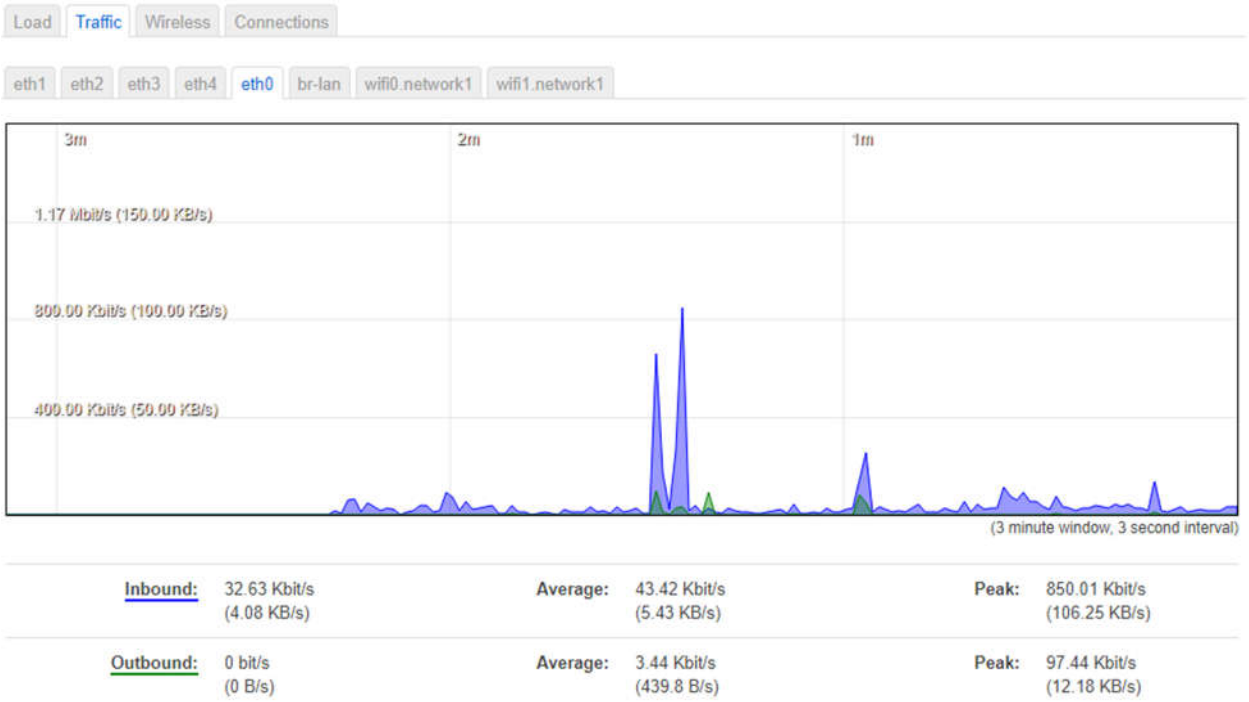
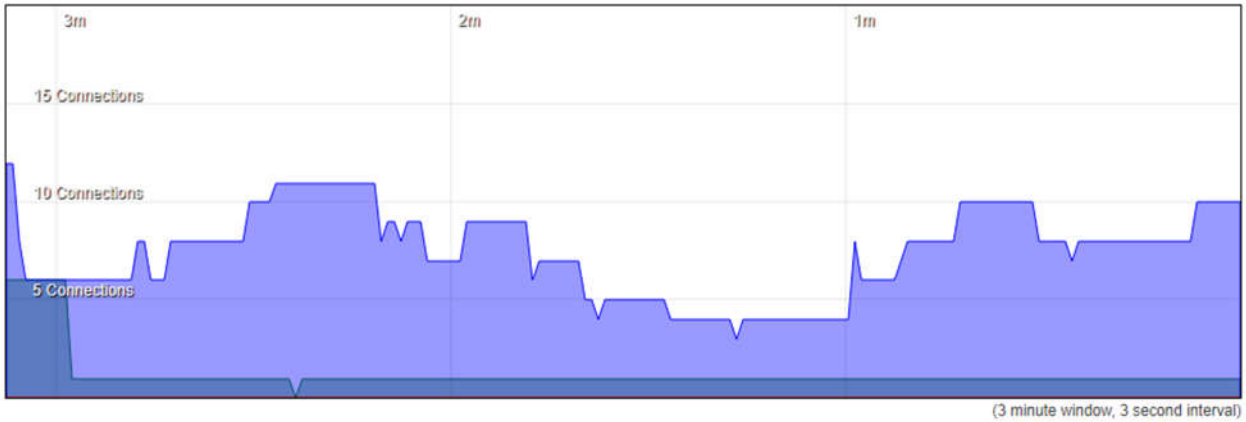

Load
Traffic
Wireless
Connections
eth1
eth2
eth3
eth4
eth0
br-lan
wifi0.network1
wifi1.network1
3m
2m
1m
1.17 Mbit/s (150.00 KB/s)
800.00 Kbit/s (100.00 KB/s)
400.00 Kbit/s (50.00 KB/s)
(3 minute window, 3 second interval)
Inbound: 32.63 Kbit/s (4.08 KB/s)
Average: 43.42 Kbit/s (5.43 KB/s)
Peak: 850.01 Kbit/s (106.25 KB/s)
Outbound: 0 bit/s (0 B/s)
Average: 3.44 Kbit/s (439.8 B/s)
Peak: 97.44 Kbit/s (12.18 KB/s)

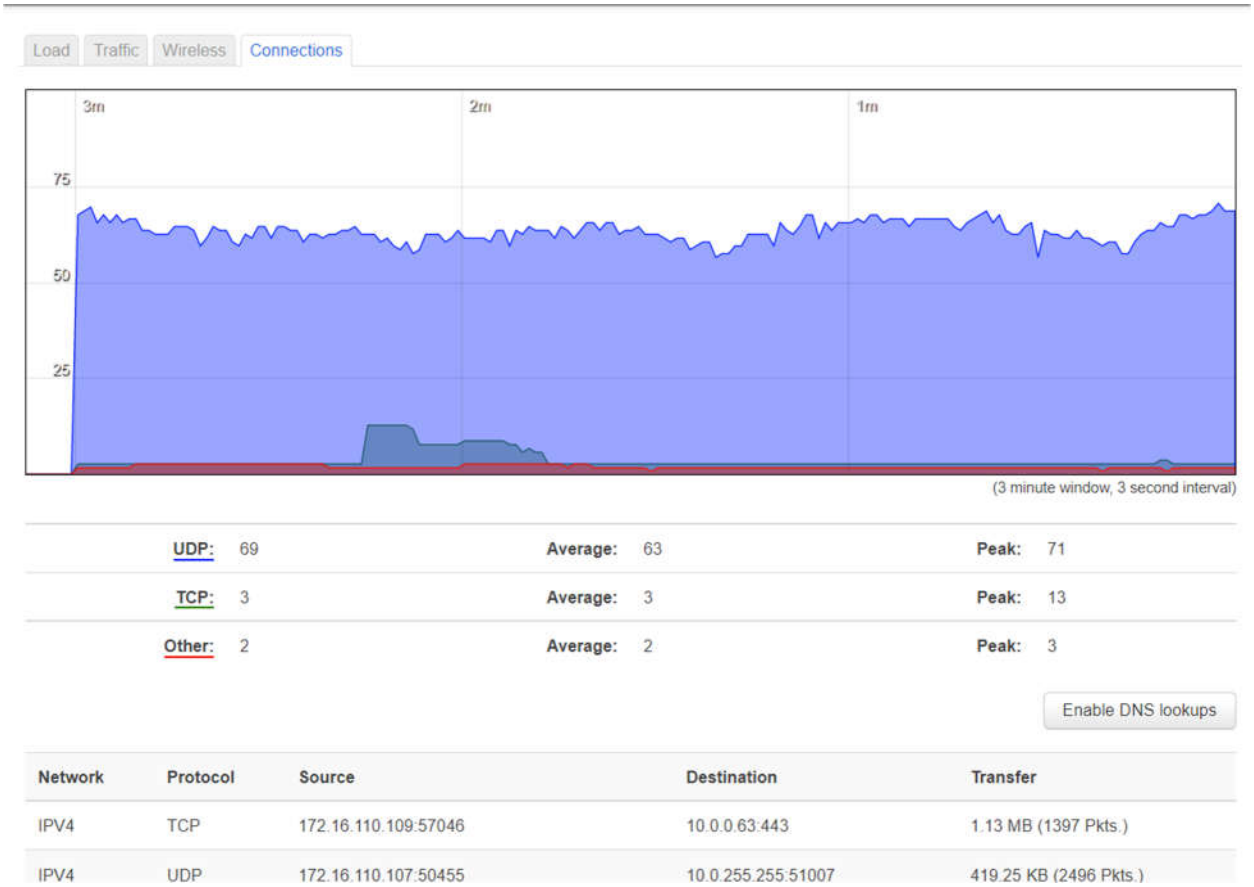


(3 minute window, 3 second interval)

UDP Connections:	10	Average:	7	Peak:	12
TCP Connections:	1	Average:	1	Peak:	6
Other Connections:	0	Average:	0	Peak:	0

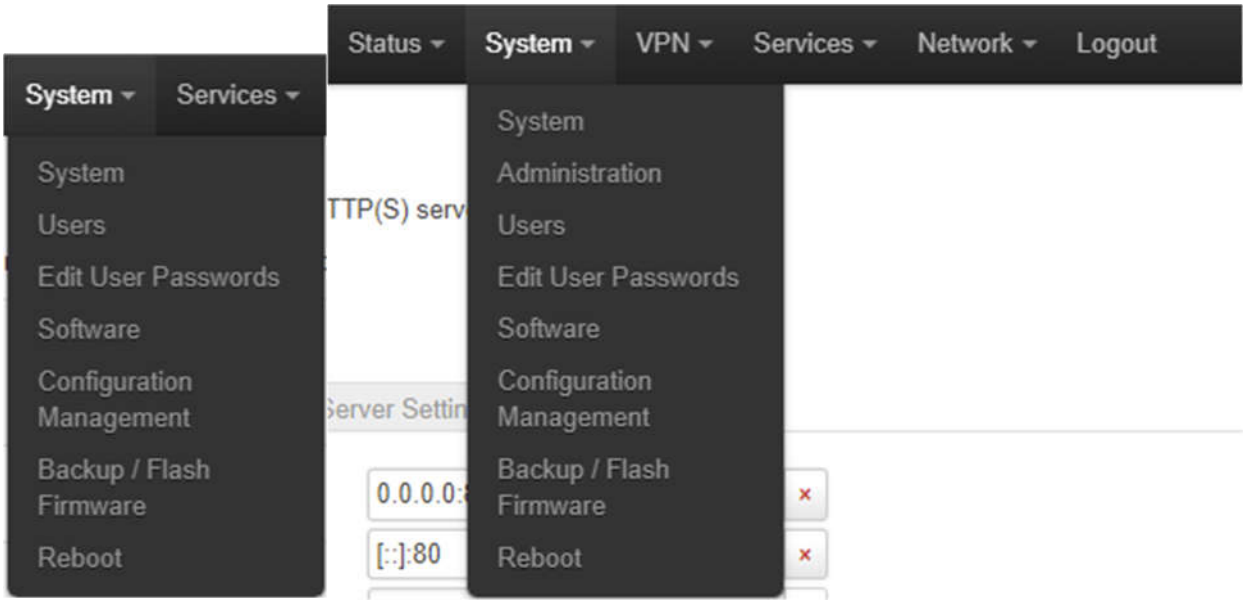
Enable DNS lookups

Network	Protocol	Source	Destination	Transfer
IPV4	TCP	192.168.2.194:52149	192.168.2.1:443	814.27 KB (1265 Pkts.)
IPV4	UDP	192.168.2.194:60348	239.255.255.250:1900	812 B (4 Pkts.)


Load
Traffic
Wireless
Connections
3m
2m
1m
75
50
25
(3 minute window, 3 second interval)
UDP: 69 Average: 63 Peak: 71
TCP: 3 Average: 3 Peak: 13
Other: 2 Average: 2 Peak: 3
Enable DNS lookups
Network Protocol Source Destination Transfer
IPV4 TCP 172.16.110.109:57046 10.0.0.63:443 1.13 MB (1397 Pkts.)
IPV4 UDP 172.16.110.107:50455 10.0.255.255:51007 419.25 KB (2496 Pkts.)

6. System

The System dropdown will show the following configuration pages.



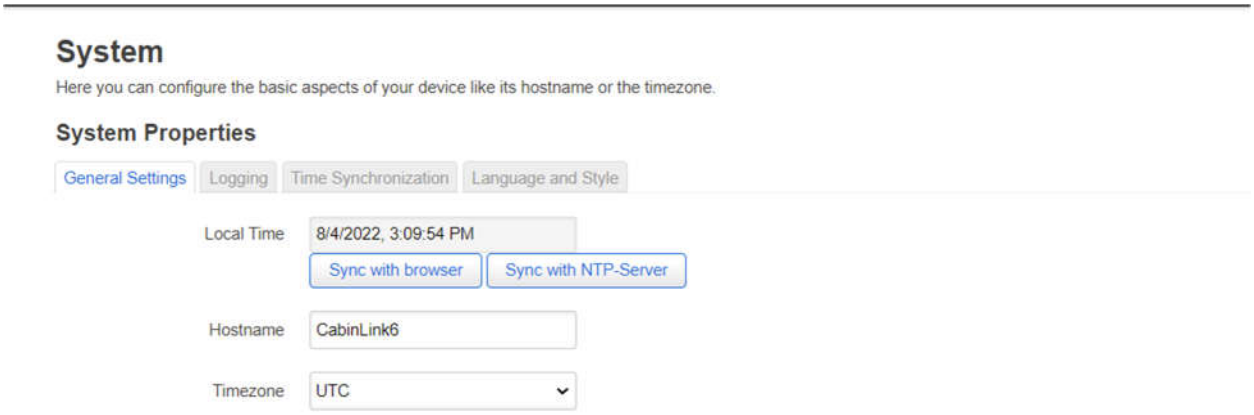
- **System** – Setting of system properties such as time, host name, logfile initialization, and language
- **Users** – Members of the "users" group on a system. To create a new group or add a new user to additional groups, modify the /etc/group file.
- **Edit User Passwords** – Configure user and root passwords
- **Software** – Manage installed software packages
- **Configuration Management** – Manage installed configurations
- **Backup/Flash Firmware** – Install new firmware, backup and restore
- **Reboot** – Reboot system

6.1 System – System

Configure the basic aspects of the CabinLink 6.

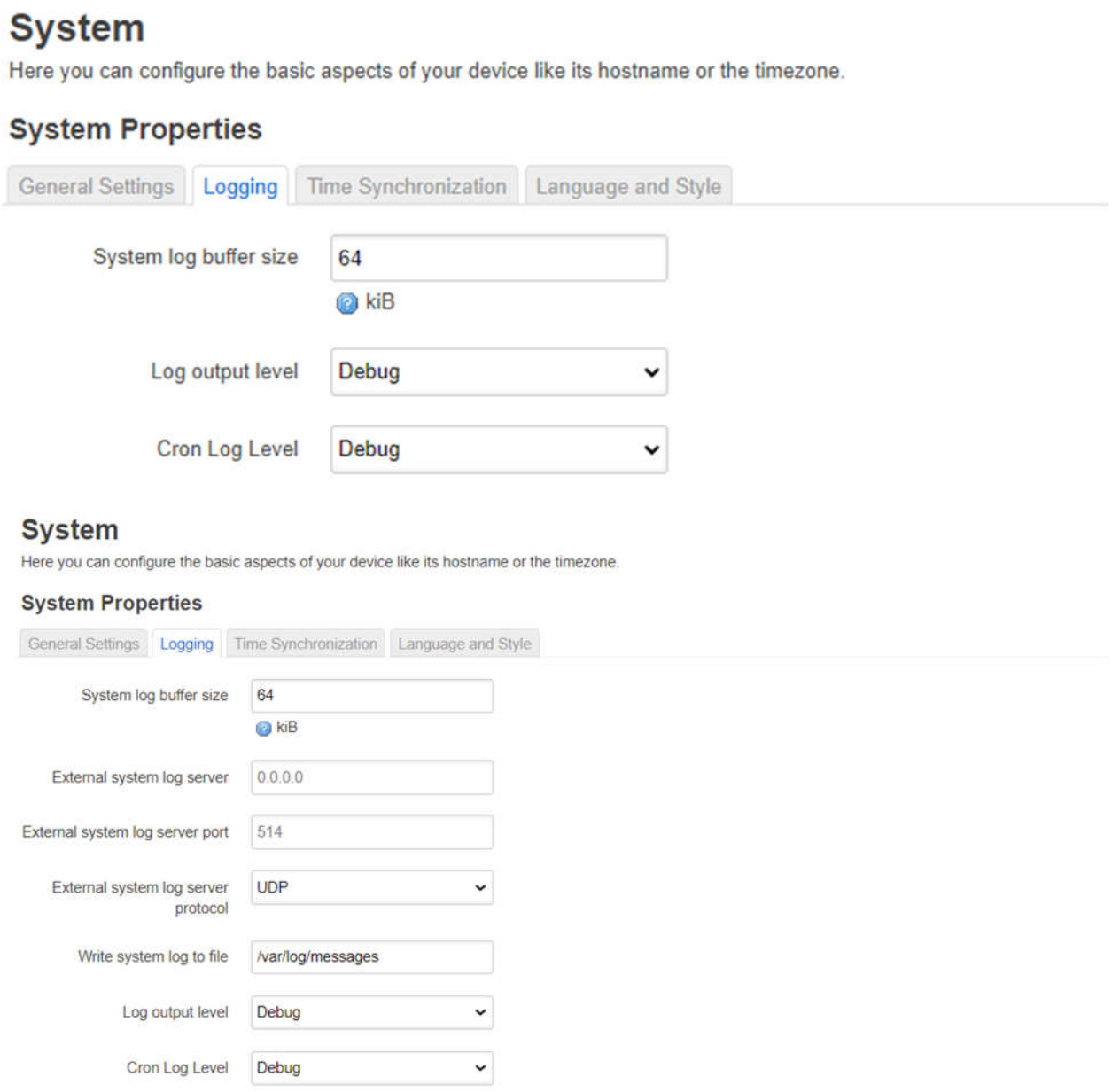
6.1.1 System – System – General Settings

The **System Properties/General Settings** screen below allows the user to set the time sync methods and the time zone of the installed units. If the Sync with NTP-server is set, then the Time Synchronization tab must be configured.



6.1.2 System – System – Logging

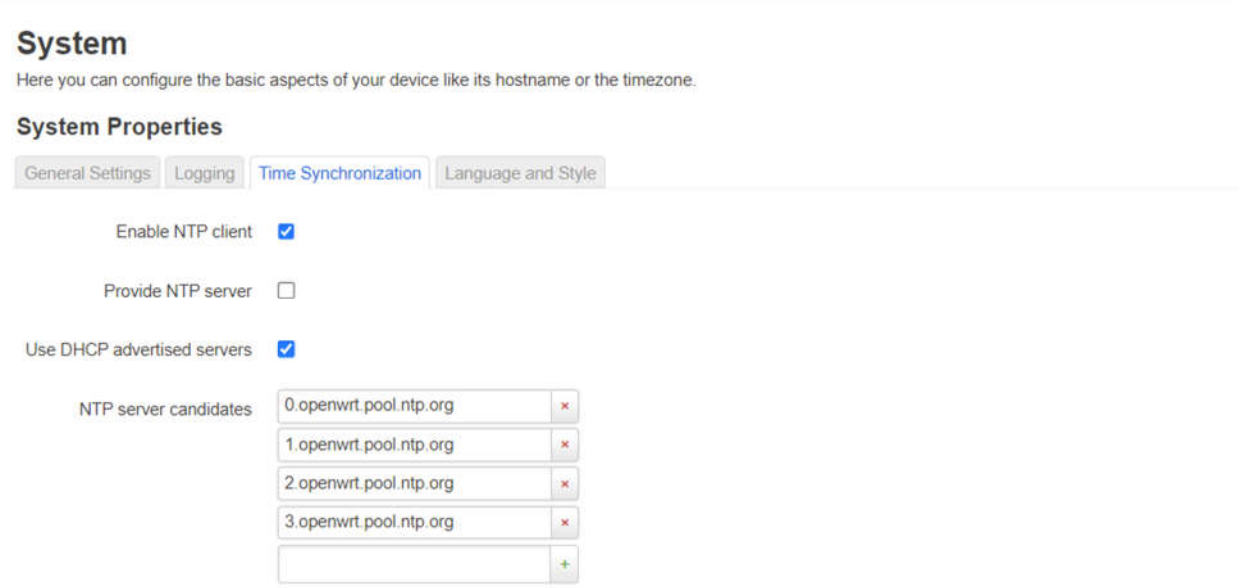
The **System Properties/Logging** screen below allows the user to set the parameters for the log files.



Log output level: The minimum level for kernel messages to be logged to the kernel log. Only messages with a log level lower than the option selected will be logged. Dropdown options include Debug, Info, Notice, Warning, Error, Critical, Alert, and Emergency.

6.1.3 System – System – Time Synchronization

The **System Properties/Time Synchronization** screen below allows the user to configure network time protocol server. You can configure the system clock manually or configure the device to use a Network Time Protocol (NTP) client.



Enable NTP client: If checked, the CL6 will acquire the time setting from the configured NTP server(s).

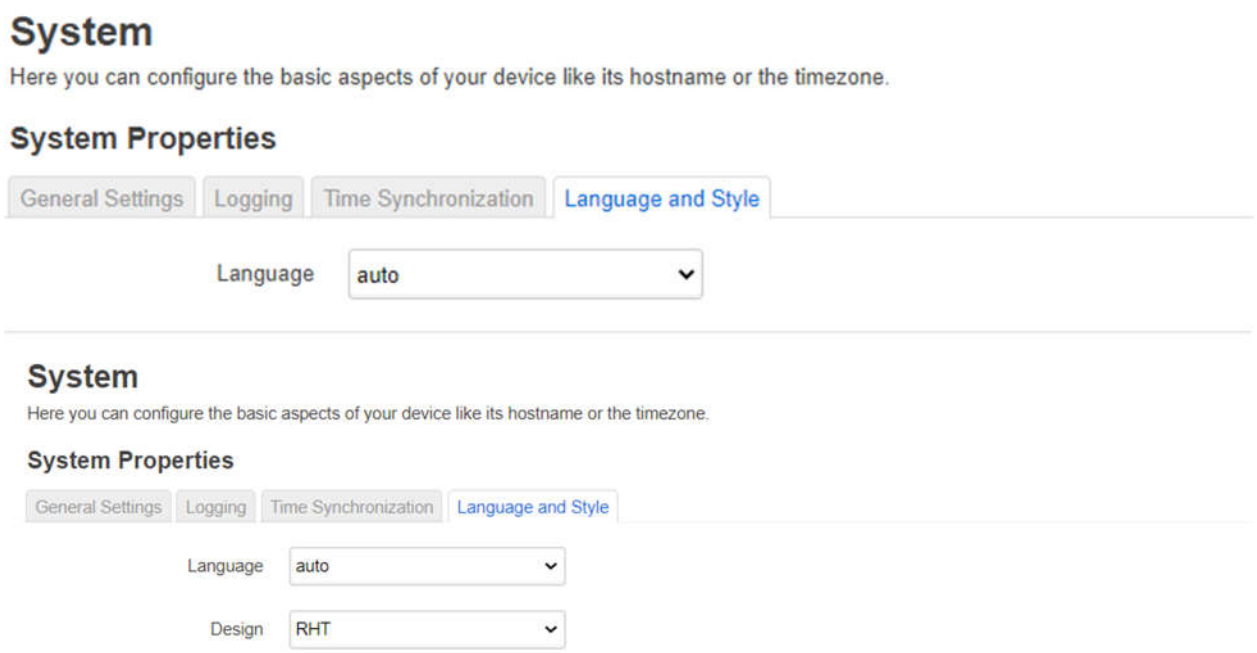
Provide NTP server: If checked, the CL6 will enable the NTP server and enable time serving.

Use DHCP advertised server: If checked, the CL6 will allow the use of DHCP-provided NTP servers.

NTP server candidates: Host name of servers potentially available to act as NTP server.

6.1.4 System – System – Language and Style

The **System Properties/Language and Style** screen below allows the user to configure the language of the user interface screens.



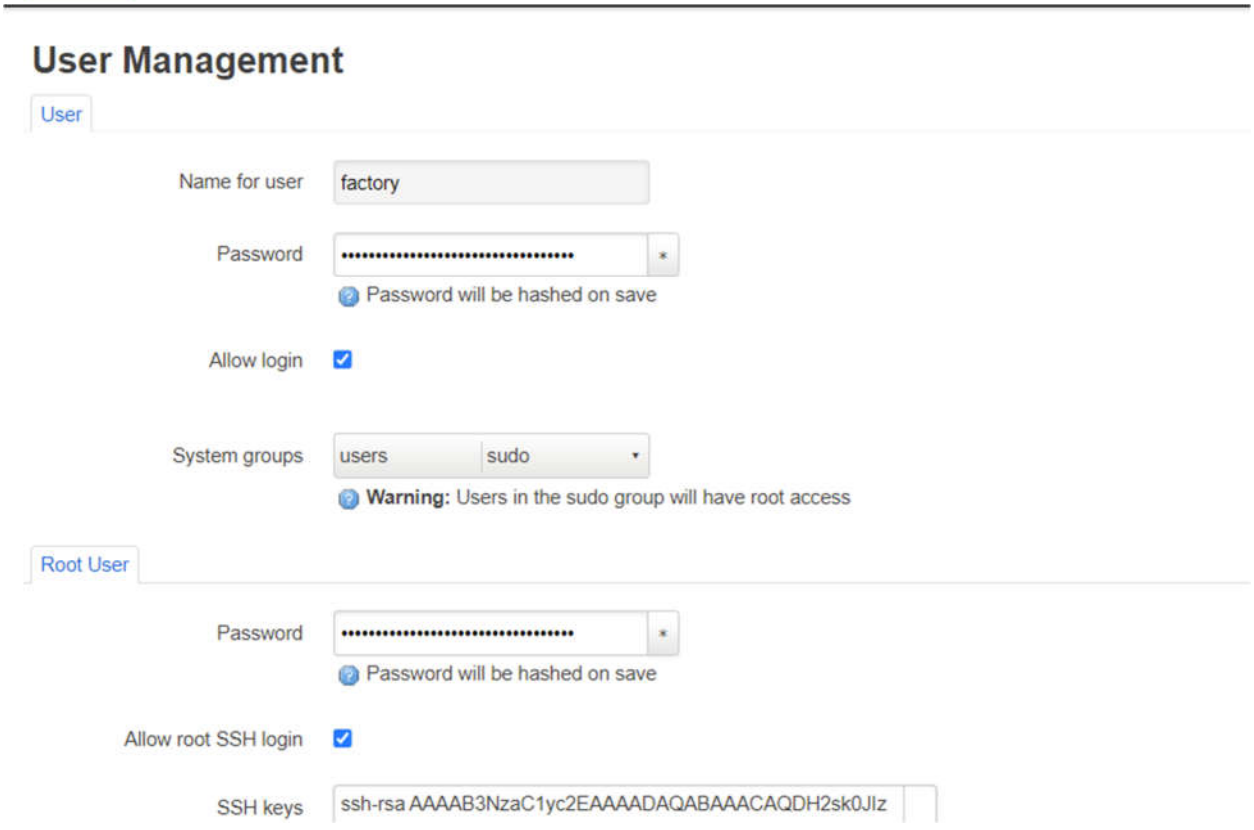
Language: Dropdown options include auto.

6.2 System – Users

The Users screen allows for the configuration of the 'root' and other user accounts via the GUI. The 'root' user configuration options include changing the password (which also changes the GUI login) and adding/removing SSH keys for passwordless access by trusted computers. The user configuration allows an administrator to add and delete user accounts, while configuring login access, passwords and user group memberships. User passwords are stored as one-way hashes, meaning that no plain text passwords are saved on the system.

6.2.1 System – Users – User

System->Users->User



Name for user: Username to give the User. Username must start with a lowercase letter or underscore. This can be followed by 0 to 31 characters that are letters, numbers, underscores, and hyphens. The last character in the username may also be "$". The username "logs" is not allowed.

Password: Password to give the User

Allow login: Allow this user to login via console.

System groups: List of system groups to add the user to. Dropdown options include root, daemon, adm, mail, dialout, audio, www-data, ftp, users, network, ntp, dnsmasq, lldp, sshd and sudo. It is important to be wary of adding users to the sudo group as they will gain root access.

Add User: Display a set of blank fields for the configuration of a new user.

Delete: Deletes the user configured below the delete button.

6.2.2 System – Users – Root User

System->Users->Root User

Password: Password for root user. This also sets the password for GUI access. After clicking Save & Apply, the password is instantly configured.

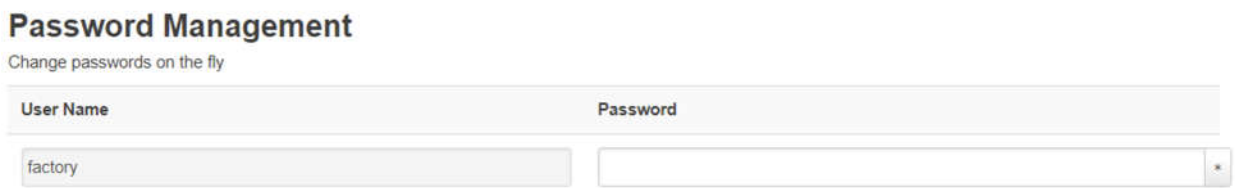
Allow root SSH login: Allow the root user to login via SSH.

SSH keys: Provide one or more authorized SSH keys to use when logging in via SSH.

