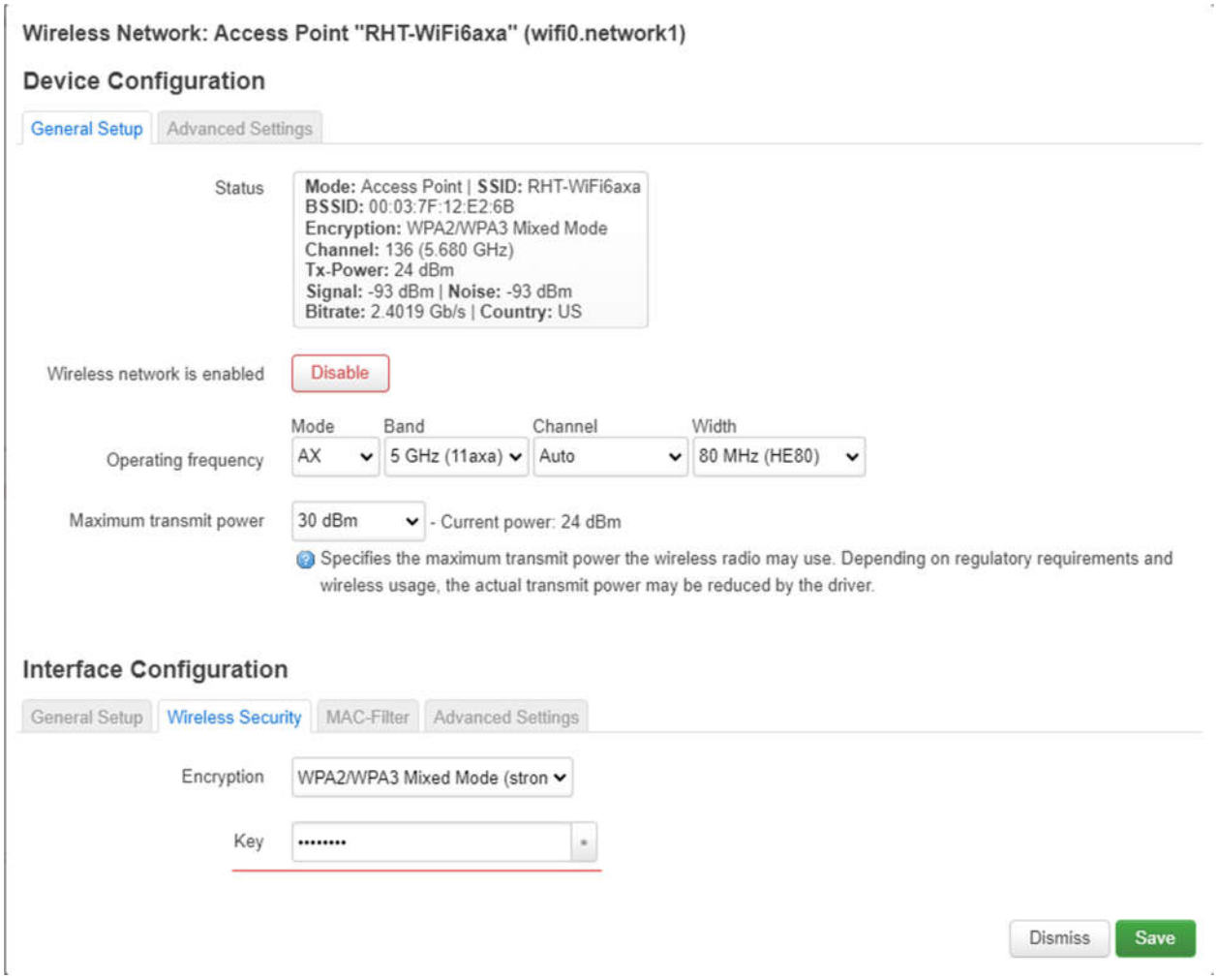
From this page, click edit on the wireless interface you want to change the SSID for.



Then, change the ESSID field to your desired SSID and save & apply your change. Each wireless interface can have their own unique SSID, or they can also share the same SSID.

3.3.3 CL6 Multiple Wireless Access Points Configuration – Changing the WiFi Password

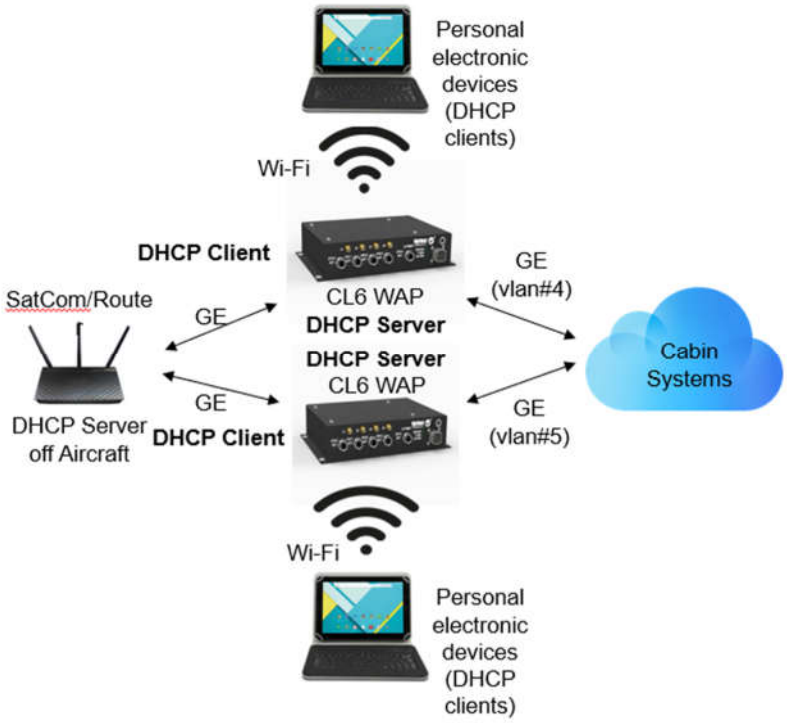
To change the password for your WiFi, click the wireless security tab on the same page.



Changing the value in the "Key" field will change the password for your WiFi. You can also change the wireless encryption type from this page by selecting an encryption type from the "Encryption" dropdown. Information on how to configure the rest of the settings on this page can be found in 8.2.

3.4 CL6 Multiple Routers with VLAN Support Configuration

In this case, there are multiple CL6's in the system. The CL6's act as layer three gateways with router responsibility. The CL6's act as DHCP servers for the wireless clients, but as a DHCP client for the SatCom interfaces.



To use this configuration, disconnect the IP address straps on both CL6's to allow the IP address to be set from the configuration file (See Setting IP Address with Switches). Navigate to System → Configuration Management on one of your CL6's and select "uc4_example_multiRTR_VLAN4" from the Current Configuration dropdown. After doing so, click the "Set as Current Config" button and then click the "Apply Current Config to System" button. Wait about 1 minute for configuration to apply to the CL6 and then reboot the unit. On the other CL6, navigate to System → Configuration Management and select "uc4_example_multiRTR_VLAN5" from the Current Configuration dropdown and follow the same procedure to apply the configuration. The CL6 with the uc4_example_multiRTR_VLAN4 configuration will have an IP address of 192.168.2.1. The CL6 with the uc4_example_multiRTR_VLAN5 configuration will have an IP address of 192.168.2.2. To access the GUI for either of the CL6's you will need to us assign a static IP address on the 192.168.2.x subnet and connect to an eth0 through eth4 LAN port.

To connect to the CL6 with the uc4_example_multiRTR_VLAN4 configuration loaded, manually assign your PC the following IP address, subnet mask, gateway, and DNS server:

IP address: 192.168.2.5

Subnet mask: 255.255.255.0

Default gateway: 192.168.2.1

Preferred DNS server: 192.168.2.1

To connect to the CL6 with the uc4_example_multiRTR_VLAN5 configuration loaded, manually assign your PC the following IP address, subnet mask, gateway, and DNS server:

IP address: 192.168.2.6

Subnet mask: 255.255.255.0

Default gateway: 192.168.2.2

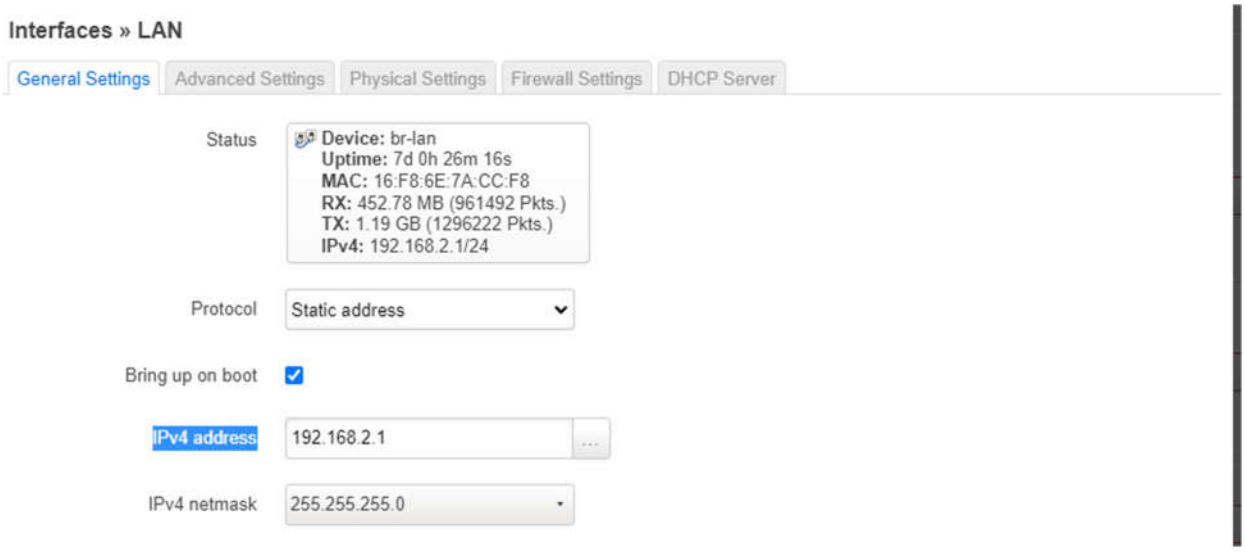
Preferred DNS server: 192.168.2.2

VLAN ID 4 (uc4_example_multiRTR_VLAN4) and VLAN ID 5 (uc4_example_multiRTR_VLAN5) network packets are communicated from of the eth1 port on each CabinLink 6.

Each CL6 has SSID's with a "-vlan" prefix, these SSID's are bridged with the VLAN interfaces. Clients connected to these SSID's will only be able to access the cabin system VLAN networks.

3.4.1 CL6 Multiple Routers with VLAN Support Configuration – Changing the LAN IP Address

To change the IP on each CL6, navigate to Network → Interfaces and click edit on the LAN interface.



Under the General Settings tab, change the IPv4 address field to the desired IP address for the CL6 and click Save. Make sure this IP address is not the same IP address as the other CL6. Information on how to configure the rest of the settings on this page can be found in 8.1.

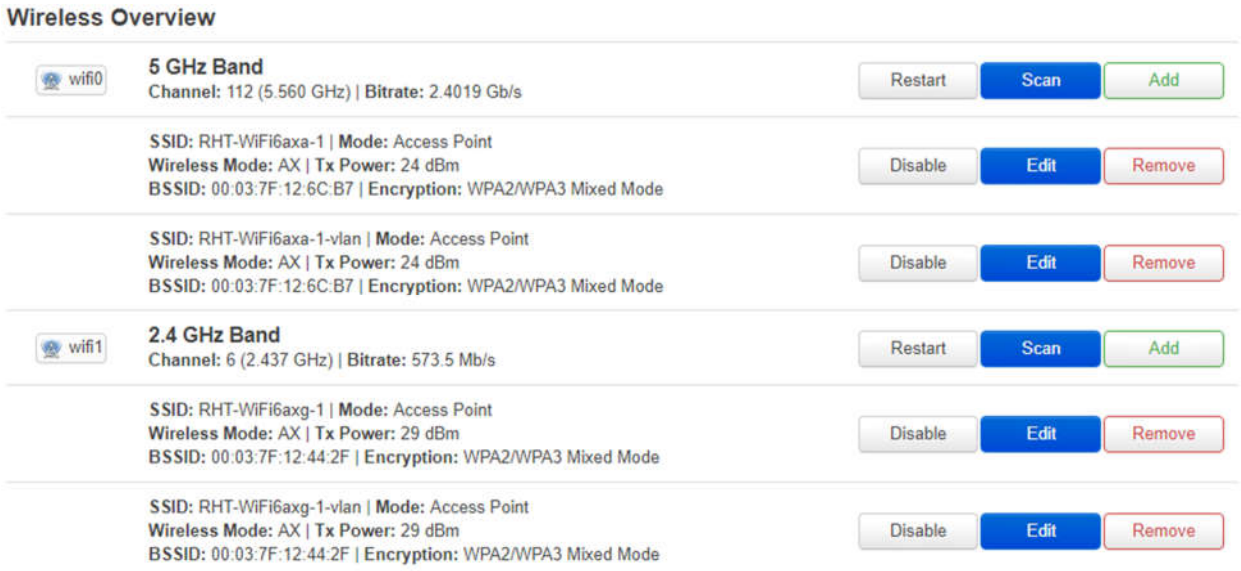
3.4.2 CL6 Multiple Routers with VLAN Support Configuration – Creating a VLAN

VLAN's can be created and configured through the Network → Interfaces GUI page. From this page, start by clicking the "Add new interface" button.

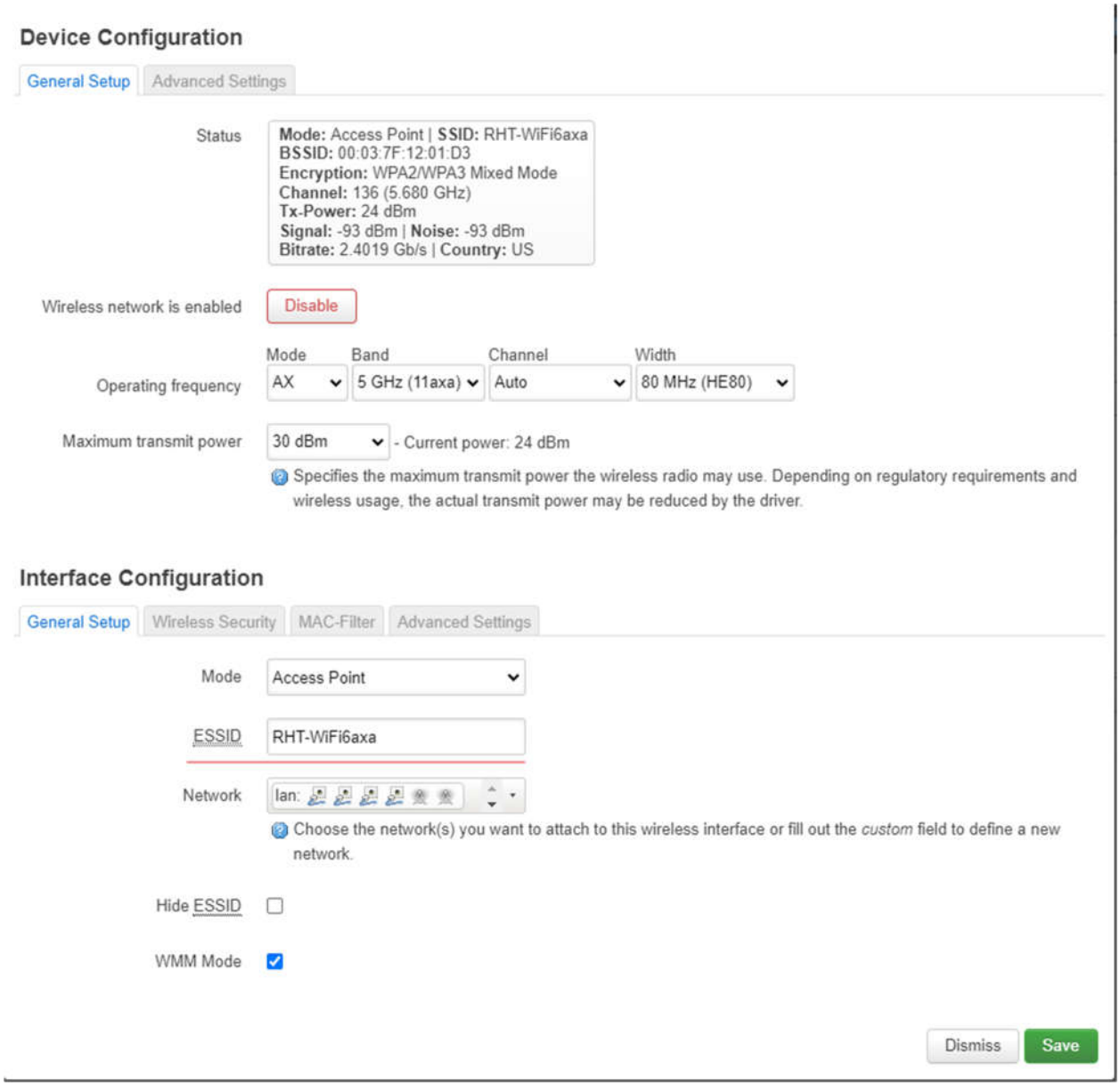
Enter the name for your VLAN interface and select Static address from the protocol dropdown. Bridge interfaces can be selected if needed. Open the interface dropdown and click on the "--custom--" text box at the bottom. Type the interface you want to create the VLAN on followed by a period and the VLAN ID you want to use (ex. eth1.2), then hit the enter key and click "Create Interface". After the interface is created, click save in the bottom right.

