5G gateway 500G User manual

5G-500G

Wireless mobile Internet Access Device via 5G
With WiFi 802.11b/g/n/ac/ax

LIGHTSPEED International Co.

VERSION: V.1.0

Technical Support:peter@lightspeed.com.tw
TEL: +886-3-5396750

www.lightspeed.com.tw

Table of contents

FCC Warning Message:

Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the 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 reasonable 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 particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined 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.

RF exposure statements

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body or nearby persons..

Copyright

Purpose

This manual includes how to use and configurethe 5G gateway 500G (Model name).

Revision History

This user manual is based on firmware version V1.0

Trademarks

All other products or technologies are the trademarks or registered trademarks of their respective companies

Headquarter

LIGHTSPEED International Co.

No.20 Lane 526 Nioupu E. Rd. HsinChu Taiwan.

1. INTRODUCTION

1.1. OVERVIEW

5G gateway 500G is a wireless mobile internet access device with 4 ports 10/100/1000 Mbps Ethernet interfaces, 1 port 2.5Gbps WAN and 802.11b/g/n/ac/ax to performwireless internet service between PC and wireless WAN via5G Cellular station.

5G gateway 500G incorporates a 5G modem, SoC, system memories, 4 Giga LANs, 1 2.5Gbps WAN 802.11 b/g/n/ac/ax, Embedded OS, various network protocols for wireless internet.

5G gateway 500Ghas some special function on wireless mobile internet like always on-line, demands on-line etc.It also provides IP flittering, Mac flittering for tight security application.

5G gateway 500Gcan be remote update anytime it is needed. Keep alive function to ensure router is on-line all the time.

5G gateway 500G is the best choice for industrial application.

1.2. MAIN FEATURE

Wireless mobile internet access device

Integrated wireless mobile 5G

41Gbps Ethernet interfaces, 2.5 Giga bits WAN

Adopt Embedded Operating System

OpenWRT User friendly Web-based Management Tool

Status LED indicates of the device status

An external power jack

Support various Network Protocol

DHCP Server

NAT(Network Address Translation)

Remote updating via HTTPS is available

802.11 b/g/n/ac/ax2.5Gbps Wifi with WPS function

IP filtering, Mac filtering to ensure tight security access.

Keep Alive function to make sure system are on-line all the time.

2. BRIEF INFORMATION

2.1. APPEARANCE

Below arethe appearance and the each part of name of 5G gateway 500G.

Figure 1: Each part's name of 5G gateway 500G - front view

Figure 2: Each part's name of 5G gateway 500G - rear view

2.2. **DESCRIPTION OF EACH PART**

2.3. POWER

Must connect the given power adapter DC 12V/5A on this jack. Gateway rating 12V,5A.

2.3.1. **WPS**(Push button)Wi-Fi Protected Setup (WPS) is designed to make the process of connecting to a secure wireless network from a computer or other device easier.

2.3.2. **Reset** (Push button)

It is software reset for5G gateway 500G.

2.3.3. WiFi ANT1, ANT2, ANT3 & ANT4

There are 4WiFi antennas with dual-bands 2.4GHz & 5GHz.

2.3.4. **USB 3.0**Type A female connector for USB 3.0 device.

2.3.5. **WAN**

2.5Gbps WAN port for ADSL or other wide-band devices.

2.3.6. **LAN 1,2,3,4.**

User can connect 5G gateway 500G with Host PC, HUB, Router etc, via Giga LAN.

2.3.7. Console

This port is hidden inside of unit to see the diagnostic data via this console port. Normally this port is for debugging. It is for manufacturer use only. The console port is using special TTL interface cable with setting as 57600bps 8 data bitnone parity 1 stop bit.

2.3.8. 4 fix **WiFi 2.4G+5G** antennas

These are for WiFi 802.11b/g/n/ac/ax 2.4GHz & 5GHz dual-bands antennas to do both transmit & receive.

2.3.9. LED **WiFi 2.4G 5G**

LED	State	Description
Green	ON	Indicates WiFi connected.
	BLINK	Indicates data are existed via WiFi
	OFF	Indicates WiFi disconnected.

2.3.10. LED **LAN 1, 2, 3, 4**.The RJ-45 connector (LAN port) has 4 LEDs. Below the table shows each status of LAN connection.

LED	State	Description
Green	ON	Indicates LAN connected.
	BLINK	Indicates data are existed via LAN.
	OFF	Indicates LAN disconnected.