6.3 System – Edit User Passwords

The Edit User Passwords screen facilitates changing passwords.

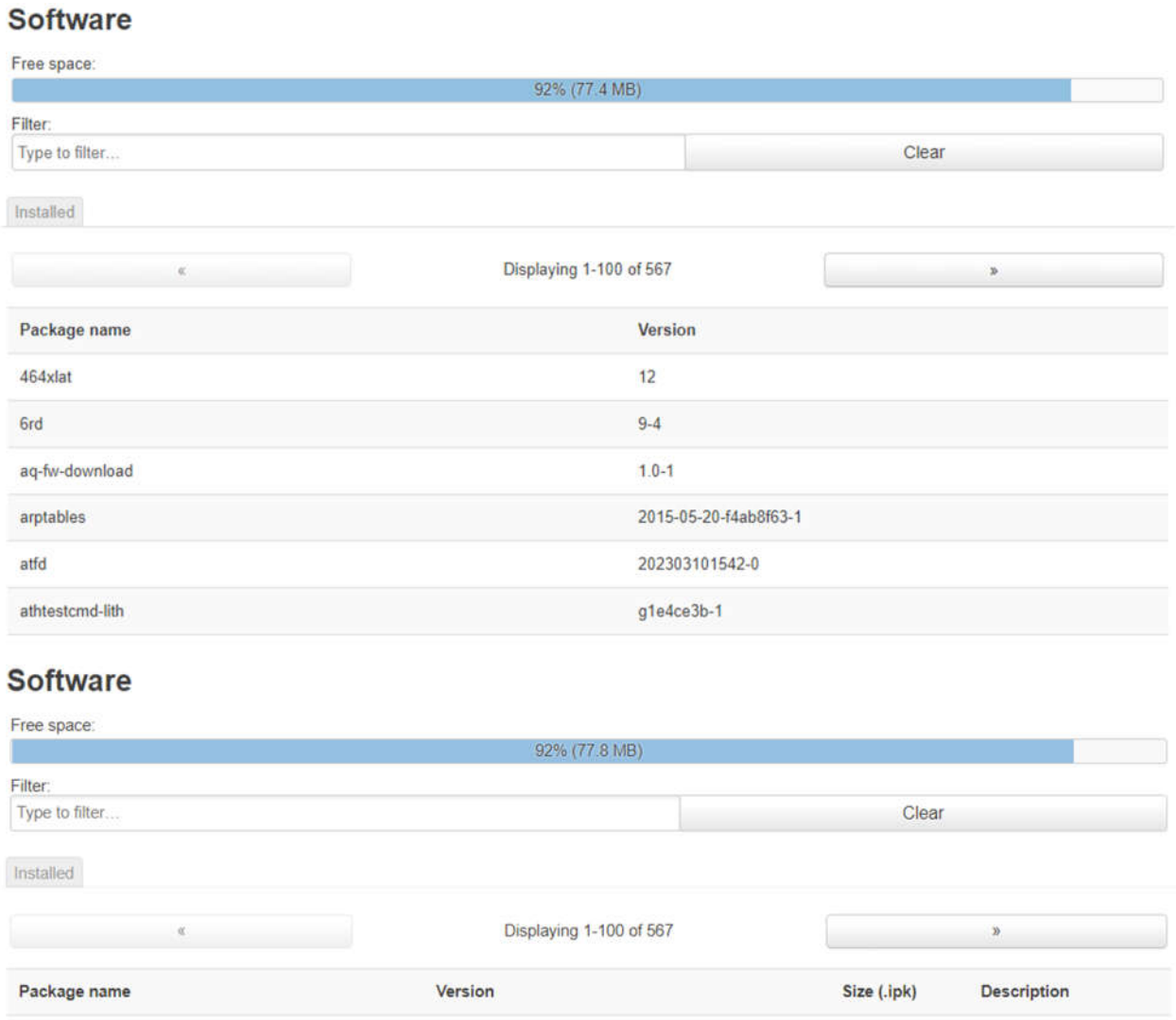
System->Edit User Passwords



6.4 System – Software

The Software screen allows the user to see how much free space is available, which packages are installed, and their version.

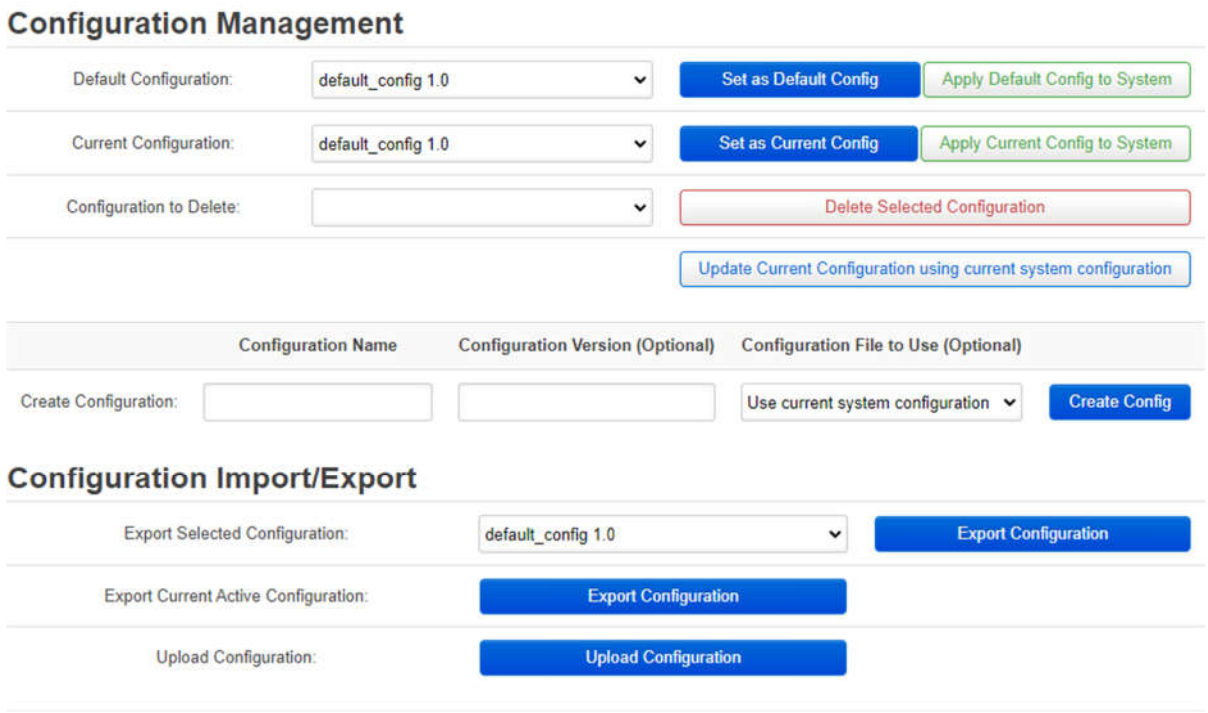
System->Software



6.5 System – Configuration Management

The Configuration Management screen allows the user to create, update, delete, set, and apply configuration files, these files contain the CL6 configuration information. It also allows users to export and upload their configurations. When loading a configuration with no root password, it is highly recommended to configure one in System->Users. When loading a configuration with a root password set, the password will not be applied until the CL6 is rebooted.

System->Configuration Management



Configuration Management

Default Configuration: The default system configuration

Set as Default Config: Set the selected configuration as the default configuration. This is the configuration that is loaded when performing a system reset.

Apply Default Config to System: Applies the default configuration to the system. You may lose connectivity to the GUI if the IP address in the configuration is different than the IP address currently being used.

Current Configuration: The configuration that is currently applied to the system

Set as Current Config: Set the selected configuration as the current configuration

Apply Current Config to System: Applies the current configuration to the system. You may lose connectivity to the GUI if the IP address in the configuration is different than the IP address currently being used.

Delete Selected Configuration: Delete the configuration that is selected in the "Configuration to Delete" dropdown. This will delete the configuration from the CL6 filesystem and is irreversible.

Update Current Configuration using current system configuration: This will update the Current Configuration with any changes made via the GUI or UCI.

Create Configuration: Create a new configuration file.

Configuration Name: Provide a name for the configuration (no spaces)

Configuration Version: Provide a version to give the configuration. If you are creating a configuration from an existing configuration with a version already defined, a new/different version number should be used.

Configuration File to Use: Either use the current system configuration or one of the existing configurations to create your new configuration.

Create Config: Create the new configuration file and save it to the CL6.

Configuration Import/Export

Export Selected Configuration: Download the selected configuration to the computer accessing the GUI

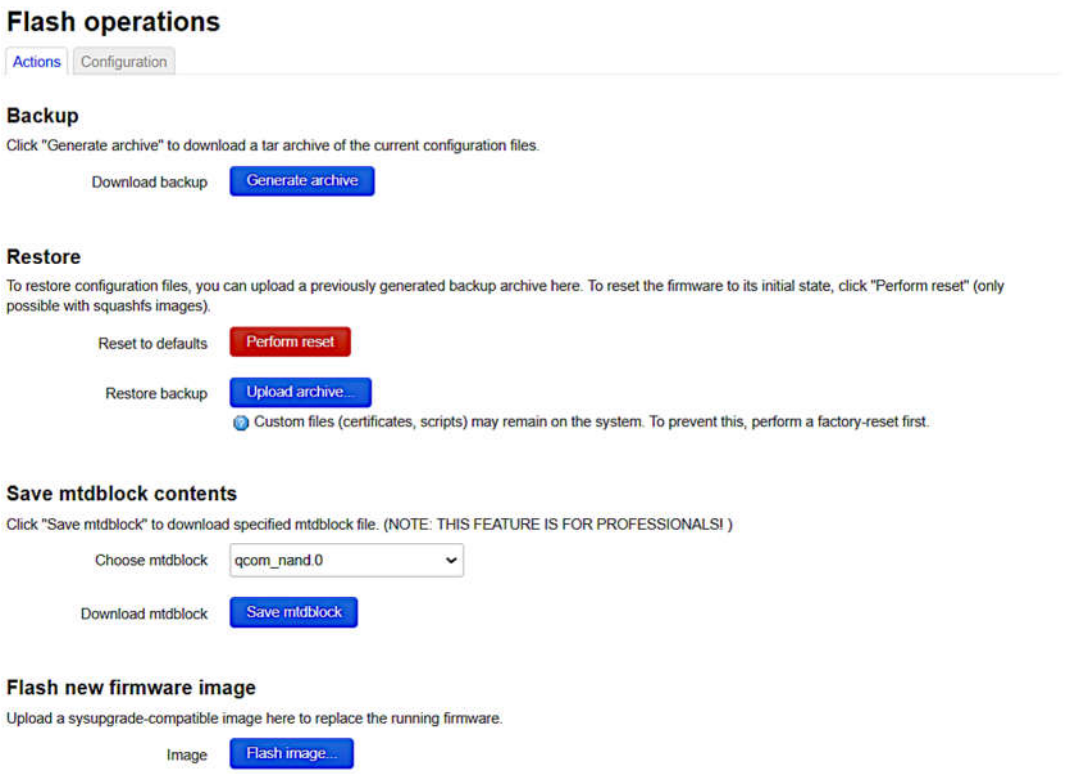
Export Current Active Configuration: Download the configuration actively being used by the CL6

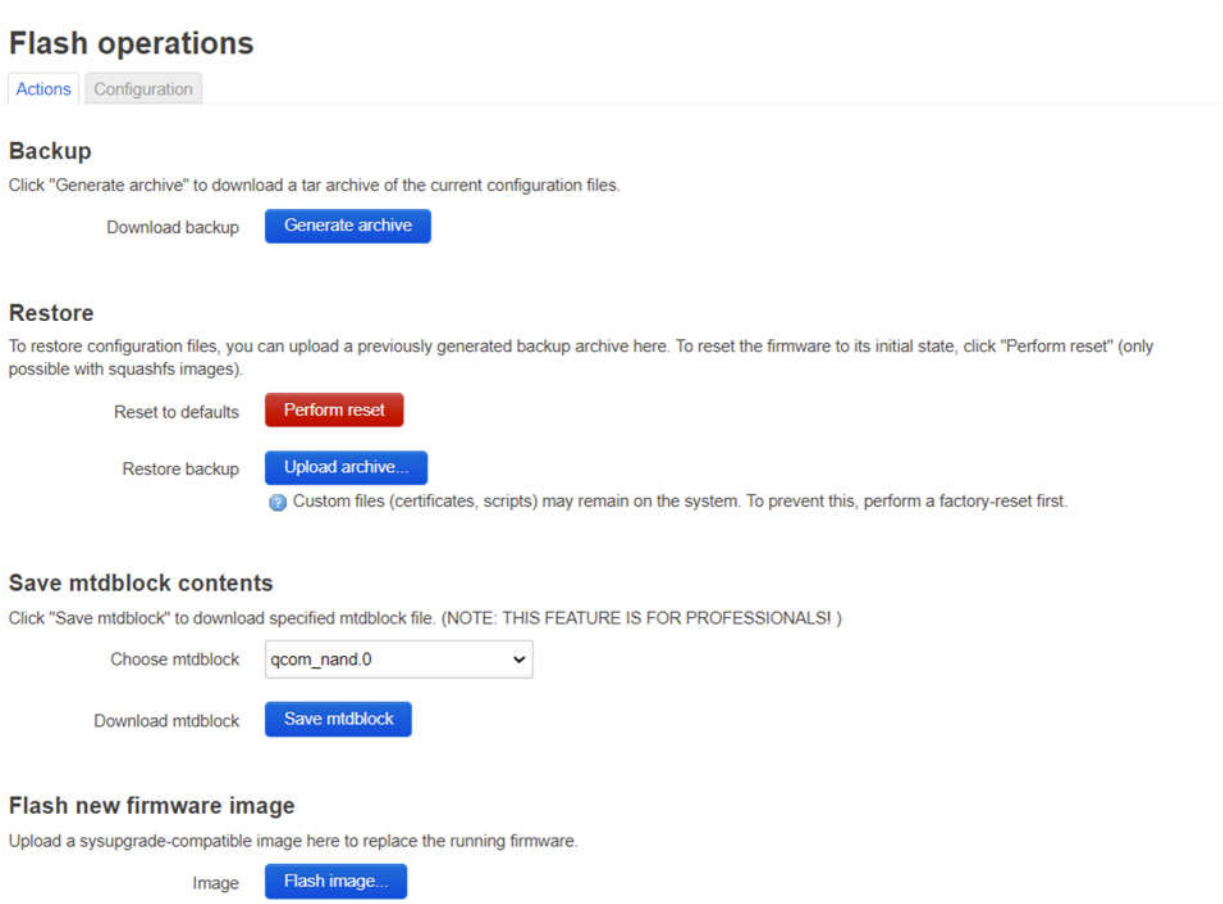
Upload Configuration: Upload a configuration file to the CL6. This should be in the same format as existing configurations on the CL6.

6.6 System – Backup/Flash Firmware

The **Backup/Flash Firmware/Actions** screen allows the user to backup, restore and upgrade the CabinLink 6 firmware.

6.6.1 System – Backup/Flash Firmware – Actions





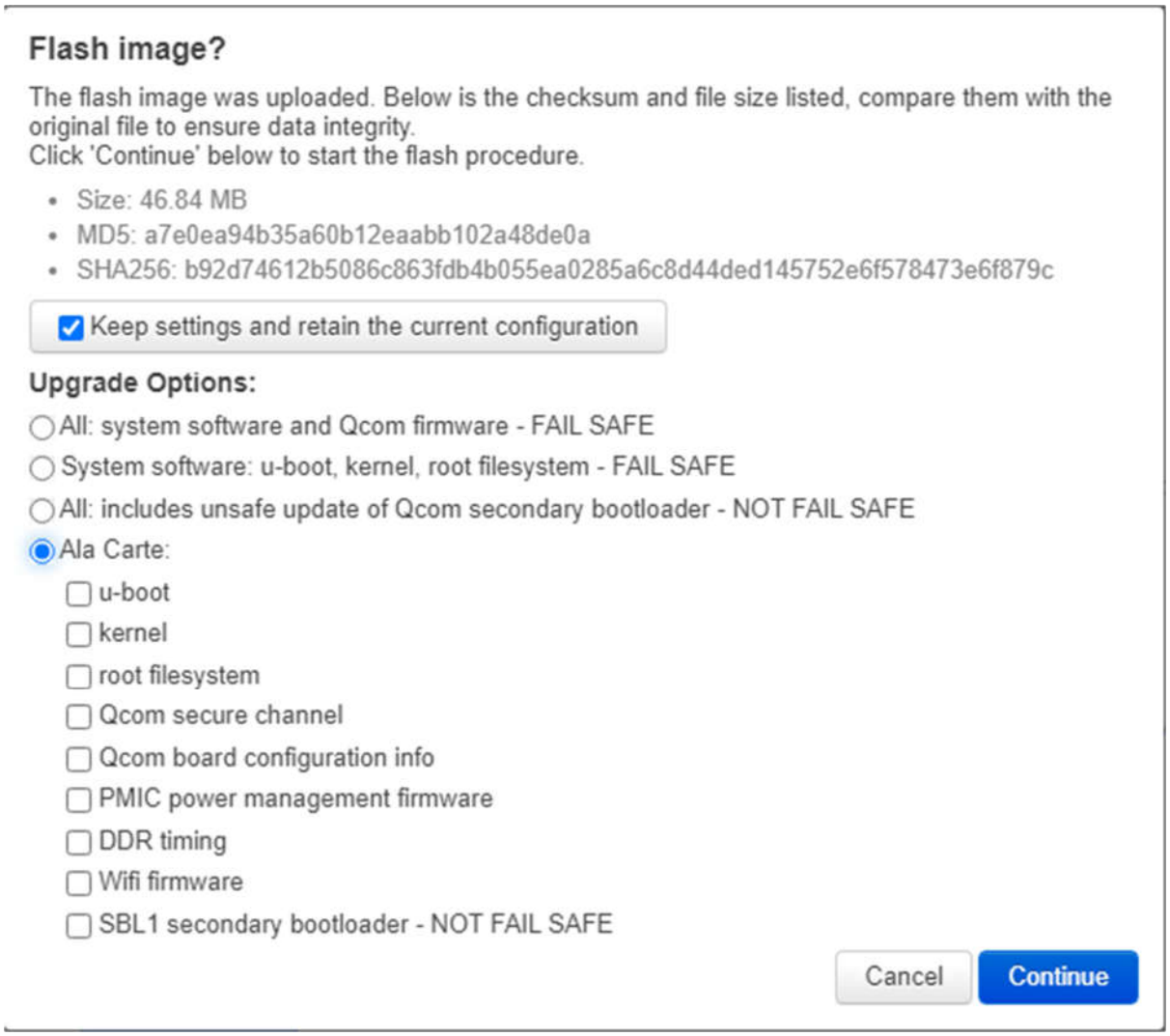
Backup: Generate and download an archive of the current CL6 configuration

Restore: Upload and restore a previous configuration backup

Save mtdblock contents: Download NOR flash partitions (factory use only)

Flash new firmware image: Upload and install CL6 firmware components and partitions. These upgrade files are provided by the manufacturer. It is advised that a configuration backup be made prior to a system upgrade. While preserving the current configuration is an upgrade option, having a configuration backup available provides extra assurance that the current configuration information is not lost.
To upload and install an upgrade file, start by clicking the "Flash image…" button.

Next click 'Browse…' and select the upgrade file from its location in your filesystem. Once the file is selected, click upload.



From this screen there are a few options.

Keep settings and retain current configuration: Keep this box checked if you are not planning to overwrite configuration files. If the box is unchecked when upgrading to a new load,

you're setting the configuration back to the default settings and may not be able to connect to the CL6.

Upgrade Options
Fail-safe upgrades will revert back to the previously installed version if an error or power loss occurs during the upgrade process. Non fail-safe means it is possible for a unit to become inoperable if an error or power loss occurs. It is recommended that non-fail safe upgrades be done only in controlled environments.

System software and Qcom firmware: This is the default upgrade option; it includes everything in ala carte except for SBL1

u-boot, kernel, root filesystem: This will upgrade the most commonly changed items

All, includes unsafe update of Qcom secondary bootloader: This will upgrade everything, including SBL1. Note that this is not a fail-safe upgrade

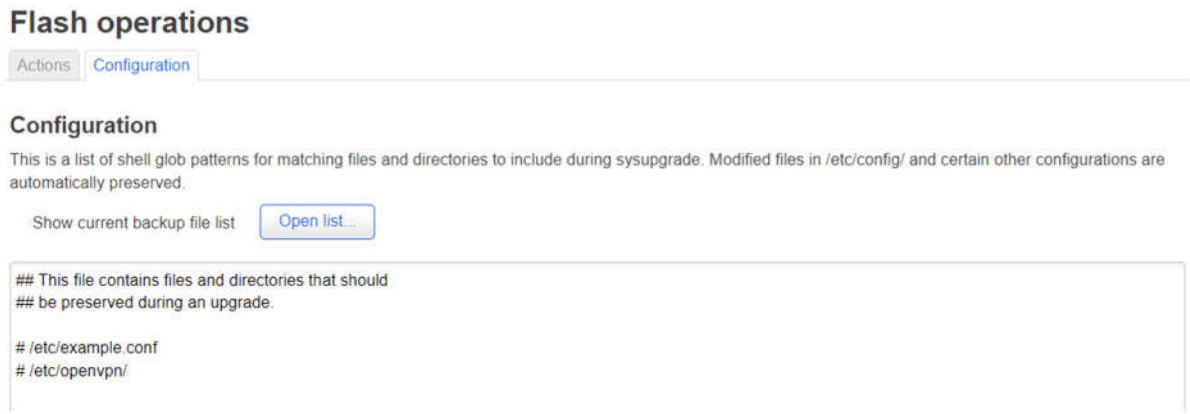
Ala Carte: Pick and choose which device partitions will be upgraded.

u-boot: Updates the APPSBL or APPSBL_1 partition on the NOR flash device.
kernel: Updates the HLOS or HLOS_1 partition on the eMMC device.
root filesystem: Updates the rootfs or rootfs_1 partition on the eMMC device.
Qcom secure channel: Updates the QSEE or QSEE_1 partition on the NOR flash device.
Qcom board configuration info: Updates the DEVCFG or DEVCFG_1 partition on the NOR flash device.
PMIC power management firmware: Updates the RPM or RPM_1 partition on the NOR flash device.
DDR timing: Updates the CDT or CDT_1 partition on the NOR flash device.
Wifi firmware: Updates the WIFIFW or WIFIFW_1 partition on the eMMC device.
SBL1 secondary bootloader: Updates the SBL1 partition on the NOR flash device.

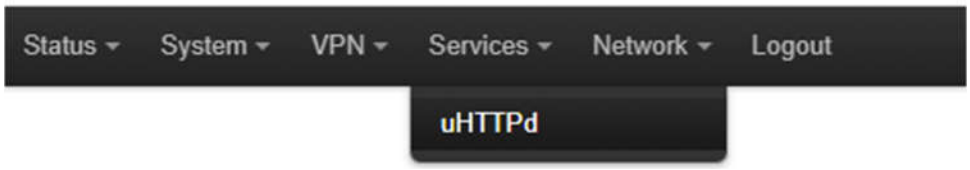
If the configuration or IP address of the CL6 is unknown after a software update, an external 'reset' operation will return the CL6 to the device's default configuration. (See CabinLink 6 System Reset for system reset operation)

6.6.2 System – Backup/Flash Firmware – Configuration

The **Backup/Flash Firmware/Configuration** screen shows additional folders and files to be added to the backup configuration archive. Editing this file is not typically needed.


Flash operations
Actions
Configuration
Configuration
This is a list of shell glob patterns for matching files and directories to include during sysupgrade. Modified files in /etc/config/ and certain other configurations are automatically preserved.
Show current backup file list
Open list...
This file contains files and directories that should
be preserved during an upgrade.
/etc/example.conf
/etc/openvpn/

7. Services



The Services dropdown shows the following information:

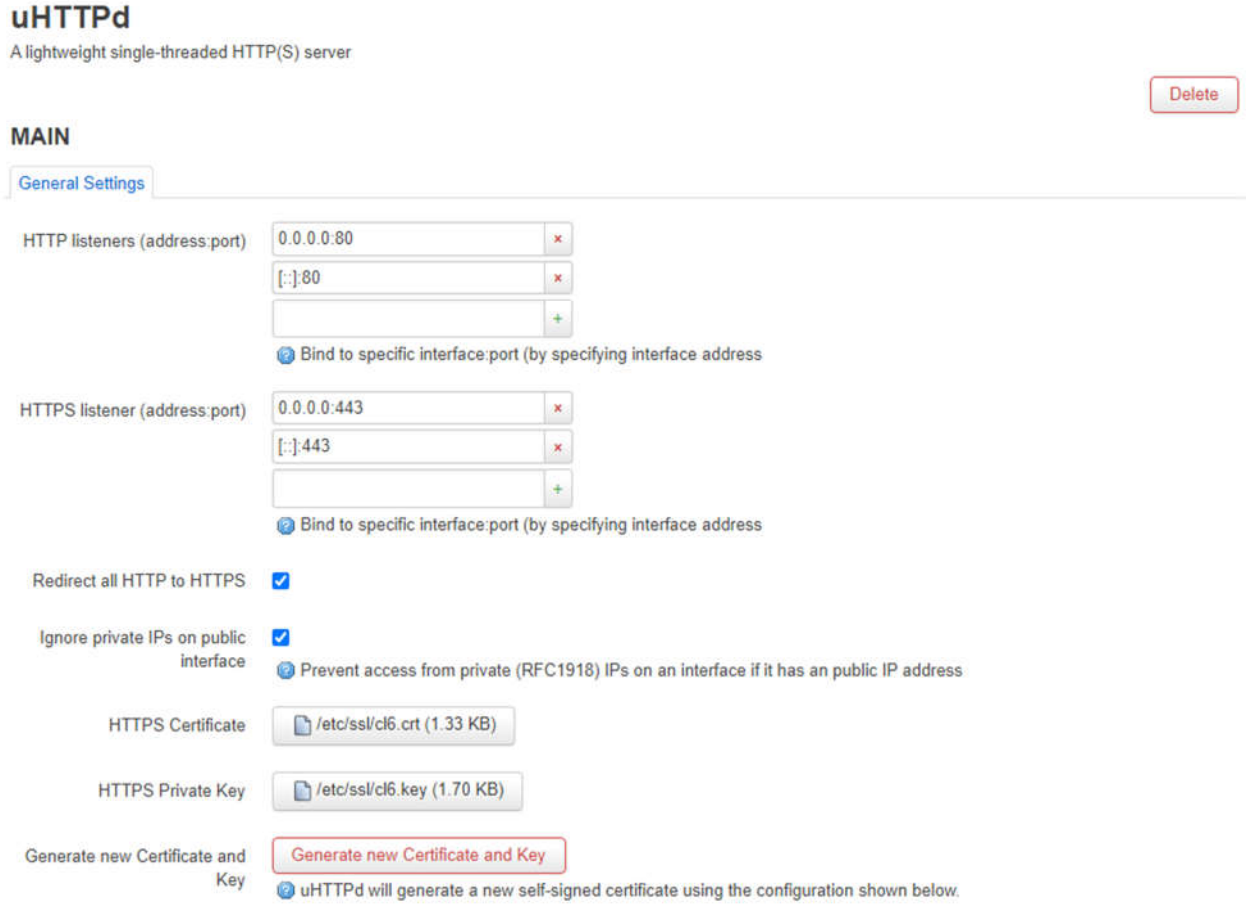
uHTTPd – The default LuCI web interface, uHTTPd is a server suitable for light tasks used with embedded devices

7.1 Services – uHTTPd

The **uHTTPd/General Settings** page displays settings to configure the uhttpd web server package.

7.1.1 Services – uHTTPd – General Settings

Services->uHTTPd->General Settings



HTTP listeners (address: port): Specifies the ports and addresses to listen on for plain HTTP access. If only a port number is given, the server will attempt to serve both IPv4 and IPv6 requests. Use 0.0.0.0:80 to bind at port 80 only on IPv4 interfaces or [::]:80 to serve only IPv6. To run on multiple addresses, specifying each, you can list one address (or address:port) per line. The firewall page can be configured to block WAN port access, allowing the web server to accept all IP traffic

HTTPS listener (address: port): Specifies the ports and addresses to listen on for encrypted HTTPS access. The format is the same as **HTTP listeners.** The firewall page can be configured to block WAN port access, allowing the web server to accept all IP traffic

Redirect all HTTP to HTTPS: Redirects management HTTP access attempts on HTTP port to the HTTPS ports.

Ignore private IPs on public interface: Prevent access from private IPs on an interface if it has a public IP address

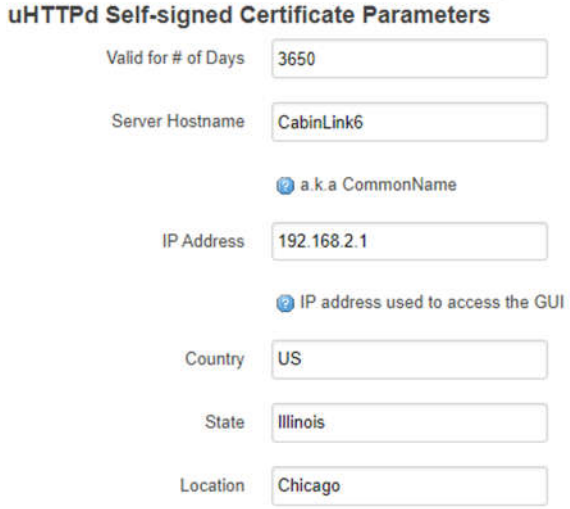
HTTPS Certificate: ASN.1/DER or PEM certificate used to serve HTTPS connections.