3.4.3 CL6 Multiple Routers with VLAN Support Configuration – Changing the SSID

To change the SSID for either network, start by navigating to Network → Wireless.



From this page, click edit on the wireless interface you want to change the SSID for.

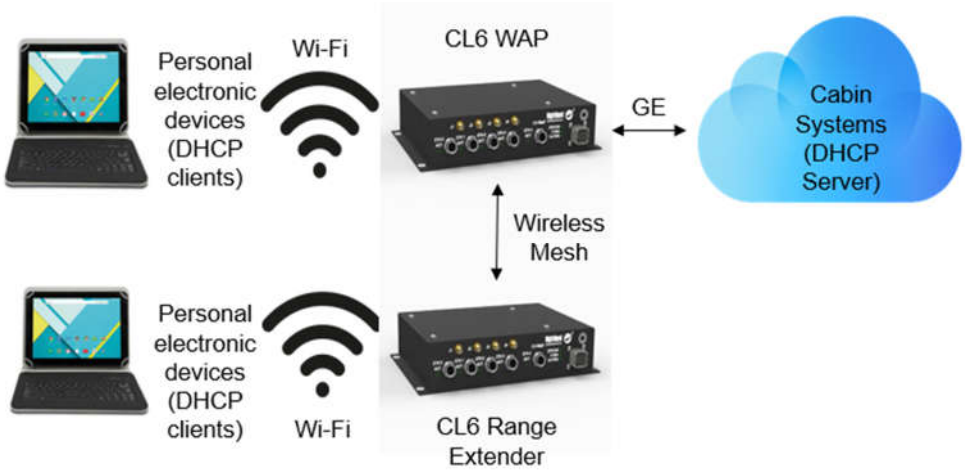


Then, change the ESSID field to your desired SSID and save & apply your change. Each wireless interface can have their own unique SSID, or they can also share the same SSID.

Information on how to configure the rest of the settings on this page can be found in 8.2.

3.5 CL6 Access Point with Range Extender/Wireless Mesh Configuration

In this case, there are multiple CL6's in the system. The CL6's act as access points (with layer two functions only). Only one of the CL6's is wired to the Cabin System. The other uses a wireless Mesh protocol to extend the Wi-Fi range without additional wiring.

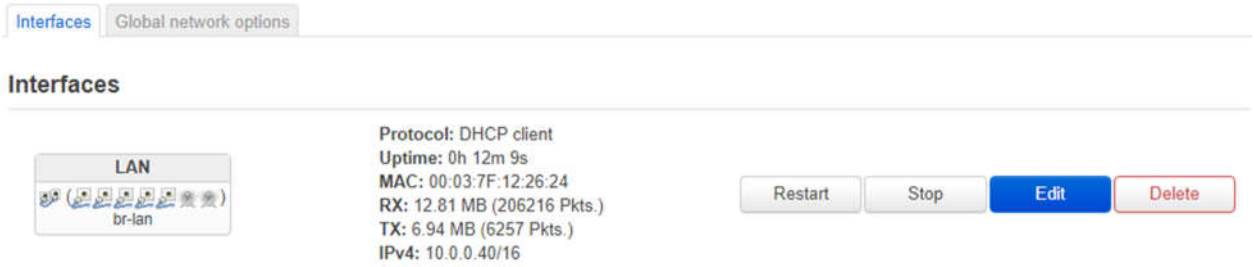


To use this configuration, you may disconnect the address straps and use DHCP per the configuration file or connect the IP address straps to ground (See Setting IP Address with Switches) and force DHCP client mode. Either method will allow the CL6 to get an IP address via DHCP. Navigate to System → Configuration Management on the CL6 you want to act as the primary access point and select "uc5_example_multiAP_wds_master" from the Current Configuration dropdown. After doing so, click the "Set as Current Config" button and then click the "Apply Current Config to System" button. Wait about 1 minute for configuration to apply to the CL6 and then reboot the unit. On the other CL6, disconnect the address straps and use DHCP per the configuration file or connect the IP address straps to ground (See Setting IP Address with Switches) and force DHCP client mode. Either method will allow the CL6 to get an IP address via DHCP. Navigate to System → Configuration Management and select "uc5_example_multiAP_wds_re" from the Current Configuration dropdown and follow the same procedure to apply the configuration. Both CL6's will receive an IP address through DHCP. The IP address of the each CabinLink 6 can be determined by issuing the "arp -a" command on a computer connected to the DHCP enabled network. The CabinLink 6's will have a MAC address starting with '00:1A:9C:14'

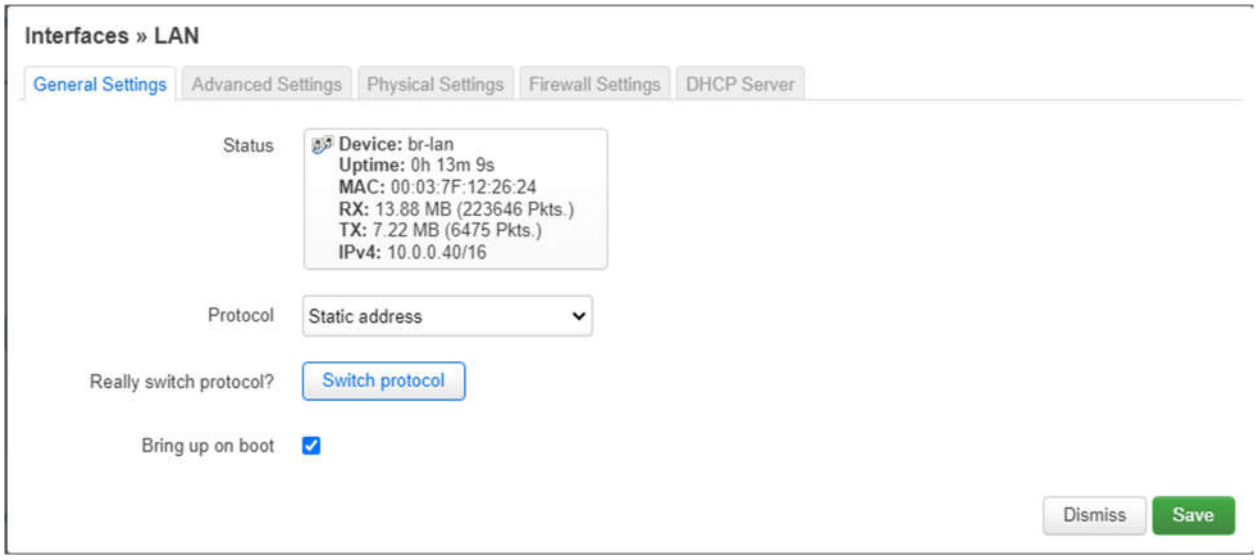
3.5.1 CL6 Access Point with Range Extender/Wireless Mesh Configuration – Assigning a static IP to the LAN interface

The CL6's can also be configured to use a static address. This can be useful as it will allow you to change the IP address to connect to a specific cabin systems network. To do so, disconnect the IP address straps on both CL6's to allow the IP address to be set from the configuration file or set the static IP address via strapping (See Setting IP Address with Switches).

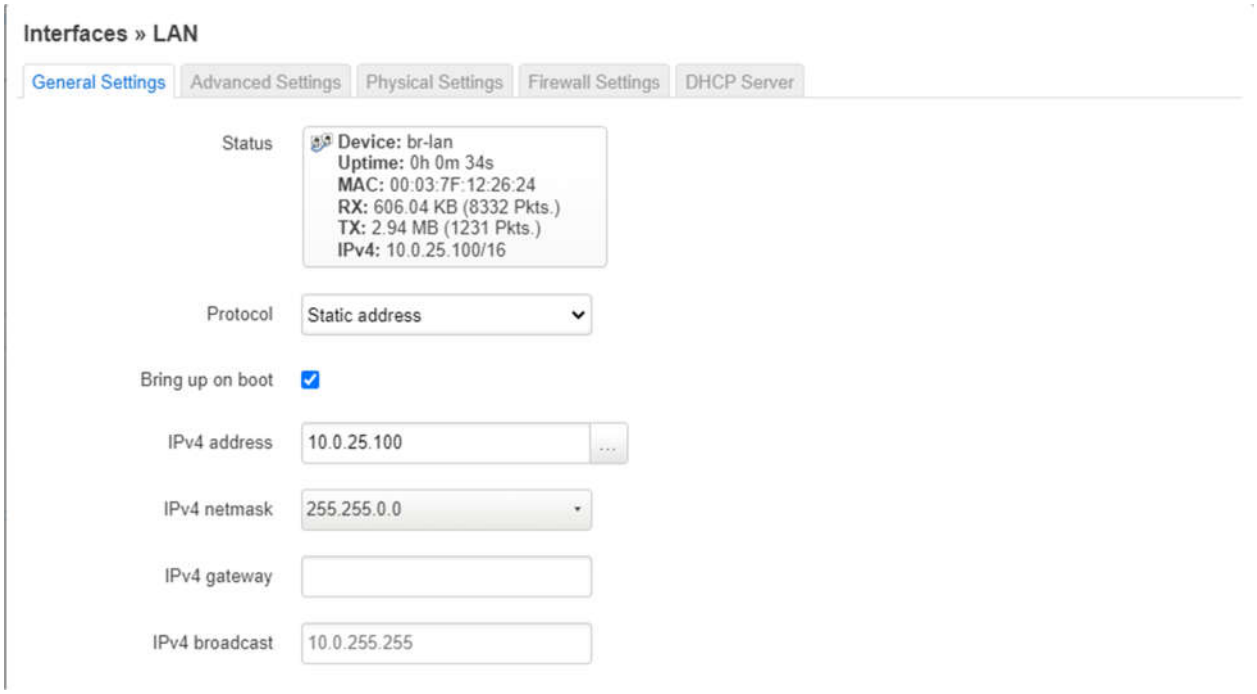
To configure a static IP address in the GUI, on the CL6 with the 'uc5_example_multiAP_wds_master' configuration loaded, navigate to Network → Interfaces and click "Edit" on the LAN interface.



Next, select static address from the Protocol dropdown and click the "Switch Protocol" button.

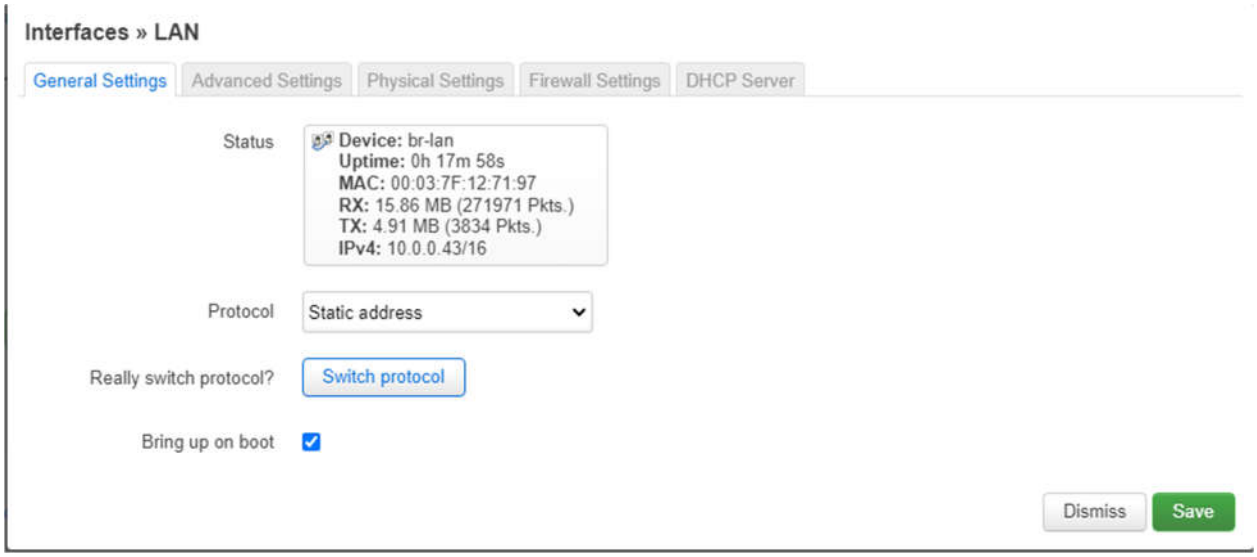


You will then need to fill in the IPv4 address and IPv4 netmask fields. It is recommended to use a valid, unused IP address outside of the DHCP IP address pool to avoid address conflicts. For this example, we'll use the IP address 10.0.25.100, which is compatible with the connected 10.0.x.x/16 network test environment.

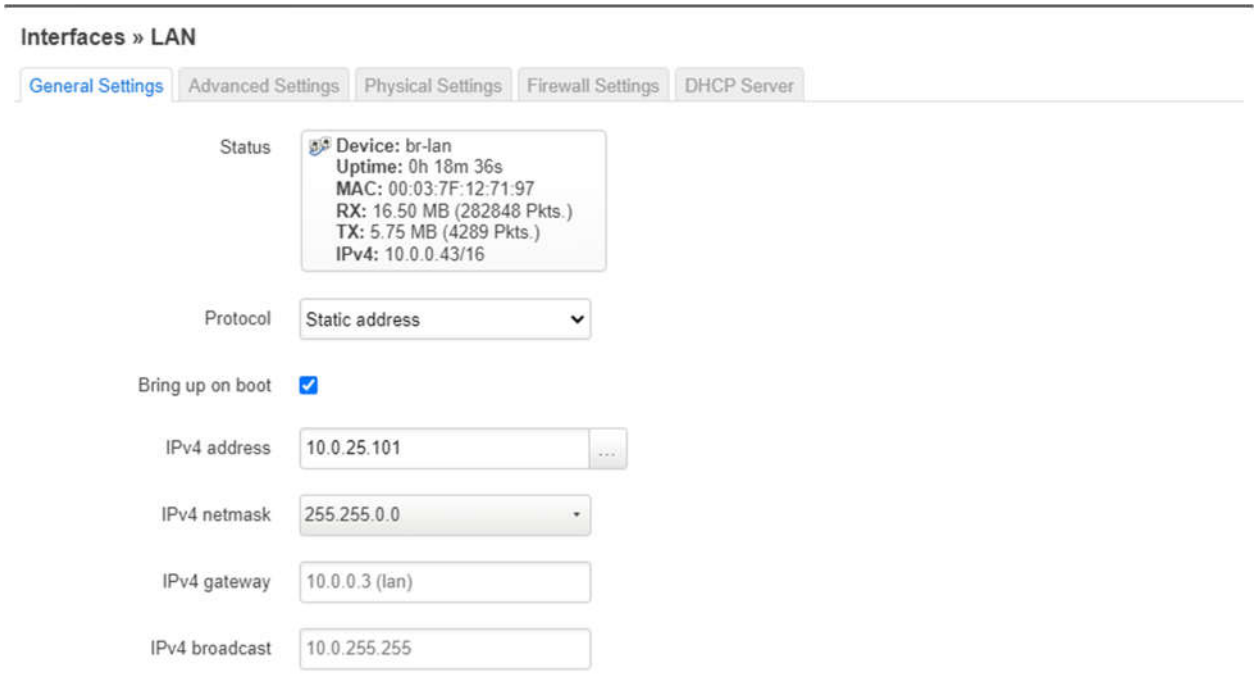


After these fields are populated, Save and apply your changes. The CL6 will now use the IP address you provided. Now, using the CL6 with the "uc5_example_multiAP_wds_re" configuration loaded, navigate to Network → Interfaces and click "Edit" on the LAN interface.

Next, select static address from the Protocol dropdown and click the "Switch Protocol" button.