[Table 1: LED Description on LAN port]

2.2.12 LED **WAN**

LED	State	Description

Green	ON	Indicates WAN connected.
	BLINK	Indicates data are existed via WAN.
	OFF	Indicates WAN disconnected.

2.2.13 LED**WPS**

LED	State	Description
Green	ON	Indicates WPS is press
	BLINK	Indicates data are existed via WPS
	OFF	Indicates WPS is off.

2.2.14 LED **ZB BT**

LED	State	Description
Green	ON	Indicates ZigBee/Bluetooth is on
	BLINK	Indicates data are existed via ZigBee/Bluetooth
	OFF	IndicateZigBee/Bluetooth is off.

2.2.15 LED **CELL 5G**

LED	State	Description
Green	ON	Indicates cellular 5G module is on
	BLINK	Indicates data are existed via 5G module.
	OFF	Indicate cellular 5G module is off.

2.2.16 LED **PWR**

LED	State	Description
Red	ON	Indicates power is on
	OFF	Indicatepower is off.

2.2.17 U-**SIM** Socket

It has 1 SIM sockets. Please follow direction to insert SIM card.

Push-in to insert and push-out to remove. It has SIM card cover for protection.

Please turn-off power, then remove SIM card cover before inserting SIM card.

2.2.18 **CELL5G ANT1, ANT2, ANT3, ANT4**

Cellular 5G antennas with SMA connectors.

These connectors ANT1, ANT2, ANT3 & ANT4 should be connected to 5G antennas.

2.2.19 **ZIGBEE BT ANT**

1 fix 2.4GHz antenna for Zigbee & Bluetooth(optional)

2.4. Packages

2.4.1. 5G gateway 500G

2.4.2. UTP Cable (Direct)

2.4.3. DC12V/5A Adapter

2.4.4. Fix WiFi antenna: 4pcs.

2.4.5. 5G antenna 4pcs.

2.5. SOFTWARE COMPOSITION.

2.5.1. OpenWRT Web-based configuration page

5G gateway 500G has a OpenWRTweb-based configuration page that user can set the options of 5G gateway 500G for user's purpose.

* *This version namewill be changed whenever this is updated.*

2.6. BEFORE USAGE

2.6.1. Installation

5G gateway 500G is a wireless mobile internet access device with PC or other LANdevices via 5G mobile station.

Please follow below steps when you install this device.

2.6.1.1. Turn off power before Inserting U-SIM card.

2.6.1.2. Connect the proper 5G antennas 4 pieces.

2.6.1.3. Connect the LAN cable between PC and LAN port of this device.

2.6.1.4. Connect the power adapter.

Figure 3: Installation of 5G gateway 500G

Checking device

5G gateway 500G is set by PPP (NAT Router) in the first time.

When you get this device in the first time, please check whether this device is correct or not.

Please follow below steps to check this device seeing the 11-Status LED's operation.

2.6.2. Install 5G gateway 500Gas following the "3.1 Installation."

** Be sure the LAN cable must be connected between PC and 5G gateway 500G.*

2.6.3. When you plug in power, the LED named "PWR" is on.

2.6.4. The LED named "CELL 5G" is on.

** You can see this LED on in 20 seconds. When this LED is not on, contact us or our office.*

2.6.5. The LED named "LAN" is on. If LAN 1 is inserted, then LAN No.1 LED will be on.

2.7. Understanding basic operation

2.7.1. Mobile Gateway mode

On Mobile Gatewaymode, 5G gateway 500G has an IP from ISP(Internet Service Provider) then 5G gateway 500G keeps the IP and shares the IP with connected Host PC via NAT.

The main feature is that 5G gateway 500G has the mobile IP from ISP and your PC connected with 5G gateway 500G has a private IP from DHCP of 5G gateway 500G.

Please refer the [WAN] settings.

3. SETTING YOUR PC ENVIRONMENT

3.1. SETTING HOST PC

3.1.1. 5G gateway 500G is set byModem routermode/Always On-lineat first time. So just connect an LAN cable (Direct) between your PC and LAN port of 5G gateway 500G. Set the network environment of your PC as automatically.

3.1.2. Setting Host PC's network environment

3.1.2.1. We assumed that the user uses the Windows . To connect between PC and 5G gateway 500G, click "My Network Places" and the right button on your mouse then click [properties] menu.