HTTPS Private Key: ASN.1/DER or PEM private key used to serve HTTPS connections.

Generate new Certificate and Key: This button will generate a new, self-signed, certificate and key. Storing them in /etc/ssl/cl6.crt and /etc/ssl/cl6.key.

7.1.2 Services – uHTTPd – Self-signed Certificate Parameters

Services->uHTTPd->uHTTPd Self-signed Certificate Parameters



Valid for # of Days: Number of days the Self-signed certificate will be valid for.

Server Hostname: Hostname of your CL6

IP Address: IP Address used to access the CL6 GUI

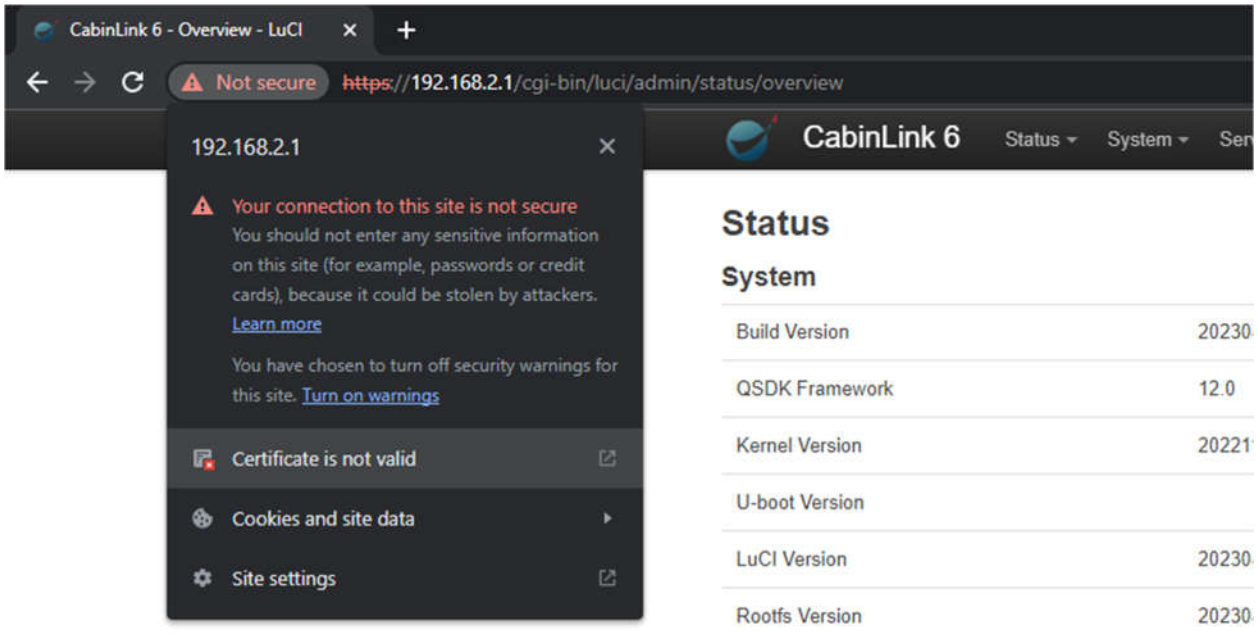
Country: ISO country code of the certificate issuer

State: State of the certificate issuer

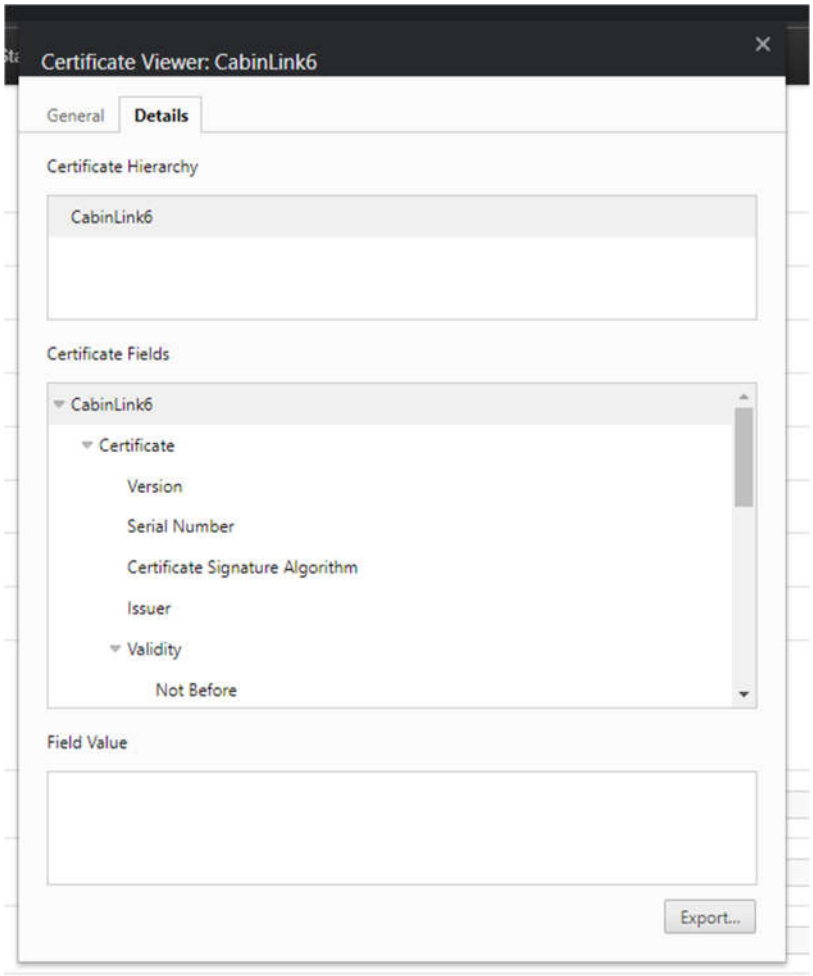
Location: Location/city of the certificate issuer

7.1.3 Services – uHTTPd – Configuring your computer to trust the Self-signed Certificate

After generating a new certificate and key using the "Generate new Certificate and Key" button, you will need to trust the certificate. To do this, start by navigating to the CL6 GUI. In this example Google Chrome is used, navigate past the warning and login. Once you are logged in, Click the "Not secure" warning to the left of the address bar. Next, click the "Certificate is not valid" button.



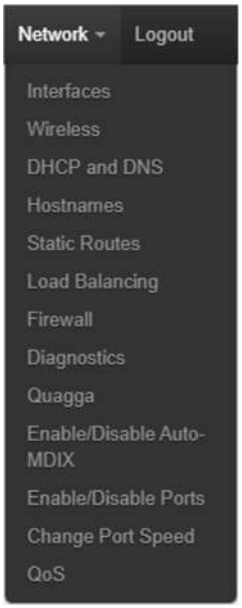
Click on the Details tab in the pop-up and click export. If you are having trouble downloading the certificate through your browser, you can also transfer the certificate from the CL6 itself. Using a tool such as WinSCP, transfer the certificate to your computer. The certificate is located at /etc/ssl/cl6.crt.



Now that you have your certificate downloaded, you need to add it to the Trusted Root Certification Authorities Store on the device you use to access the CL6 GUI. The process for this varies between browsers and operating systems, it is well documented online.

Once you have confirmed it has been saved in the Trusted Root Certification Authorities Store, close your browser, and reopen it. Navigate to the CL6 GUI, you shouldn't see any more warnings about invalid certificates. Any time you change the CL6 IP address you will have to go through this process again to make the warnings go away.

8. Network



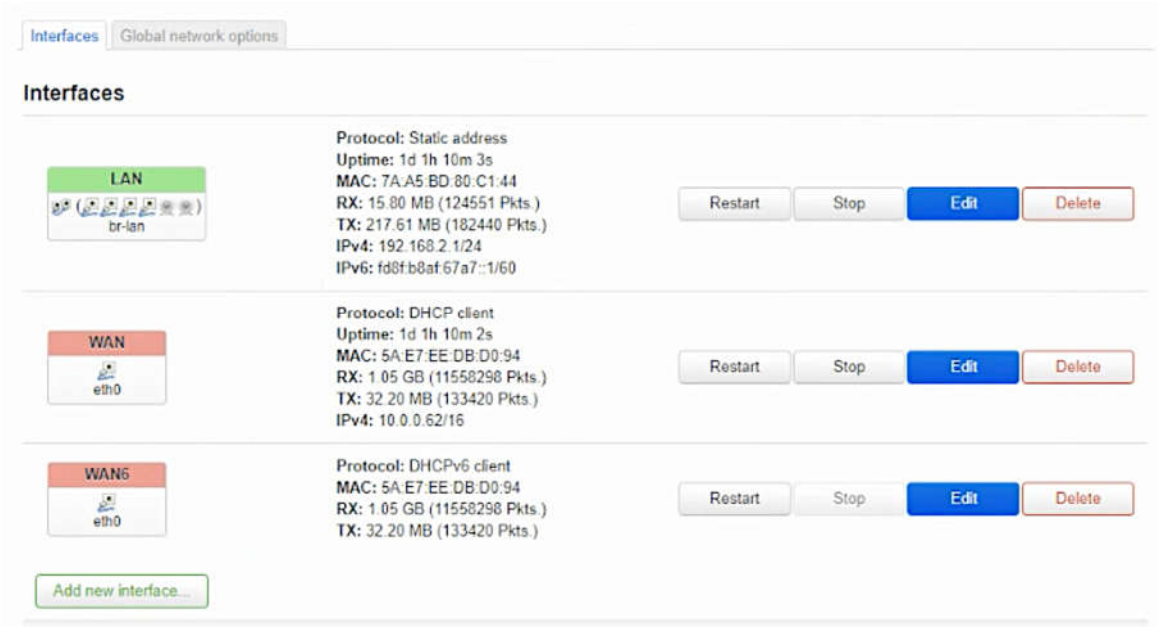
The Network dropdown shows the following information:

- **Interfaces** – Configuration of LAN and WAN ports
- **Wireless** – Configuration of two wireless radios – 5GHz and 2.5GHz band
- **DHCP and DNS** – Configuration of the Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS)
- **Hostnames** – Configure devices' names mapped to IP address on a network
- **Static Routes** – Configure routes through which a host or network can be reached
- **Load Balancing** – Configure distribution of several processes across multiple devices, depending on how busy they are
- **Firewall** – Configure rules that filters data entering or leaving a network
- **Enable/Disable Ports** – Enable or Disable ethernet ports and wireless networks on boot-up
- **Change Port Speed** – Configure port speed for ethernet ports
- **QoS** – Quality of Service, or setting a product to provide a certain service

8.1 Network – Interfaces

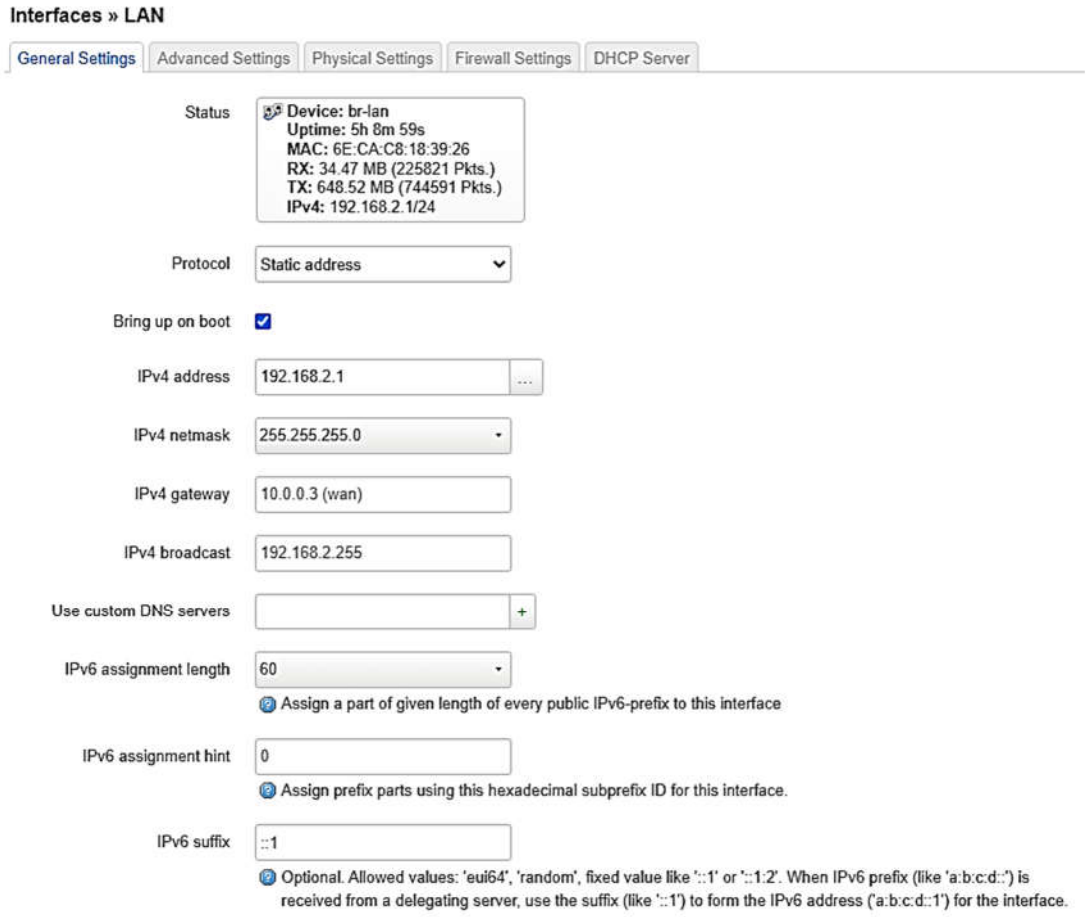
The Interface page allows for the configuration of the CL6 LAN and WAN ports. This is where logical interfaces are created. LAN for the local network and WAN interface in case of a router configuration where an external wide area network is connected. When multiple physical interfaces are added to a logical interface, the physical interface must be added to the network bridge through the Edit screen. Additionally, each interface can be started and stopped using the Stop/Start button. The Restart button can be used to restart the interface. The Edit button will redirect you to a screen for configuration of the interface. The Delete button will remove the interface from your configuration.

Network->Interfaces



8.1.1 Network – Interfaces – LAN/Edit – General Settings

Network->Interfaces->LAN/Edit->General Settings



Editing **Interfaces** requires configuration of the following options:

Status: Relevant information on the interface updated in real time.

Protocol: Specifies the protocol to use with this interface. Dropdown options include MAP/LW4over6, L2TP, DHCP client, GRE tunnel over IPv4, PPP, static address, PPtP, PPPoE, 464XLAT (CLAT), GRE tunnel over IPv6, IPv6-over-IPv4 (6rd), GRETAP tunnel over IPv6, Dual-Stack Lite (RFC6333), GRETAP tunnel over IPv4, DHCPv6 client and unmanaged.

Bring up on boot: Specifies whether to bring up interface on CL6 boot

IPv4 address: IP address to give the interface

IPv4 netmask: Netmask to give the interface

IPv4 gateway: Default gateway for the interface. If no gateway is specified, the parent interface gateway is inherited. If set to 0.0.0.0 no gateway will be specified for the route. Typically the gateway would be defined on the WAN port.

IPv4 broadcast: Broadcast address for the interface

Use custom DNS servers: Alternative DNS servers to be used

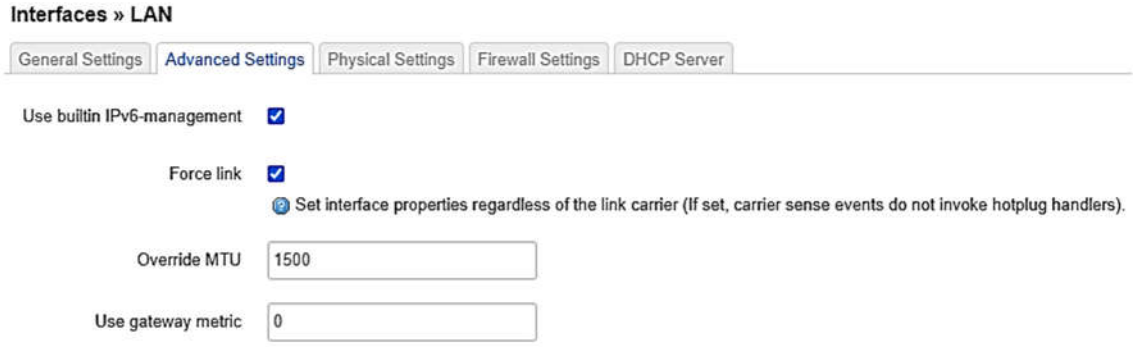
IPv6 assignment length: Assign a part of given length of every public IPv6-prefix to this interface. Dropdown options include 60, 64 and disabled

IPv6 assignment hint: Assign prefix parts using this hexadecimal subprefix ID for this interface

IPv6 suffix: Optional. Allowed values are eui64, random, a fixed value like ::1 or ::1:2

8.1.2 Network – Interfaces – LAN/Edit – Advanced Settings

Network->Interfaces->LAN/Edit->Advanced Settings



Use builtin IPv6-management: Specifies whether to enable (1) or disable (0) IPv6 on this interface (Barrier Breaker and later only)

Force link: Specifies whether IP address, route, and optionally gateway are assigned to the interface regardless of the link being active ('1') or only after the link has become active ('0'); when set to '1', carrier sense events do not invoke hotplug handlers

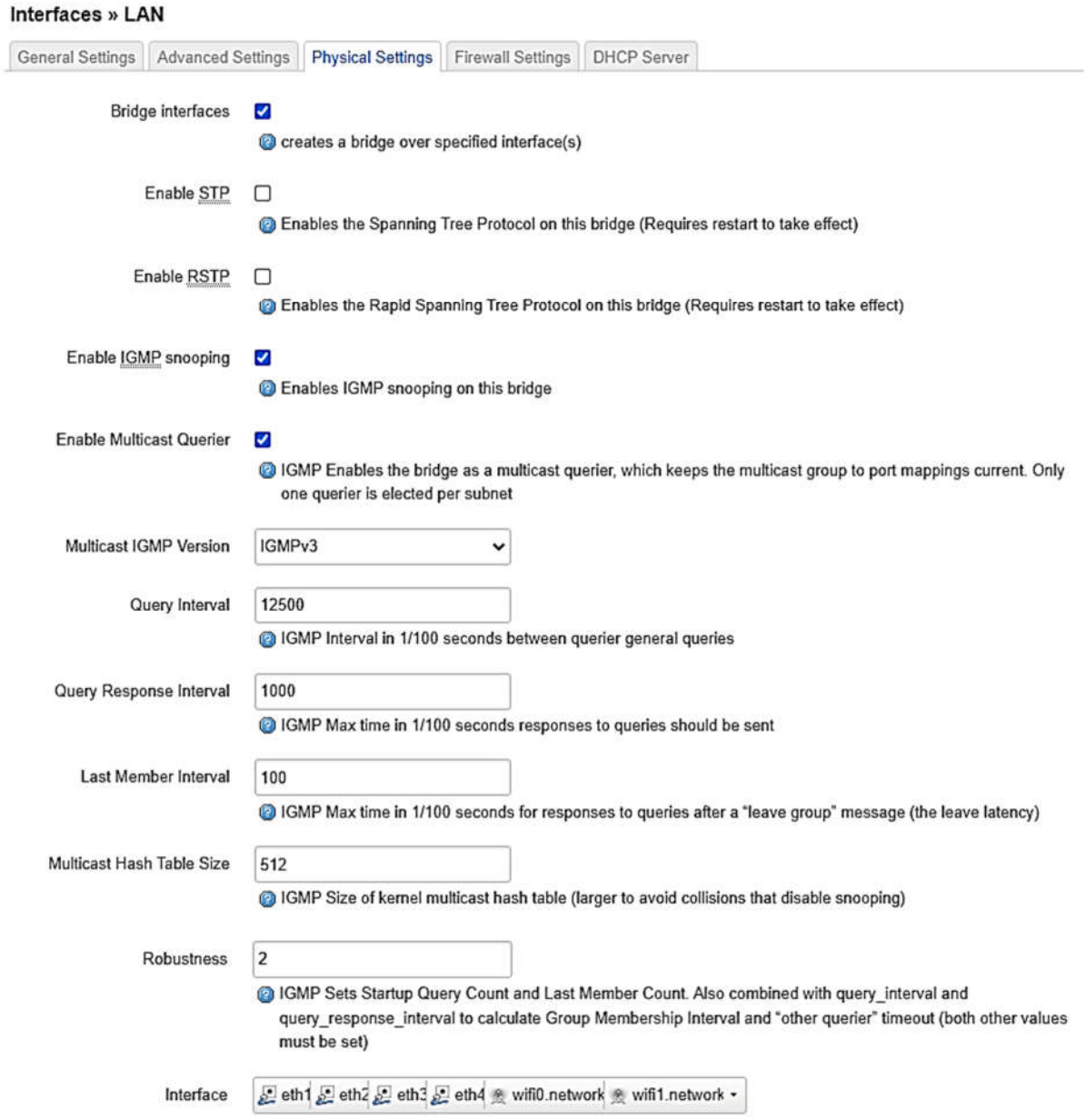
Override MTU: Override the default MTU on this interface. (WAN interface)

Use gateway metric: Route metric or cost of using gateway route. (WAN interface)

Commentary: Static IP addresses need IP, subnet, gateway, and DNS set (if using). The LAN side typically bridges all enabled wired ports with one or more wireless interfaces. When bridged, the IP configuration must be done on the bridged interface, not the physical interfaces. The UCI interface configures the network interfaces, bridging and interface properties. (see /etc/config/network)

8.1.3 Network – Interfaces – LAN/Edit – Physical Settings

Network->Interfaces->LAN/Edit->Physical Settings



Bridge interfaces: Creates a bridge over specified interface(s)

Enable STP: Enables the Spanning Tree Protocol on this bridge, which requires restart to take effect

Enable RSTP: Enables the Rapid Spanning Tree Protocol on this bridge, which requires restart to take effect

Enable IGMP snooping: Enables IGMP snooping on this bridge

Enable Multicast Querier: IGMP Enables the bridge as a multicast querier, which keeps the multicast group to port mappings current. Only one querier is elected per subnet.

Multicast IGMP Version: Which version of IGMP to use. Dropdown options include IGMPv2 and IGMPv3.

Query Interval: IGMP Interval in 1/100 seconds between querier general queries

Query Response Interval: IGMP Max time in 1/100 seconds responses to queries should be sent

Last Member Interval: IGMP Max time in 1/100 seconds for responses to queries after a "leave group" message (the leave latency)

Multicast Hash Table Size: IGMP Size of kernel multicast hash table (larger to avoid collisions that disable snooping)

Robustness: IGMP Sets Startup Query Count and Last Member Count

Interface: Interfaces to be included in the bridge

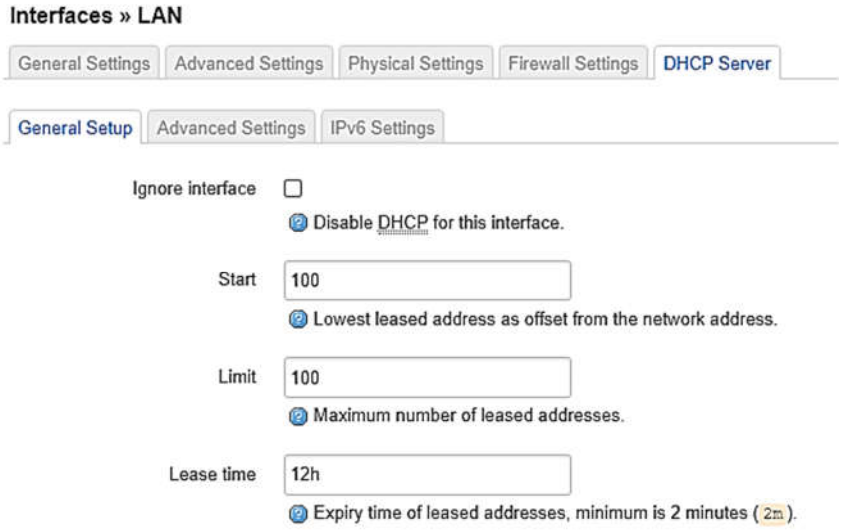
8.1.4 Network – Interfaces – LAN/Edit – Firewall Settings

Network->Interfaces->LAN/Edit->Firewall Settings

Create/Assign firewall-zone: Choose the firewall zone you want to assign to this interface. Dropdown options include lan, wan, custom and unspecified (which removes the interface from the associated zone).

8.1.5 Network – Interfaces – LAN/Edit – DHCP Server – General Setup

Network->Interfaces->LAN/Edit->DHCP Server->General Setup



Ignore interface: Disable DHCP for this interface

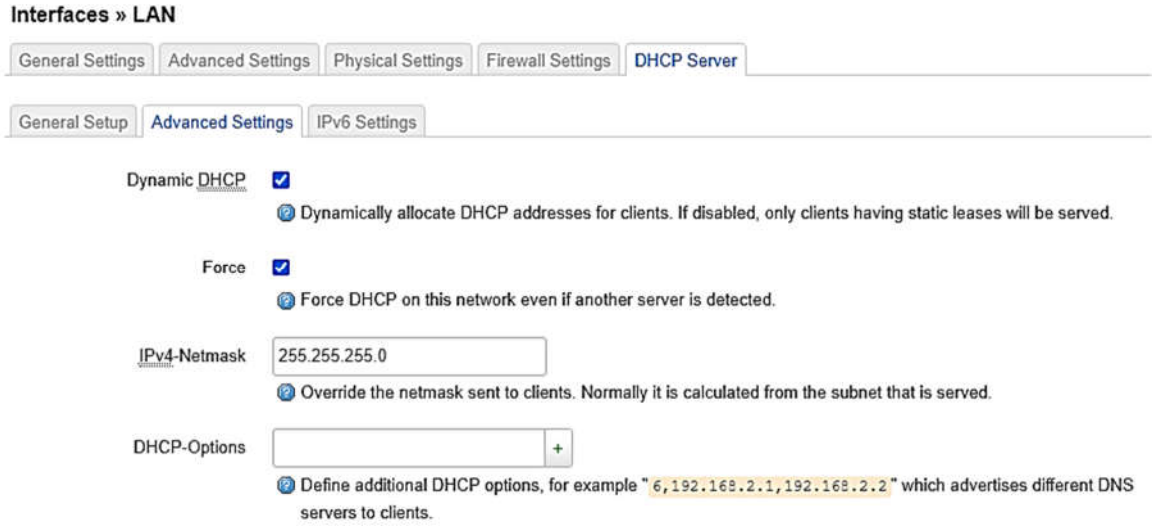
Start: Lowest leased address as offset from the network address

Limit: Maximum number of leased addresses

Lease time: Expiration time of leased addresses, the minimum of which is 2 minutes

8.1.6 Network – Interfaces – LAN/Edit – DHCP Server – Advanced Settings

Network->Interfaces->LAN/Edit->DHCP Server->Advanced Settings



Dynamic DHCP: Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.

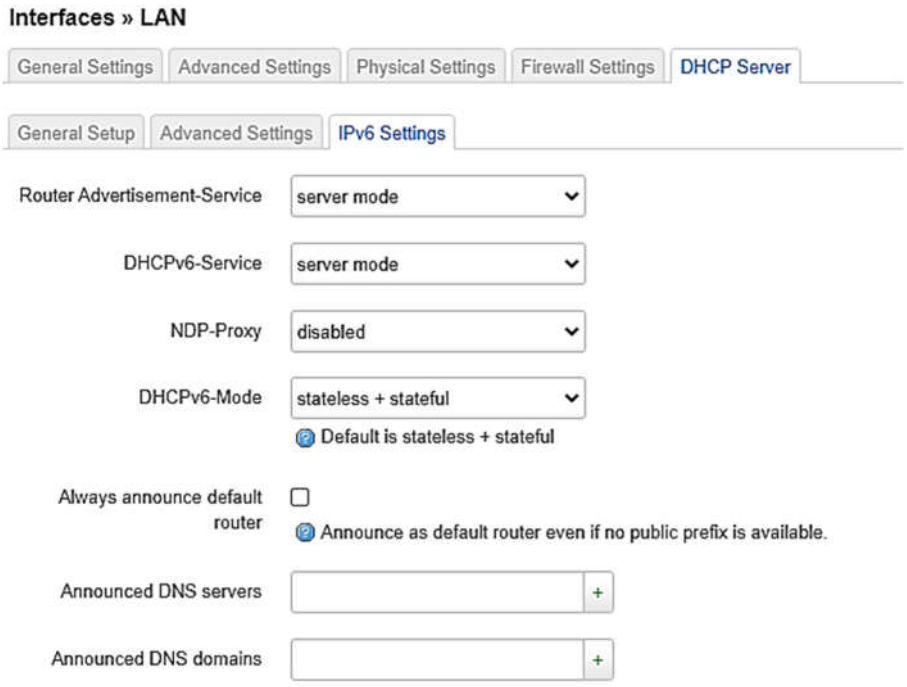
Force: Force DHCP on this network even if another server is detected

IPv4-Netmask: Override the netmask sent to clients. Normally it's calculated from the subnet that is served.

DHCP-Options: Define additional DHCP options, which advertise different DNS servers to clients

8.1.7 Network – Interfaces – LAN/Edit – DHCP Server – IPv6 Settings

Network->Interfaces->LAN/Edit->DHCP Server->IPv6 Settings



Router Advertisement-Service: Specifies whether Router Advertisements should be enabled, relayed, a hybrid of both, or disabled. Dropdown options include disabled, server mode, relay mode and hybrid mode.

DHCPv6-Service: Specifies whether DHCPv6 server should be enabled, relayed, a hybrid of both, or disabled. Dropdown options include disabled, server mode, relay mode and hybrid mode.

NDP-Proxy: Specifies whether Network Discovery Protocol should be relayed or disabled. Dropdown options include disabled, relay mode and hybrid mode.