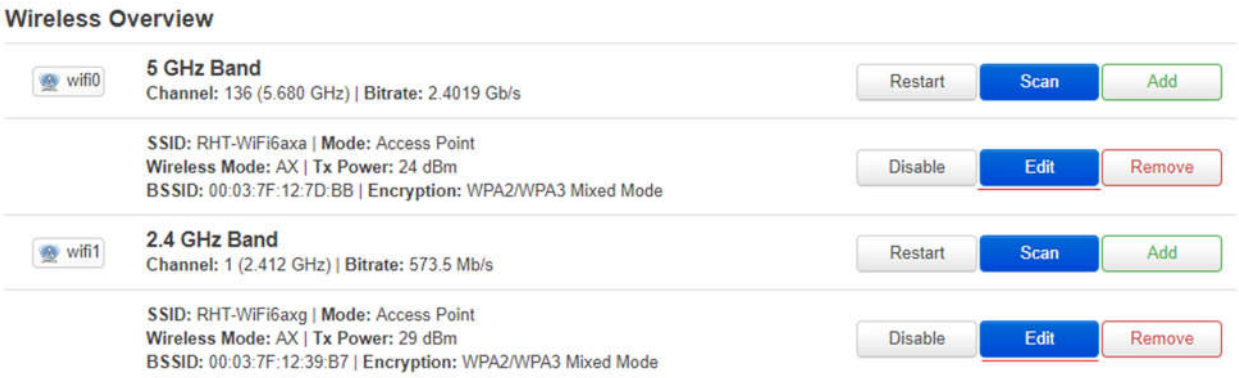
You will then need to fill in the IPv4 address and IPv4 netmask fields. It is recommended to use a valid, unused IP address outside of the DHCP IP address pool to avoid address conflicts. For this example, we'll use the IP address 10.0.25.101, which is compatible with the connected 10.0.x.x/16 network test environment.



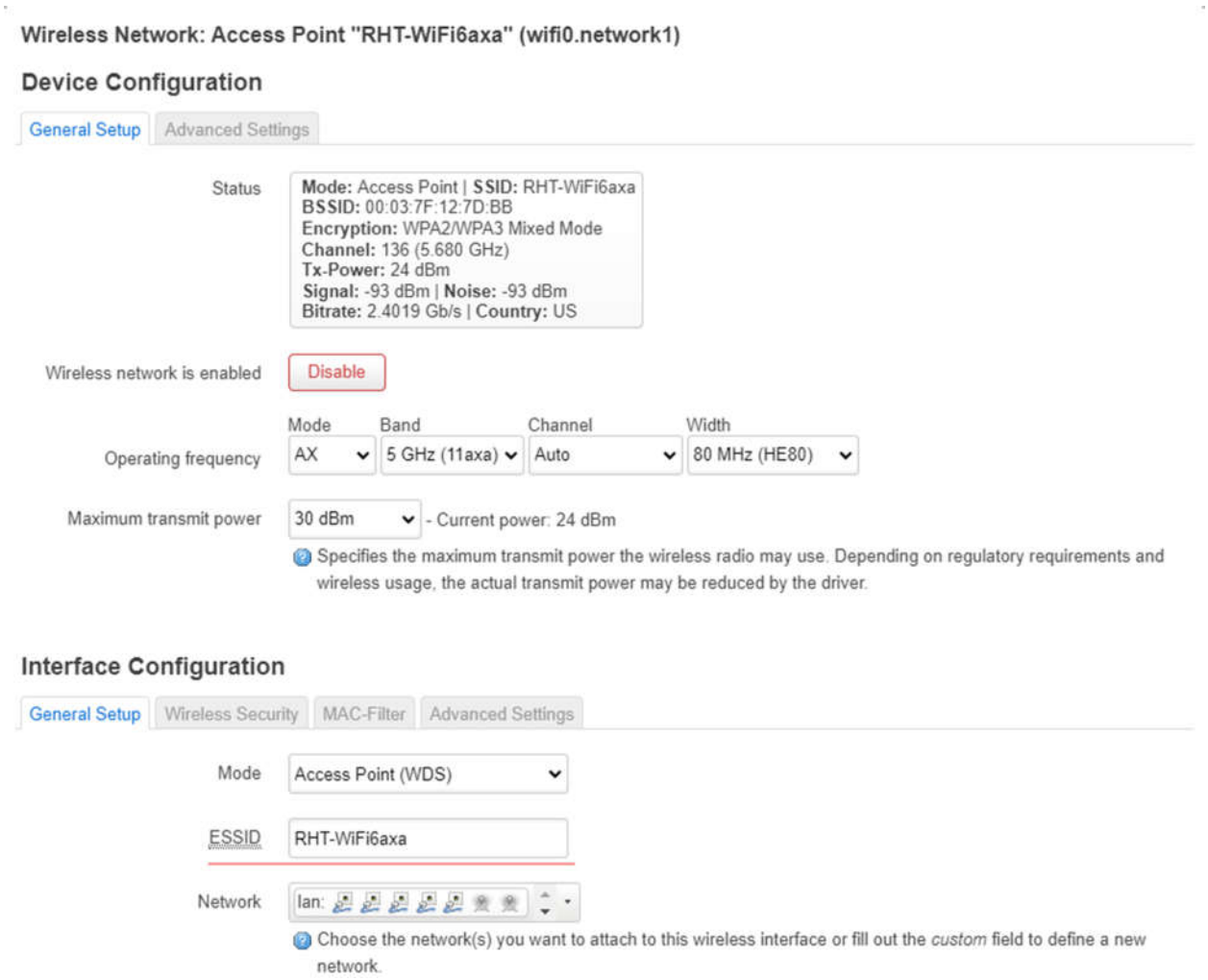
Now, restart both CL6's for the configurations to fully apply.

3.5.2 CL6 Access Point with Range Extender/Wireless Mesh Configuration – Changing the SSID

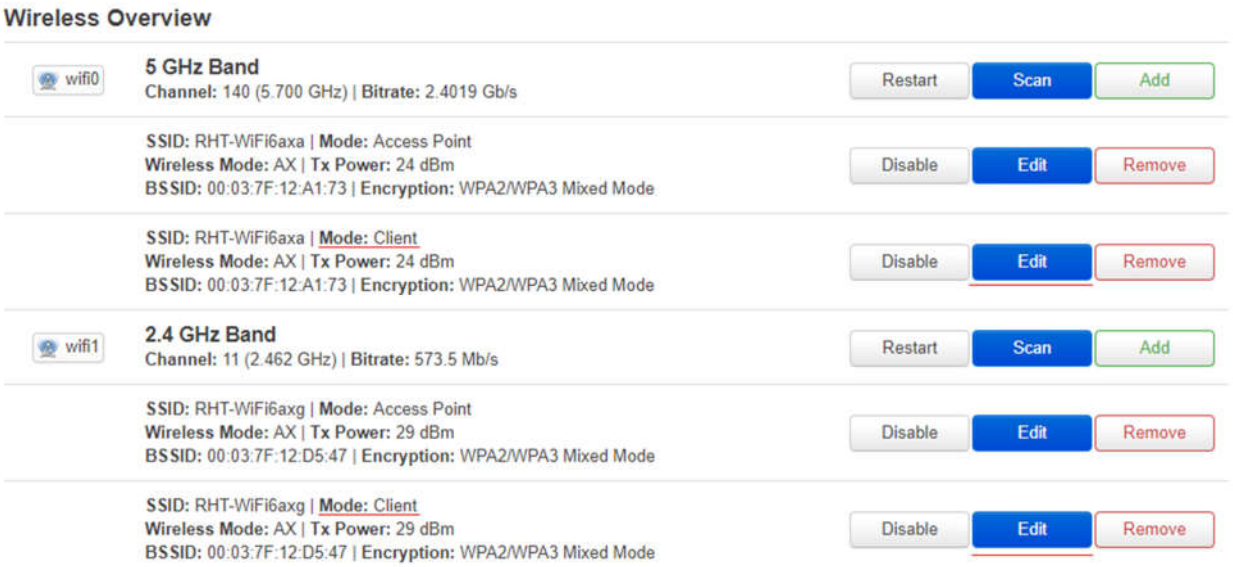
To change the SSID for the WiFi network, start by accessing the GUI on the CL6 with the "uc5_example_multiAP_wds_master" configuration loaded and navigate to Network → Wireless.



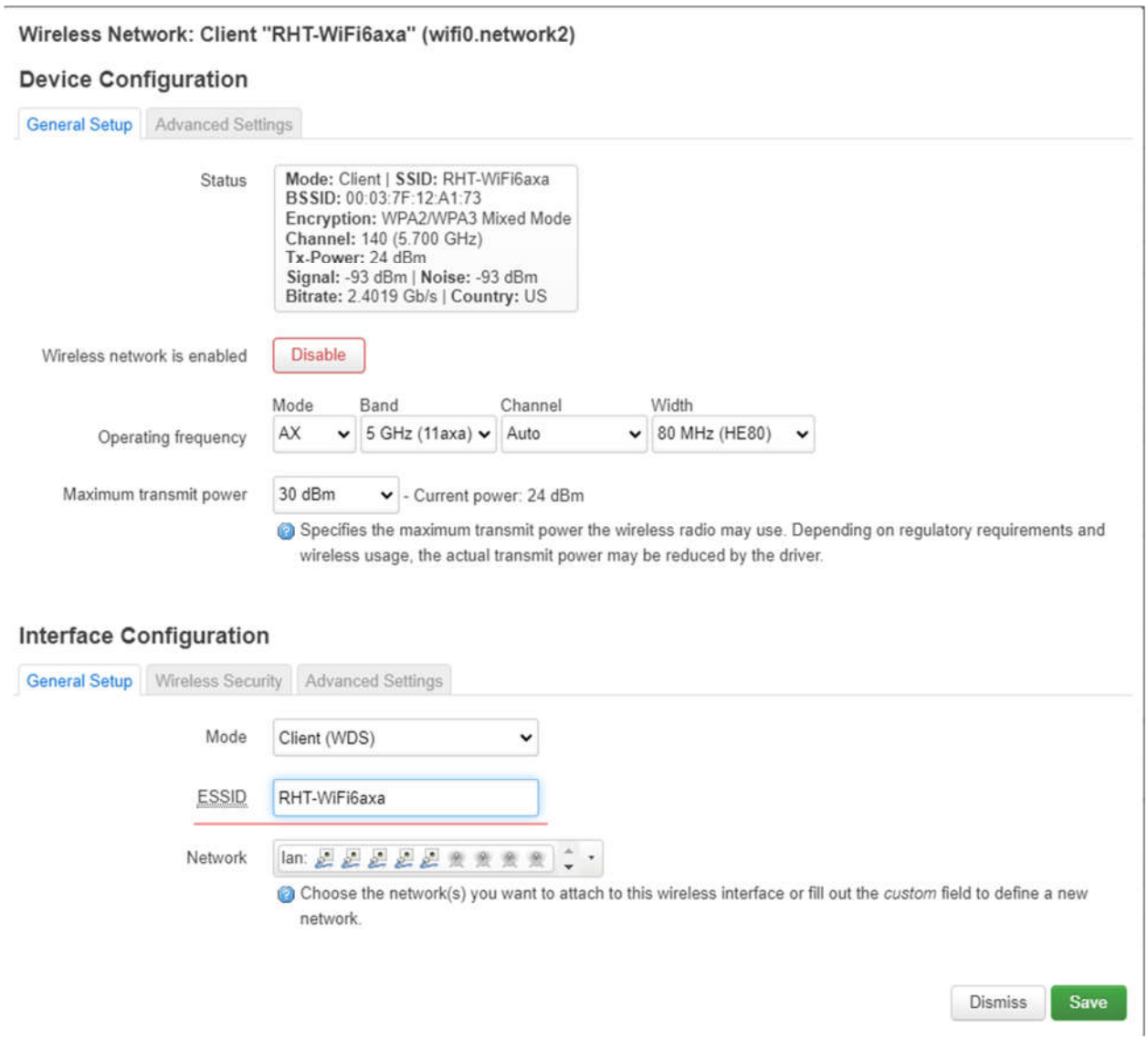
Click "Edit" on the wireless interface you want to change the SSID for and change the ESSID field to your desired SSID.



After changing the SSID, save and apply your changes. Then, access the GUI on CL6 with the "uc5_example_multiAP_wds_re" configuration loaded and navigate to Network → Wireless.



All changes made to the wireless interfaces on the CL6 with the uc5_example_multiAP_wds_master configuration must be mirrored on the wireless interfaces operating in client mode on the range extender CL6 using the uc5_example_multiAP_wds_re configuration. Click "Edit" on each wireless interface operating in client mode and change the ESSID field to the SSID you chose on the CL6 with the uc5_example_multiAP_wds_master configuration.



After changing the ESSID's on the interfaces running in client mode, save and apply your changes. Finally, reboot both CL6's.

The wireless interfaces operating in Access Point mode on the CL6 with the uc5_example_multiAP_wds_re configuration can have a different SSID and password than the wireless interfaces operating in Client mode.

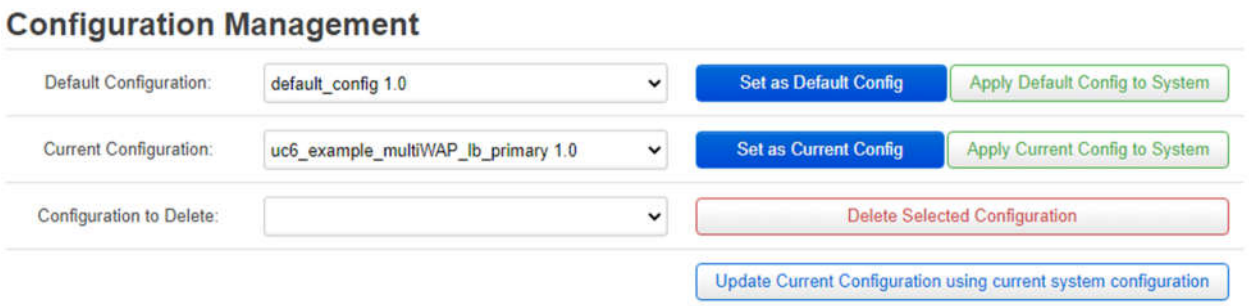
Information on how to configure the rest of the settings on this page can be found in 8.2.

3.6 CL6 Multiple Wireless Access Points with Load Balancing Configuration

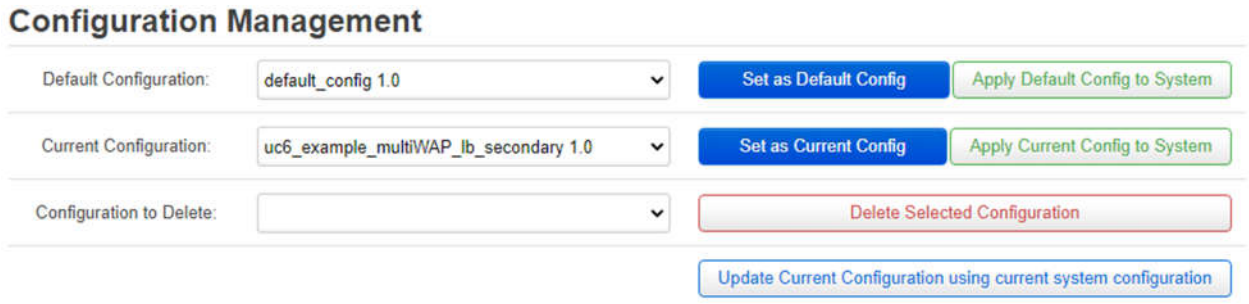
In this case, there are multiple CL6's in the system. The CL6's act as wireless access points (with layer two functions only). The WAPs are daisy-chained to the Cabin System to improve coverage in the aircraft. The WAPs automatically manage load-balancing between the multiple WAPs (if they share an SSID) so clients can seamlessly roam between the wireless access points.

Start by disconnecting the IP address straps on both CL6's to allow the IP address to be set from the configuration file (See Setting IP Address with Switches). The CL6 comes with two configuration files to mimic this use case. One configuration is for the CL6 that will act as the primary access point and one configuration is for the CL6 that will act as the secondary access point. It is important to note that in this use case, each access point is assigned a static IP. 10.0.25.100 for the primary access point and 10.0.25.101 for the secondary access point. The IP addresses should be changed to match the configuration of your Cabin System network prior to loading them in the CL6 GUI's. Alternatively, configure a PC to match these static IP subnets (10.0.x.x/16). After changing the IP addresses you'll need to modify the PC address again, otherwise you risk losing access to the GUI. If configuration problems occur, you can reset the CL6 to the default configuration by following the steps listed in CabinLink 6 System Reset.

To load these configurations onto each CL6 navigate to System → Configuration Management. On the CL6 that you want to act as the primary access point, select the uc6_example_multiWAP_lb_primary configuration from the "Current Configuration" dropdown.