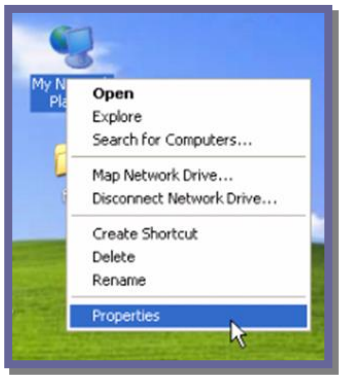


Figure 4: Step 1 of setting your PC's network environment.

3.1.2.2. Check the "Local Area Connection" then click the right button on your mouse then click [Properties] menu.

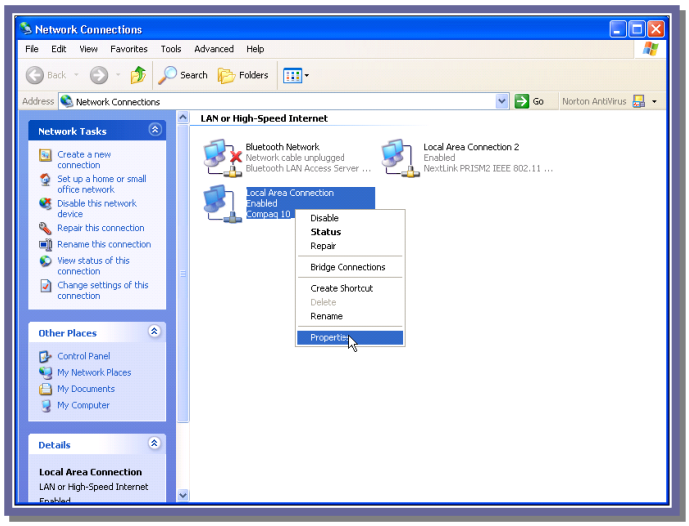


Figure 5: Step 2 of setting your PC's network environment

3.1.2.3. Double click the “Internet Protocol [TCP/IP]” item.

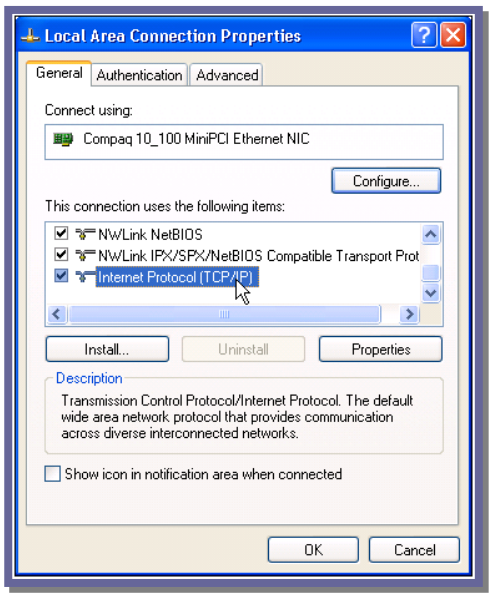


Figure 6: Step 3 of setting your PC’s network environment

3.1.2.4. Check the “Obtain an IP address automatically” .

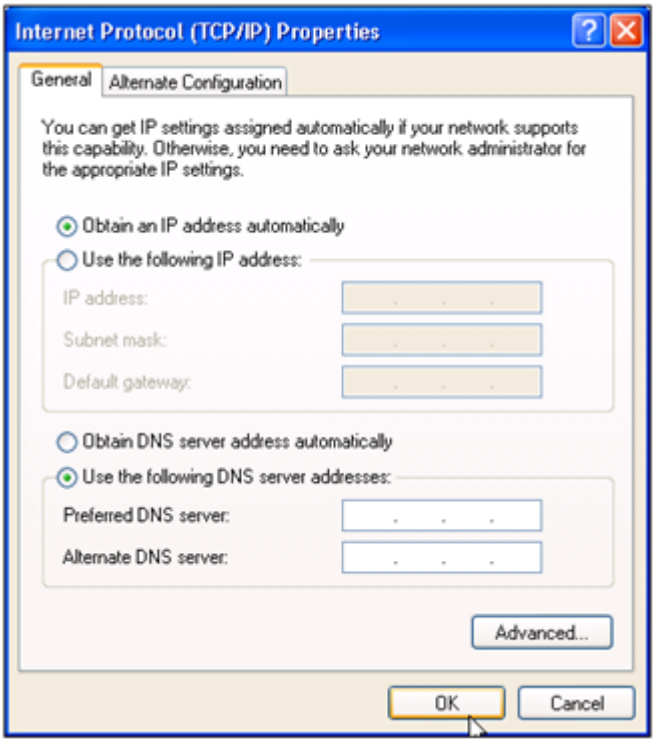


Figure 7: Step 4 of setting your PC’s network environment

3.1.2.5. Host PC’s setting is finished. Connect a LAN cable and a power cable on 5G gateway 500G. Wait till the “IP” LED is on then access Internet wirelessly.