DHCPv6-Mode: Router advertisement mode. Dropdown options include stateless, stateless + stateful, and stateful-only.

Always announce default router: Announce as default router, even if no public prefix is available

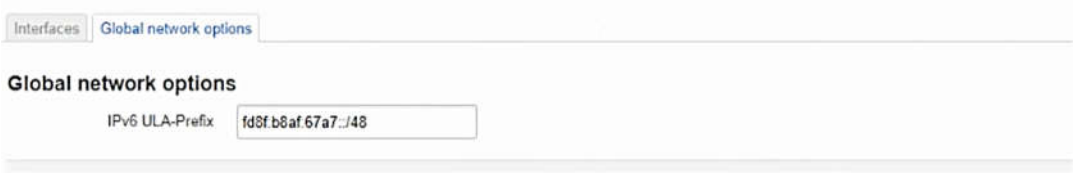
Announced DNS servers: DNS servers to announce on the network.

Announced DNS domains: DNS domain handed out to DHCP clients

8.1.8 Network – Interfaces – Global Network Options

The **Interfaces/Global network options** page allows you to set the Unique Local Address prefix.

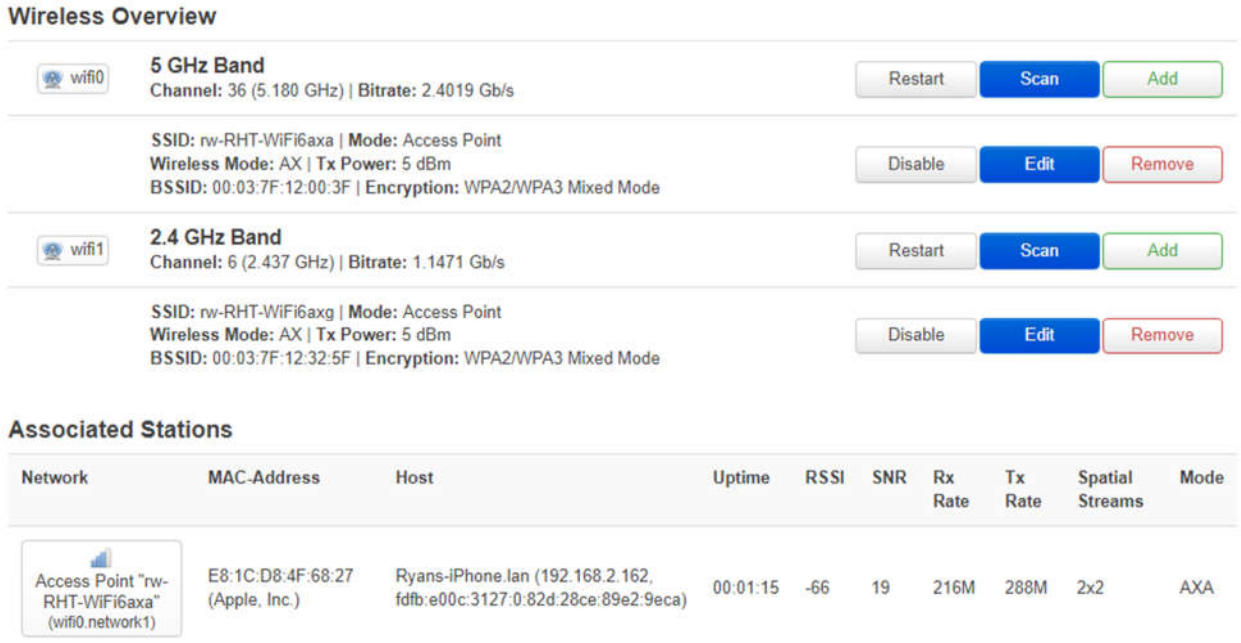
Network->Interfaces->Global network options



8.2 Network – Wireless

The Wireless overview screen is used to configure the wireless settings for the CabinLink 6. From here you can independently configure the 2.4GHz and 5 GHz wireless radios as well as view the clients connected to each of these radios. Each radio has a restart, scan, and add button. The restart button will restart that radio, the scan button will scan for wireless networks and allow you to connect to one, and the add button will take you to a screen that will allow you to create additional VAP's (Virtual Access Points) on that radio. The Associated Stations section will list the network each client is connected to, the client's MAC address, the OUI of the MAC address, the IP assigned to the client as well as their hostname if one can be found, the uptime of the client (how long they have been connected to the network), the RSSI (Received Signal Strength Indicator) of the Client, the SNR of the client, the Receive (RX)/Transmit (TX) rates of the client, the number of spatial streams, and the IEEE standard the client is using to connect.

Network->Wireless

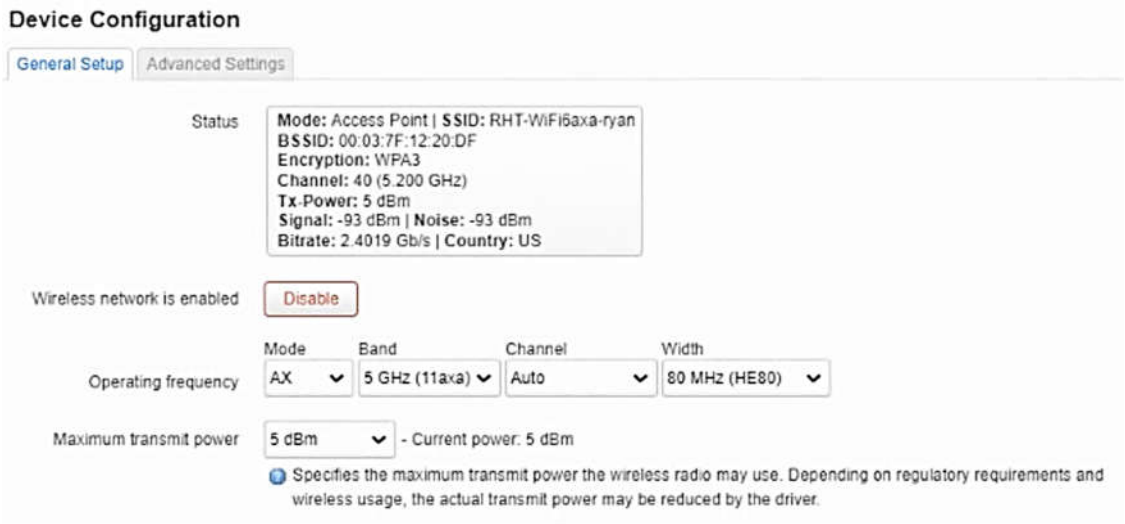


The Restart button will reboot the corresponding Wi-Fi device. The scan button will scan for nearby networks, giving information such as the channel they are operating on and the encryption they are using. You can also join one of these networks if you know the passphrase, this will configure a wireless interface in client mode. The disable button will disable the wireless interface, this is not recommended way to disable a wireless interface. The recommended way would be to disable the associated ath interface is via the Enable/Disable ports screen (8.11). The Edit button will allow you to configure the associated wireless interface, and the Remove button will delete the associated wireless interface.

8.2.1 Network – Wireless – Edit – Device Configuration – General Setup

Editing Wireless Overview requires configuration of **Device Configuration/General Setup**:

Network->Wireless->Edit->Device Configuration->General Setup



Status: Relevant information about the wireless network.

Wireless network is enabled: Enable/Disable the wireless network.

Operating frequency: Specifies the hardware mode, band, channel of operation and channel width**.** Dropdown options include:

Maximum transmit power: Sets the maximum allowed transmit power, increasing this value will increase the range of your wireless signal. The actual transmit power may be reduced by the driver based on regulatory domain, channel selected, configured country code.

Channel Bonding for 40 MHz wide bands on 5 GHz radio

Channel	Frequency (MHz)	Plus Bandwidth	Primary Channel, Secondary Channel	Minus Bandwidth	Primary Channel, Secondary Channel
36	5180	HT40+	36,40		
40	5200			HT40-	40,36
44	5220	HT40+	44,48		
48	5240			HT40-	48,44
52	5260	HT40+	52,56		
56	5280			HT40-	56,52
60	5300	HT40+	60,64		
64	5320			HT40-	64,60
100	5500	HT40+	100,104		
104	5520			HT40-	104,100
108	5540	HT40+	108,112		
112	5560			HT40-	112,108
116	5580	HT40+	116,120		
120	5600			HT40-	120,116
124	5620	HT40+	124,128		
128	5640			HT40-	128,124
132	5660	HT40+	132,136		
136	5680			HT40-	136,132
140	5700				
149	5745	HT40+	149,153		
153	5765			HT40-	153,149
157	5785	HT40+	157,161		
161	5805			HT40-	161,157

Note: Selecting 'HT40' provides auto selection of primary and secondary channels

Channel Bonding for 40 MHz wide bands on 2.4 GHz radio

Channel	Frequency (MHz)	Plus Bandwidth	Primary Channel, Secondary Channel	Minus Bandwidth	Primary Channel, Secondary Channel
1	2412	HT40+	1,5		
2	2417	HT40+	2,6		
3	2422	HT40+	3,7		
4	2427	HT40+	4,8		
5	2432	HT40+	5,9	HT40-	5,1
6	2437	HT40+	6,10	HT40-	6,2
7	2442	HT40+	7,11	HT40-	7,3
8	2447			HT40-	8,4
9	2452			HT40-	9,5
10	2457			HT40-	10,6
11	2462			HT40-	11,7

Note: Selecting 'HT40' provides auto selection of primary and secondary channels

Channel Bonding for 80 MHz wide bands on 5 GHz radio

Channels	Frequency	Bandwidth
36 – 48	5170 – 5250	HT80, HE80
52 – 64	5250 – 5330	HT80, HE80
100 – 112	5490 – 5570	HT80, HE80
116 – 128	5570 – 5650	HT80, HE80
132 – 144	5650 – 5730	HT80, HE80
149 – 161	5735 – 5815	HT80, HE80
36 – 48	5170 – 5250	HT80, HE80

Note: Channels are selected according to specification (e.g. selecting channel 36, 40, 44, or 48 has identical results)

Theroetical Max Throughput Per Spatial Stream

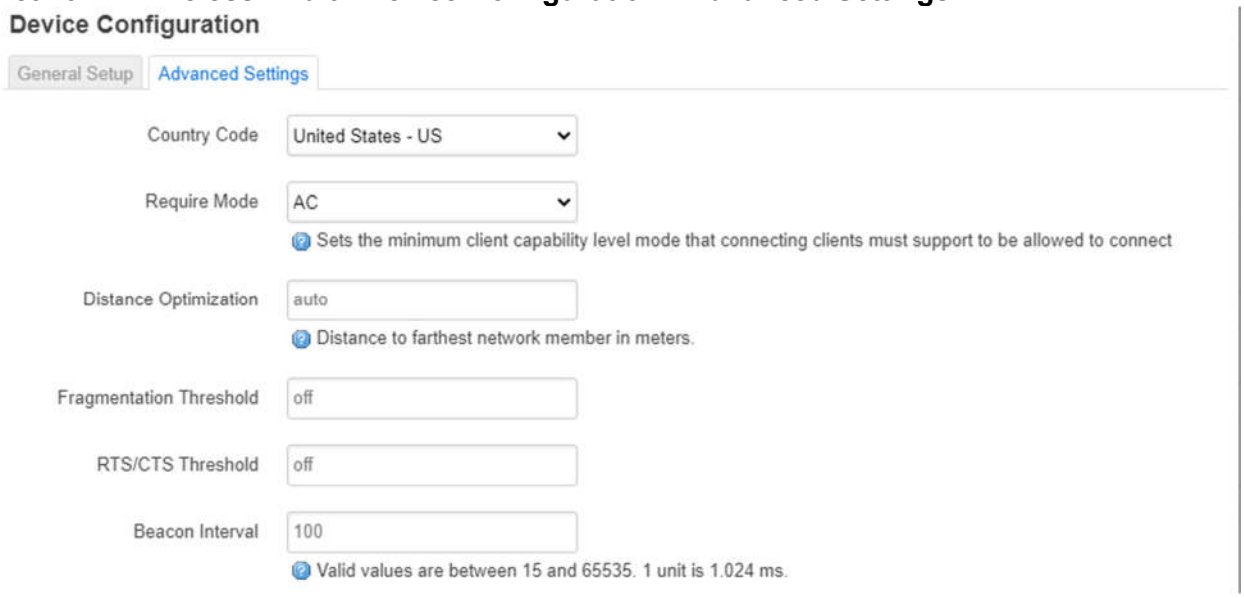
HW Mode	20 MHz Data Rate (Mbps)	40 MHz Data Rate (Mbps)	80 MHz Data Rate (Mbps)
AX	143.4	286.8	600.4
AC	86.7	200	433.3
N	72.2	150	N/A
Legacy	54	N/A	N/A

Note: The CL6 supports 4 spatial streams.

8.2.2 Network – Wireless – Edit – Device Configuration – Advanced Settings

Editing Wireless Overview requires configuration of **Device Configuration/Advanced Settings**:

Network->Wireless->Edit->Device Configuration->Advanced Settings



Country Code: Specifies the country code, affects the available channels and transmission powers. Uses a two-letter country code described in the country code table located in the appendix. CL6 has pending certification for US, Canada, EU, and Japan. CL6 is not certified to operate in other countries.

Require Mode: Sets the minimum client capability level mode that connecting clients must support to be allowed to connect. Dropdown options include None, N for 2.4GHz; None, N, AC for 5GHz.

Distance Optimization: Distance to farthest network member in meters. Leaving the field blank (auto) means the driver will optimize timings for distance. This setting if more useful for longer distances and fixed location use cases.

Fragmentation Threshold: The frame size threshold in bytes that limits the frame size transmitted over the network. The threshold must be an even integer between 256 and 2,346, the latter of which is the default.

If the frame size exceeds the set threshold, it activates the fragmentation function and sends the frame in multiples. If the frames are less than or equal to the threshold, fragmentation is not used.

While fragmentation involves more overhead to divide and reassemble the frames, plus increases the network's message traffic, it can help improve the network's reliability and performance.

RTS/CTS Threshold: The Request to Send Threshold value indicates how many octets are in an MPDU (MAC protocol data unit) and must be an integer from 0 to 2,347, the latter of which is the default

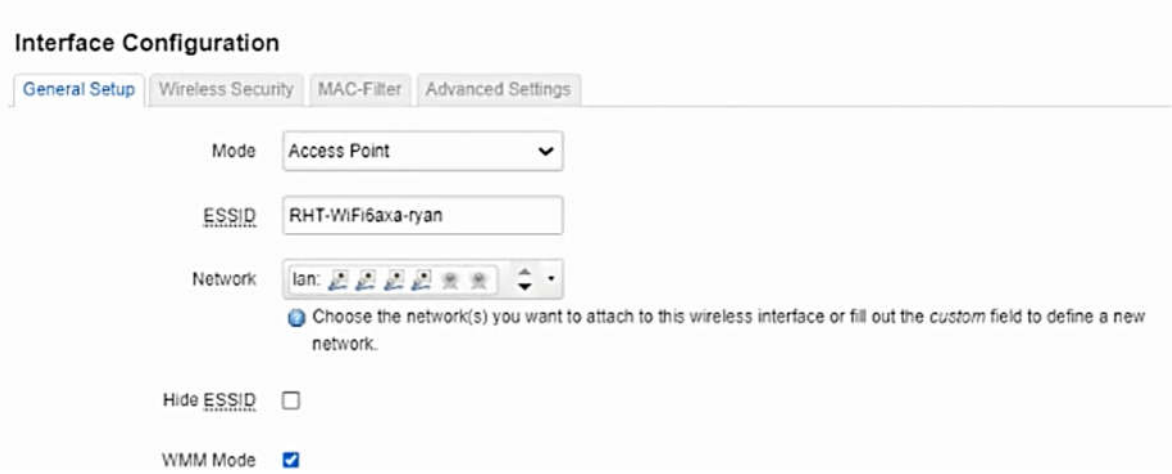
The RTS Threshold helps control the CL6 device's traffic flow. A lower threshold sends RTS frames more frequently – using more bandwidth and reducing the frames' throughput – while a higher one helps a network recover from a busy network's potential interference or collisions.

Beacon Interval: Set the beacon interval. This is the time interval between beacon frames, measured in units of 1.024 ms. Valid values are between 15 and 65535, with a default of 100.

8.2.3 Network – Wireless – Edit – Interface Configuration – General Setup

Editing Wireless Overview requires configuration of **Interface Configuration/General Setup.**

Network->Wireless->Edit->Interface Configuration->General Setup



Mode: Specifies the operation mode of the wireless network interface controller. Possible values are Access Point, Client, Ad-Hoc, 802.11s, Pseudo Ad-Hoc, Monitor, Access Point (WDS) and Access Point (Client). Dropdown options include Access Point, Client, Ad-Hoc, 802.11s, Pseudo Ad-Hoc (ahdemo), Monitor, Access Point (WDS) and Client (WDS)

ESSID: The broadcasted SSID of the wireless network

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

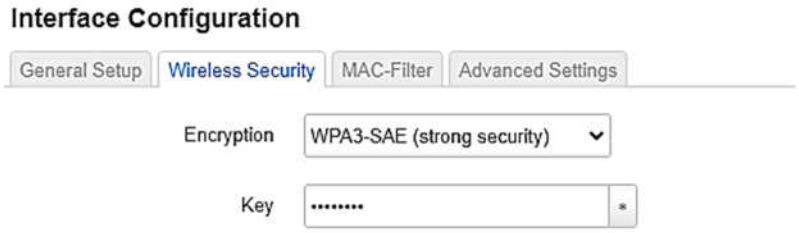
Hide ESSID: Disables the broadcasting of the SSID if the box is checked.

WMM Mode: Enables WiFi Multimedia Mode. This will optimize WiFi signal quality and performance when multiple applications compete for network resources. Voice and Video performance will be prioritized.

8.2.4 Network – Wireless – Edit – Interface Configuration – Wireless Security

Editing Wireless Overview requires configuration of **Interface Configuration/Wireless Security**.

Network->Wireless->Edit->Interface Configuration->Wireless Security



Encryption: Dropdown options include WPA2/WPA3 Mixed Mode (strong security), WPA2-PSK (strong security), WPA2-EAP (strong security),WPA3-SAE (strong security), WEP (weak security), WEP Shared Key (weak security) and No Encryption (open network).

Key: Passphrase to use for the SSID, must be between 8 and 63 characters

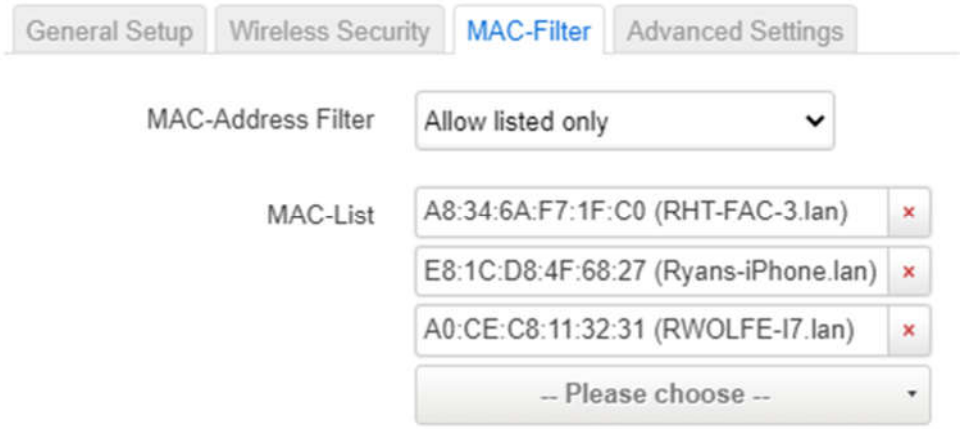
Used Key Slot: Allows user to select which key to use as the WEP passphrase.

Key #1-4: Configurable Passphrases for WEP encryption. Select which one you want to use using the 'Used key slot' dropdown.

8.2.5 Network – Wireless – Edit – Interface Configuration – Mac-Filter

Editing Wireless Overview requires configuration of **Interface Configuration/MAC-Filter** with dropdown options including disable, Allow listed only and Allow all except listed.

Network->Wireless->Edit->Interface Configuration->MAC-Filter



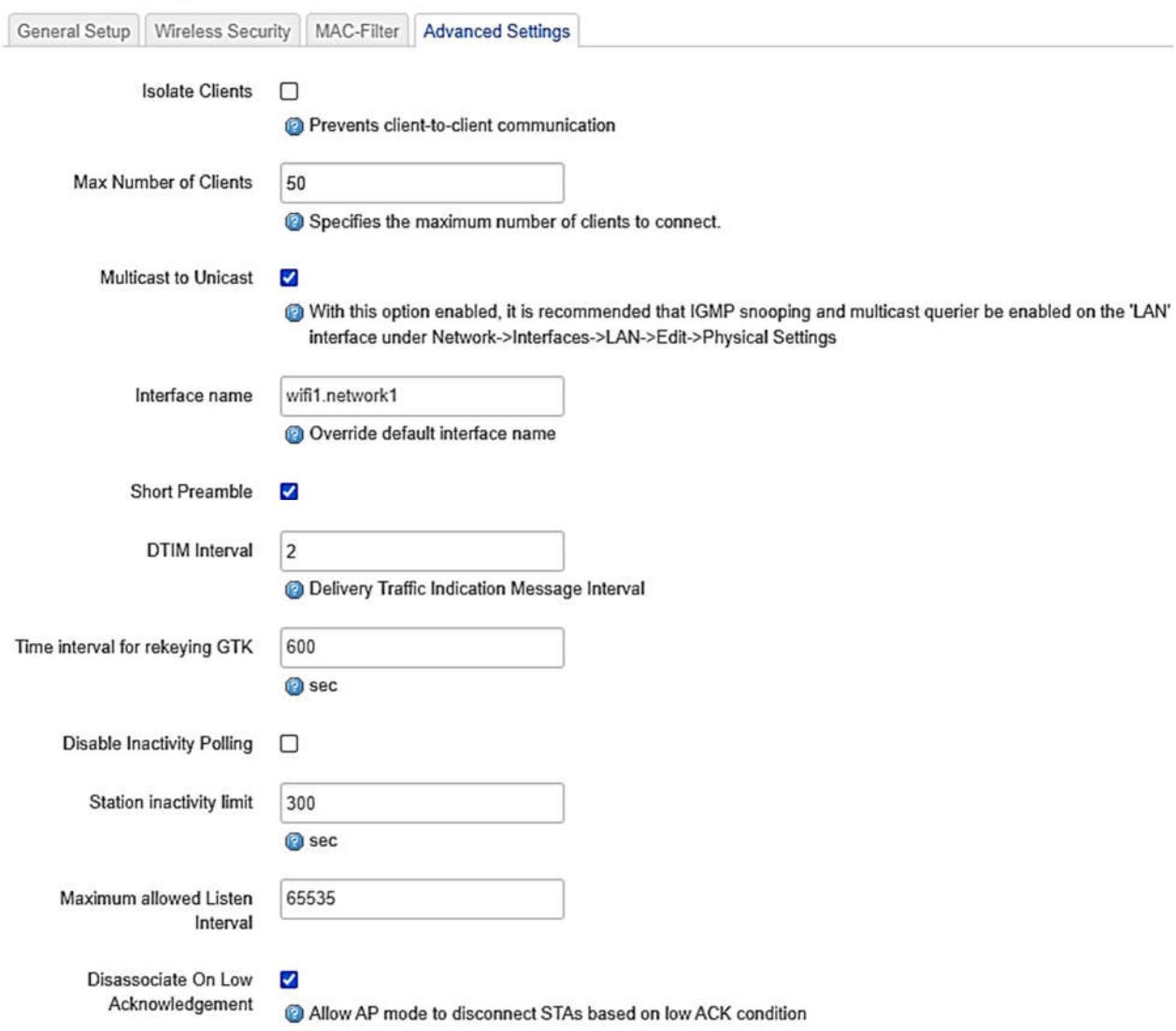
MAC-Address Filter: Enable MAC-address filtering. Options include disabled, Allow listed only, Allow all except listed. Selecting disabled will allow anyone with the passphrase for your SSID to connect to the network, Allow listed only' will only allow devices whose MAC addresses are in the MAC-List field to connect to the network, Allow all except listed will deny access to your network for any MAC address in the MAC-List.

MAC-List: List of MAC addresses to whitelist or blacklist on your network.

8.2.6 Network – Wireless – Edit – Interface Configuration – Advanced Settings

Editing Wireless Overview requires configuration of **Interface Configuration/Advanced Settings**:

Network->Wireless->Edit->Interface Configuration->Advanced Settings



Isolate Clients: Isolates wireless clients from each other to prevent communication between wireless clients

Max Number of Clients: Set the maximum number of clients that can connect to the SSID

Multicast to Unicast: Enable/Disable multicast to unicast packet conversion. The maximum number of multicast streams that can be converted is 64 per VAP. If there are more than 64 multicast streams, the remaining packets will be sent without any conversion. It is recommended that IGMP snooping and multicast querier be enabled on the LAN interface under Network->Interfaces->LAN->Edit->Physical Settings. See 8.1 for more information on configuration of the multicast querier.

Interface Name: Specifies a custom name for the Wi-Fi interface, which is otherwise automatically named. Maximum length: 15 characters.

Short Preamble: Enable the use of short preamble, this uses shorter data strings which results in faster speeds

DTIM Interval: Set the DTIM (delivery traffic information message) period. There will be one DTIM per this many beacon frames. This may be set between 1 and 255

Time interval for rekeying GTK: WPA Group Cipher rekeying interval in seconds

Disable Inactivity Polling: The inactivity polling can be disabled to disconnect stations based on inactivity timeout so that idle stations are more likely to be disconnected even if they are still in range of the AP.

Station inactivity limit: Station inactivity limit in seconds: If a station does not send anything in the given number of seconds, an empty data frame is sent to it in order to verify whether it is still in range. If this frame is not ACKed, the station will be disassociated and then deauthenticated.

Maximum allowed Listen Interval: Maximum allowed Listen Interval (how many Beacon periods STAs are allowed to remain asleep)

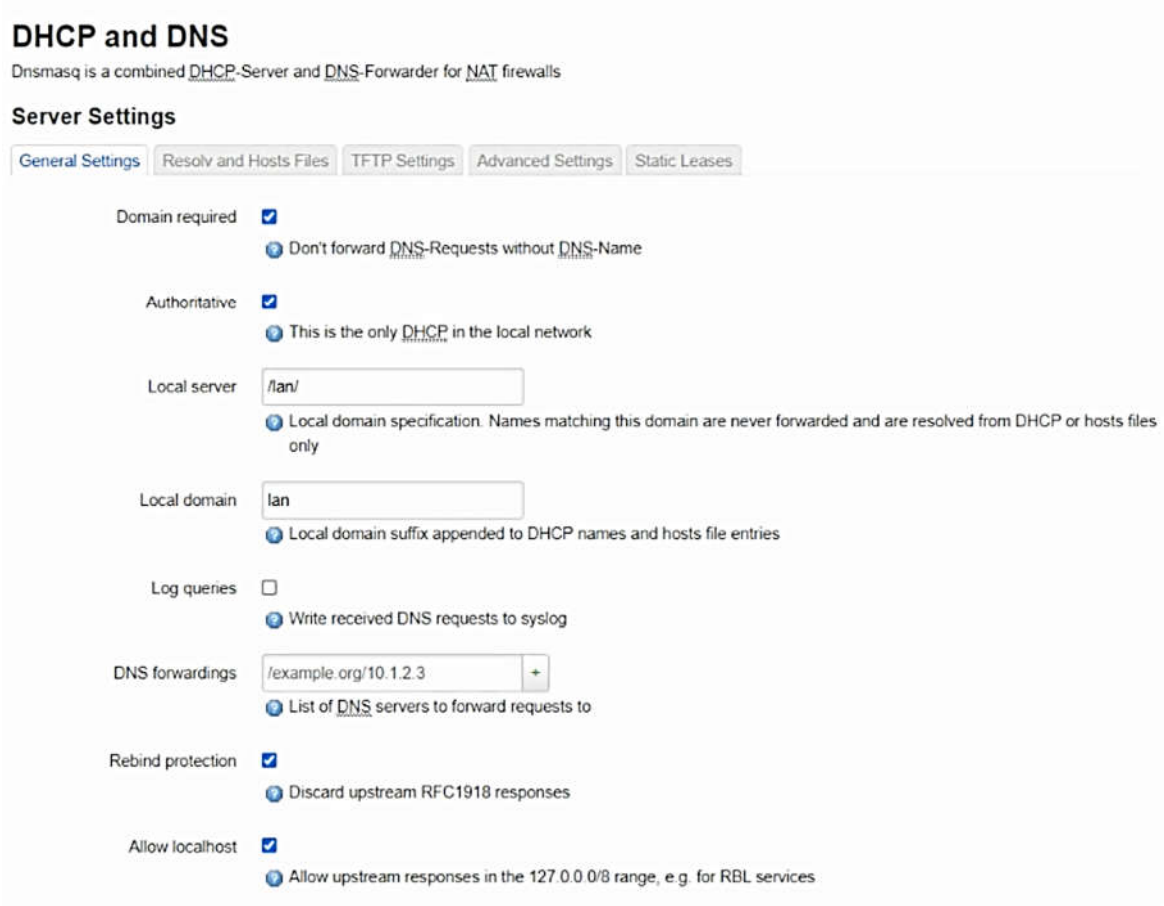
8.3 Network – DHCP and DNS

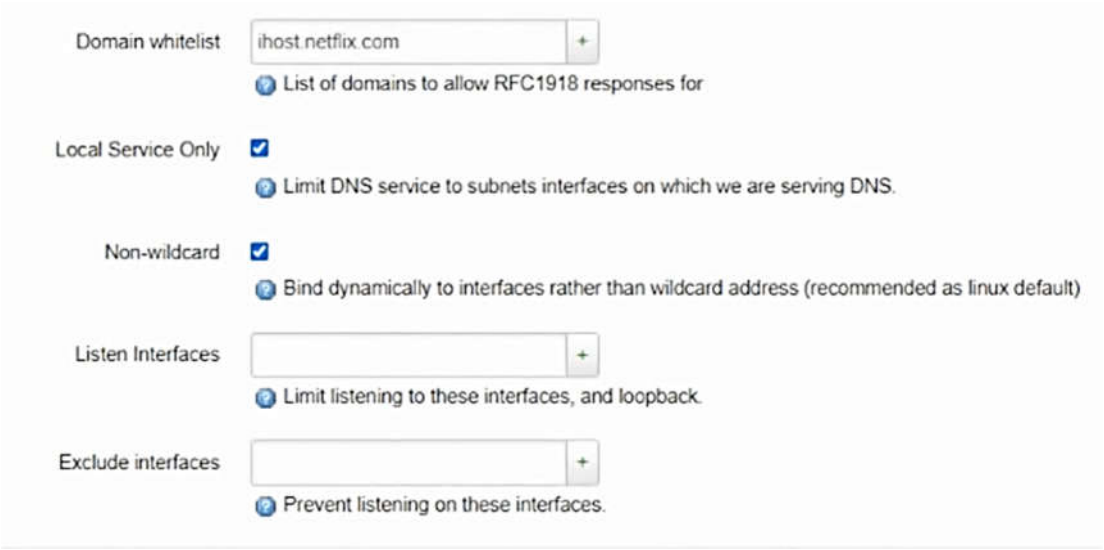
The IP address of each LAN port can be either statically set or set by the Dynamic Host Configuration Protocol (DHCP) service. DHCP assigns addresses/subnet/gateway if specified in the UCI configuration. CL6 utilizes dnsmasq to provide DHCP and DNS services. Ports are configurable to specify which Domain Name System (DNS) they should use. DNS can be enabled for a static DHCP lease. CL6 utilizes dnsmasq to provide DHCP and DNS services, which is typically automatic if using DHCP. Static IP configurations likely require a UCI command to configure the nameserver.