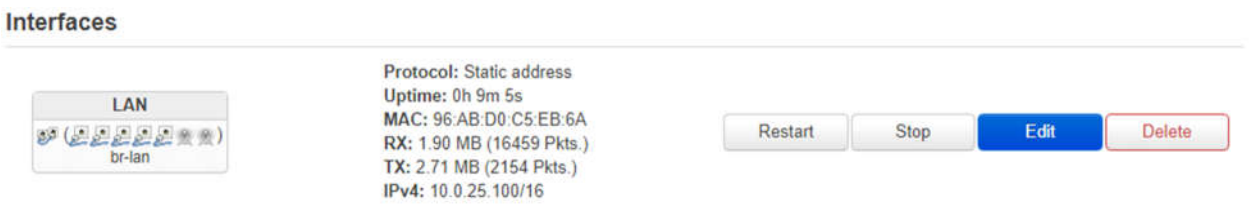
Once the uc6_example_multiWAP_lb_primary configuration is selected, click "Set as current config" and then click "Apply Current Config to System". Now, from the CL6 you want to act as the secondary access point, navigate to System → Configuration Management. This time you will need to select the uc6_example_multiWAP_lb_secondary configuration from the "Current Configuration" dropdown. Once it is selected click "Set as current config" and then click "Apply Current Config to System".

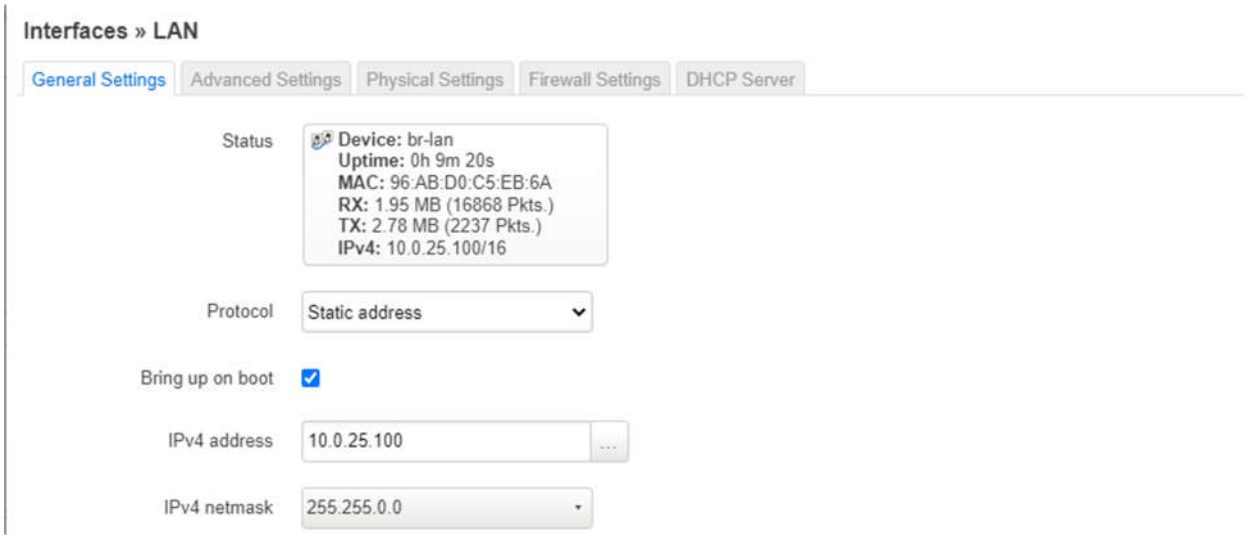


Once this is done, reboot both CL6's. The IP address on the primary access point will be set to 10.0.25.100 and the IP address on the secondary access point will be set to 10.0.25.101.

3.6.1 CL6 Multiple Wireless Access Points with Load Balancing Configuration – Changing the IP of the LAN interface

If you want to change the IP address of the primary access point, navigate to Network → Interfaces and click edit on the LAN interface.

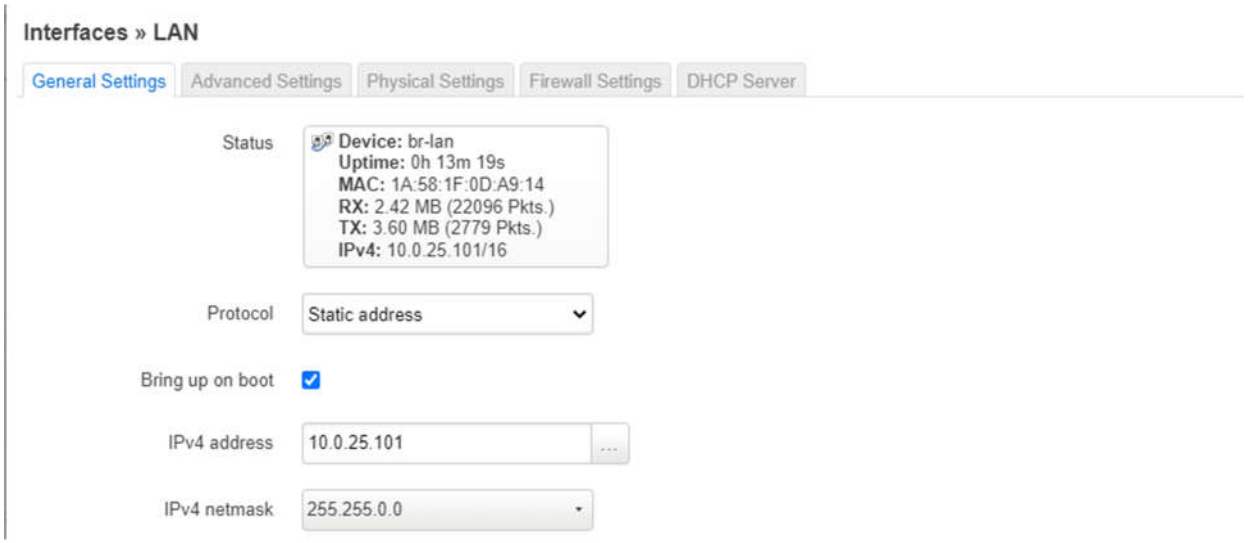




Under the General Settings tab, change the IPv4 address field to the desired IP address for the CL6 and set the netmask, then click Save.

To change the IP address on the secondary access point, simply navigate to Network → Interfaces and click edit on the LAN interface.

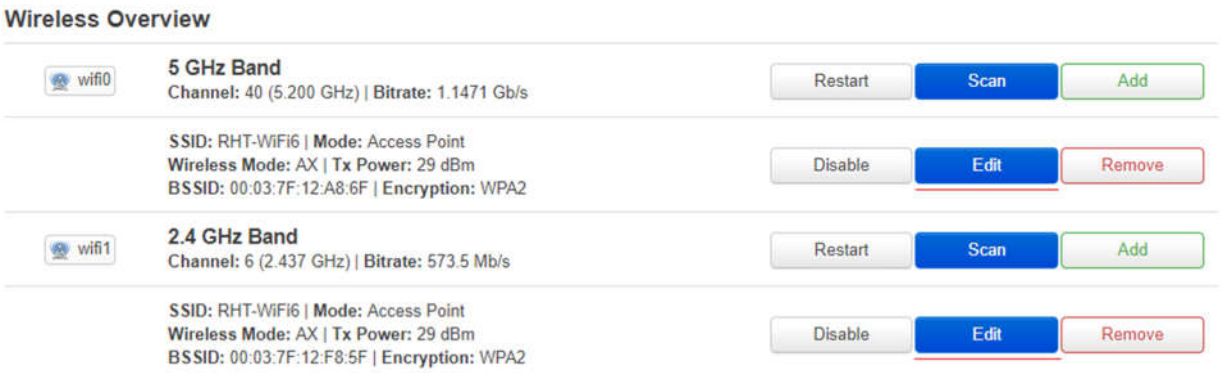
Under the General Settings tab, change the IPv4 address field to the desired IP address for the CL6 and set the netmask, then click Save.



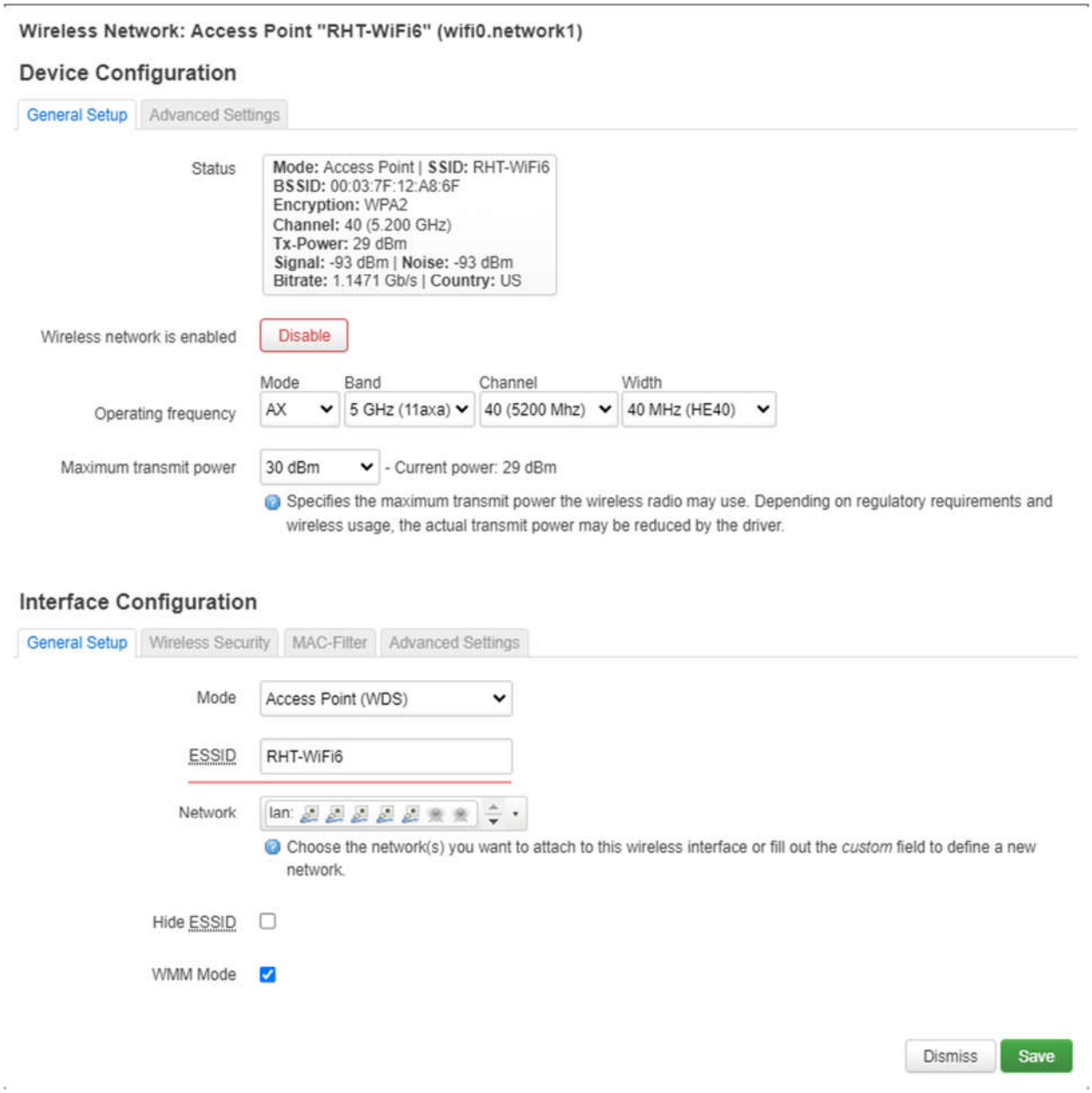
After you finish saving & applying these changes, reboot both the primary and secondary access points. Information on how to configure the rest of the settings on this page can be found in 8.1.

3.6.2 CL6 Multiple Wireless Access Points with Load Balancing Configuration – Changing the SSID

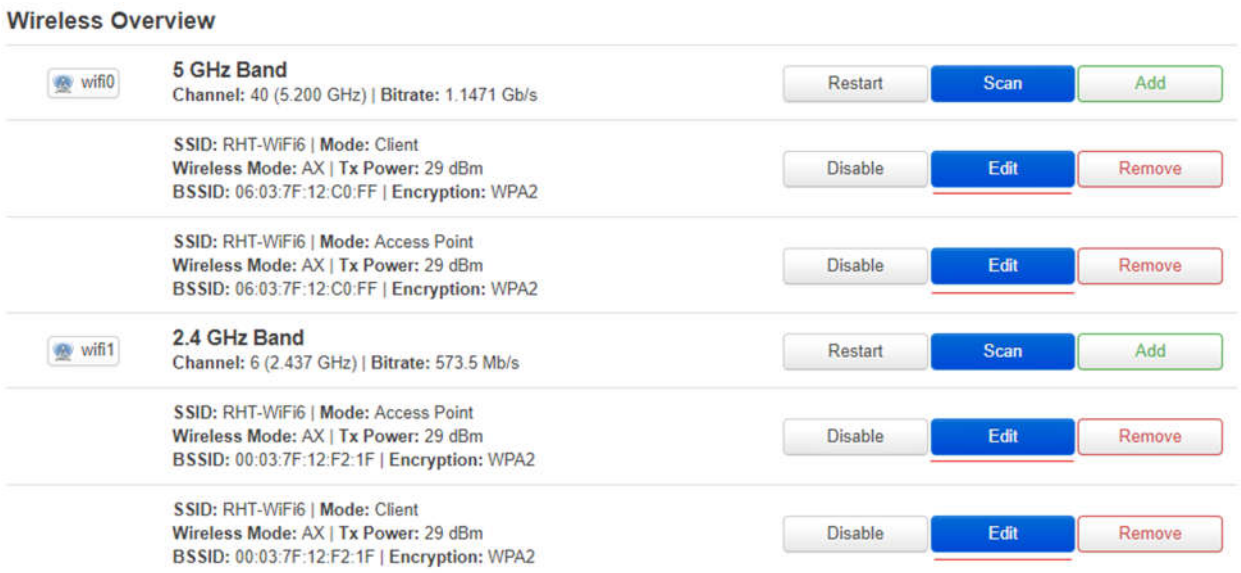
To change the SSID for the Multi-AP network, start by accessing the GUI on the primary access point and navigate to Network → Wireless.



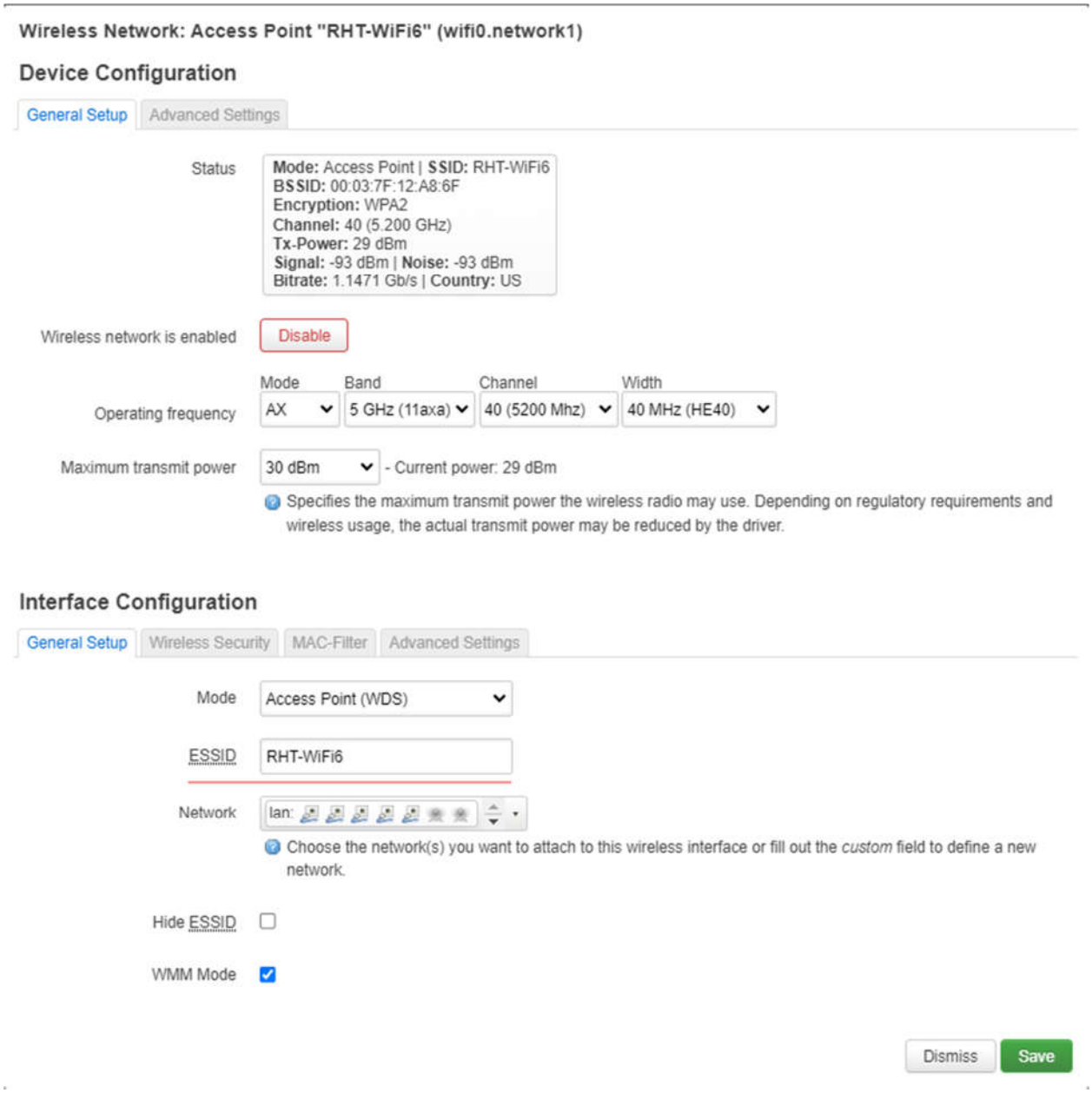
Click "Edit" on each wireless interface and change the ESSID field to your desired SSID.