3.2. Configuration interface

3.2.1. This web-based configuration are give you to easily program the 5G gateway 500G

3.2.2. How to access

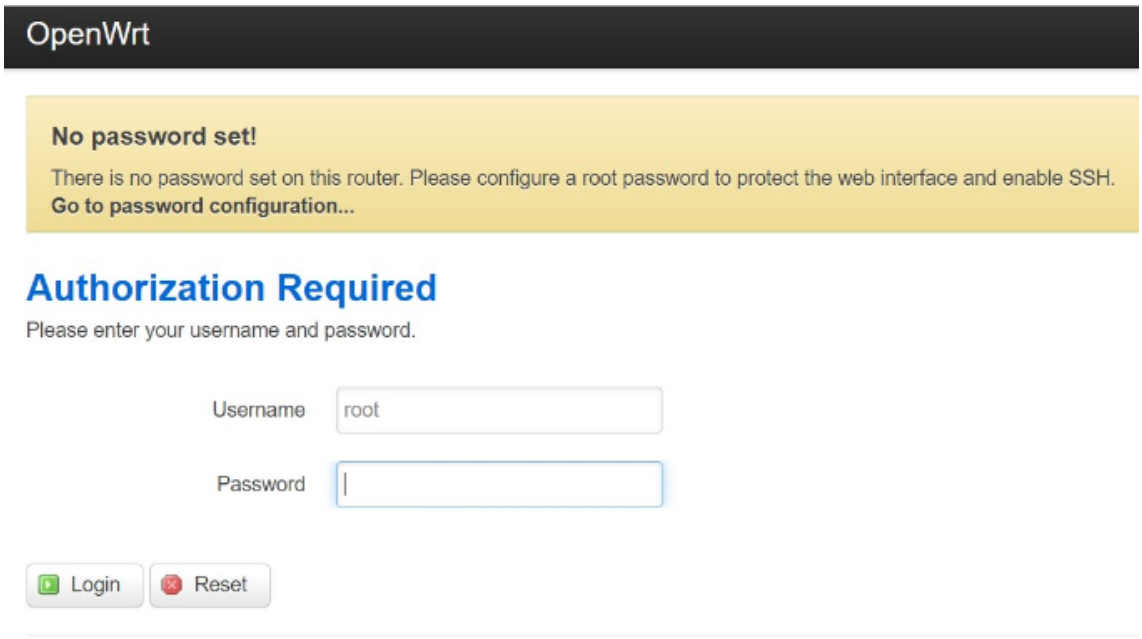
Lunch the web browser and puthttp://192.168.1.1on the address filed in browser than pop-up login page like follow