8.3.1 Network – DHCP and DNS – General Settings

The **DHCP and DNS/General Settings** screen appears as follows.

Network->DHCP and DNS->General Settings





Domain required: Tells dnsmasq never to forward queries for plain names, without dots or domain parts, to upstream nameservers. If the name is not known from /etc/hosts or DHCP then a "not found" answer is returned

Authoritative: Force dnsmasq into authoritative mode. This speeds up DHCP leasing. Used if this is the only server on the network

Local server: Look up DNS entries for this domain from /etc/hosts. This follows the same syntax as server entries, see the man page

Local domain: Local domain suffix appended to DHCP names and host file entries

Log queries: Log the results of DNS queries (/var/log/messages), dump cache on SIGUSR1, include requesting IP

DNS forwardings: Specify upstream servers directly. List of DNS servers to forward requests to. See the dnsmasq man page for syntax details

Rebind protection: Enables DNS Domain Name System rebind attack protection by discarding upstream RFC1918 responses

Allow localhost: Allows upstream 127.0.0.0/8 responses, required for DNS based blacklist services, only takes effect if rebind protection is enabled

Log queries: Write received DNS requests to syslog

Domain whitelist: List of domains to allow RFC1918 responses for, only takes effect if rebind protection is enabled

Local Service Only: Accept DNS queries only from hosts whose address is on a local subnet, ie a subnet for which an interface exists on the server

Non-wildcard: Bind dynamically to interfaces rather than wildcard addresses (recommend as linux default)

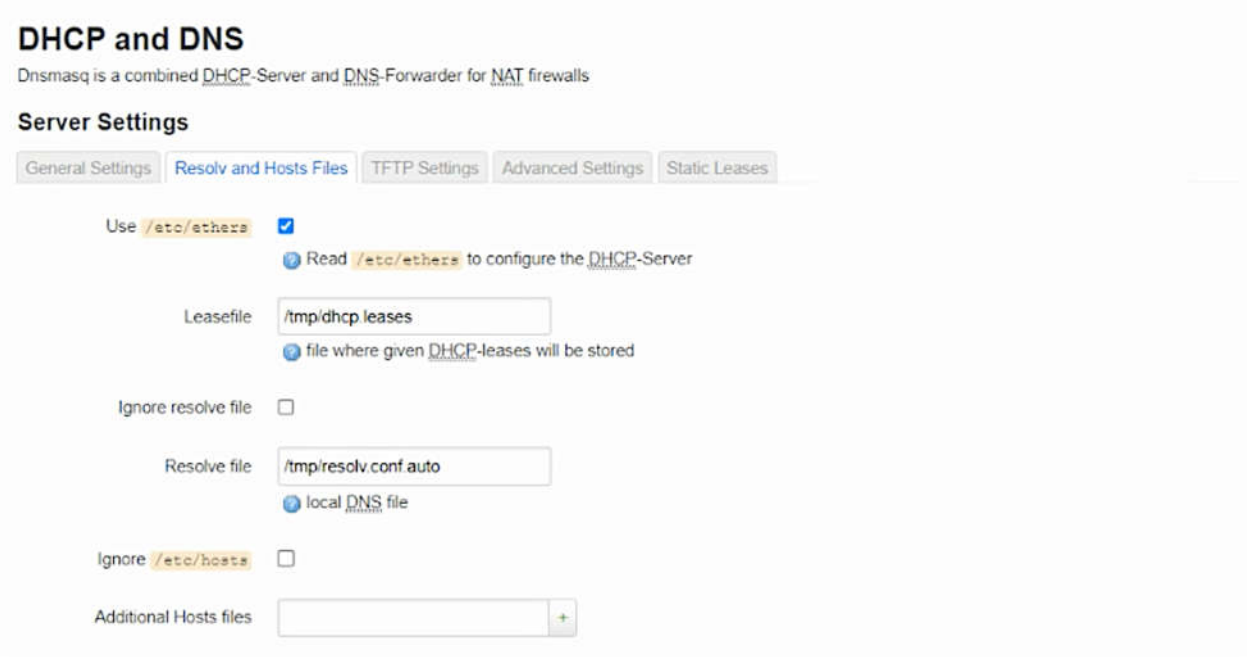
Listen Interfaces: List of interfaces to listen on. If unspecified, dnsmasq will listen to all interfaces except those listed in Exclude interfaces. Note that dnsmasq listens on loopback by default. Specifying interfaces for DHCP is not required here. This will be done when turning on DHCP for a specific interface (Network->Interfaces)

Exclude interfaces: Interfaces dnsmasq should not listen on. Specifying interfaces for DHCP is not required here. This will be done when turning on DHCP for a specific interface (Network->Interfaces)

8.3.2 Network – DHCP and DNS – Resolv and Hosts Files

The **DHCP and DNS/Resolv and Hosts Files** screen reads:

Network->DHCP and DNS->Resolv and Hosts Files



Use/etc/ethers: Read /etc/ethers for information about hosts for the DHCP server. The format of /etc/ethers is a hardware address, followed by either a hostname or dotted-quad IP address. When read by dnsmasq these lines have exactly the same effect as --dhcp-host options containing the same information. /etc/ethers is re-read when dnsmasq receives SIGHUP. IPv6 addresses are NOT read from /etc/ethers.

Leasefile: File where given DHCP-leases will be stored

Ignore resolve file: Don't read upstream servers from /etc/resolv.conf

Resolve file: Path/filename of local resolve.conf file

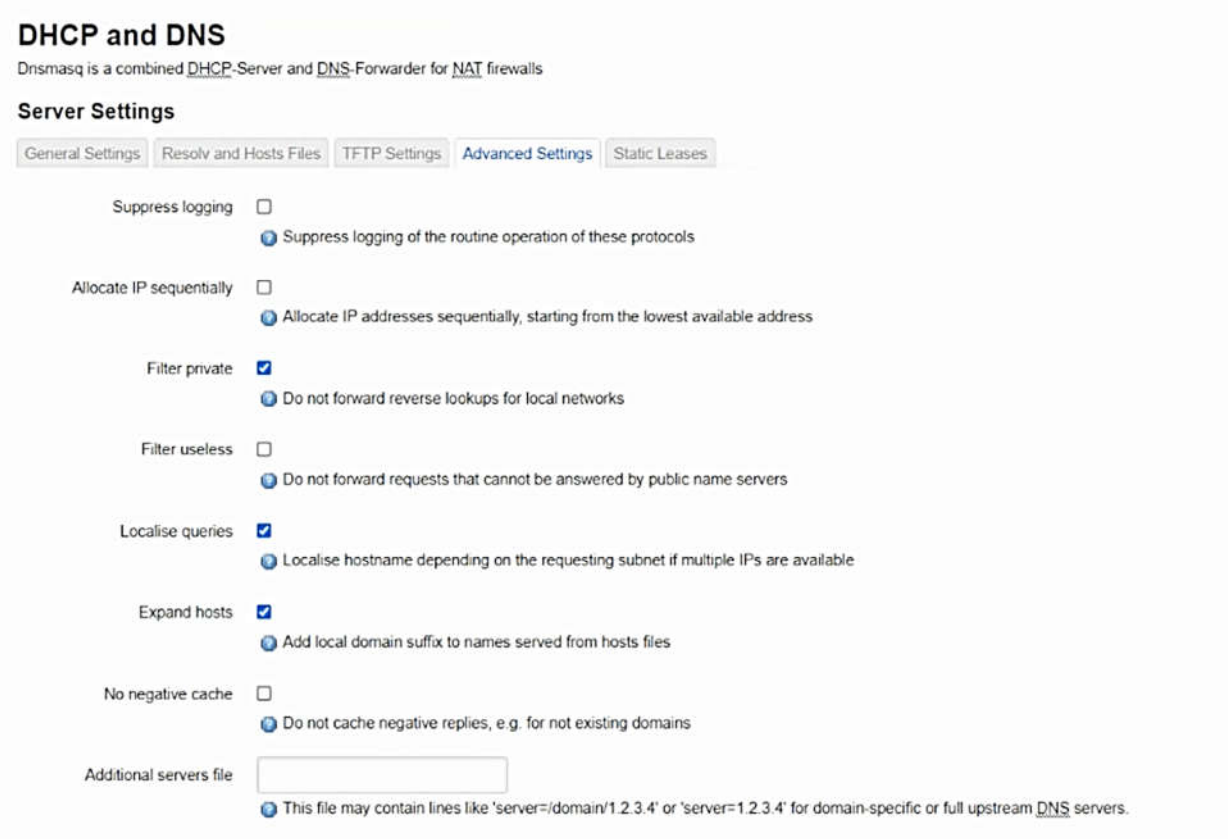
Ignore/etc/hosts: Don't use /etc/hosts for DNS lookup

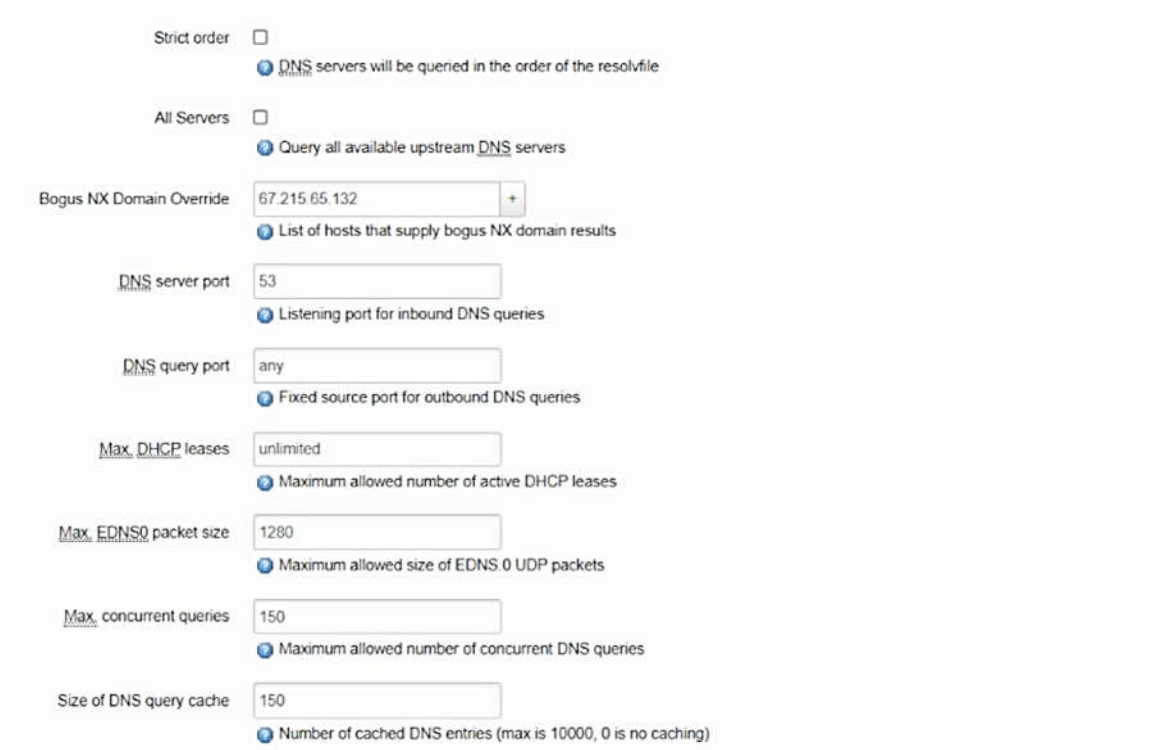
Additional Hosts files: Additional host files to read for serving DNS responses. Syntax in each file is the same as /etc/hosts

8.3.3 Network – DHCP and DNS – Advanced Settings

The **DHCP and DNS/Advanced Settings** screen looks like the one below.

Network->DHCP and DNS->Advanced Settings





Suppress logging: Suppress logging of the routine operation of these protocols

Allocate IP sequentially: Allocate IP addresses sequentially, starting from the lowest available address

Filter private: Do not forward reverse lookups for local networks

Filter useless: Do not forward requests that cannot be answered by public name servers. Make sure it is disabled if you need to resolve SRV records or use SIP phones

Localize queries: Choose IP address to match the incoming interface if multiple addresses are assigned to a host name in /etc/hosts

Expand hosts: Add the local domain part to names found in /etc/hosts

No negative cache: Do not cache negative replies

Additional servers file: Specify upstream servers directly. If one or more optional domains are given, that server is used only for those domains and they are queried only using the specified server. Syntax is server=/*.mydomain.local/192.168.100.1 or see the dnsmasq man page for details.

Strict order: DNS servers will be queried in the order of the resolvfile

All Servers: Query all available upstream DNS servers

Bogus NX Domain Override: 'List of IPs that are bogus NX domain results. This transforms replies which contain the specified address or subnet into "No such domain" replies. IPv4 and IPv6 are supported. This is intended to counteract devious moves made by various DNS servers that began returning the address of an advertising web page in response to queries for unregistered names, instead of the required NXDOMAIN response. This option tells dnsmasq to fake the correct response when it sees specific returned IP addresses.

DNS server port: Listening port for inbound DNS queries

DNS query port: Fixed source port for outbound DNS queries

Max DHCP leases: Maximum allowed number of active DHCP leases

Max EDNS0 packet size: Maximum allowed size of EDNS.0 UDP packets

Max concurrent queries: Maximum allowed number of concurrent DNS queries

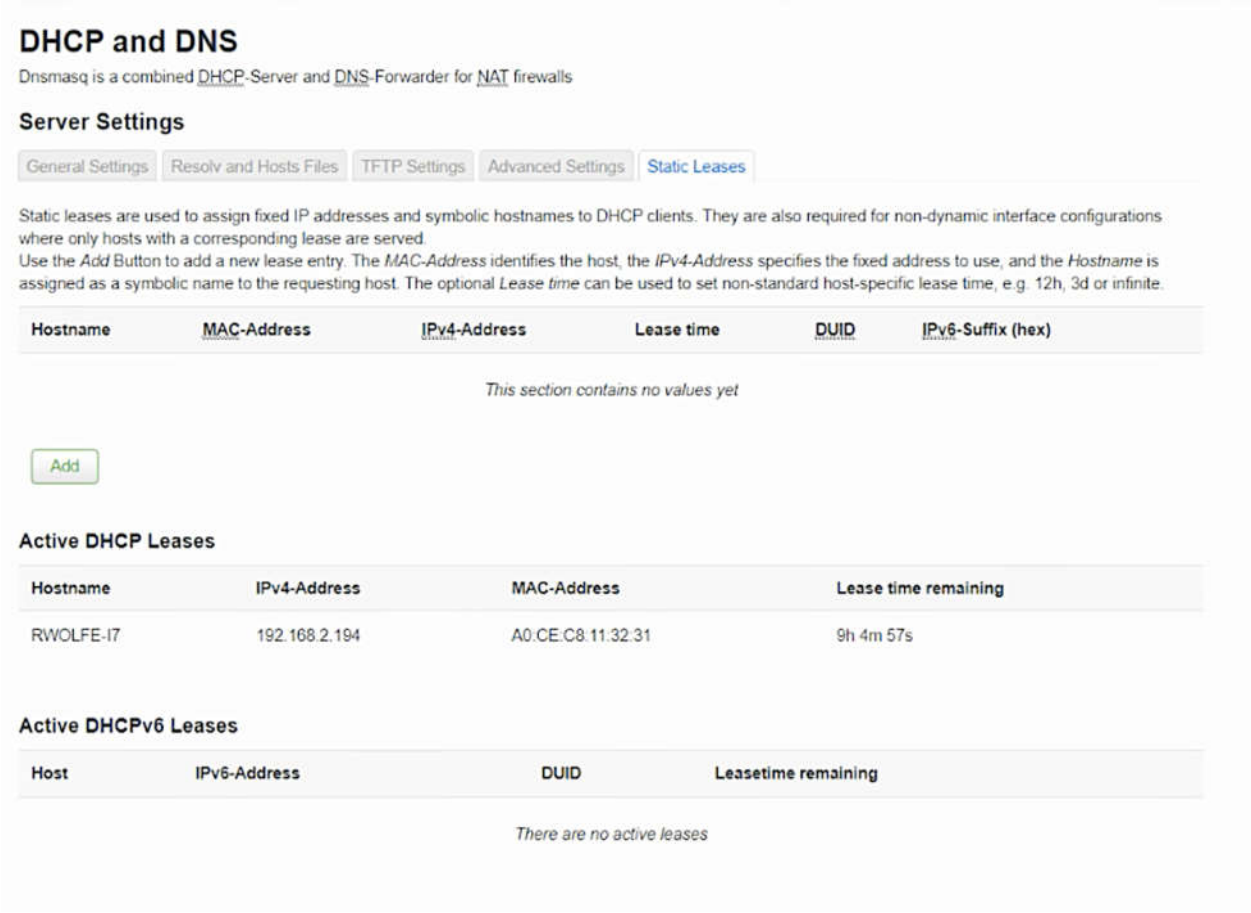
Size of DNS query cache: Number of cached DNS entries, where the maximum is 100 and 0 is no caching

8.3.4 Network – DHCP and DNS – Static Leases

The **DHCP and DNS/Static Leases** screen allows users to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served. Active IPv4 and IPv6 DHCP leases are also displayed on this tab.

Use the Add Button to add a new lease entry. The MAC-Address identifies the host, the IPv4-Address specifies the fixed address to use, and the Hostname is assigned as a symbolic name to the requesting host. The optional Lease time can be used to set non-standard host-specific lease time, e.g. 12h, 3d or infinite.

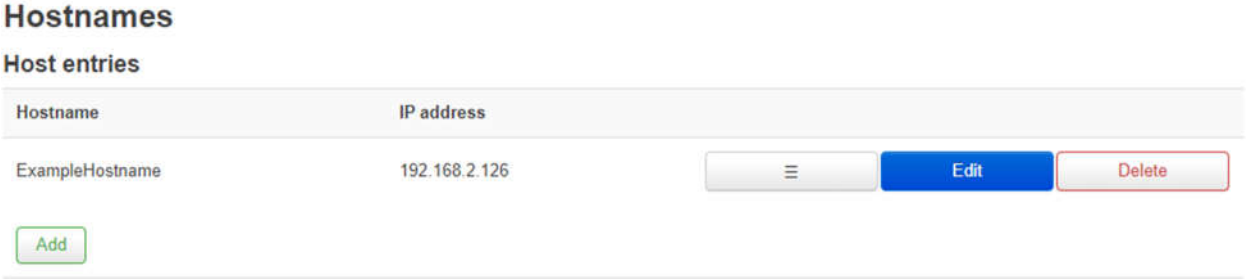
Network->DHCP and DNS->Static Leases



8.4 Network – Hostnames

Assign a hostname to a given IP address. This is a configuration option for assigning hostnames to devices on LAN or WAN networks, rather than using the traditional /etc/hosts file.

Network->Hostnames



Hostname: Hostname to assign.

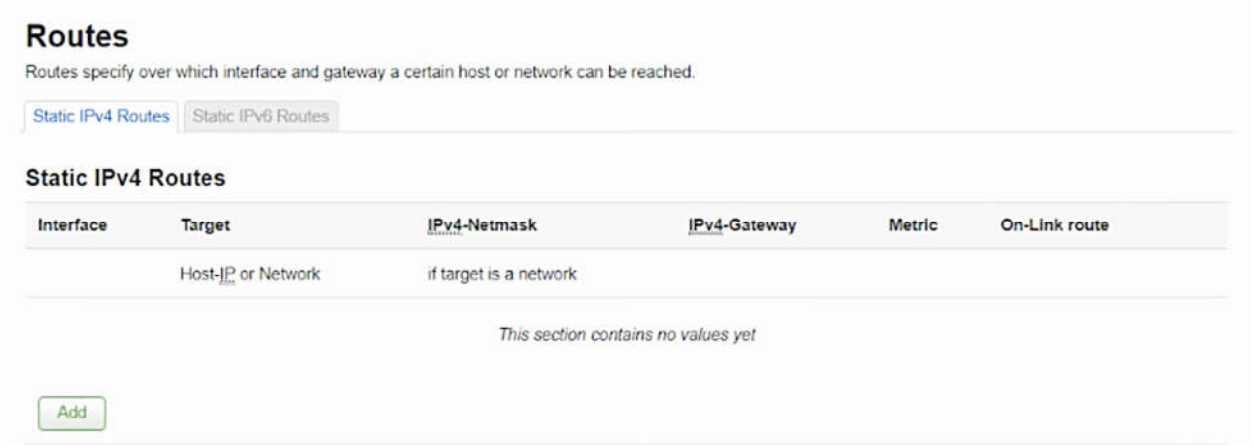
IP address: The IP address to be used for this host

8.5 Network – Static Routes

The following pages describe the configuration of IPv4 and IPv6 connections to ISP or upstream router. For uplink with native IPv4 connectivity, you can use the default configuration. Currently active routes can be viewed at the **Status->Routes** GUI page.

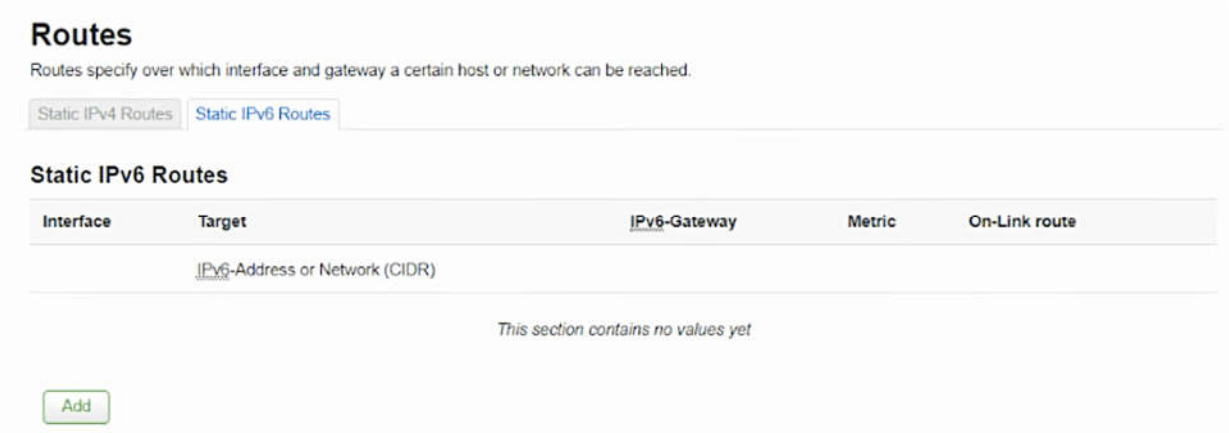
8.5.1 Network – Static Routes – Static IPv4 Routes

Network->Static Routes->Static IPv4 Routes



8.5.2 Network – Static Routes – Static IPv6 Routes

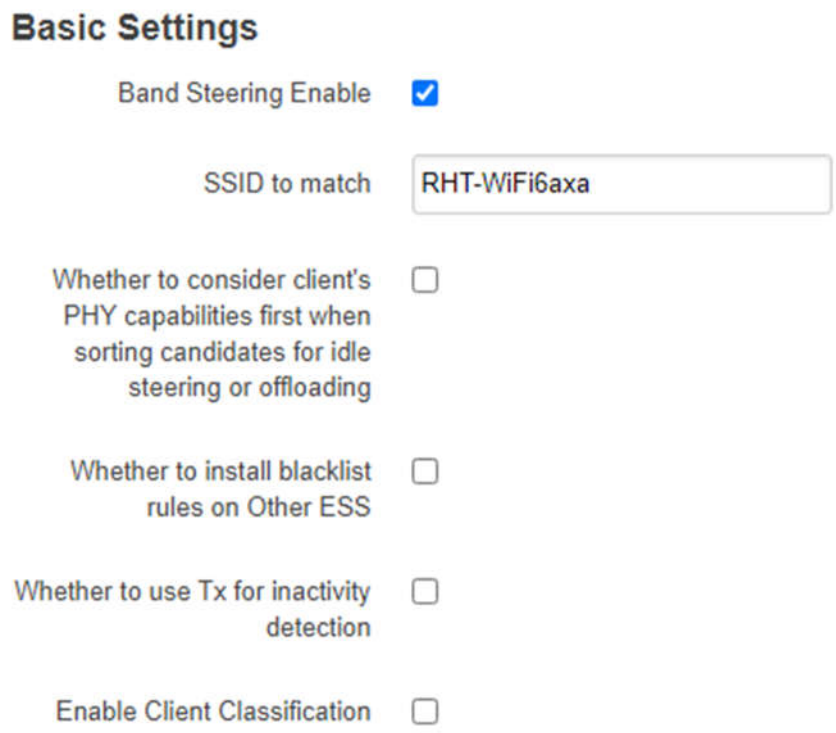
Network->Static Routes->Static IPv6 Routes



8.6 Network – Load Balancing

The Load Balancing page shows configuration of WHC(Whole Home Coverage) load balancing features.

8.6.1 Network – Load Balancing – Basic Settings



Band Steering Enable: Whether or not the load balancing logic is enabled

SSID to match: The SSID to match when limiting band steering to a single SSID

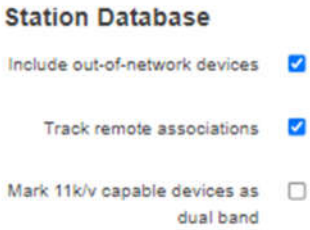
Whether to consider client's PHY capabilities first when sorting candidates for idle steering or offloading: Boolean flag indicating whether preference should be given to putting or keeping 802.11ac clients on 5 GHz or not

Whether to install backlist rules on Other ESS: To ensure bandwidth fairness and throughput, when a client is steered from one VAP to another on the same ESS(Extended Service Set), all VAPs on other ESSes must be blacklisted. A mechanism to disable band steering on specific SSIDs is implemented.

Whether to use Tx for inactivity detection: The client activity detection logic, used by band steering, is extended to be triggered upon successful Tx completion. By default, the idle client detection feature is enabled.

Enable Client Classification: In a Wi-Fi SON environment, mesh node client handling based on classification is introduced, providing a mechanism to classify clients into different groups and define specific behavior for each of the groups.