After changing the SSID for both the 2.4 and 5 GHz interfaces, save and apply your changes. Then, access the GUI on the secondary access point and navigate to Network → Wireless.



Click "Edit" on each wireless interface and change the ESSID field to your desired SSID. This must be the same SSID you set on your primary access point.



After changing the ESSID on all four wireless interfaces, save and apply your changes. Finally, reboot both the primary and secondary access points.

Information on how to configure the rest of the settings on this page can be found in 8.2.

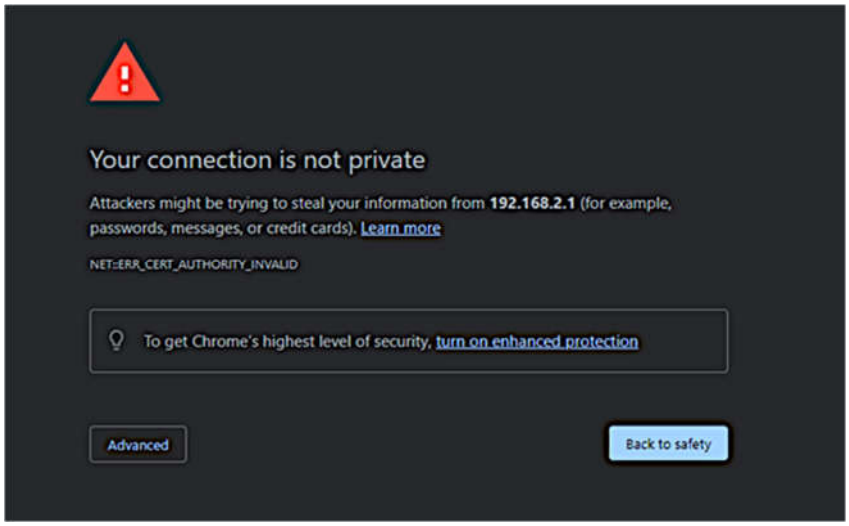
All load balancing and band steering settings are configurable on the Network → Load Balancing page. More information for each setting on this page can be found in 8.6.

4. CabinLink 6 GUI Configuration

The CL6 can be configured by two methods. The following sections describe the GUI screens that can be used to set most of the system's options. The Appendix describes the command line interface that is also available via the serial console. The factory default IP addresses are used in this user guide, depending on your configuration a different IP address may be required to access the GUI.

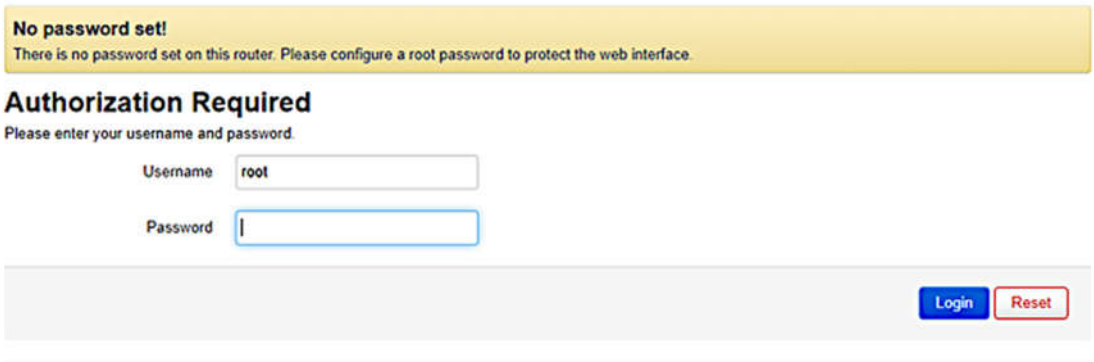
In order to configure the CL6 Wireless Access Point, enter the web-based configuration as follows:

1. Using a device connected to the LAN interfaces, enter the CL6 IP address into the address bar in a bowser window. The GUI screens cannot be accessed from the WAN network with the default iptables rules.
2. The window may show a warning similar to the following. This warning appears until valid certificates are configured in the system.
    a. Click ADVANCED
    b. Then click "Proceed to 192.168.2.1 (unsafe)"



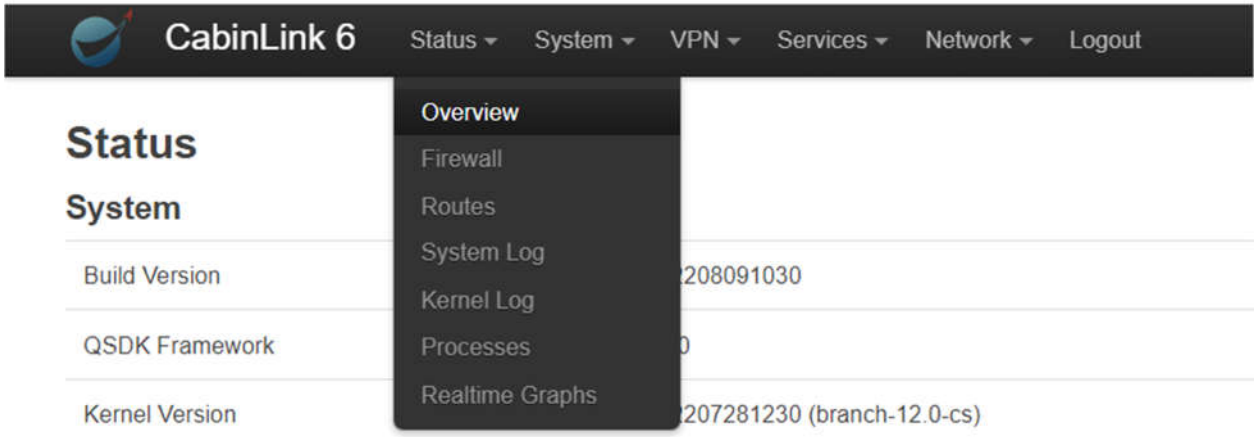
3. Initial login screen is displayed.
    a. If your CL6 has a preconfigured password, enter it in the password field
    b. Click Login

Note: If no password is configured you must set one after the initial login


No password set!
There is no password set on this router. Please configure a root password to protect the web interface.
Authorization Required
Please enter your username and password.
Username
root
Password
Login
Reset

5. Viewing system Status

The Status dropdown will show the following parameters.



5.1 Status – Overview

The Status Overview screen will show the following system parameters.

Status->Overview

Network

IPv4 Upstream

Protocol: DHCP client
Address: 10.0.0.77/16
Gateway: 10.0.0.3
DNS 1: 10.0.0.5
Expires: 1h 1m 24s
Connected: 18h 58m 36s

Device: Ethernet Adapter: "eth0"
MAC-Address: 56:78:44:35:C6:71

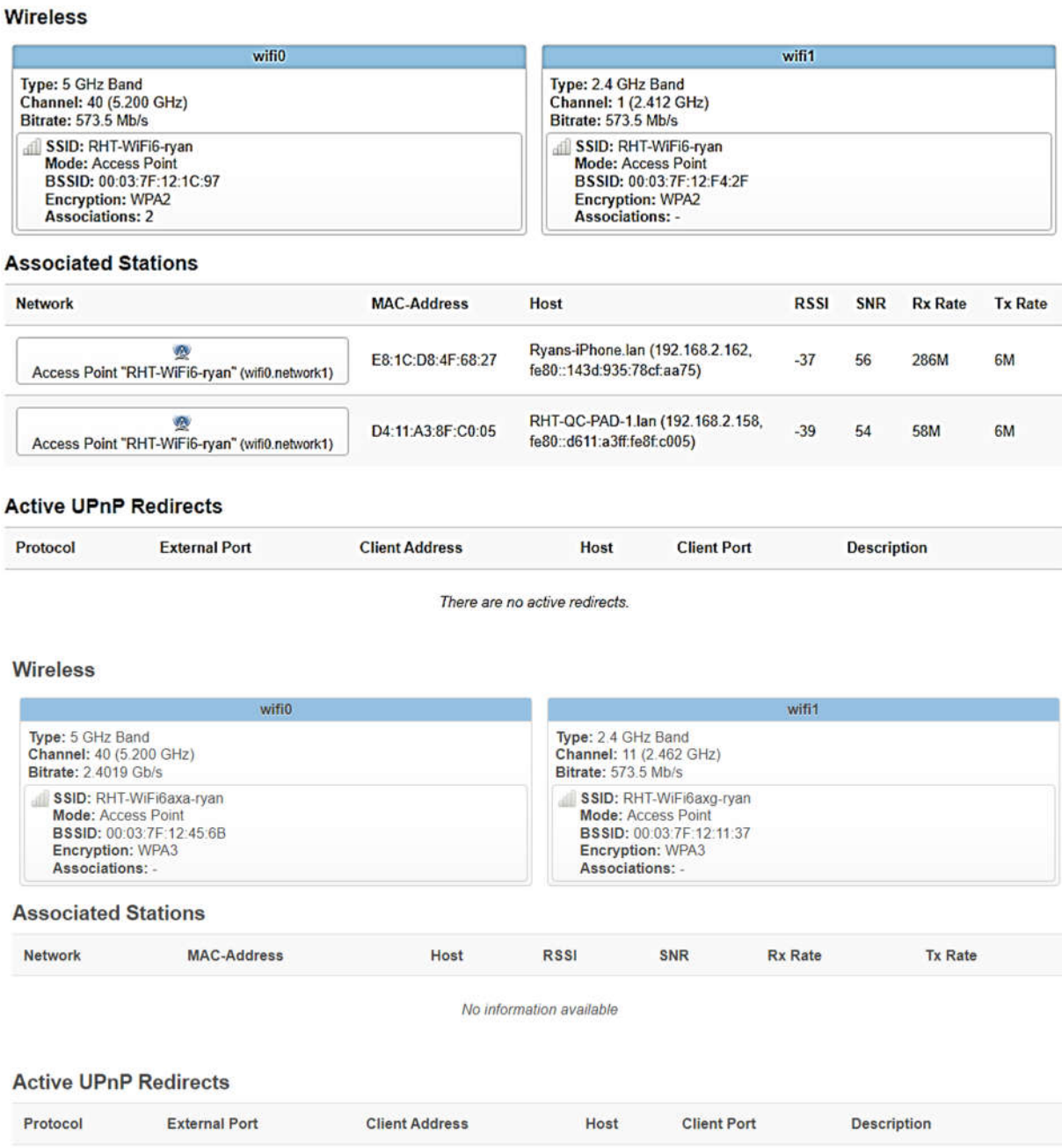
Active Connections	163 / 16384 (0%)

Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
RHT-QC-PAD-1	192.168.2.158	D4:11:A3:8F:C0:05	11h 44m 7s
Ryans-iPhone	192.168.2.162	E8:1C:D8:4F:68:27	11h 31m 37s
RWOLFE-I7	192.168.2.194	A0:CE:C8:11:32:31	9h 52m 13s

Active DHCPv6 Leases

Host	IPv6-Address	DUID	Leasetime remaining
RWOLFE-I7	fd13:1e2c:52ae::32e	0001000126d0ad0c3417ebbe9372	11h 1m 33s



The Status Overview page shows the following information:

- **System** – List of the versions of software packages
- **Memory** – Memory usage for the system
- **Network** – Active network connections

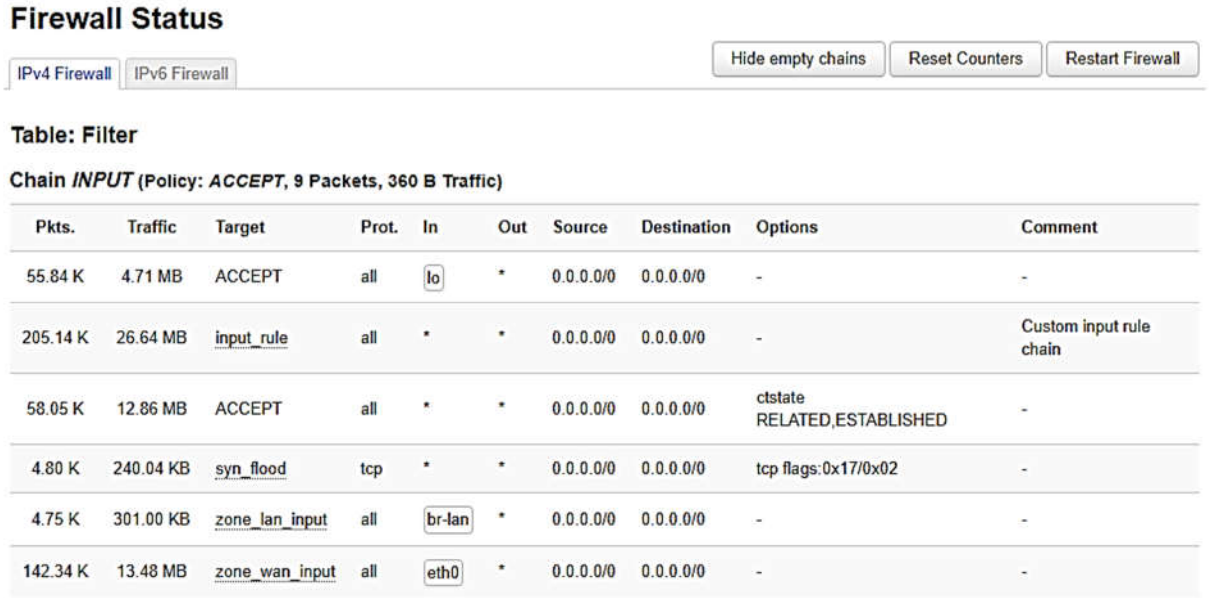
- **Active DHCP Leases** – configured and allocated DHCP leases
- **Active DHCPv6 Leases** – configured and active DHCPv6 leases
- **Wireless** – Wireless channel configuration
- **Associated Stations** – connected stations devices
- **Dynamic DNS** – DNS configurations

5.2 Status – Firewall

The screens in the Firewall status pages show the configuration of the IPv4 and IPv6 firewalls. The user may also restart the firewall from this page. See the **Network/Firewall** page to set firewall rules.

5.2.1 Status – Firewall – IPv4 Firewall

Status->Firewall->IPv4 Firewall



Chain *FORWARD* (Policy: *DROP*, 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
11.65 K	2.26 MB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	PHYSDEV match --physdev-is-bridged	-
0	0 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	PHYSDEV match --physdev-is-bridged	-
10.57 K	1.49 MB	forwarding_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom forwarding rule chain
8.71 K	1.18 MB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
1.86 K	312.36 KB	zone_lan_forward	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_wan_forward	all	eth0	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	reject	all	*	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	PHYSDEV match --physdev-is-bridged	-

Chain *OUTPUT* (Policy: *ACCEPT*, 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
57.76 K	4.88 MB	ACCEPT	all	*	lo	0.0.0.0/0	0.0.0.0/0	-	-
71.75 K	33.56 MB	output_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom output rule chain
68.06 K	33.30 MB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
11	3.06 KB	zone_lan_output	all	*	br-lan	0.0.0.0/0	0.0.0.0/0	-	-
3.68 K	263.90 KB	zone_wan_output	all	*	eth0	0.0.0.0/0	0.0.0.0/0	-	-

Chain *MINIUPNPD* (2 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment

No rules in this chain.