Default login credential is

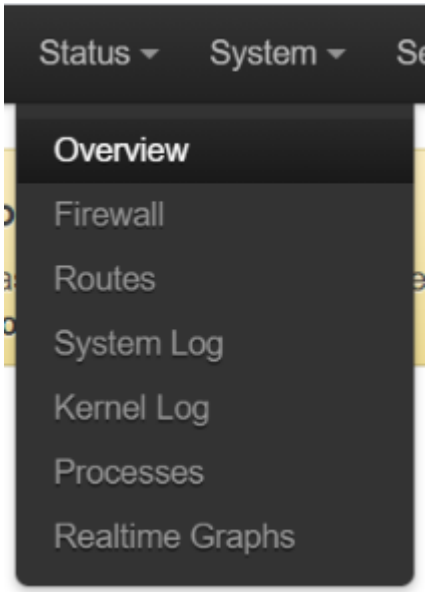
User name: root

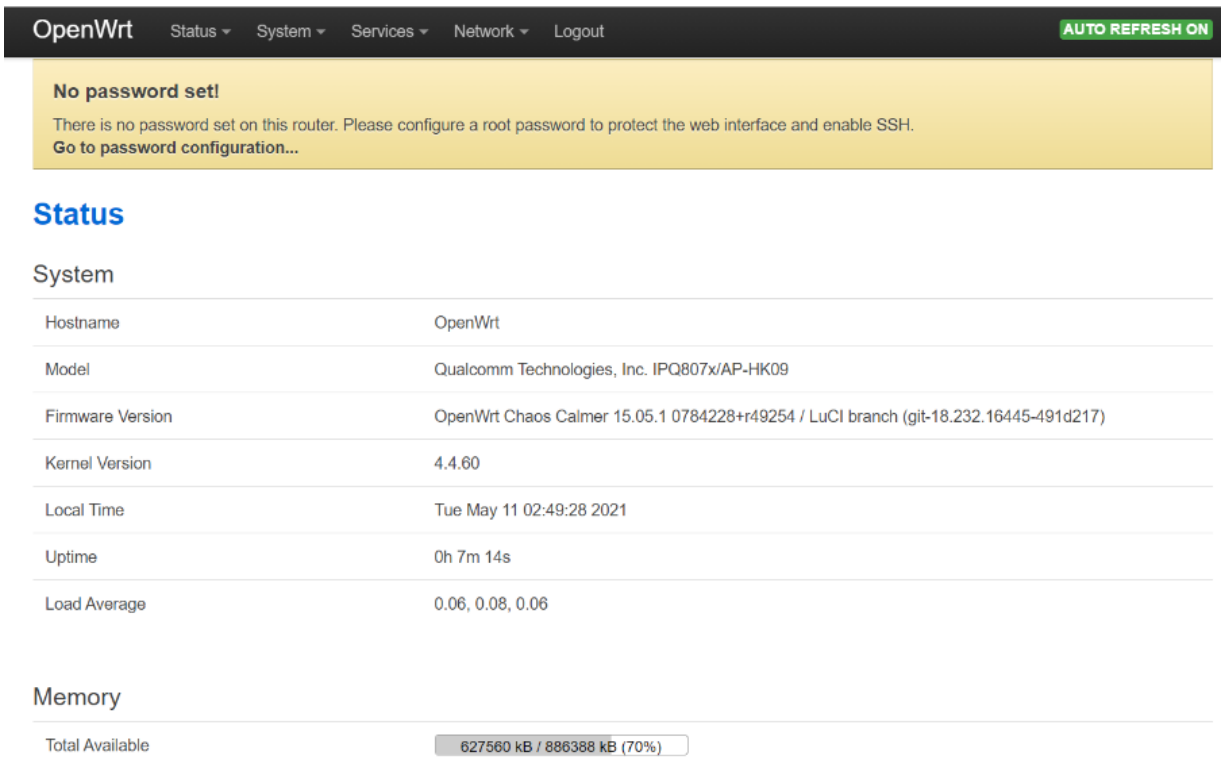
Password:

(No password)



Under “Status”, select “Overview”, it will show all the current status.


Status
System
Overview
Firewall
Routes
System Log
Kernel Log
Processes
Realtime Graphs


OpenWrt
Status
System
Services
Network
Logout
AUTO REFRESH ON
No password set!
There is no password set on this router. Please configure a root password to protect the web interface and enable SSH.
Go to password configuration...
Status
System
Hostname OpenWrt
Model Qualcomm Technologies, Inc. IPQ807x/AP-HK09
Firmware Version OpenWrt Chaos Calmer 15.05.1 0784228+r49254 / LuCI branch (git-18.232.16445-491d217)
Kernel Version 4.4.60
Local Time Tue May 11 02:49:28 2021
Uptime 0h 7m 14s
Load Average 0.06, 0.08, 0.06
Memory
Total Available 627560 kB / 886388 kB (70%)

Active Connections	84 / 16384 (0%)

DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
?	192.168.1.211	f8:0d:ac:cc:fc:60	11h 46m 54s

DHCPv6 Leases

Hostname	IPv6-Address	DUID	Leasetime remaining

There are no active leases.

Wireless

Generic 802.11axa Wireless Controller (wifi0)

0%
SSID: LS5G500_5G_630A
Mode: Master
Channel: 100 (5.500 GHz)
Bitrate: 2.401 Mbit/s

Generic 802.11axg Wireless Controller (wifi1)

0%
SSID: LS5G500_2G_630A
Mode: Master
Channel: 11 (2.462 GHz)
Bitrate: 0.573 Mbit/s
BSSID: 00:03:7F:12:02:F7
Encryption: WPA2 PSK (CCMP)

Associated Stations

MAC-Address	Network	Signal	Noise	RX Rate	TX Rate
00:00:00:00:00:00	Master "LS5G500_5G_630A"	-95 dBm	-93 dBm	0.0 Mbit/s	0.0 Mbit/s
00:00:00:00:00:00	Master "LS5G500_2G_630A"	-95 dBm	-93 dBm	0.0 Mbit/s	0.0 Mbit/s