8.6.2 Network – Load Balancing – Station Database

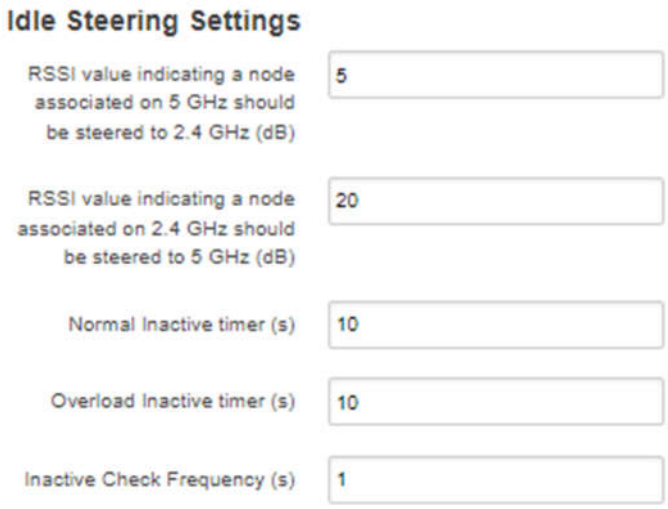


Include out-of-network devices: Whether or not out-of-network devices should be included in the database or not

Track remote associations: Whether the station database should track only local associations or both local and remote associations

Mark 11k/v capable devices as dual band: Enable for interoperation of dual-band, tri-band mesh modes in Wi-Fi SON environments

8.6.3 Network – Load Balancing – Idle Steering Settings



RSSI value indicating a node associated on 5 GHz should be steered to 2.4 GHz (dB): The point at which the measured or estimated RSSI on 2.4 GHz dictates a node associated on 5 GHz should be steered to 2.4 GHz

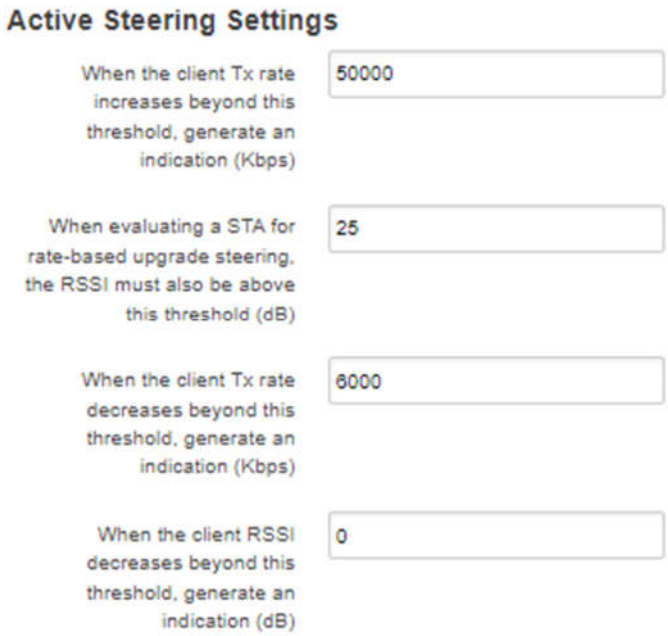
RSSI value indicating a node associated on 2.4 GHz should be steered to 5 GHz (dB): The point at which the measured or estimated RSSI on 5 GHz dictates a node associated on 2.4 GHz should be steered to 5 GHz

Normal inactive timer (s): Number of seconds for the inactivity value under no overload conditions on both bands

Overload inactive timer (s): Number of seconds for the inactivity value when the serving band is overloaded

Inactive Check Frequency (s): In seconds, how frequently to check for inactive associated STAs on both bands

8.6.4 Network – Load Balancing – Active Steering Settings



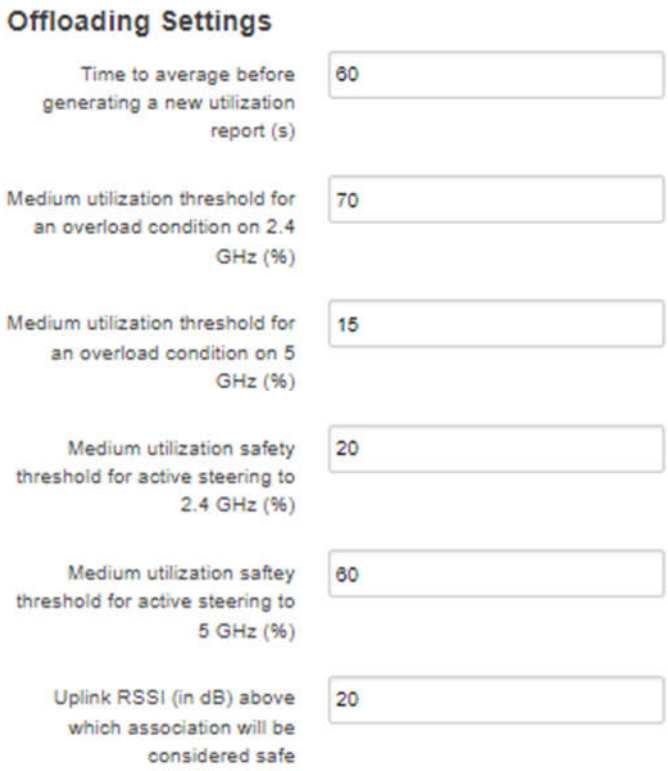
When the client Tx rate increases beyond this threshold, generate an indication (kbps): The rate at which a rate crossing event should be generated for a potential active client upgrade to 5 GHz

When evaluating a STA for rate-based upgrade steering, the RSSI must also be above this threshold (dB): The value the uplink RSSI on 2.4 GHz must be above to be considered for active steering to 5 GHz

When the client Tx rate decreases beyond this threshold, generates an indication (kbps): The rate at which a rate crossing event should be generated for a potential active client downgrade to 2.4 GHz

When the client RSSI decreases beyond this threshold, generate an indication (dB): The value the uplink RSSI on 5 GHz may be below to be considered for active steering to 2.4 GHz

8.6.5 Network – Load Balancing – Offloading Settings



Time to average before generating a new utilization report (s): Time to average before generating a new utilization report on both bands

Medium utilization threshold for an overload condition on 2.4 GHz (%): Medium utilization threshold for an overload condition on 2.4 GHz

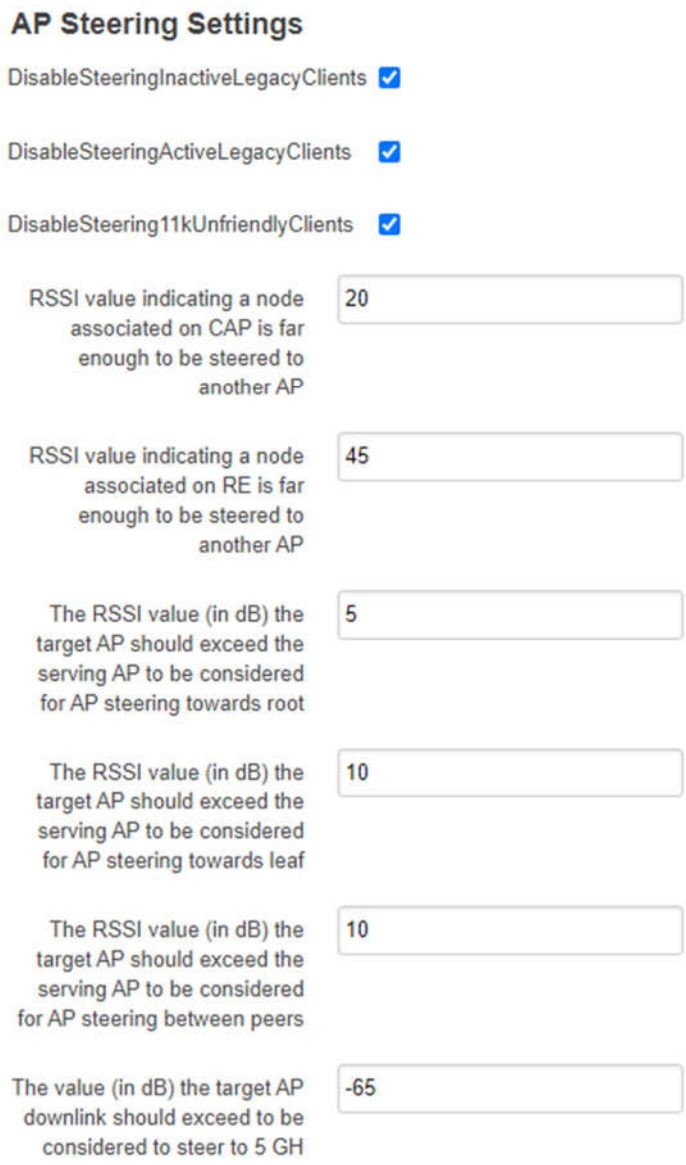
Medium utilization threshold for an overload condition on 5 GHz (%): Medium utilization threshold for an overload condition on 5 GHz

Medium utilization safety threshold for active steering to 2.4 GHz (%): The percentage of medium utilization that the measured plus projected utilization is allowed to reach before all further upgrade steering is disallowed until a new utilization measurement is done

Medium utilization safety threshold for active steering to 5 GHz (%): The percentage of medium utilization that the measured plus projected utilization is allowed to reach before all further upgrade steering is disallowed until a new utilization measurement is done

Uplink RSSI (in dB) above which association will be considered safe: Uplink RSSI above which pre-association steering and post-association offloading is allowed

8.6.6 Network – Load Balancing – AP Steering Settings



DisableSteeringInactiveLegacyClient: Configures AP steering of inactive legacy clients. Legacy clients are clients that support 802.11v basic service set (BSS) transition management (BTM) and do not support radio resource management (802.11k). Configure as 0 for monitoring/steering of inactive legacy clients.

DisableSteeringActiveLegacyClient: Configures AP steering of active legacy clients. Legacy clients are clients that support 802.11v basic service set (BSS) transition management (BTM)

and do not support radio resource management (802.11k). Configure as 0 for monitoring/steering of active legacy clients.

DisableSteering11kUnfriendlyClient: Configures AP steering of clients that are 802.11k unfriendly, load balancer will treat these clients as legacy clients. Configure as 0 for monitoring/steering of 802.11k unfriendly clients

RSSI value indicating a node associated on CAP is far enough to be steered to another AP: RSSI value (in dB) below which the uplink RSSI of a STA associated to the Central AP (CAP) must fall for it to be considered as a candidate for AP steering.

RSSI value indicating a node associated on RE is far enough to be steered to another AP:

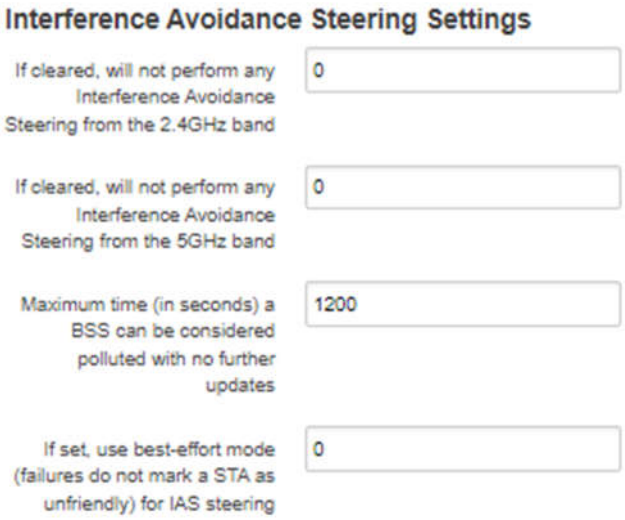
The RSSI value (in dB) the target AP should exceed the serving AP to be considered for AP steering towards root: In multi-AP mode, the RSSI value of the CAP but be better than that of the serving RE, as measured by an 802.11k Beacon Measurement, for the STA to be steered to the CAP

The RSSI value (in dB) the target AP should exceed the serving AP to be considered for AP steering towards leaf: In multi-AP mode, the amount of an RSSI of an RE must be better than that of the CAP, as measured by an 802.11k Beacon Measurement, for the STA to be steered to the RE

The RSSI value (in dB) the target AP should exceed the serving AP to be considered for AP steering between peers: In multi-AP mode, the amount the RSSI of an RE must be better than that of the serving RE, as measured by an 802.11k Beacon Measurement, for the STA to be steered to the RE

The value (in dB) the target AP downlink should exceed to be considered to steer to 5 GH: In multi-AP mode, the value of the downlink RSSI, as measured by an 802.11k Beacon Measurement, must be above for a 5 GHz channel to be preferred over 2.4 GHz when AP steering is used

8.6.7 Network – Load Balancing – Interference Avoidance Steering Settings



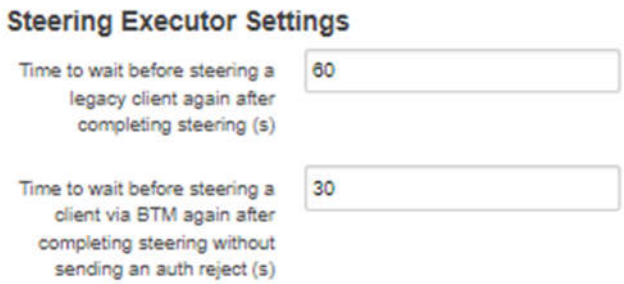
If cleared, will not perform any Interference Avoidance Steering from the 2.4 GHz band: Whether to enable Interference Avoidance Steering on 2.4 GHz. 0 to disable Interference Avoidance Steering on 2.4GHz, 1 to enable Interference Avoidance Steering on 2.4GHz.

If cleared, will not perform any Interference Avoidance Steering from the 5 GHz band: Whether to enable Interference Avoidance Steering on 5 GHz. 0 to disable Interference Avoidance Steering on 5GHz, 1 to enable Interference Avoidance Steering on 5GHz.

Maximum time (in seconds) a BSS can be considered polluted with no further updates: The number of seconds after which a BSS(Basic Service Set) that was previously marked as polluted is considered no longer polluted

If set, use best-effort mode (failures do not mark a STA as unfriendly) for IAS steering: Whether best effort steering should be used when the reason for the steering is IAS

8.6.8 Network – Load Balancing – Steering Executor Settings



Time to wait before steering a legacy client again after completing steering (s): Time to wait prior to steering the client again after a steering when either the legacy steering mechanism is used or the 802.11v BSS Transition Management mechanism is used but the client still attempts to authenticate on a BSS other than the target one

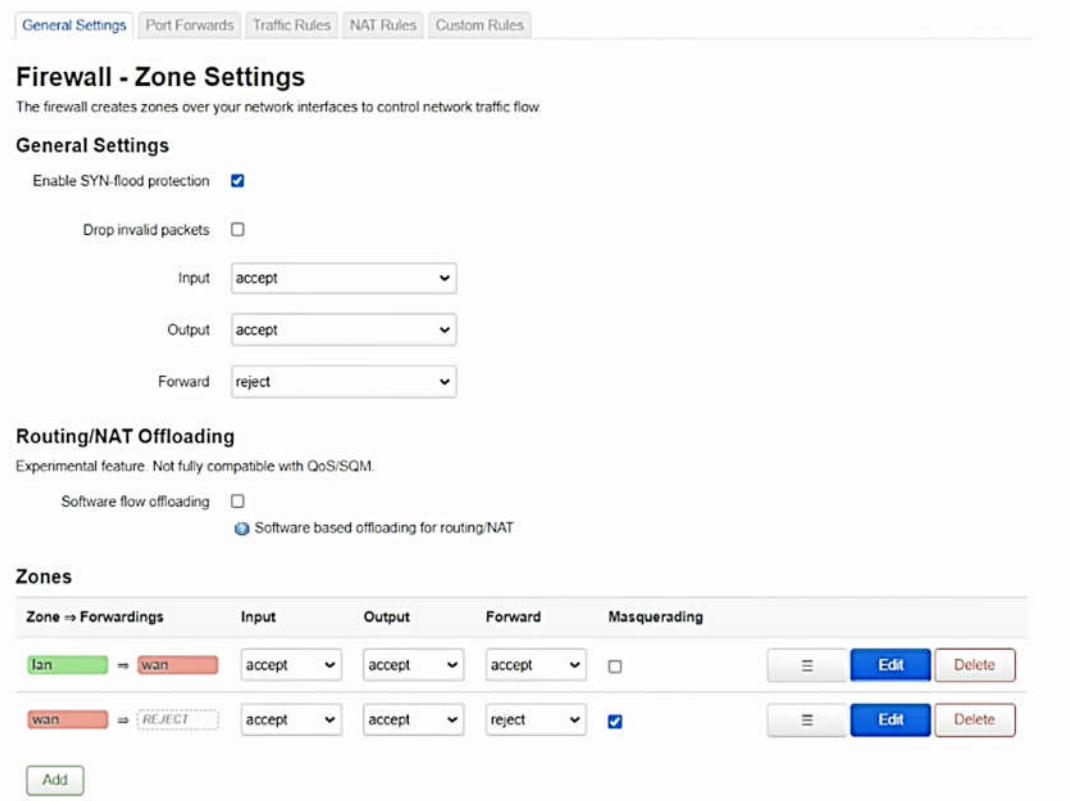
Time to wait before steering a client via BTM again after completing steering without sending an auth reject (s): Time to wait prior to steering an 11v-capable client again after a successful steering within BTMAssociationTime

8.7 Network – Firewall

The Firewall page allows users to create zones over their network interfaces to control network traffic flow. The Firewall is only used in Router mode for controlling LAN/WAN traffic flow.

8.7.1 Network – Firewall – General Settings

Network->Firewall->General Settings



Enable SYN-flood protection: Enable protection from SYN flood denial-of-service attacks

Drop invalid packets: Drop invalid packets that don't match any active connection

Input: Set rules for what happens to traffic entering the router through an interface in this zone. Dropdown options include accept, reject and drop.

Output: Set rules for what happens to traffic originating from the router, going through an interface in leaving this zone. Dropdown options include accept, reject and drop.

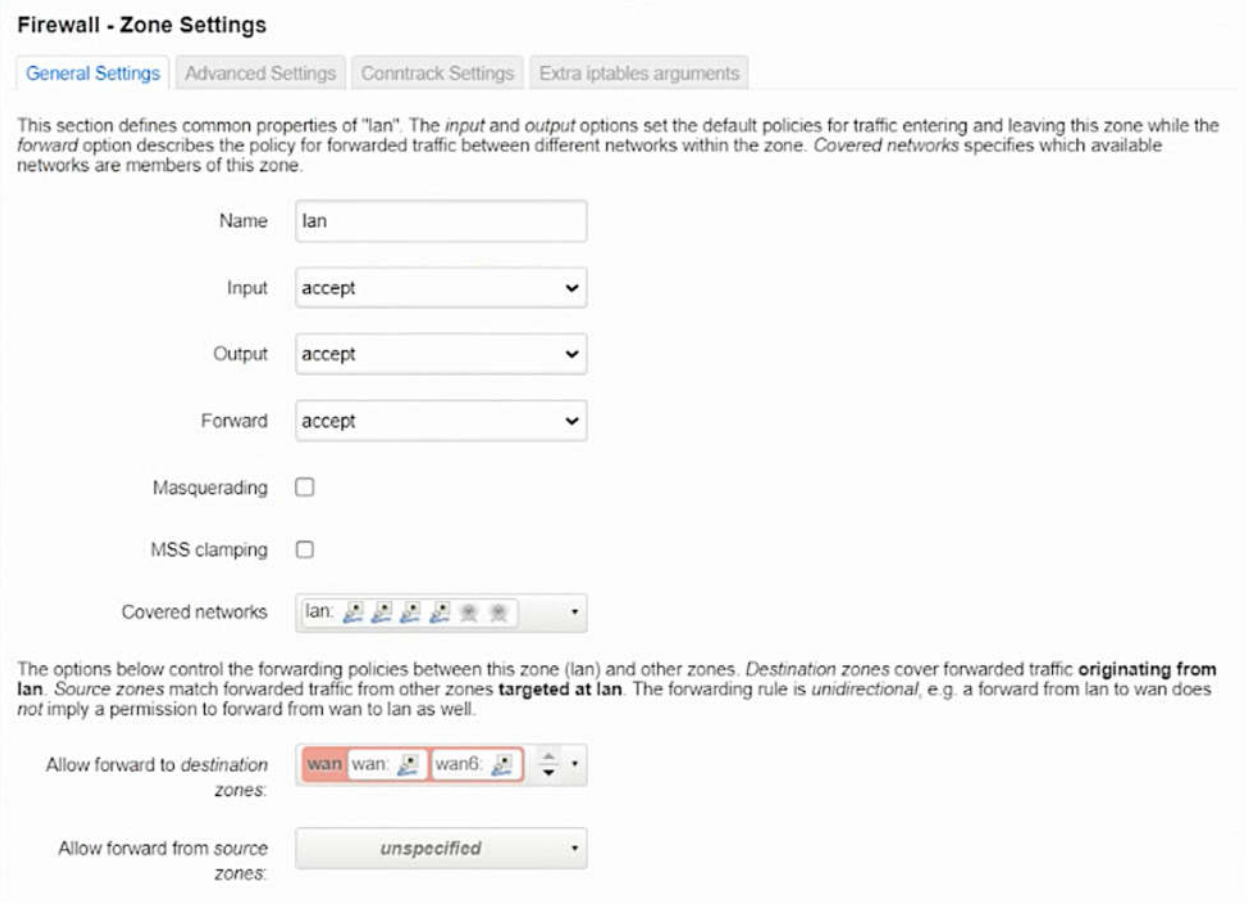
Forward: Describes rules for traffic passing between different networks in the same zone. Dropdown options include accept, reject and drop.

Software flow offloading: Enable offloading of the Linux kernel for known packet path

Zones: Group one or more interfaces to serve as a source or destination for forwarding, rules and redirects

8.7.2 Network – Firewall – General Settings – Zones/Edit/Add – General Settings

Editing Firewall zones requires configuration of the following options under General Settings:
Network->Firewall->General Settings->Zones/Edit/Add->General Settings



Name: What the following section defines common properties of

Input: Set rules for what happens to traffic entering the router through an interface in this zone. Dropdown options include accept, reject and drop.

Output: Set rules for what happens to traffic originating from the router, going through an interface in leaving this zone. Dropdown options include accept, reject and drop.

Forward: Describes rules for traffic passing between different networks in the same zone. Dropdown options include accept, reject and drop.

Masquerading: Specify whether NAT (IP Masquerading) is applied to outgoing traffic. Required for most LAN -> WAN traffic.

MSS clamping: Enable Maximum Segment Size clamping for outgoing traffic.

Covered networks: Specify which available networks are members of this zone. Dropdown options include lan, wan and wan6.

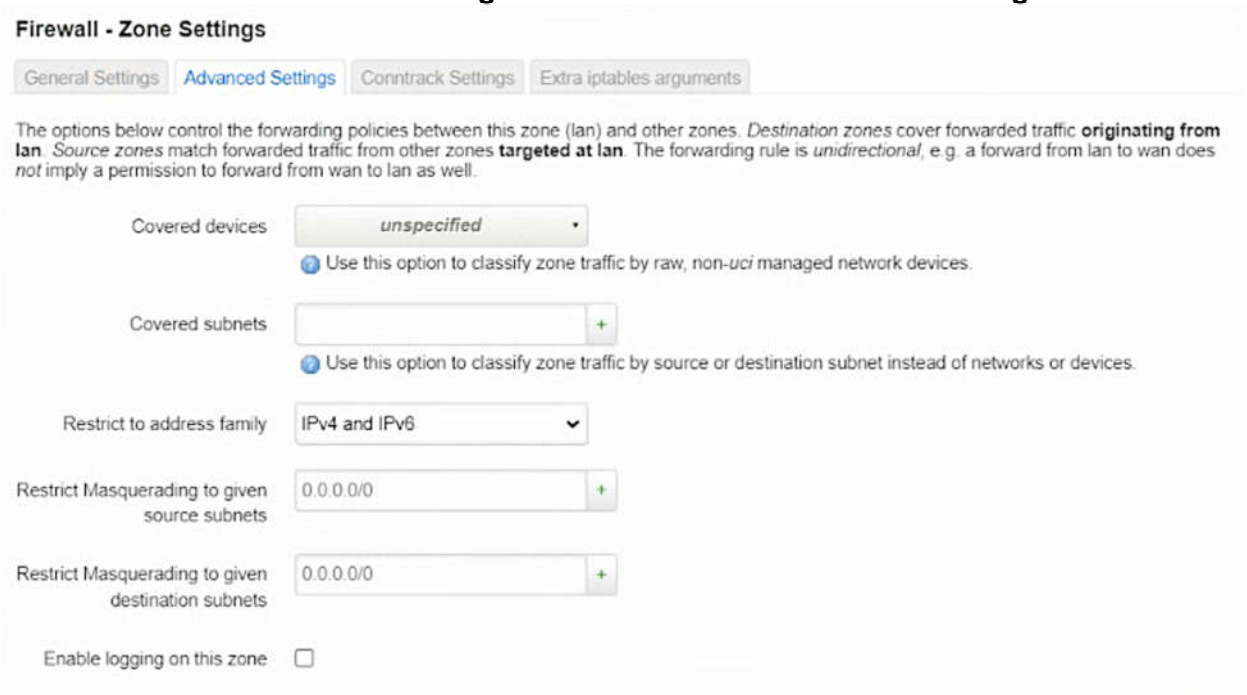
Allow forward to destination zones: Control unidirectional forwarded traffic originating from this zone to another defined zone. Dropdown options include wan and wan6.

Allow forward from source zones: Match forwarded traffic from other zones, targeted at this zone. Dropdown options include wan and wan6.

8.7.3 Network – Firewall – General Settings – Zones/Edit/Add – Advanced Settings

Editing Firewall zones requires configuration of the following options under **Firewall Zones/Advanced Settings**.

Network->Firewall->General Settings->Zones/Edit/Add->Advanced Settings



Covered devices: Classify zone traffic by raw, non-*uci* managed network devices

Covered subnets: Classify zone traffic by source or destination subnet instead of networks or devices

Restrict to address family: Restrict the firewall rules to IPv4, IPv6 or both.

Restrict Masquerading to given source subnets: Limit masquerading to just the given source subnets. Negation is possible by prefixing the subnet with "!" and multiple subnets are not allowed.

Restrict Masquerading to given destination subnets: Limit masquerading to the given destination subnets. Negation is possible by prefixing the subnet with "!" and multiple subnets are not allowed.

Enable logging on this zone: Enable logging in the filter and/or mangle tables for this zone.

8.7.4 Network – Firewall – General Settings – Zones/Edit/Add – Conntrack Settings

Editing Firewall zones requires configuration of the following options under **Firewall Zones/Conntrack Settings**.

Network->Firewall->General Settings->Zones/Edit/Add->Conntrack Settings

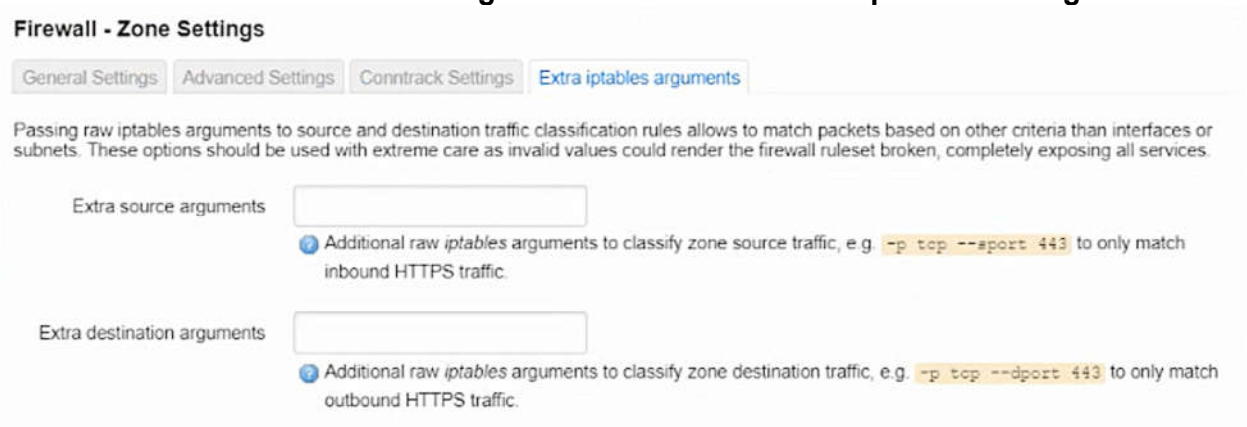
Allow "invalid" traffic: Do not install extra rules to reject forwarded traffic with conntrack state invalid. This may be required for complex asymmetric route setups.

Automatic helper assignment: Automatically assign conntrack helpers based on traffic protocol and port

8.7.5 Network – Firewall – General Settings – Zones/Edit/Add – Extra iptables Settings

Editing Firewall zones requires configuration of the following options under **Firewall Zones/Extra iptables arguments**.

Network->Firewall->General Settings->Zones/Edit/Add->Extra iptables Settings



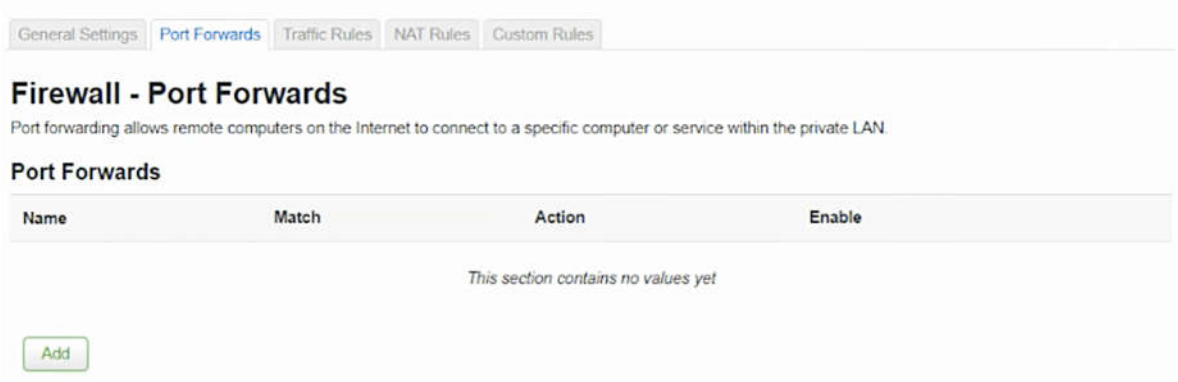
Extra source arguments: Additional arguments passed to *iptables* to classify zone source traffic, which is useful is specify extra match options

Extra destination arguments: Additional arguments passed directly to *iptables* to classify zone destination traffic

8.7.6 Network – Firewall – Port Forwards

The **Firewall/Port Forwards** page allows remote computers on the internet to connect to a specific computer or service within the private LAN.