Chain *RATE-LIMIT* (0 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	limit: avg 1000/sec burst 1000	-
0	0 B	DROP	all	*	*	0.0.0.0/0	0.0.0.0/0	-	-

Chain *reject* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	REJECT	tcp	*	*	0.0.0.0/0	0.0.0.0/0	reject-with tcp-reset	-
0	0 B	REJECT	all	*	*	0.0.0.0/0	0.0.0.0/0	reject-with icmp-port-unreachable	-

Chain *syn_flood* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
4.95 K	247.42 KB	RETURN	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02 limit: avg 25/sec burst 50	-
0	0 B	DROP	all	*	*	0.0.0.0/0	0.0.0.0/0	-	-

Chain *zone_lan_dest_ACCEPT* (4 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
11	3.06 KB	ACCEPT	all	*	br-lan	0.0.0.0/0	0.0.0.0/0	-	-

Chain *zone_lan_forward* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
1.95 K	320.19 KB	forwarding_lan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom lan forwarding rule chain
1.95 K	320.19 KB	zone_wan_dest_ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Zone lan to wan forwarding policy
0	0 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate DNAT	Accept port forwards
0	0 B	zone_lan_dest_ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	-	-

Chain *zone_lan_input* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
5.04 K	318.38 KB	input_lan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom lan input rule chain
0	0 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate DNAT	Accept port redirections
5.04 K	318.38 KB	zone_lan_src_ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	-	-

Chain *zone_lan_output* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
11	3.06 KB	output_lan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom lan output rule chain
11	3.06 KB	zone_lan_dest_ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	-	-

Chain *zone_lan_src_ACCEPT* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
5.04 K	318.38 KB	ACCEPT	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	ctstate NEW,UNTRACKED	-

Chain *zone_wan_forward* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	forwarding_wan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom wan forwarding rule chain
0	0 B	zone_lan_dest_ACCEPT	esp	*	*	0.0.0.0/0	0.0.0.0/0	-	Allow-IPSec-ESP
0	0 B	zone_lan_dest_ACCEPT	udp	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:500	Allow-ISAKMP
0	0 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate DNAT	Accept port forwards
0	0 B	MINIUPNPD	all	*	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_wan_dest_ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	-	-

Chain *zone_wan_input* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
144.41 K	13.69 MB	input_wan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom wan input rule chain
1.02 K	337.81 KB	ACCEPT	udp	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:68	Allow-DHCP-Renew
111	6.66 KB	ACCEPT	icmp	*	*	0.0.0.0/0	0.0.0.0/0	icmptype 8	Allow-Ping
0	0 B	ACCEPT	2	*	*	0.0.0.0/0	0.0.0.0/0	-	Allow-IGMP
0	0 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate DNAT	Accept port redirections
143.27 K	13.35 MB	MINIUPNPD	all	*	*	0.0.0.0/0	0.0.0.0/0	-	-
143.27 K	13.35 MB	zone_wan_src_ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	-	-

Chain *zone_wan_dest_ACCEPT* (3 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
128	6.45 KB	DROP	all	*	eth0	0.0.0.0/0	0.0.0.0/0	ctstate INVALID	Prevent NAT leakage
5.67 K	595.90 KB	ACCEPT	all	*	eth0	0.0.0.0/0	0.0.0.0/0	-	-

Chain *zone_wan_output* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
3.81 K	273.03 KB	output_wan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom wan output rule chain
3.81 K	273.03 KB	zone_wan_dest_ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	-	-

Chain *zone_wan_src_ACCEPT* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
143.39 K	13.36 MB	ACCEPT	all	eth0	*	0.0.0.0/0	0.0.0.0/0	ctstate NEW,UNTRACKED	-

Table: NAT

Chain *PREROUTING* (Policy: *ACCEPT*, 459405 Packets, 153.27 MB Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
459.41 K	153.27 MB	prerouting_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom prerouting rule chain
8.32 K	876.40 KB	zone_lan_prerouting	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	-	-
451.09 K	152.40 MB	zone_wan_prerouting	all	eth0	*	0.0.0.0/0	0.0.0.0/0	-	-

Chain *POSTROUTING* (Policy: *ACCEPT*, 745 Packets, 89.67 KB Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
6.40 K	673.59 KB	postrouting_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom postrouting rule chain
112	24.63 KB	zone_lan_postrouting	all	*	br-lan	0.0.0.0/0	0.0.0.0/0	-	-
5.65 K	583.78 KB	zone_wan_postrouting	all	*	eth0	0.0.0.0/0	0.0.0.0/0	-	-

Chain *zone_lan_postrouting* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
112	24.63 KB	postrouting_lan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom lan postrouting rule chain

Chain *zone_lan_prerouting* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
8.36 K	881.63 KB	prerouting_lan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom lan prerouting rule chain

Chain *zone_wan_postrouting* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
5.66 K	584.17 KB	postrouting_wan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom wan postrouting rule chain
5.65 K	583.51 KB	MINIUPNPD-POSTROUTING	all	*	*	0.0.0.0/0	0.0.0.0/0	-	-
5.66 K	584.17 KB	MASQUERADE	all	*	*	0.0.0.0/0	0.0.0.0/0	-	-

Chain *zone_wan_prerouting* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
452.15 K	152.73 MB	prerouting_wan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom wan prerouting rule chain
452.15 K	152.73 MB	MINIUPNPD	all	*	*	0.0.0.0/0	0.0.0.0/0	-	-

Chain *FORWARD* (Policy: *ACCEPT*, 23891 Packets, 4.02 MB Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
1.55 K	86.74 KB	TCPMSS	tcp	*	eth0	0.0.0.0/0	0.0.0.0/0	tcp flags:0x06/0x02 TCPMSS clamp to PMTU	Zone wan MTU fixing
1.55 K	81.79 KB	TCPMSS	tcp	eth0	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x06/0x02 TCPMSS clamp to PMTU	Zone wan MTU fixing

Chain *qos_Default* (0 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	CONNMARK	all	*	*	0.0.0.0/0	0.0.0.0/0	CONNMARK restore mask 0xf	-
0	0 B	qos_Default_ct	all	*	*	0.0.0.0/0	0.0.0.0/0	mark match 0x0/0xf	-
0	0 B	MARK	udp	*	*	0.0.0.0/0	0.0.0.0/0	mark match 0x0/0xf0 length 0:500 MARK xset 0x22/0xff	-
0	0 B	MARK	icmp	*	*	0.0.0.0/0	0.0.0.0/0	MARK xset 0x11/0xff	-
0	0 B	MARK	tcp	*	*	0.0.0.0/0	0.0.0.0/0	mark match 0x0/0xf0 tcp spts:1024:65535 dpts:1024:65535 MARK xset 0x44/0xff	-
0	0 B	MARK	udp	*	*	0.0.0.0/0	0.0.0.0/0	mark match 0x0/0xf0 udp spts:1024:65535 dpts:1024:65535 MARK xset 0x44/0xff	-
0	0 B	CONNMARK	all	*	*	0.0.0.0/0	0.0.0.0/0	CONNMARK save mask 0xff	-

Chain *qos_Default_ct* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	MARK	tcp	*	*	0.0.0.0/0	0.0.0.0/0	mark match 0x0/0xf tcp multiport ports 22,53 MARK xset 0x11/0xff	ssh, dns
0	0 B	MARK	udp	*	*	0.0.0.0/0	0.0.0.0/0	mark match 0x0/0xf udp multiport ports 22,53 MARK xset 0x11/0xff	ssh, dns
0	0 B	MARK	tcp	*	*	0.0.0.0/0	0.0.0.0/0	mark match 0x0/0xf tcp multiport ports 20,21,25,80,110,443,993,995 MARK xset 0x33/0xff	ftp, smtp, http(s), imap
0	0 B	CONNMARK	all	*	*	0.0.0.0/0	0.0.0.0/0	CONNMARK save mask 0xff	-

Table: Raw

Chain *PREROUTING* (Policy: *ACCEPT*, 731948 Packets, 187.06 MB Traffic)

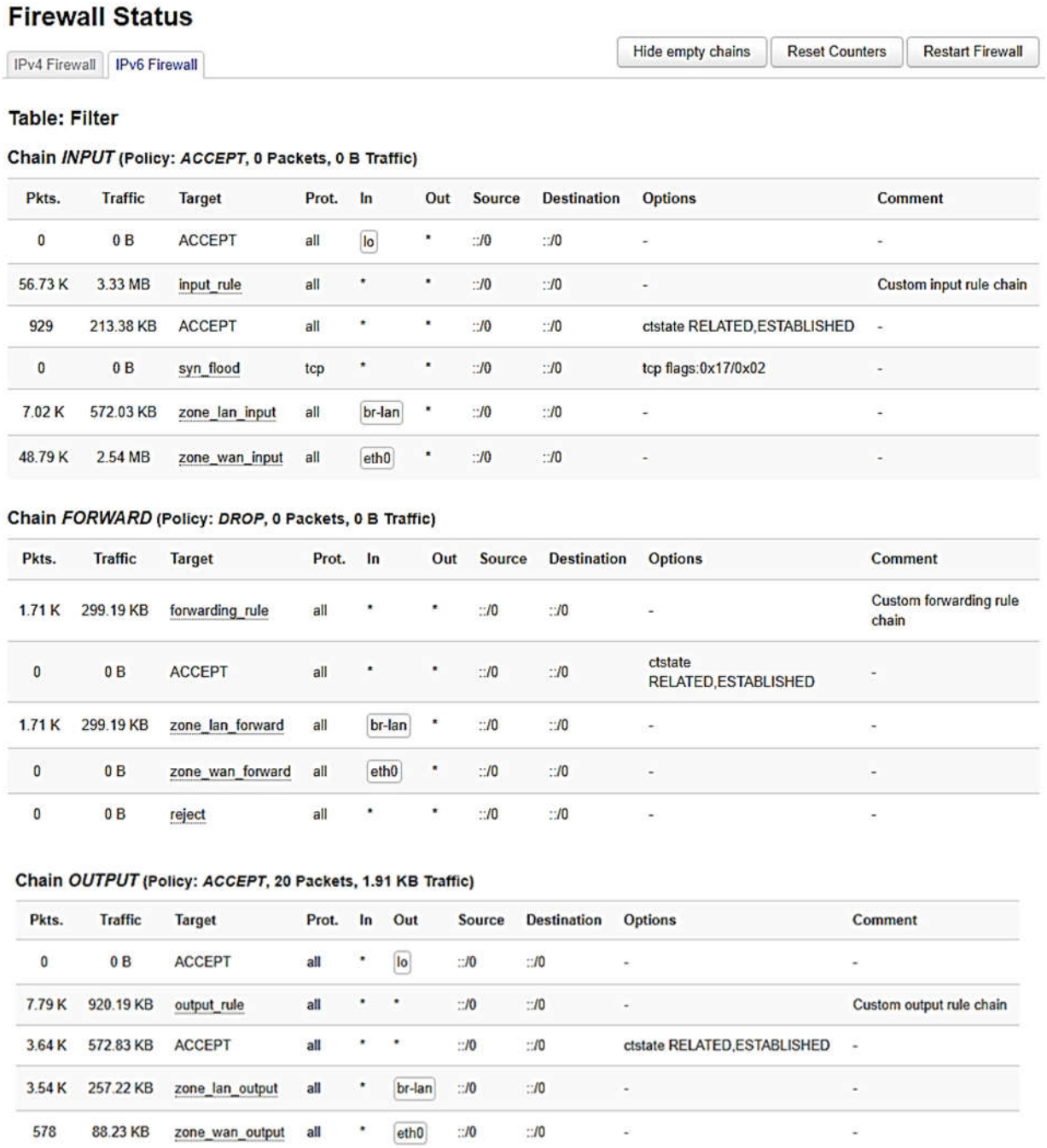
Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
62.16 K	12.77 MB	zone_lan_helper	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	-	lan CT helper assignment

Chain *zone_lan_helper* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	CT	udp	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:10080 CT helper amanda	Amanda backup and archiving proto
0	0 B	CT	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:21 CT helper ftp	FTP passive connection tracking
0	0 B	CT	udp	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:1719 CT helper RAS	RAS proto tracking
0	0 B	CT	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:1720 CT helper Q.931	Q.931 proto tracking
0	0 B	CT	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:6667 CT helper irc	IRC DCC connection tracking
0	0 B	CT	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:1723 CT helper pptp	PPTP VPN connection tracking
0	0 B	CT	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:5060 CT helper sip	SIP VoIP connection tracking
0	0 B	CT	udp	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:5060 CT helper sip	SIP VoIP connection tracking
0	0 B	CT	udp	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:161 CT helper snmp	SNMP monitoring connection tracking
0	0 B	CT	udp	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:69 CT helper tftp	TFTP connection tracking
0	0 B	CT	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:554 CT helper rtsp	RTSP connection tracking

5.2.2 Status – Firewall – IPv6 Firewall

Status->Firewall->IPv6 Firewall



Firewall Status

IPv4 Firewall | IPv6 Firewall

Hide empty chains | Reset Counters | Restart Firewall

Table: Filter

Chain *INPUT* (Policy: *ACCEPT*, 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	ACCEPT	all	lo	*	::/0	::/0	-	-
56.73 K	3.33 MB	input_rule	all	*	*	::/0	::/0	-	Custom input rule chain
929	213.38 KB	ACCEPT	all	*	*	::/0	::/0	ctstate RELATED,ESTABLISHED	-
0	0 B	syn_flood	tcp	*	*	::/0	::/0	tcp flags:0x17/0x02	-
7.02 K	572.03 KB	zone_lan_input	all	br-lan	*	::/0	::/0	-	-
48.79 K	2.54 MB	zone_wan_input	all	eth0	*	::/0	::/0	-	-

Chain *FORWARD* (Policy: *DROP*, 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
1.71 K	299.19 KB	forwarding_rule	all	*	*	::/0	::/0	-	Custom forwarding rule chain
0	0 B	ACCEPT	all	*	*	::/0	::/0	ctstate RELATED,ESTABLISHED	-
1.71 K	299.19 KB	zone_lan_forward	all	br-lan	*	::/0	::/0	-	-
0	0 B	zone_wan_forward	all	eth0	*	::/0	::/0	-	-
0	0 B	reject	all	*	*	::/0	::/0	-	-

Chain *OUTPUT* (Policy: *ACCEPT*, 20 Packets, 1.91 KB Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	ACCEPT	all	*	lo	::/0	::/0	-	-
7.79 K	920.19 KB	output_rule	all	*	*	::/0	::/0	-	Custom output rule chain
3.64 K	572.83 KB	ACCEPT	all	*	*	::/0	::/0	ctstate RELATED,ESTABLISHED	-
3.54 K	257.22 KB	zone_lan_output	all	*	br-lan	::/0	::/0	-	-
578	88.23 KB	zone_wan_output	all	*	eth0	::/0	::/0	-	-

Chain *reject* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	REJECT	tcp	*	*	::/0	::/0	reject-with tcp-reset	-
0	0 B	REJECT	all	*	*	::/0	::/0	reject-with icmp6-port-unreachable	-

Chain *syn_flood* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	RETURN	tcp	*	*	::/0	::/0	tcp flags:0x17/0x02 limit: avg 25/sec burst 50	-
0	0 B	DROP	all	*	*	::/0	::/0	-	-

Firewall Status

IPv4 Firewall | IPv6 Firewall

Hide empty chains | Reset Counters | Restart Firewall

Table: Filter

Chain *INPUT* (Policy: *ACCEPT*, 4 Packets, 160 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
12.93 K	1.06 MB	ACCEPT	all	lo	*	0.0.0.0/0	0.0.0.0/0	-	-
29.17 K	3.51 MB	input_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom input rule chain
6.11 K	1.26 MB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
547	28.34 KB	syn_flood	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02	-
213	14.09 KB	zone_lan_input	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	-	-
22.84 K	2.24 MB	zone_wan_input	all	eth0	*	0.0.0.0/0	0.0.0.0/0	-	-

Chain *FORWARD* (Policy: *DROP*, 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
12.32 K	950.39 KB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	PHYSDEV match --physdev-is-bridged	-
0	0 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	PHYSDEV match --physdev-is-bridged	-

Chain *zone_lan_dest_ACCEPT* (4 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
5.92 K	698.91 KB	ACCEPT	all	*	br-lan	::/0	::/0	-	-

Chain *zone_lan_forward* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
2.27 K	433.91 KB	forwarding_lan_rule	all	*	*	::/0	::/0	-	Custom lan forwarding rule chain
2.27 K	433.91 KB	zone_wan_dest_ACCEPT	all	*	*	::/0	::/0	-	Zone lan to wan forwarding policy
2.27 K	433.91 KB	zone_lan_dest_ACCEPT	all	*	*	::/0	::/0	-	-

Chain *zone_lan_input* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
7.31 K	596.12 KB	input_lan_rule	all	*	*	::/0	::/0	-	Custom lan input rule chain
7.31 K	596.12 KB	zone_lan_src_ACCEPT	all	*	*	::/0	::/0	-	-

Chain *zone_lan_output* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
3.65 K	264.99 KB	output_lan_rule	all	*	*	::/0	::/0	-	Custom lan output rule chain
3.65 K	264.99 KB	zone_lan_dest_ACCEPT	all	*	*	::/0	::/0	-	-