Dynamic DNS

Configuration	Next Update	Hostname/Domain	Registered IP	Network
myddns_ipv4	*Disabled*	yourhost.example.com	*No data*	IPv4 / wan
myddns_ipv6	*Disabled*	yourhost.example.com	*No data*	IPv6 / wan6

00:00:00:00:00:00	Master "LS5G500_2G_630A"	-95 dBm	-93 dBm	0.0 Mbit/s	0.0 Mbit/s

Dynamic DNS

Configuration	Next Update	Hostname/Domain	Registered IP	Network
myddns_ipv4	*Disabled*	yourhost.example.com	*No data*	IPv4 / wan
myddns_ipv6	*Disabled*	yourhost.example.com	*No data*	IPv6 / wan6

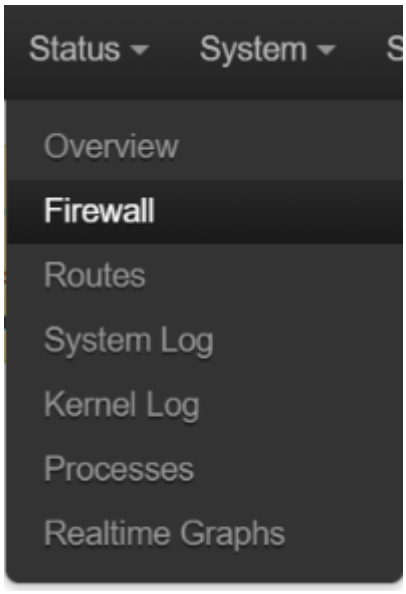
Multi-WAN Status

Active UPnP Redirects

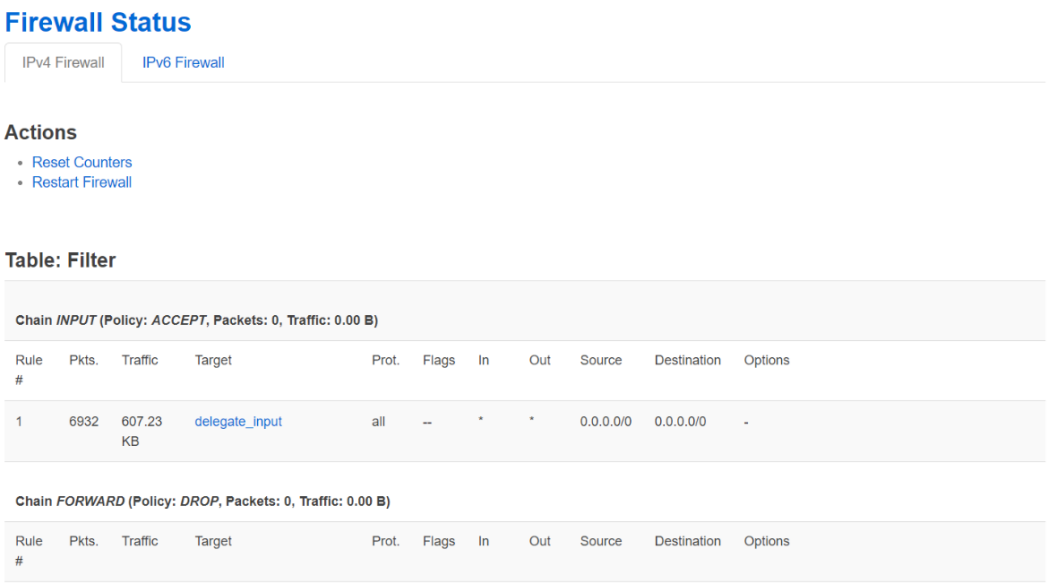
Protocol	External Port	Client Address	Client Port

There are no active redirects.

Select “Firewall”.



It will show all firewall options:



Firewall Status

IPv4 Firewall | IPv6 Firewall

Actions

- Reset Counters
- Restart Firewall

Table: Filter

Chain *INPUT* (Policy: *ACCEPT*, Packets: 0, Traffic: 0.00 B)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	6932	607.23 KB	delegate_input	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain *FORWARD* (Policy: *DROP*, Packets: 0, Traffic: 0.00 B)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options

Chain *FORWARD* (Policy: *DROP*, Packets: 0, Traffic: 0.00 B)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	472	68.13 KB	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	PHYSDEV match --physdev-is-bridged
2	0	0.00 B	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	PHYSDEV match --physdev-is-bridged
3	0	0.00 B	delegate_forward	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-
4	0	0.00 B	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	PHYSDEV match --physdev-is-bridged