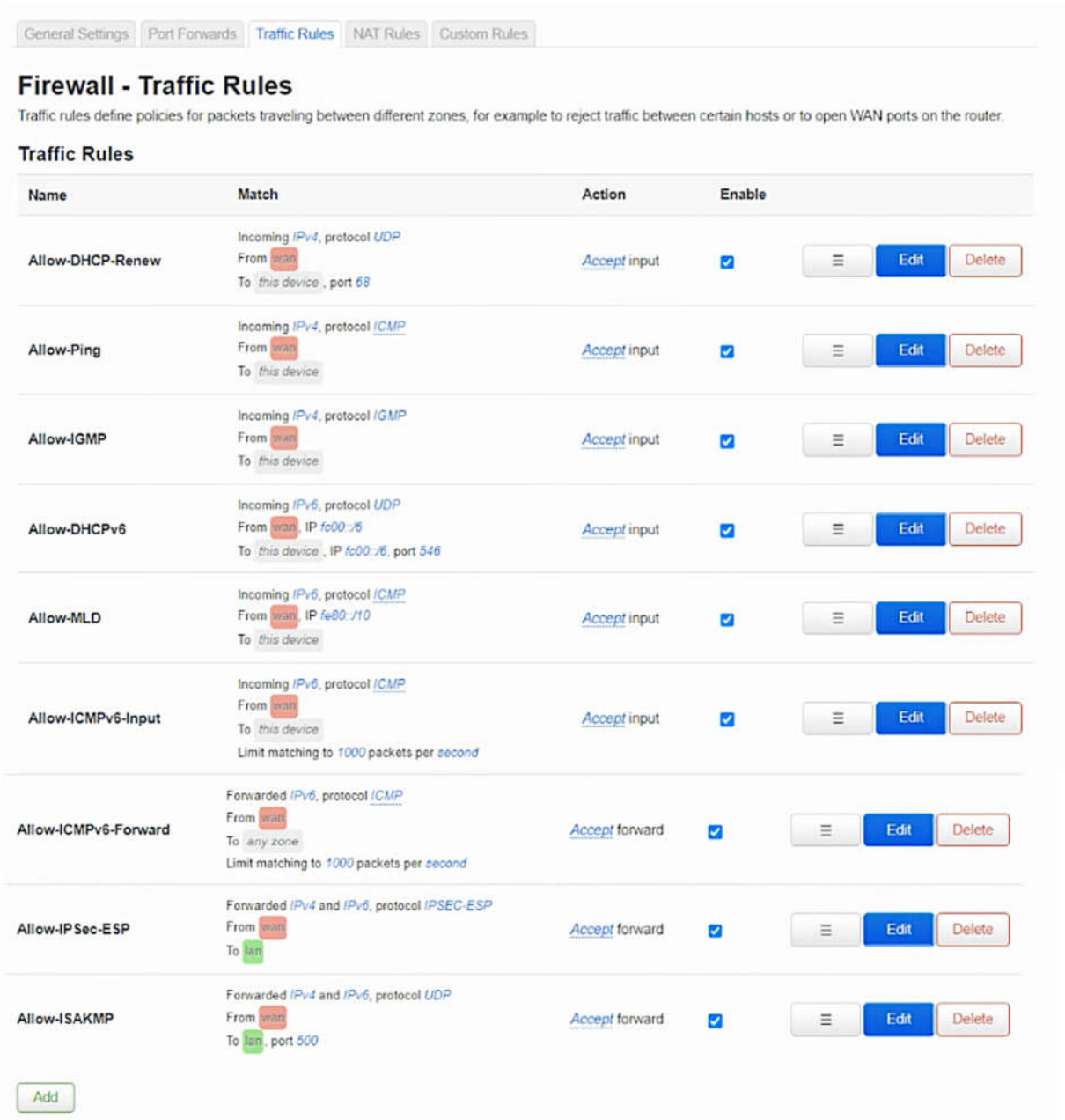
Network->Firewall->Port Forwards



8.7.7 Network – Firewall – Traffic Rules

The **Firewall/Traffic Rules** page defines policies for packets traveling between different zones.

Network->Firewall->Traffic Rules



The default set of traffic rules include:

Allow-DHCP-Renew: Accepts packets on port 68 for DHCP renewal

Allow-Ping: Allows the WAN to be pinged

Allow-IGMP: Allows IGMP traffic

Allow-DHCPv6: Opens port 546 to successfully send and receive DHCPv6 solicitation and advertisement messages

Allow-MLD: Allow MLD queries to receive the multicast packets on the WAN link.

Allow-ICMPv6-Input: Allow incoming IPv6 ICMP traffic (Used for ping request on IPv6)

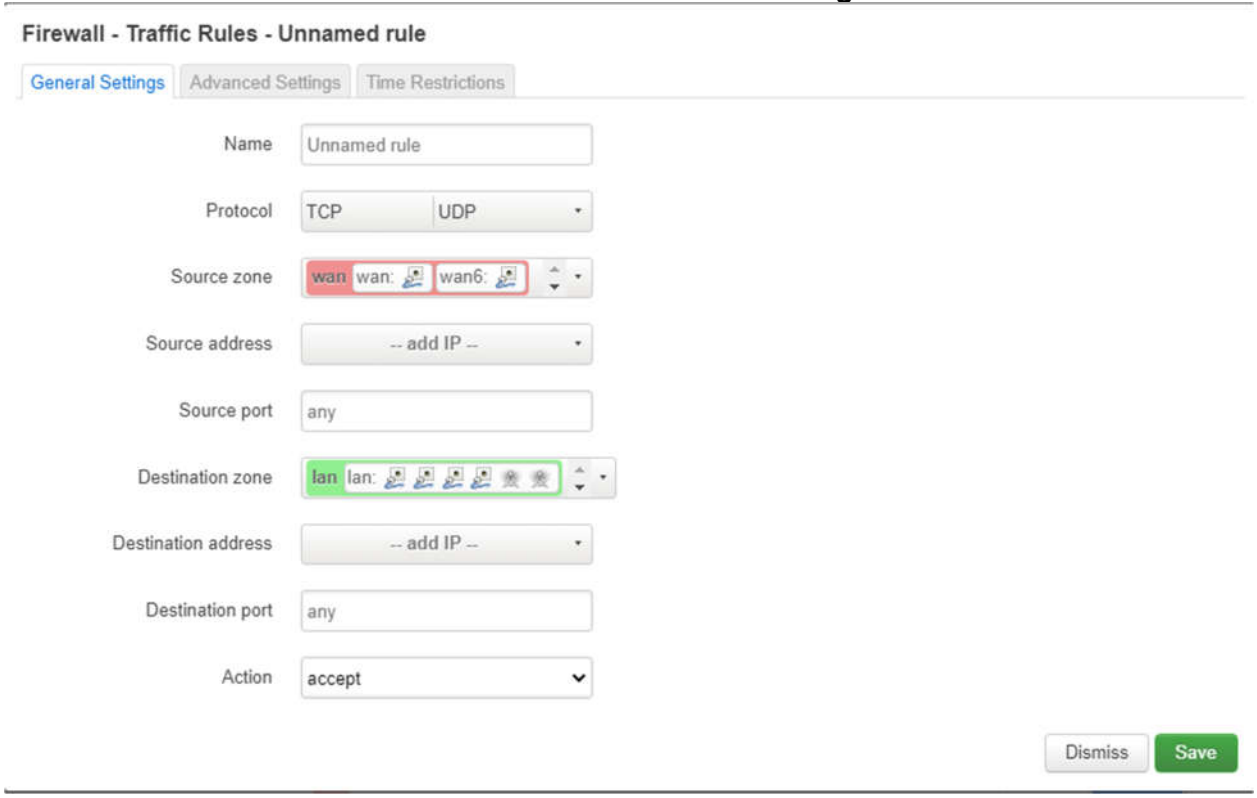
Allow-ICMPv6-Forward: Allow forwarding IPv6 ICMP traffic (Used for ping request on IPv6)

Allow-IPSec-ESP: Permit IPsec over ESP traffic from WAN to LAN

Allow-ISAKMP: Permit ISAKMP over UDP traffic from WAN to LAN

8.7.8 Network – Firewall – Traffic Rules – Edit/Add – General Settings

Network->Firewall->Traffic Rules->Edit/Add->General Settings



Name: Name to give the firewall traffic rule

Protocol: Match incoming traffic using the given protocol. Dropdown options include TCP, UDP, ICMP, IGMP, IPSEC-ESP and any

Source zone: Specifies the traffic source zone. Refers to one of the defined zone names. Dropdown options include device (output), any zone (forward), lan and wan

Source address: Match incoming traffic from the specified source IP address

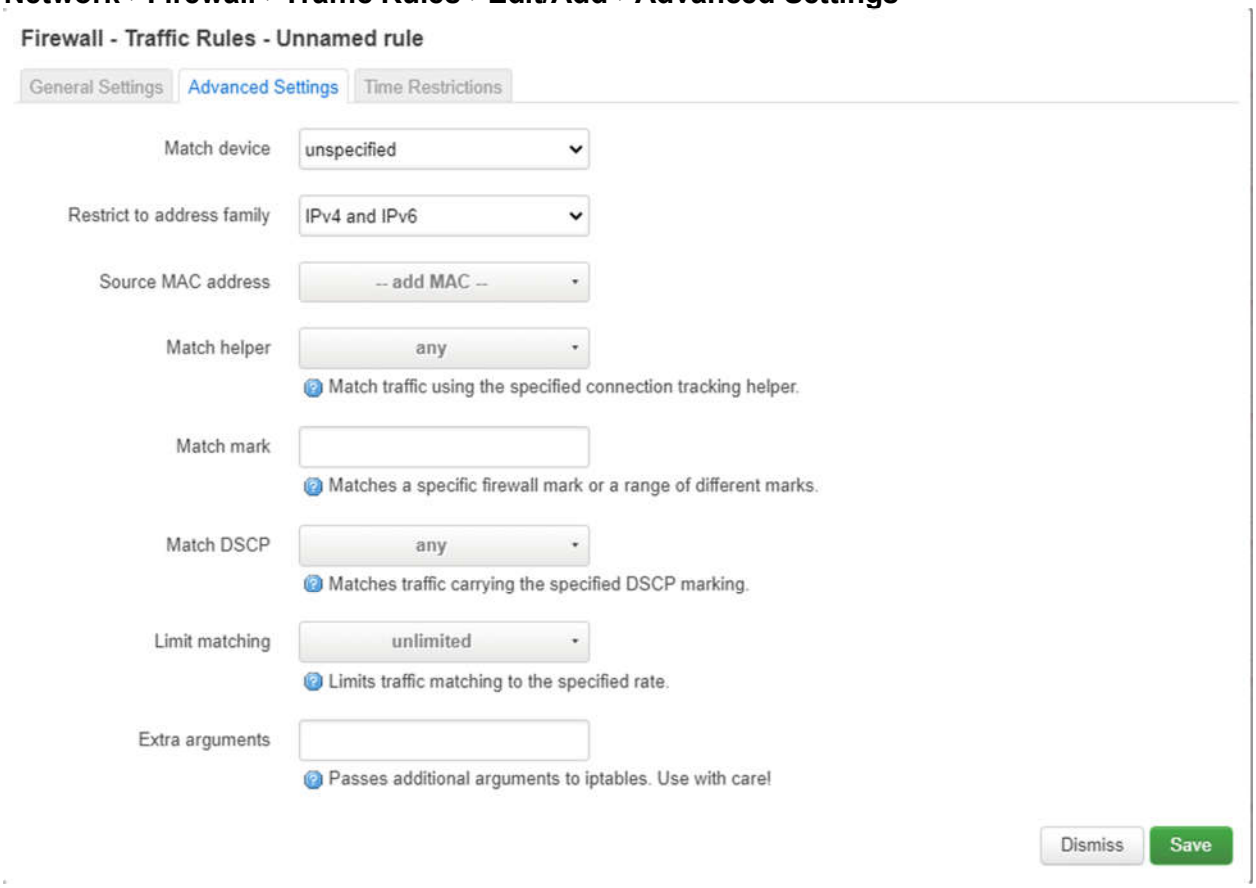
Destination zone: Specifies the traffic destination zone. Refers to one of the defined zone names. Dropdown options include device (output), any zone (forward), lan and wan

Destination address: Match incoming traffic directed to the specified destination IP address

Action: Firewall action for matched traffic. Dropdown options include drop, accept, reject, don't track, assign conntrack helper, apply firewall mark, XOR firewall mark and DSCP classification

8.7.9 Network – Firewall – Traffic Rules – Edit/Add – Advanced Settings

Network->Firewall->Traffic Rules->Edit/Add->Advanced Settings



Match device: Match traffic to inbound or outbound device. Dropdown options include unspecified, inbound device and outbound device

Restrict to address family: Protocol family to generate rules for. Dropdown options include IPv4 and IPv6, IPv4 only and IPv6 only

Match ICMP type: Select specific ICMP types to match. Values can be either exact ICMP type numbers or type names

Source MAC address: Match incoming traffic from the specified MAC address

Match Helper: Match traffic using the specified connection tracking helper. Dropdown options include Amanda backup and archiving proto (AMANDA), FTP passive connection tracking (FTP), RAS proto tracking (RAS), Q.931 proto tracking (Q.931), IRC DCC connection tracking (IRC), NetBIOS name service broadcast tracking (NETBIOS-NS), PPTP VPN connection tracking (PPTP), SANE scanner connection tracking (SANE), SIP VoIP connection tracking (SIP), SNMP monitoring connection tracking (SNMP), TFTP connection tracking (TFTP), RTSP connection tracking (RTSP)

Match Mark: If specified, match traffic against the given firewall mark, e.g. 0xFF to match mark 255 or 0x0/0x1 to match any even mark value. The match can be inverted by prefixing the value with an exclamation mark, e.g. !0x10 to match all but mark #16.

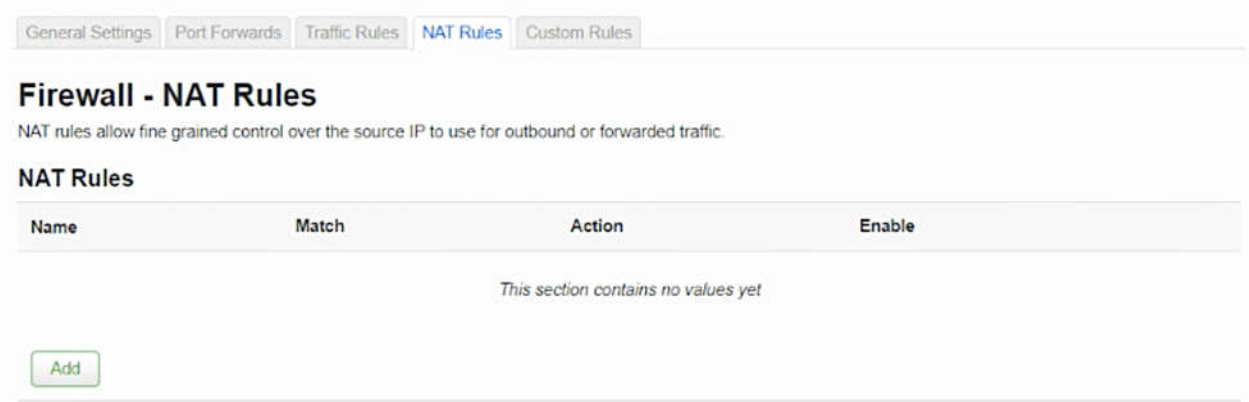
Match DSCP: Matches traffic carrying the specified DSCP marking.

Limit Matching: Maximum average matching rate; specified as a number, with an optional /second, /minute, /hour or /day suffix.

Extra Arguments: Extra arguments to pass to iptables

8.7.10 Network – Firewall – NAT Rules

Network->Firewall->NAT Rules



8.7.11 Network – Firewall – Custom Rules

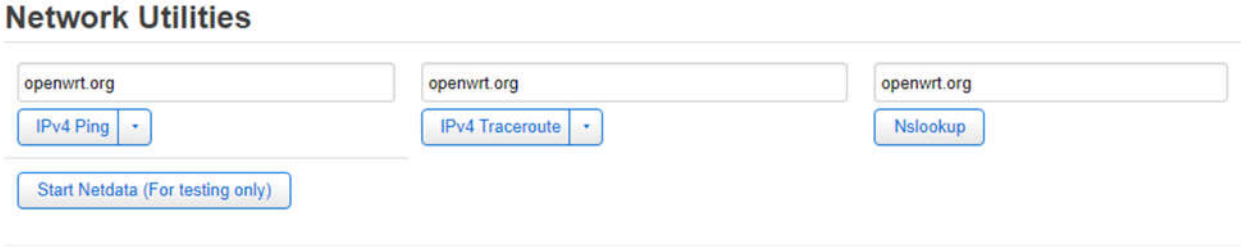
The **Firewall/Custom Rules** page allows users to execute arbitrary iptables commands, which are not otherwise covered by the firewall framework.

Network->Firewall->Custom Rules

8.8 Network – Diagnostics

Network Utilities on the Diagnostics page include dropdowns for IPv4 Ping and IPv6 Ping, IPv4 Traceroute and IPv6 Traceroute. There is a button for Nslookup, as well as a button to start Netdata and open the Netdata dashboard in a new tab. Netdata is for test purposes only and is not intended for secure operating environments.

Network->Diagnostics

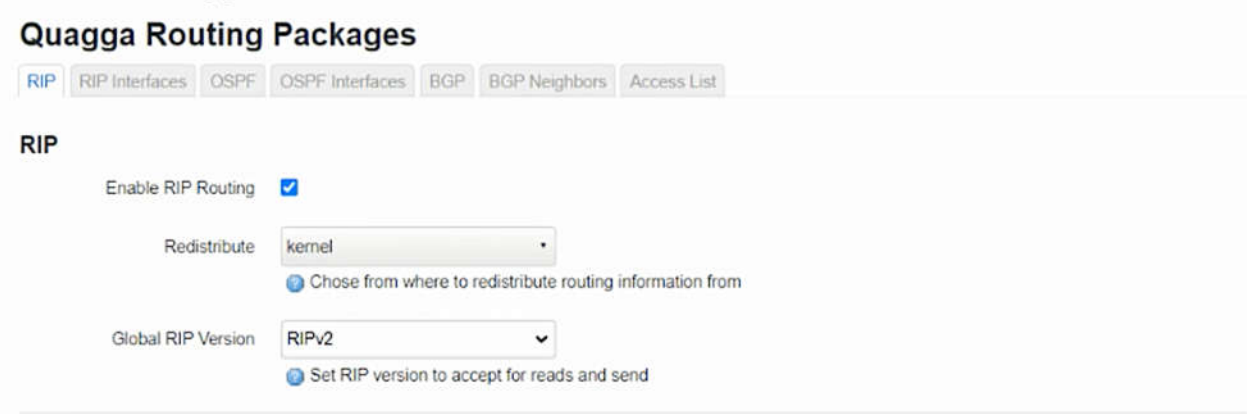


8.9 Network – Quagga

Quagga is a software suite the CabinLink 6 uses to implement RIP, OSPF, and BGP routing protocols.

8.9.1 Network – Quagga – RIP

Network->Quagga->RIP



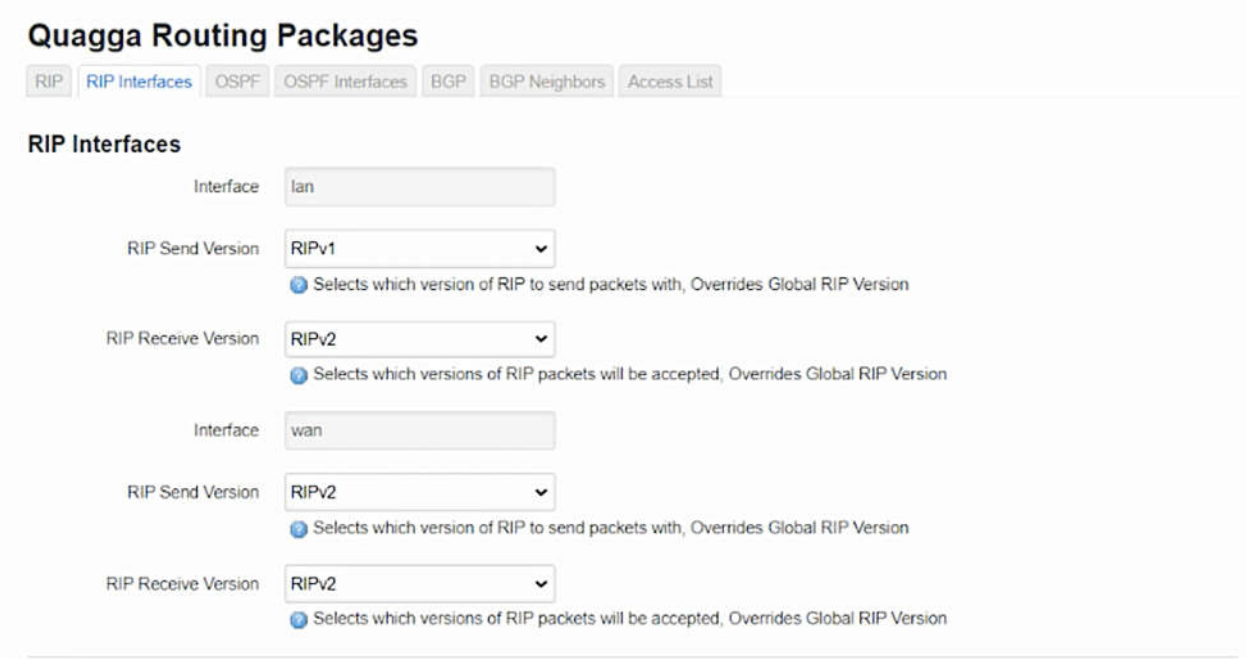
Enable RIP Routing: Enable the Routing Information Protocol (RIP)

Redistribute: Choose from where to redistribute routing information from. Dropdown options include kernel, static, connected, ospf and bgp.

Global RIP Version: RIP version used to send and accept packets. Dropdown options include RIPv1 and RIPv2.

8.9.2 Network – Quagga – RIP Interfaces

Network->Quagga->RIP Interfaces



Interface: The interface for the inbound and outbound RIP packets

RIP Send Version: Selects which version of RIP to send packets with, Overrides Global RIP Version. Dropdown options include RIPv1, RIPv2, and RIPv1 and RIPv2.

RIP Receive Version: Selects which versions of RIP packets will be accepted, Overrides Global RIP Version. Dropdown options include RIPv1, RIPv2, and RIPv1 and RIPv2.

8.9.3 Network – Quagga – OSPF

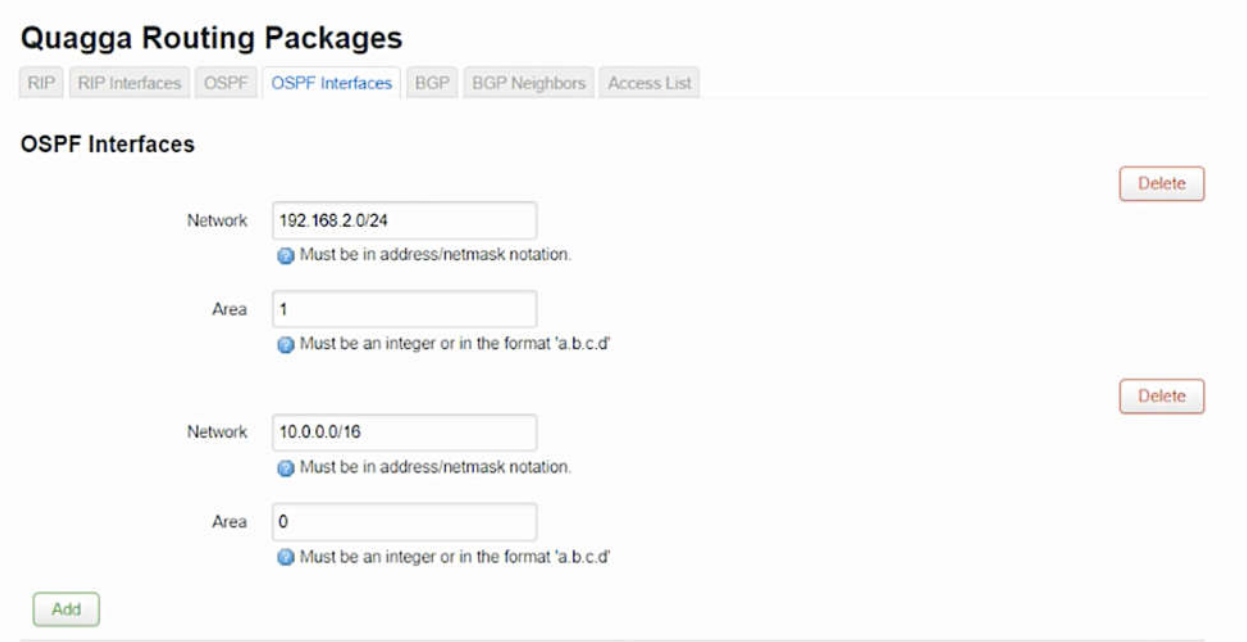
Network->Quagga->OSPF

Enable OSPF Routing: Enable the Open Shortest Path First (OSPF) protocol

Redistribute: Choose from where to redistribute routing information from. Dropdown options include kernel, static, connected, rip and bgp.

8.9.4 Network – Quagga – OSPF Interfaces

Network->Quagga->OSPF Interfaces

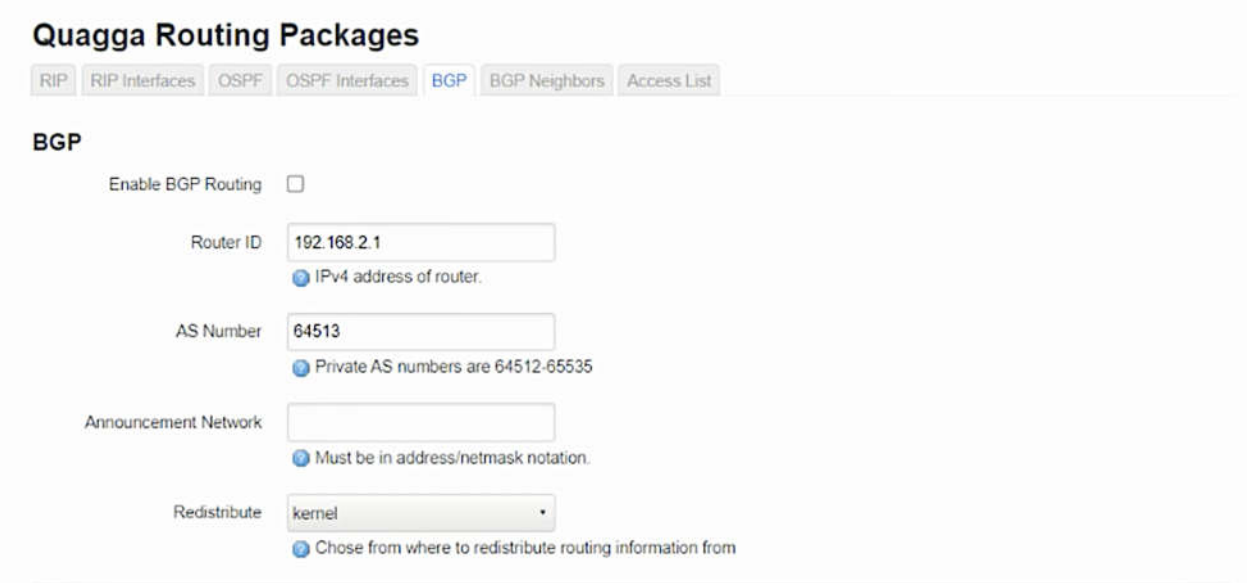


Network: IP address range of the interface to enable OSPF on. Must be in address/netmask notation

Area: Must be an integer or in the format 'a.b.c.d'

8.9.5 Network – Quagga – BGP

Network->Quagga->BGP



Enable BGP Routing: Enable the Border Gateway Protocol (BGP)

Router ID: IPv4 address of router

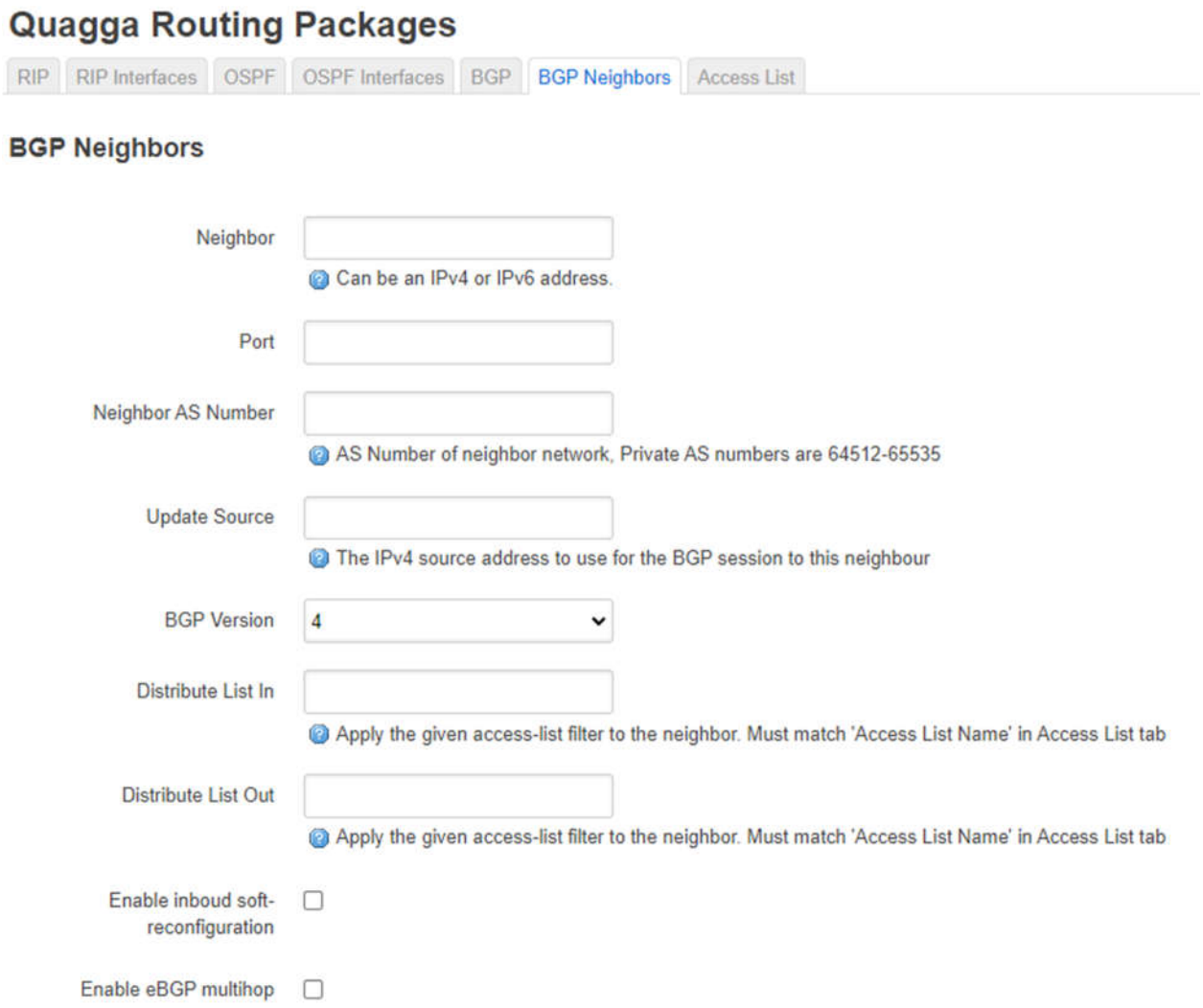
AS Number: AS number is an identification of autonomous system. BGP protocol uses the AS number for detecting whether the BGP connection is internal one or external one. Private AS numbers are 64512-65535