Chain *zone_lan_src_ACCEPT* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
7.31 K	596.12 KB	ACCEPT	all	br-lan	*	::/0	::/0	ctstate NEW,UNTRACKED	-

Chain *zone_wan_dest_ACCEPT* (3 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	DROP	all	*	eth0	::/0	::/0	ctstate INVALID	Prevent NAT leakage
593	90.53 KB	ACCEPT	all	*	eth0	::/0	::/0	-	-

Chain *zone_wan_forward* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	forwarding_wan_rule	all	*	*	::/0	::/0	-	Custom wan forwarding rule chain
0	0 B	ACCEPT	icmpv6	*	*	::/0	::/0	ipv6-icmptype 128 limit: avg 1000/sec burst 5	Allow-ICMPv6-Forward
0	0 B	ACCEPT	icmpv6	*	*	::/0	::/0	ipv6-icmptype 129 limit: avg 1000/sec burst 5	Allow-ICMPv6-Forward
0	0 B	ACCEPT	icmpv6	*	*	::/0	::/0	ipv6-icmptype 1 limit: avg 1000/sec burst 5	Allow-ICMPv6-Forward
0	0 B	ACCEPT	icmpv6	*	*	::/0	::/0	ipv6-icmptype 2 limit: avg 1000/sec burst 5	Allow-ICMPv6-Forward
0	0 B	ACCEPT	icmpv6	*	*	::/0	::/0	ipv6-icmptype 3 limit: avg 1000/sec burst 5	Allow-ICMPv6-Forward
0	0 B	ACCEPT	icmpv6	*	*	::/0	::/0	ipv6-icmptype 4 code 0 limit: avg 1000/sec burst 5	Allow-ICMPv6-Forward
0	0 B	ACCEPT	icmpv6	*	*	::/0	::/0	ipv6-icmptype 4 code 1 limit: avg 1000/sec burst 5	Allow-ICMPv6-Forward
0	0 B	zone_lan_dest_ACCEPT	esp	*	*	::/0	::/0	-	Allow-IPSec-ESP
0	0 B	zone_lan_dest_ACCEPT	udp	*	*	::/0	::/0	udp dpt:500	Allow-ISAKMP
0	0 B	MINIUPNPD	all	*	*	::/0	::/0	-	-
0	0 B	zone_wan_dest_ACCEPT	all	*	*	::/0	::/0	-	-

Chain *zone_wan_input* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
50.18 K	2.61 MB	input_wan_rule	all	*	*	::/0	::/0	-	Custom wan input rule chain
0	0 B	ACCEPT	udp	*	*	fc00::/6	fc00::/6	udp dpt:546	Allow-DHCPv6
0	0 B	ACCEPT	icmpv6	*	*	fe80::/10	::/0	ipv6-icmptype 130 code 0	Allow-MLD
0	0 B	ACCEPT	icmpv6	*	*	fe80::/10	::/0	ipv6-icmptype 131 code 0	Allow-MLD
0	0 B	ACCEPT	icmpv6	*	*	fe80::/10	::/0	ipv6-icmptype 132 code 0	Allow-MLD

Chain *zone_wan_output* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
595	90.83 KB	output_wan_rule	all	*	*	::/0	::/0	-	Custom wan output rule chain
595	90.83 KB	zone_wan_dest_ACCEPT	all	*	*	::/0	::/0	-	-

Chain *zone_wan_src_ACCEPT* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
49.82 K	2.59 MB	ACCEPT	all	eth0	*	::/0	::/0	ctstate NEW,UNTRACKED	-

Firewall Status

IPv4 Firewall | IPv6 Firewall

Hide empty chains | Reset Counters | Restart Firewall

Table: Filter

Chain *INPUT* (Policy: *ACCEPT*, 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	ACCEPT	all	lo	*	::/0	::/0	-	-
6.05 K	324.23 KB	input_rule	all	*	*	::/0	::/0	-	Custom input rule chain
0	0 B	ACCEPT	all	*	*	::/0	::/0	ctstate RELATED,ESTABLISHED	-
0	0 B	syn_flood	tcp	*	*	::/0	::/0	tcp flags:0x17/0x02	-
435	31.32 KB	zone_lan_input	all	br-lan	*	::/0	::/0	-	-
5.62 K	292.91 KB	zone_wan_input	all	eth0	*	::/0	::/0	-	-

Chain *FORWARD* (Policy: *DROP*, 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
4	288 B	forwarding_rule	all	*	*	::/0	::/0	-	Custom forwarding rule chain
0	0 B	ACCEPT	all	*	*	::/0	::/0	ctstate RELATED,ESTABLISHED	-

Chain *FORWARD* (Policy: *ACCEPT*, 2394 Packets, 465.93 KB Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	TCPMSS	tcp	*	eth0	::/0	::/0	tcp flags:0x06/0x02 TCPMSS clamp to PMTU	Zone wan MTU fixing
0	0 B	TCPMSS	tcp	eth0	*	::/0	::/0	tcp flags:0x06/0x02 TCPMSS clamp to PMTU	Zone wan MTU fixing

Chain *qos_Default* (0 References)

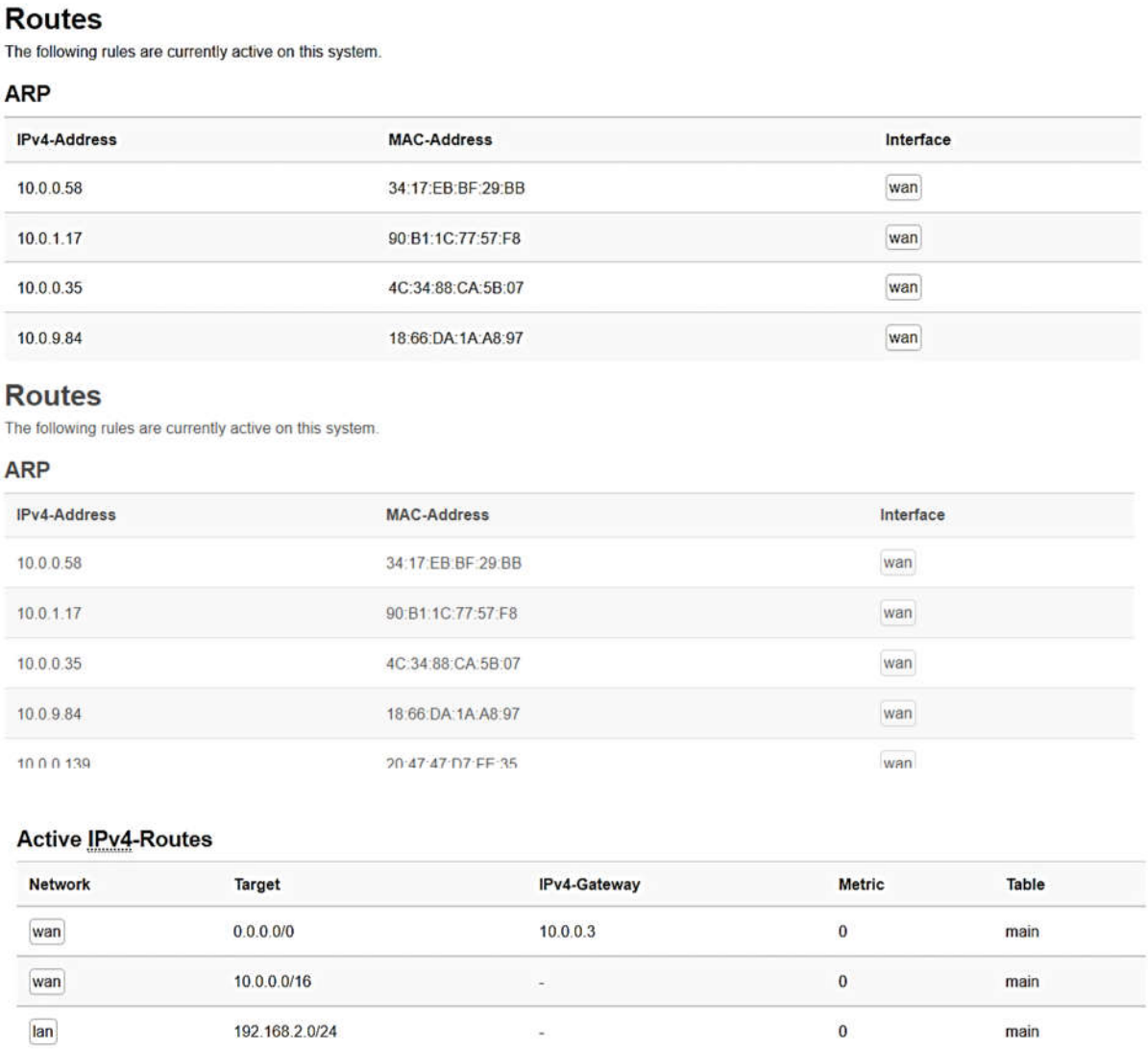
Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	CONNMARK	all	*	*	::/0	::/0	CONNMARK restore mask 0xf	-
0	0 B	qos_Default_ct	all	*	*	::/0	::/0	mark match 0x0/0xf	-
0	0 B	MARK	udp	*	*	::/0	::/0	mark match 0x0/0xf0 length 0:500 MARK xset 0x22/0xff	-
0	0 B	MARK	icmp	*	*	::/0	::/0	MARK xset 0x11/0xff	-
0	0 B	MARK	tcp	*	*	::/0	::/0	mark match 0x0/0xf0 tcp spts:1024:65535 dpts:1024:65535 MARK xset 0x44/0xff	-
0	0 B	MARK	udp	*	*	::/0	::/0	mark match 0x0/0xf0 udp spts:1024:65535 dpts:1024:65535 MARK xset 0x44/0xff	-
0	0 B	CONNMARK	all	*	*	::/0	::/0	CONNMARK save mask 0xff	-

Chain *qos_Default_ct* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	MARK	tcp	*	*	0.0.0.0/0	0.0.0.0/0	mark match 0x0/0xf tcp multiport ports 22,53 MARK xset 0x11/0xff	ssh, dns
0	0 B	MARK	udp	*	*	0.0.0.0/0	0.0.0.0/0	mark match 0x0/0xf udp multiport ports 22,53 MARK xset 0x11/0xff	ssh, dns
0	0 B	MARK	tcp	*	*	0.0.0.0/0	0.0.0.0/0	mark match 0x0/0xf tcp multiport ports 20,21,25,80,110,443,993,995 MARK xset 0x33/0xff	ftp, smtp, http(s), imap
0	0 B	CONNMARK	all	*	*	0.0.0.0/0	0.0.0.0/0	CONNMARK save mask 0xff	-

5.3 Status – Routes

The Routes status page shows the active routes. See the **Network/Static Routes** page to change route configuration.



Routes

The following rules are currently active on this system.

ARP

IPv4-Address	MAC-Address	Interface
10.0.0.58	34:17:EB:BF:29:BB	wan
10.0.1.17	90:B1:1C:77:57:F8	wan
10.0.0.35	4C:34:88:CA:5B:07	wan
10.0.9.84	18:66:DA:1A:A8:97	wan

Routes

The following rules are currently active on this system.

ARP

IPv4-Address	MAC-Address	Interface
10.0.0.58	34:17:EB:BF:29:BB	wan
10.0.1.17	90:B1:1C:77:57:F8	wan
10.0.0.35	4C:34:88:CA:5B:07	wan
10.0.9.84	18:66:DA:1A:A8:97	wan
10.0.0.139	20:47:47:D7:FF:35	wan

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric	Table
wan	0.0.0.0/0	10.0.0.3	0	main
wan	10.0.0.0/16	-	0	main
lan	192.168.2.0/24	-	0	main

IPv6 Neighbours

IPv6-Address	MAC-Address	Interface
fd13:1e2c:52ae:0:3c28:9487:8e8a:d1cc	A0:CE:C8:11:32:31	lan
fd13:1e2c:52ae:0:89b9:7cd4:8ecf:9304	D4:11:A3:8F:C0:05	lan

Active IPv6-Routes

Network	Target	Source	Metric	Table
lan	fd13:1e2c:52ae::/64	-	1024	main

5.4 Status – Network Status

The Network Status page shows a table of properties for both the wired and wireless interfaces. Columns for the wired interfaces include the interface name, link status, port speed, duplex, auto negotiation, and a list of the interfaces it is a member of.
Columns for the wireless interfaces include the interface name, the operating mode of the interface, the bandwidth of the interface, the channel the interface is operating on, the security mode of the interface, and and a list of the interfaces it is a member of.

Status->Network Status

Network Interface Status

Wired

Interface	Link	Speed	Duplex	Auto Negotiation	Member of
eth0	Up	1000Mb/s	Full	On	WAN WAN6
eth1	Up	1000Mb/s	Full	On	LAN
eth2	Down	Unknown	Unknown	On	LAN
eth3	Down	Unknown	Unknown	On	LAN
eth4	Down	Unknown	Unknown	On	LAN

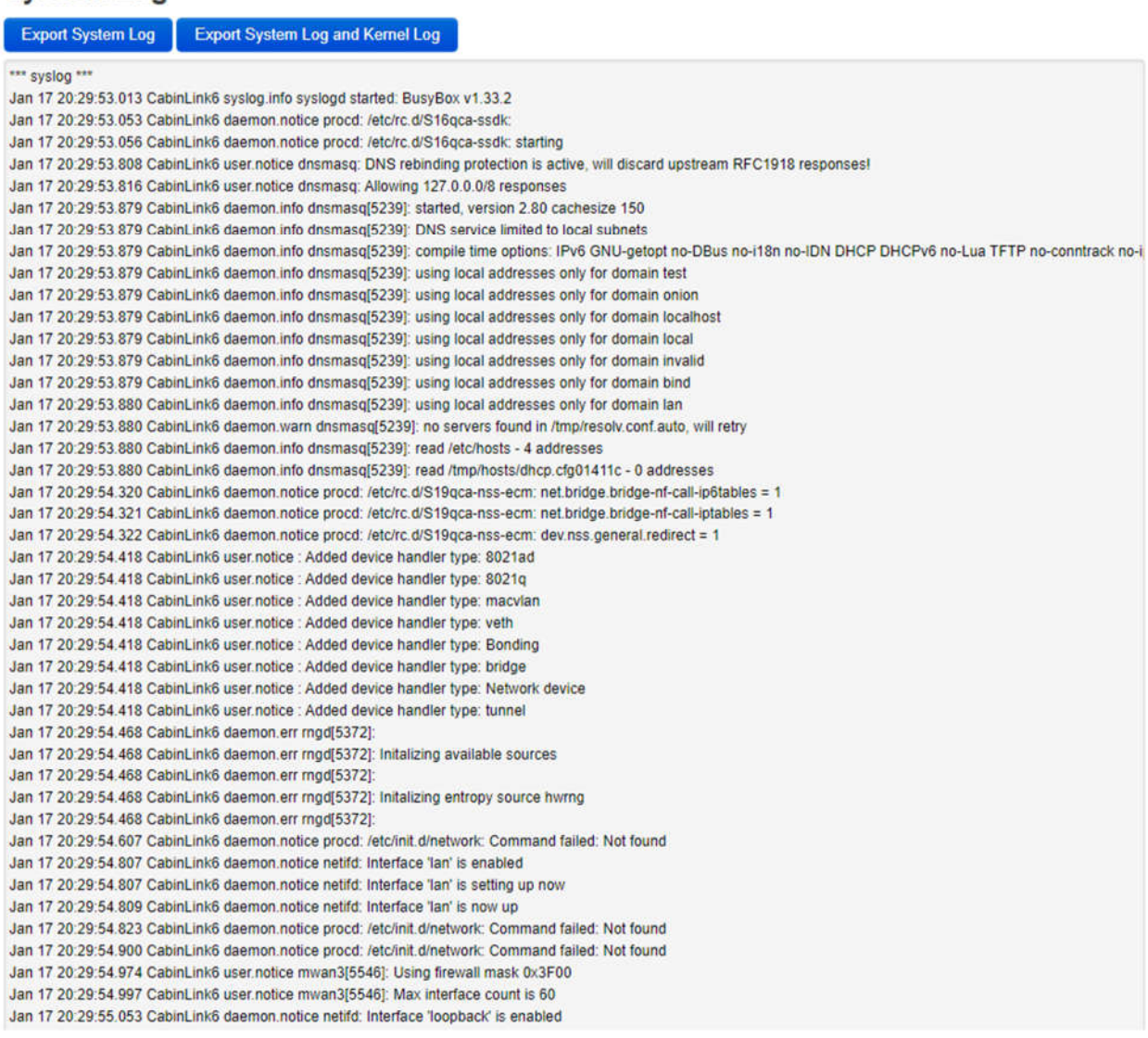
Wireless

Interface	Mode	Bandwidth	Channel	Security	Member of
ath0 (rw-RHT-WiFi6axa)	802.11axa	80 MHz	36	WPA2/WPA3 Mixed Mode	LAN
ath1 (rw-RHT-WiFi6axg)	802.11axg	40 MHz	6	WPA2/WPA3 Mixed Mode	LAN

5.5 Status – System Log

The System Log page shows log activity. The buttons at the top of the page can be used to download the system log or download both the system log and the kernel log.