Chain *OUTPUT* (Policy: *ACCEPT*, Packets: 0, Traffic: 0.00 B)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	7038	1.01 MB	delegate_output	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain *delegate_forward* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	0	0.00 B	forwarding_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	/* user chain for forwarding */

Chain *delegate_output* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	1444	90.46 KB	ACCEPT	all	--	*	lo	0.0.0.0/0	0.0.0.0/0	-
2	5594	941.31 KB	output_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	/* user chain for output */
3	5594	941.31 KB	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED
4	0	0.00 B	zone_lan_output	all	--	*	br-lan	0.0.0.0/0	0.0.0.0/0	-
5	0	0.00 B	zone_wan_output	all	--	*	eth4	0.0.0.0/0	0.0.0.0/0	-

Chain *reject* (References: 3)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	0	0.00 B	REJECT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	reject-with tcp-reset
2	0	0.00 B	REJECT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	reject-with icmp-port-unreachable

Chain *syn_flood* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	40	2.03 KB	RETURN	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02 limit: avg 25/sec burst 50
2	0	0.00 B	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain *zone_lan_dest_ACCEPT* (References: 4)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	0	0.00 B	ACCEPT	all	--	*	br-lan	0.0.0.0/0	0.0.0.0/0	-

Chain *zone_lan_forward* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	0	0.00 B	forwarding_lan_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	/* user chain for forwarding */
2	0	0.00 B	zone_wan_dest_ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	/* forwarding lan -> wan */
3	0	0.00 B	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	ctstate DNAT /* Accept port forwards */

Chain *zone_lan_input* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	876	65.35 KB	input_lan_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	/* user chain for input */
2	0	0.00 B	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	ctstate DNAT /* Accept port redirections */
3	876	65.35 KB	zone_lan_src_ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain *zone_lan_output* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	0	0.00 B	output_lan_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	/* user chain for output */
2	0	0.00 B	zone_lan_dest_ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain *zone_lan_src_ACCEPT* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options

Chain *zone_lan_src_ACCEPT* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	876	65.35 KB	ACCEPT	all	--	br-lan	*	0.0.0.0/0	0.0.0.0/0	-

Chain *zone_wan_dest_ACCEPT* (References: 2)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	0	0.00 B	ACCEPT	all	--	*	eth4	0.0.0.0/0	0.0.0.0/0	-

Chain *zone_wan_dest_REJECT* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	0	0.00 B	reject	all	--	*	eth4	0.0.0.0/0	0.0.0.0/0	-

Chain *zone_wan_forward* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options

Chain *zone_wan_forward* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	0	0.00 B	MINIUPNPD	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-
2	0	0.00 B	forwarding_wan_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	/* user chain for forwarding */
3	0	0.00 B	zone_lan_dest_ACCEPT	esp	--	*	*	0.0.0.0/0	0.0.0.0/0	/* @rule[7] */
4	0	0.00 B	zone_lan_dest_ACCEPT	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:500 /* @rule[8] */
5	0	0.00 B	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	ctstate DNAT /* Accept port forwards */
6	0	0.00 B	zone_wan_dest_REJECT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain *zone_wan_input* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	0	0.00 B	input_wan_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	/* user chain for input */
2	0	0.00 B	ACCEPT	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:68 /* Allow-DHCP-Renew */
3	0	0.00 B	ACCEPT	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	icmptype 8 /* Allow-Ping */

2	0	0.00 B	ACCEPT	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:68 /* Allow-DHCP-Renew */
3	0	0.00 B	ACCEPT	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	icmptype 8 /* Allow-Ping */
4	0	0.00 B	ACCEPT	2	--	*	*	0.0.0.0/0	0.0.0.0/0	/* Allow-IGMP */
5	0	0.00 B	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	ctstate DNAT /* Accept port redirections */
6	0	0.00 B	zone_wan_src_REJECT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain *zone_wan_output* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	0	0.00 B	output_wan_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	/* user chain for output */
2	0	0.00 B	zone_wan_dest_ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain *zone_wan_src_REJECT* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	0	0.00 B	reject	all	--	eth4	*	0.0.0.0/0	0.0.0.0/0	-

Table: NAT

Chain *PREROUTING* (Policy: *ACCEPT*, Packets: 777, Traffic: 51.49 KB)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	777	51.49 KB	delegate_prerouting	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain *POSTROUTING* (Policy: *ACCEPT*, Packets: 242, Traffic: 15.07 KB)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	242	15.07 KB	delegate_postrouting	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain *delegate_postrouting* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	242	15.07 KB	postrouting_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	/* user chain for postrouting */