Announcement Network: The network to announce to all neighbors. Must be in address/netmask notation

Redistribute: Choose from where to redistribute routing information from

8.9.6 Network – Quagga – BGP Neighbors

Network->Quagga->BGP Neighbors



Neighbor: IPv4 or IPv6 address of neighbor to peer with

Port: Optional Port to use to connect to neighbor

Neighbor AS Number: AS number of the neighbor network

Update Source: Specify the IPv4 source address to use for the BGP session to this neighbor

BGP Version: BGP Version to use for the neighbor. BGP version 4 is the default value. BGP version 4+ means that the neighbor supports Multiprotocol Extensions for BGP-4. BGP version

4- is for when the neighbor speaks the old Internet-Draft revision 00's Multiprotocol Extensions for BGP-4. Dropdown options include 4, 4+, and 4-

Distribute List In: Apply the given access-list filter to the neighbor. Must match 'Access List Name' in Access List tab

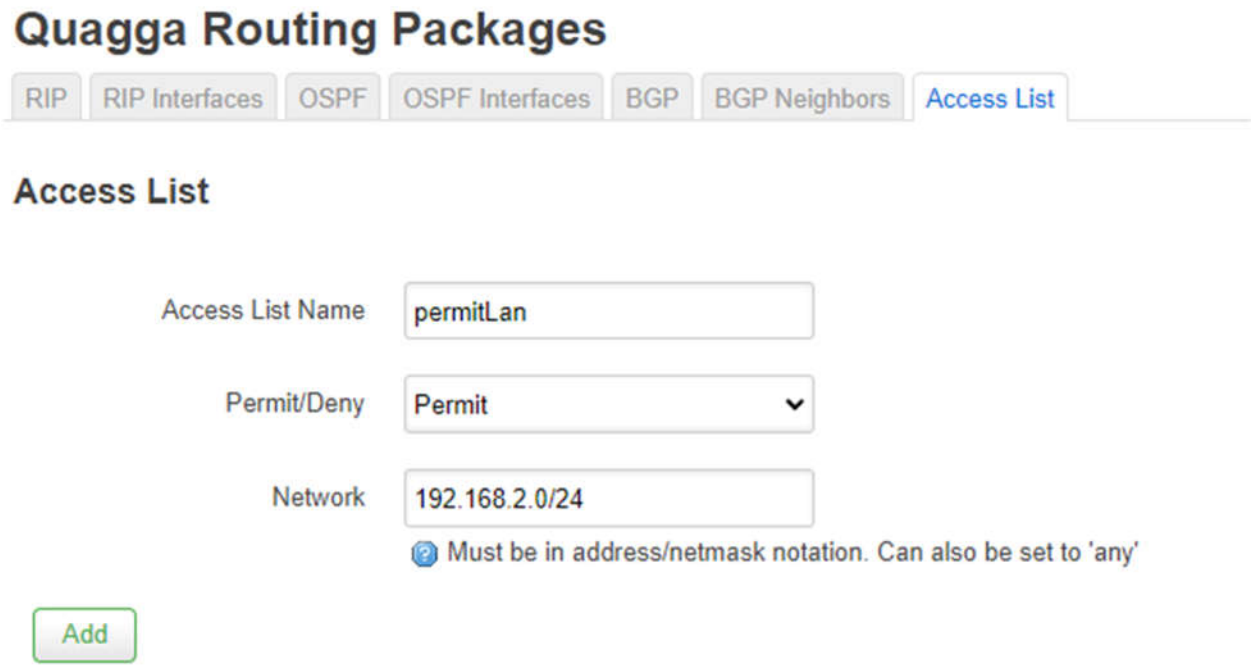
Distribute List Out: Apply the given access-list filter to the neighbor. Must match 'Access List Name' in Access List tab

Enable inbound soft-reconfiguration: Enables you to generate inbound updates from a neighbor, change and activate BGP policies without clearing the BGP session

Enable eBGP Multihop: Enables a neighbor connection between two eBGP peers that do not have a direct connection

8.9.7 Network – Quagga – Access List

Network->Quagga->Access List



Access List Name: Name to give the access list

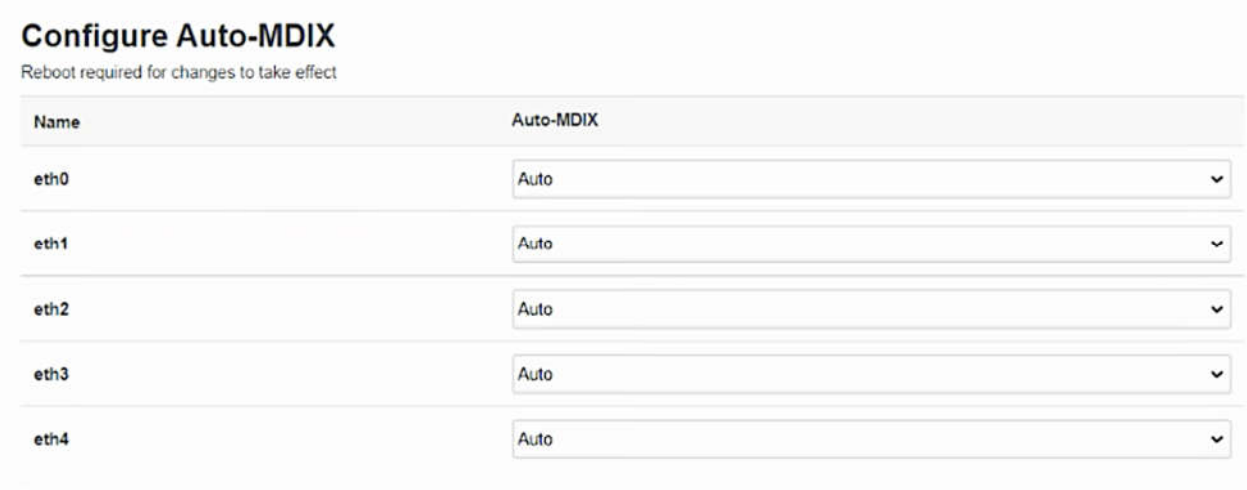
Permit/Deny: Permit or deny access to the given IPv4 network

Network: IPv4 address to perform filtering on in address/netmask notation

8.10 Network – Enable/Disable Auto-MDIX

LAN ports are configurable to set Medium Dependent Interface (MDIX) on, off or auto. By default it is set to auto.

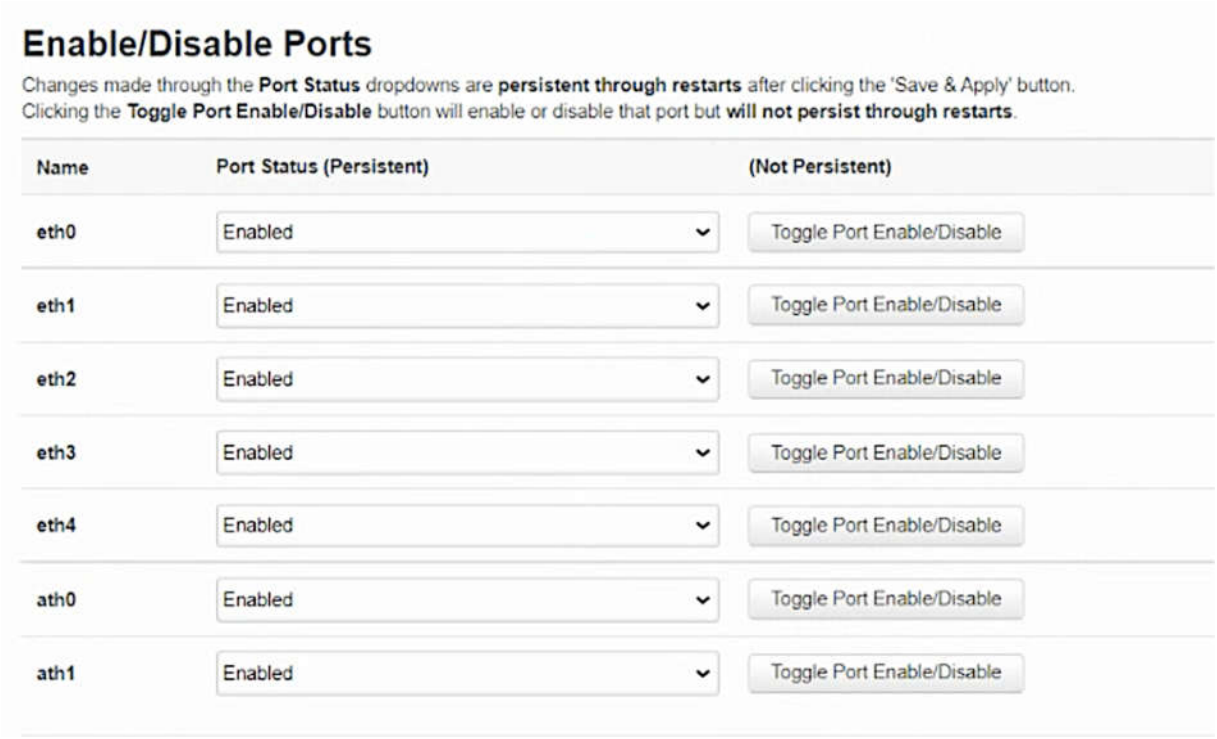
Network->Enable/Disable Auto-MDIX



8.11 Network – Enable/Disable Ports

This page allows you to enable or disable ports on the CL6. Disabling an eth port will disable the associated ethernet port on the CL6. Disabling an ath port will disable the Wi-Fi network associated with that port. Changes made through the Port Status dropdowns will be persistent through restarts.

Network->Enable/Disable Ports



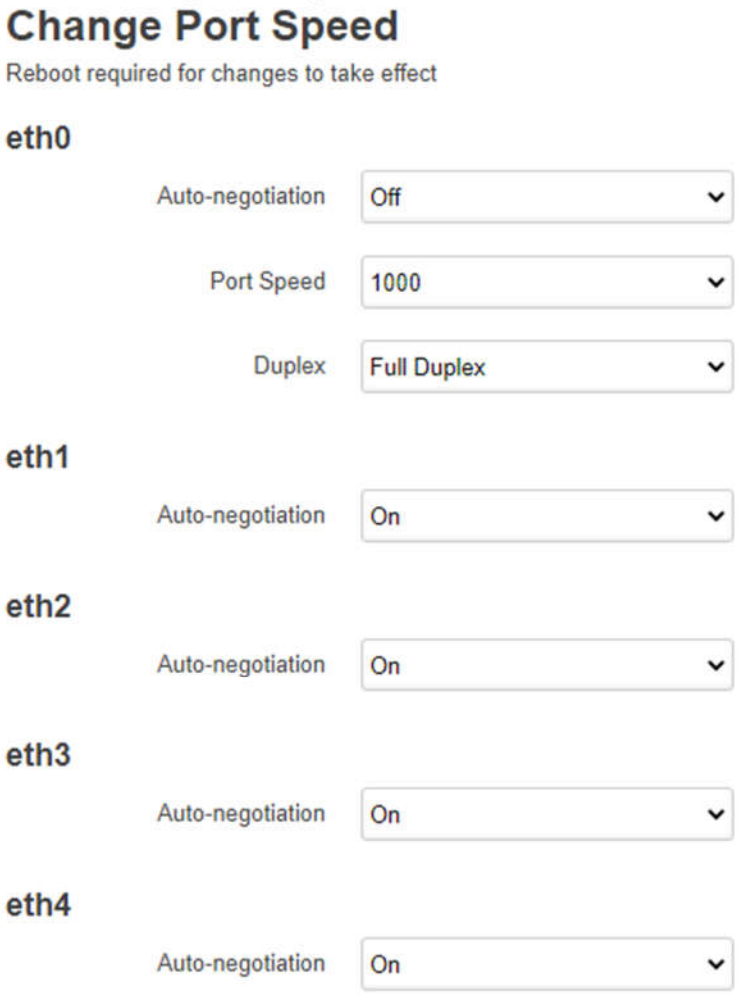
Port Status (Persistent)
In order to set the desired Wi-Fi state (enable/disable) at boot time, the Wi-Fi state option in the UCI configuration file should be set before the CL6 unit is booted. In the Port Status column, set the CL6 to the desired state and reboot the unit.

Not Persistent
If you would like to change the state at runtime, you can enable and disable Wi-Fi using the **Not Persistent** column, and these changes will take effect immediately (without a reboot).

8.12 Network – Change Port Speed

Configure the port speed for each ethernet port on the CL6. Auto-negotiation is enabled by default. To configure Port Speed and Duplex, set Auto-negotiation to off. Port Speed dropdown options include 10, 100, and 1000. Eth4 has an additional option of 2500. Duplex dropdown options include Half Duplex and Full Duplex

Network->Change Port Speed



8.13 Network – Airtime Fairness

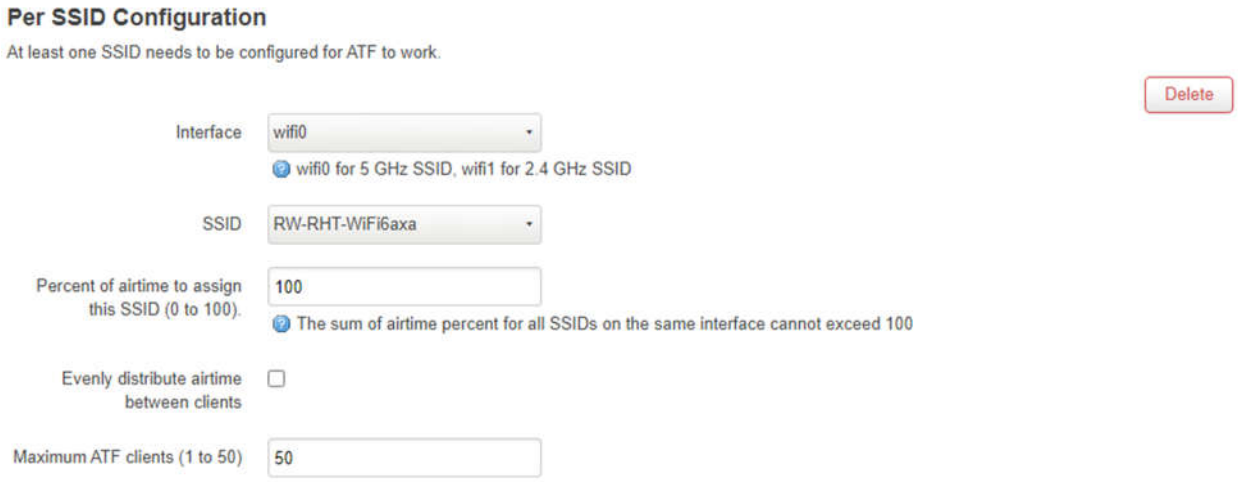
The Airtime Fairness page allows users to configure SSIDs to distribute bandwidth evenly between clients based on the maximum allowed clients for a SSID.

Network->Airtime Fairness

Enable Airtime Fairness: Enable/Disable

Allow users to share unused bandwidth on 5GHz SSIDs: When the box is checked, unallocated airtime will be distributed between connected clients. When the box is unchecked, clients will be limited to their configured bandwidth.

Allow users to share unused bandwidth on 2.4GHz SSIDs: When the box is checked, unallocated airtime will be distributed between connected clients. When the box is unchecked, clients will be limited to their configured bandwidth.



Interface: Wireless interface to use for the SSID configuration. Wifi0 for 5GHz SSIDs, wifi1 for 2.4GHz SSIDs

SSID: SSID to use for this ATF configuration

Percent of airtime to assign this SSID: Percent of the interface's total bandwidth to distribute between clients associated to the SSID.

Maximum ATF clients: Maximum number of clients for SSID. This field is used for per client airtime calculation and will not limit the amount of clients that can connect to the SSID.

9. CabinLink 6 System Reset

To perform a system reset on the CL6, pin 2 of the external J5 connector needs to be grounded for a time of 10 seconds or more and then disconnected. See Figure 7 for the location of pin 2 on the J5 connector. When a system reset is performed, the default configuration file will be applied to the system. 6.5 explains how to change your default configuration. After the reset is performed, the GUI can be accessed using the IP address defined in your default configuration.

10. CabinLink 6 Command Line Access

By default, an SSH server runs on the CabinLink 6. Any configured user login account, including the root user, may use an SSH client and perform a password login.

The CL6 also supports SSH key login for the root account. This is supported by all operating systems. Users will need to install a SSH client, such as PuTTY, that allows SSH key login. A SSH keygen tool, e.g. ssh-keygen, is also needed to generate public/private SSH keys.

Once a public SSH key is generated on the PC, navigate to System->Users->Root User (6.2.2) in the GUI. Scroll down to the Root User section and check the box that says "Allow root SSH login". After this is done, paste the public SSH key(s) into the SSH keys field and click "Save & Apply". A different key may be added for each computer requiring root access to the CL6.

You should now be able to access the CL6 via SSH using the computer you generated the SSH keys for. Use a SSH client such as PuTTY and configure it to connect to the CL6 using a Host key.

With an established SSH connection, you will be able to remotely control and configure the CL6 through the commands listed in section 4.1 in the CL6 ICD (References 1.1).

With an optional CL6 test board (PN 2924-200031), which breaks out the J5 pins (Figure 7) for test and debug, a serial DB9 connector provides console access. To do so, start by connecting the test board to the J5 connector. Then, connect a serial cable with a DB9 connector to the test board from a host computer. From the host computer, run a serial terminal application and configure the serial port for 115200 baud, no parity, 8 data bits, and one stop bit (N81). Open the connection to gain access to the CL6 command line.

Appendix A – Acronyms

Terminology and Abbreviations

BSS	Basic Service Set
CL6	CabinLink 6
DSCP	Differentiated Services Code Point
ESS	Extended Service Set
GUI	Graphical User Interface
ICD	Interface Control Document
LRU	Line-Replaceable Unit
OUI	Organizationally Unique Identifier
PVID	Port Virtual Local Area Network Identifier
QoS	Quality of Service
SNR	Signal-to-noise ratio
SSH	Secure Shell
SSID	Service Set Identifier
VAP	Virtual Access Point
VLAN	Virtual Local Area Network
WAP	Wireless Access Point
WHC	Whole Home Coverage

Appendix B – 2.4 GHz and 5 GHz radio supported operating modes

For 5 GHz Band

Mode	Band	Channel	Width
AX	5 GHz (11axa)	Auto, 36-165	20 MHz (HE20), 40 MHz (HE40), 40 MHz (HE40-), 40 MHz (HE40+), 80 MHz (HE80)
AC	5 GHz (11ac), 5 GHz (11a)	Auto, 36-165	20 MHz (VHT20), 40 MHz (VHT40), 40 MHz (VHT40-), 40 MHz (VHT40+), 80 MHz (VHT80)
N	5 GHz (11na)	Auto, 36-165	20 MHz (HT20), 40 MHz (HT40), 40 MHz (HT40-), 40 MHz (HT40+)
Legacy	5 GHz (11a)	Auto, 36-165	

For 2.4 GHz Band

Mode	Band	Channel	Width
AX	2.4 GHz (11axg)	Auto, 1-11	20 MHz (HE20), 40 MHz (HE40), 40 MHz (HE40-), 40 MHz (HE40+),
N	2.4 GHz (11ng)	Auto, 1-11	20 MHz (HT20), 40 MHz (HT40), 40 MHz (HT40-), 40 MHz (HT40+)
Legacy	2.4 GHz (11b), 2.4 GHz (11bg), 2.4 GHz (11g)	Auto, 1-11	

Appendix C – Supported Country Codes

Country	Country Code
Afghanistan	AF
Albania	AL
Algeria	DZ
American Samoa	AS
Argentina	AR
Aruba	AW
Armenia	AM
Australia	AU
Austria	AT
Azerbaijan	AZ
Bahamas	BS
Bahrain	BH
Bangladesh	BD
Barbados	BB
Bermuda	BM
Belarus	BY
Belgium	BE
Belize	BZ
Bhutan	BT
Bolivia	BO
Bosnia Herzegovina	BA
Brazil	BR
Brunei Darussalam	BN
Bulgaria	BG
Burkina Faso	BF
Canada	CA
Cayman Islands	KY
Central Africa Republic	CF
Chad	TD
Cote D'ivoire	CI
Chile	CL
China	CN
Christmas Island	CX
Colombia	CO
Costa Rica	CR

Croatia	HR
Curacao	CW
Cyprus	CY
Czech Republic	CZ
Denmark	DK
Dominica	DM
Dominican Republic	DO
Ecuador	EC
Egypt	EG
El Salvador	SV
Estonia	EE
Ethiopia	ET
Faroe Islands	FO
Finland	FI
France	FR
French Guiana	GF
Georgia	GE
Germany	DE
Ghana	GH
Gibraltar	GI
Greece	GR
Greenland	GL
Grenada	GD
Guadeloupe	GP
Guam	GU
Guatemala	GT
Honduras	HN
Hong Kong	HK
Hungary	HU
Iceland	IS
India	IN
Indonesia	ID
Iraq	IQ
Ireland	IE
Israel	IL
Italy	IT
Jamaica	JM
Japan	JP

Jordan	JO
Kazakhstan	KZ
Kenya	KE
Korea Roc	KR
Kuwait	KW
Latvia	LV
Lebanon	LB
Lesotho	LS
Libya	LY
Liechtenstein	LI
Lithuania	LT
Luxembourg	LU
Macau	MO
Macedonia	MK
Malawi	MW
Malaysia	MY
Maldives	MV
Malta	MT
Marshall Islands	MH
Martinique	MQ
Mauritania	MR
Mauritius	MU
Mayotte	YT
Mexico	MX
Micronesia	FM
Moldova	MD
Monaco	MC
Morocco	MA
Mongolia	MN
Montenegro	ME
Netherlands	NL
Netherlands Antilles	AN
New Zealand	NZ
Nicaragua	NI
Nigeria	NG
Northern Mariana Islands	MP
Norway	NO
Oman	OM

Pakistan	PK
Panama	PA
Palau	PW
Papua New Guinea	PG
Paraguay	PY
Peru	PE
Philippines	PH
Poland	PL
Portugal	PT
Puerto Rico	PR
Qatar	QA
Reunion	RE
Romania	RO
Russia	RU
Rwanda	RW
Saudi Arabia	SA
St Barthelemy	BL
St Kitts Nevis	KN
St Martin	MF
St Pierre Miquelon	PM
St Vincent Grenadines	VC
Samoa	WS
Serbia	RS
Senegal	SN
Singapore	SG
Slovakia	SK
Slovenia	SI
South Africa	ZA
Spain	ES
Sri Lanka	LK
St Lucia	LC
Suriname	SR
Sweden	SE
Switzerland	CH
Taiwan	TW
Tanzania	TZ
Thailand	TH
Togo	TG

Trinidad Y Tobago	TT
Tunisia	TN
Turkey	TR
Turks Caicos	TC
United Arab Emirates	AE
Uganda	UG
Ukraine	UA
United Kingdom	GB
United States	US
Uruguay	UY
Uzbekistan	UZ
Vanuatu	VU
Venezuela	VE
Viet Nam	VN
Virgin Islands	VI
Yemen	YE
Wallis Futuna	WF
Zimbabwe	ZW
Asia	XA
Myanmar	MM
Cambodia	KH
Haiti	HT
Namibia	NA
Nepal	NP
Aland Islands	AX
Andorra	AD
Antigua and Barbuda	AG
Cameroon	CM
Cook Islands	CK
Falkland Islands	FK
French Southern Territories	TF
Guernsey	GG
Heard Island and McDonald Islands	HM
Isle of Man	IM
Jersey	JE
Montserrat	MS
New Calcedonia	NC
Niue	NU

Norfolk Island	NF
Saint Helena Ascension and Tristan Da Cunha	SH
San Marino	SM
Sint Maarten (Dutch Part)	SX
Sao Tome and Principe	ST
Svalbard and Jan Mayen	SJ
United States Minor Outlying Islands	UM
Virgin Islands British	VG
Anguilla	AI
French Polynesia	PF
Isle of Man	IM
Guyana	GY
Holy See	VA
Congo	CG
Congo Democratic Republic	CD

Appendix D – Compliance Statements

1. Compliance Statements for User's Manual

a. USA – FCC Supplier Declaration of Conformity Product Identification and Responsible Party

RightHand Technologies [2.1077(a)(3)]
www.righthandtech.com
7450 W Wilson
Chicago IL 60187

CabinLink6 [2.1077(a)(1)]

We, RightHand Technologies of Chicago IL, declare under our sole responsibility that the product CabinLink6 Product complies with Part 15 Subpart B of FCC CFR47 Rules.

b. FCC Compliance Statement FCC 15.19 Labeling Requirements

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reason-able protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a installation. If this equipment does cause harmful interference to radio or television reception, which can be deter-mined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- *Reorient or relocate the receiving antenna.*
- *Increase the separation between the equipment and receiver.*
- *Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.*
- *Consult the dealer or an experienced radio/TV technician for help.*

c. FCC RF Exposure Statement

The device shall be used in such a manner that the potential for human contact normal operation is minimized. This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum

distance of 20cm between the radiator and your body. This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

d. Canada ISED Compliance Statement

CAN ICES-3 (B)/NMB-3(B)

This device complies with Industry Canada's license-exempt RSSs. Operation is subject to the following two conditions:

(1) This device may not cause interference; and
(2) This device must accept any interference, including interference that may cause undesired operation of the device

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1) l'appareil ne doit pas produire de brouillage;
2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, when operated in 5150 to 5250 MHz frequency range, this device is restricted to indoor use to reduce the potential for harmful interference with co-channel Mobile Satellite Systems. Users are advised that high power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Conformément aux réglementations d'Industrie Canada, en cas d'utilisation dans la plage de fréquences de 5150 à 5250 MHz, cet appareil doit uniquement être utilisé en intérieur afin de réduire les risques d'interférence avec les systèmes satellites mobiles partageant le même canal. Les utilisateurs êtes avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

e. Canada RF Exposure Statement

The device shall be used in such a manner that the potential for human contact normal operation is minimized. This equipment complies with RSS-102 radiation exposure limits. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body. This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

Le dispositif doit être utilisé de manière à minimiser le potentiel de fonctionnement normal par contact humain. Cet équipement est conforme aux limites d'exposition au rayonnement RSS-102. Cet équipement doit être installé et utilisé avec une distance minimale de 20 cm entre le radiateur et votre corps. Cet appareil et son (ses) antenne (s) ne doivent pas être co-localisés ou utilisés

conjointement avec une autre antenne ou un autre émetteur

f. European Union Compliance Statement

Hereby, Manufacturer declares that this CabinLink6 Product is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.

Note: The manufacturers shall ensure that each item of radio equipment is accompanied by a copy of the EU declaration of conformity or by a simplified EU declaration of conformity (Article 10(9) RED)]

Hereby, Manufacturer declares that this device operates on frequencies that are harmonized in the European Union in one or more member states in the frequency range(s)

- *WLAN 2412-2472 MHz < 20 dBm*
- *WLAN 5150-5250 MHz < 23 dBm*
- *WLAN 5250-5350 MHz < 20 dBm*
- *WLAN 5470-5725 MHz < 27 dBm*
- *WLAN 5725-5825 MHz < 36 dBm*

Users are advised that high power radars are allocated as primary users of the bands 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to Licensed Exempt WLAN devices.

g. European Union RF Exposure Statement

The device shall be used in such a manner that the potential for human contact normal operation is minimized. This equipment complies with EN 62311:2008 and basic restrictions listed in 1999/519/EC. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body. This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

h. WEEE

This product is manufactured to ensure compliance with European Union regulations and policies that preserve, protect and improve the quality of the environment, protect human health and utilize natural resources prudently and rationally. In compliance with the Waste Electrical and Electronic Equipment (WEEE) directive return this product it to a local recycling center, the original dealer or supplier at the end of life. Otherwise return device to the following office:

RightHand Technologies, 7450 W Wilson Chicago IL.
773-774-7600
www.righthandtech.com

i. RoHS

The Product is in conformity with Directive 2011/65/EU on Restriction of the use of certain Hazardous Substances in electrical and electronic equipment.

j. REACH

The Product is in conformity with Regulation (EC) No 1907/2006 concerning Registration, Evaluation, Authorization and Restriction of Chemicals (REACH). The list of controlled substances is available at https://echa.europa.eu/candidate-list-table.