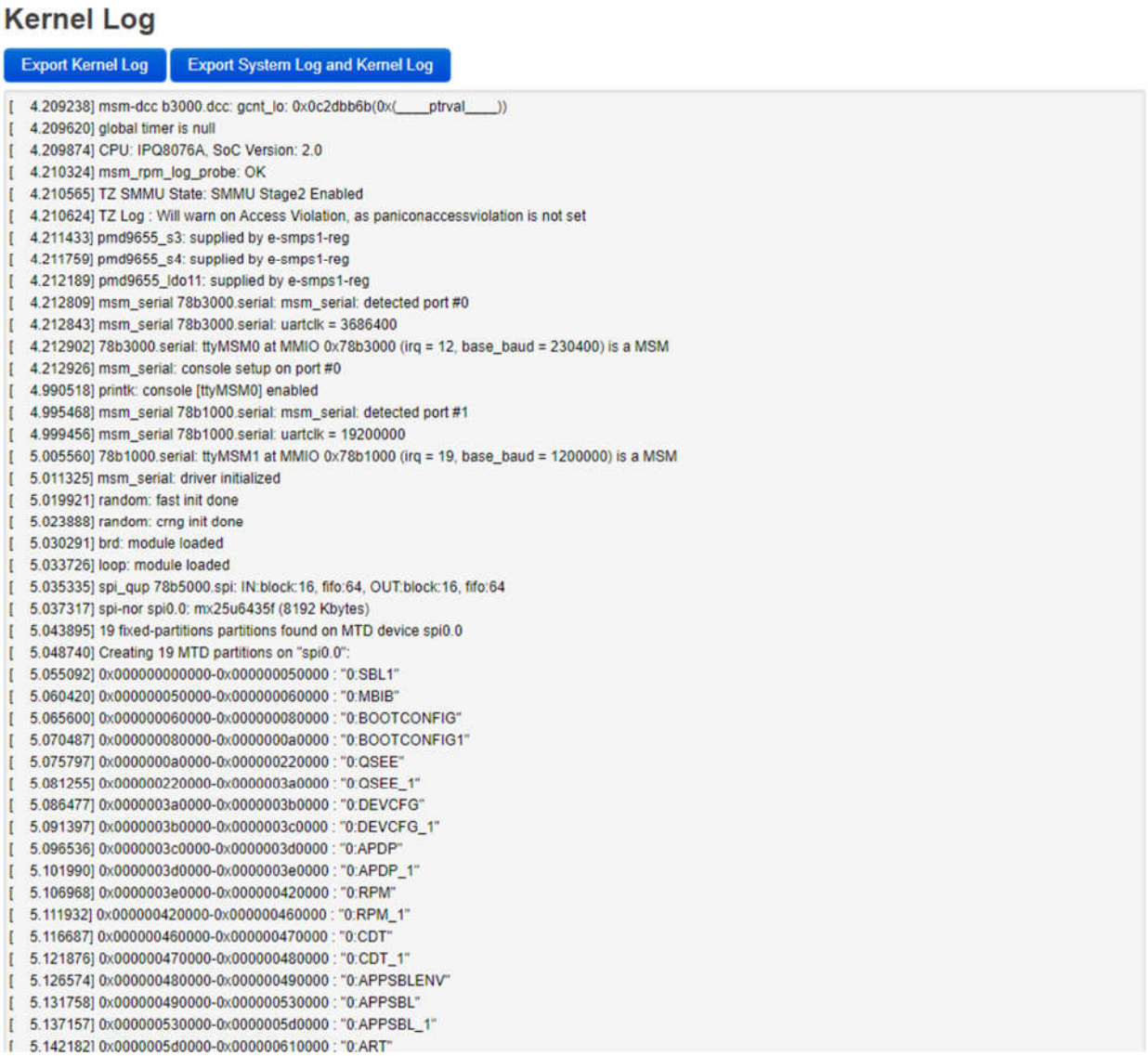
Status->System Log



5.6 Status – Kernel Log

The Kernel Log page shows the output of the kernel ring buffer. The buttons at the top of the page can be used to download the kernel log or download both the system log and the kernel log.

Status->Kernel Log

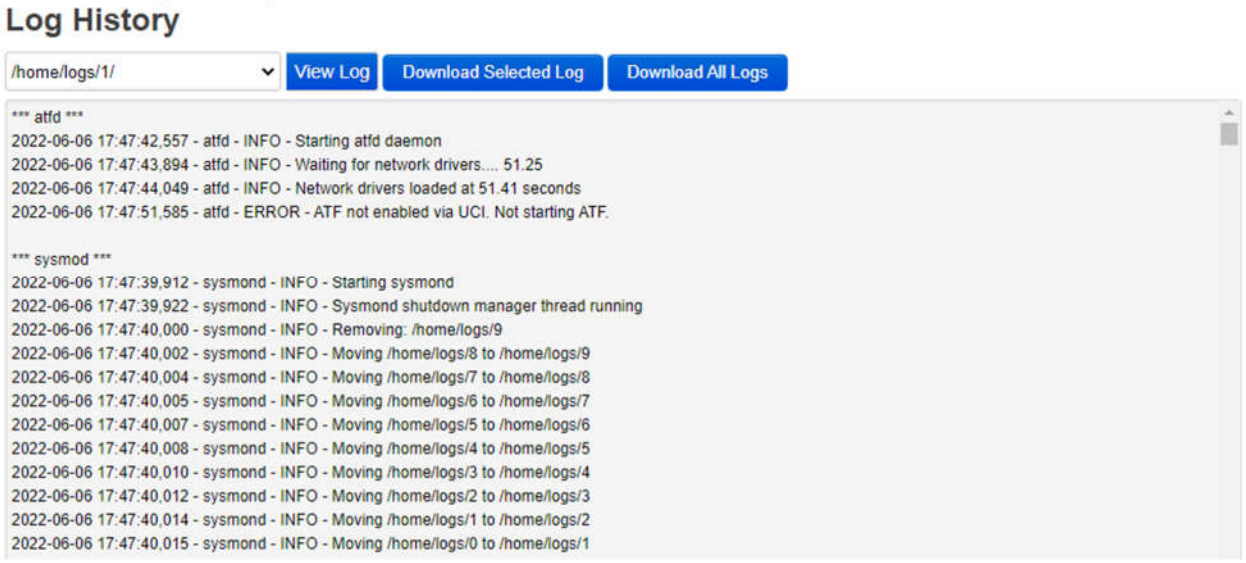


5.7 Status – Log History

The Log History page allows you to view the logs from the last 9 reboots. Open the dropdown to select which log you want to view/download. /home/logs/1/ will show you the logs from one reboot ago, while /home/logs/9/ will show you the logs from 9 reboots ago. Clicking the View

Log button will display the contents of the selected log directory on the screen. Download Selected Log will download a compressed tarball of the log selected in the dropdown. Download All Logs will download a compressed tarball of all the logs in the /home/logs/ directory.

Status->Log History



5.8 Status – System Health

The System Health page displays temperature and voltage states. Temperature columns include the temperature sensor name, the current temperature, the low temperature limit, the low fault state, the high temperature limit, the high fault state, and the sensor fault state.

Status->System Health

System Health

Temperatures

Sensor	Temp (°C)	Low Limit (°C)	Low Fault	High Limit (°C)	High Fault	Sensor Fault
NSS top	63	-35	False	110	False	False
NSS UBI32_0	63	-35	False	110	False	False
NSS UBI32_1	64	-35	False	110	False	False
WCSS PHYA_0	63	-35	False	110	False	False
WCSS PHYA_1	62	-35	False	110	False	False
A53 core0	64	-35	False	110	False	False
A53 core1	63	-35	False	110	False	False
A53 core2	63	-35	False	110	False	False
A53 core3	63	-35	False	110	False	False
A53 MHM	64	-35	False	110	False	False
WCSS PHYB	63	-35	False	110	False	False
WCSS PHYA_2	62	-35	False	110	False	False
se98a	44	-35	False	100	False	False
ucd90124a 0x68	36	-35	False	100	False	False
ucd90124a 0x69	30	-35	False	100	False	False
ltc3350	56	-35	False	100	False	False

Rail Voltage columns include the rail name, the current voltage, the nominal voltage, the under voltage limit, the under voltage fault state, the over voltage limit, the over voltage fault state, and the sensor fault state.

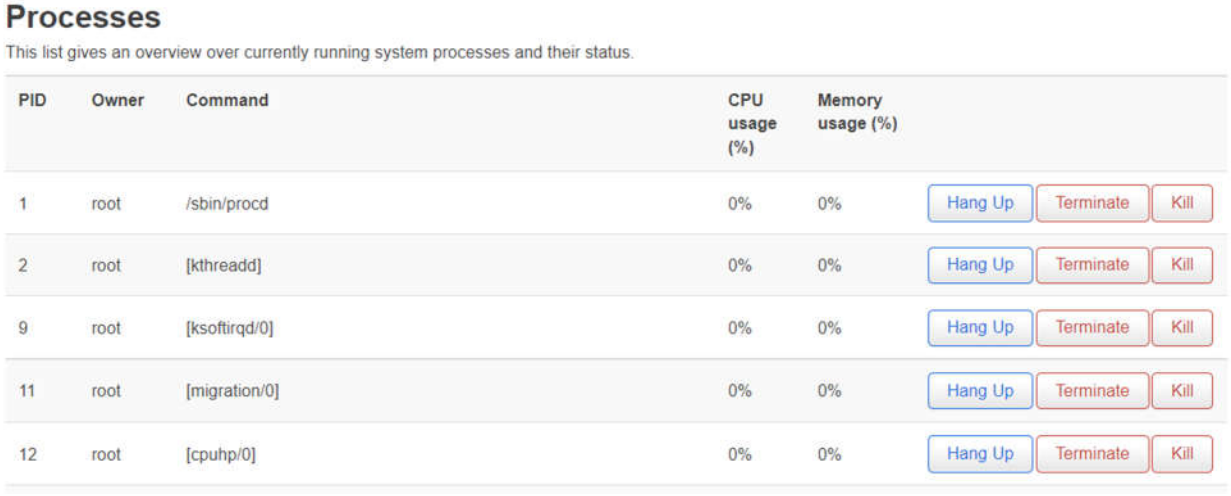
Rail Voltages

Rail	Voltage	Nominal	Under Voltage Limit	Under Voltage Fault	Over Voltage Limit	Over Voltage Fault	Sensor Fault
12V_IN	11.829	12.000	10.200	False	13.800	False	False
VDD_3V3_PMIC	3.306	3.300	2.805	False	3.795	False	False
VDD_1V4_LDO_IN	1.324	1.400	1.190	False	1.610	False	False
VDD_1V9_PMIC	1.893	1.900	1.615	False	2.185	False	False
AVDD_2G_FEM	4.941	5.000	4.250	False	5.750	False	False
AVDDA_5GS_FEM	4.913	5.000	4.250	False	5.750	False	False
VDD33_PCIE1	3.315	3.300	2.805	False	3.795	False	False
P_SCAP	9.141	9.200	7.820	False	10.580	False	False
12V_SCAP	11.702	12.000	10.200	False	13.800	False	False
VDD_2P2_LDO	2.191	2.200	1.870	False	2.530	False	False
P28V0A	27.105	28.000	23.801	False	32.199	False	False
VDD_WCSS_CX	0.781	0.788	0.670	False	0.906	False	False
VDD_APC_CX	0.676	0.828	0.500	False	1.200	False	False
VDD105_NAPA	1.048	1.050	0.893	False	1.208	False	False
VDD1V8_NAPA	1.782	1.800	1.530	False	2.070	False	False
VDD_0V85_LDO2	0.843	0.850	0.722	False	0.977	False	False
VDD_0V925_LDO4	0.917	0.925	0.786	False	1.064	False	False
VDD_1V8_LDO6	1.786	1.800	1.530	False	2.070	False	False
VDD18_IRON	1.794	1.800	1.530	False	2.070	False	False
VDD1V05_IRON	1.040	1.050	0.893	False	1.208	False	False
VDD_SOC_MX	0.936	0.920	0.782	False	1.058	False	False

5.9 Status – Processes

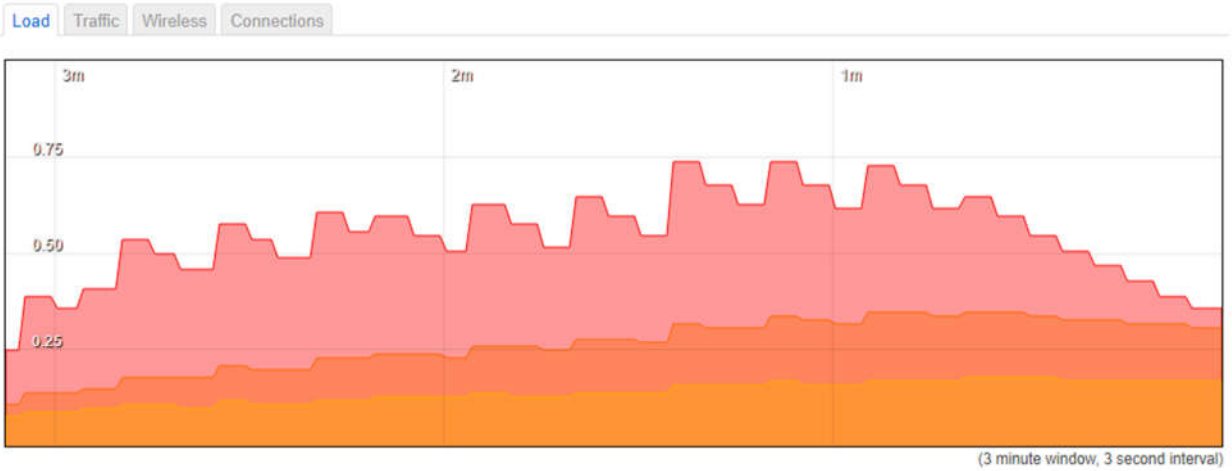
The Processes page shows the active processes currently running on the status. It allows the user to terminate or kill an active process.

Status->Processes



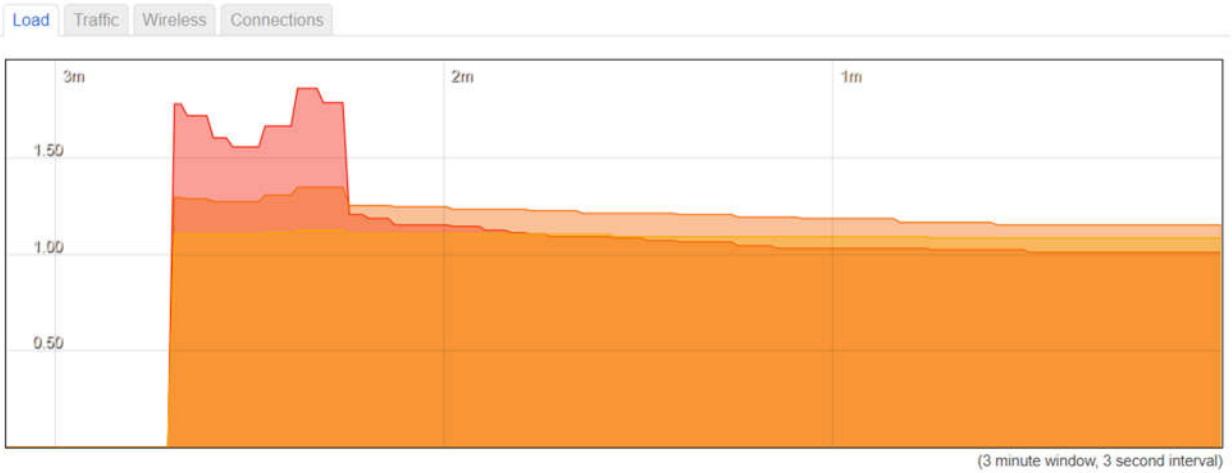
5.10 Status – Realtime Graphs

The Realtime Graphs pages show the traffic load for current configurations over time.



Load represents CPU over or under-utilization in a Linux system. An idle system will have a load of 0, while an overloaded system will have a load greater than 4.0.

1 Minute Load:	0.36	Average:	0.56	Peak:	0.74
5 Minute Load:	0.31	Average:	0.27	Peak:	0.35
15 Minute Load:	0.17	Average:	0.14	Peak:	0.18



1 Minute Load:	1.02	Average:	1.17	Peak:	1.86
5 Minute Load:	1.16	Average:	1.21	Peak:	1.35
15 Minute Load:	1.09	Average:	1.10	Peak:	1.13