2	8	1.09 KB	zone_lan_postrouting	all	--	*	br-lan	0.0.0.0/0	0.0.0.0/0	-
3	0	0.00 B	zone_wan_postrouting	all	--	*	eth4	0.0.0.0/0	0.0.0.0/0	-

Chain *delegate_prerouting* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	777	51.49 KB	prerouting_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	/* user chain for prerouting */
2	777	51.49 KB	zone_lan_prerouting	all	--	br-lan	*	0.0.0.0/0	0.0.0.0/0	-
3	0	0.00 B	zone_wan_prerouting	all	--	eth4	*	0.0.0.0/0	0.0.0.0/0	-

Chain *zone_lan_postrouting* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	8	1.09 KB	postrouting_lan_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	/* user chain for postrouting */

2	8	1.09 KB	zone_lan_postrouting	all	--	*	br-lan	0.0.0.0/0	0.0.0.0/0	-
3	0	0.00 B	zone_wan_postrouting	all	--	*	eth4	0.0.0.0/0	0.0.0.0/0	-

Chain *delegate_prerouting* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	777	51.49 KB	prerouting_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	/* user chain for prerouting */
2	777	51.49 KB	zone_lan_prerouting	all	--	br-lan	*	0.0.0.0/0	0.0.0.0/0	-
3	0	0.00 B	zone_wan_prerouting	all	--	eth4	*	0.0.0.0/0	0.0.0.0/0	-

Chain *zone_lan_postrouting* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	8	1.09 KB	postrouting_lan_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	/* user chain for postrouting */

Chain *zone_lan_prerouting* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	777	51.49 KB	prerouting_lan_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	/* user chain for prerouting */

Chain *zone_wan_postrouting* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	0	0.00 B	postrouting_wan_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	/* user chain for postrouting */
2	0	0.00 B	MASQUERADE	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain *zone_wan_prerouting* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	0	0.00 B	MINIUPNPD	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-
2	0	0.00 B	prerouting_wan_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	/* user chain for prerouting */

Table: Mangle

Chain *PREROUTING* (Policy: *ACCEPT*, Packets: 6998, Traffic: 616.14 KB)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	6998	616.14 KB	fwmark	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain *FORWARD* (Policy: *ACCEPT*, Packets: 380, Traffic: 52.24 KB)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	380	52.24 KB	mssfix	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain *mssfix* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	0	0.00 B	TCPMSS	tcp	--	*	eth4	0.0.0.0/0	0.0.0.0/0	tcp flags:0x06/0x02 /* wan (mtu_fix) */ TCPMSS clamp to PMTU

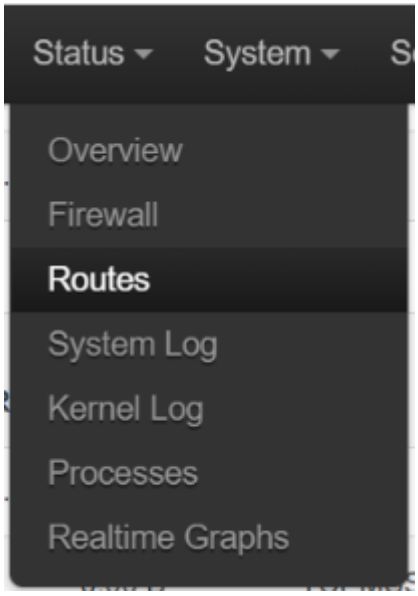
Table: Raw

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	380	52.24 KB	mssfix	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-
Chain *mssfix* (References: 1)										
Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	0	0.00 B	TCPMSS	tcp	--	*	eth4	0.0.0.0/0	0.0.0.0/0	tcp flags:0x06/0x02 /* wan (mtu_fix) */ TCPMSS clamp to PMTU

Table: Raw

Chain *PREROUTING* (Policy: *ACCEPT*, Packets: 6998, Traffic: 616.14 KB)										
Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	6998	616.14 KB	delegate_notrack	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Select “Routes”



It will show:

Routes

The following rules are currently active on this system.

ARP

IPv4-Address	MAC-Address	Interface
192.168.1.211	f8:0d:ac:cc:fc:60	br-lan

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric	Table
wan6	0.0.0.0/0	192.168.2.1	0	main
lan	192.168.1.0/24		0	main
wan6	192.168.2.0/24		0	main

Active IPv6-Routes

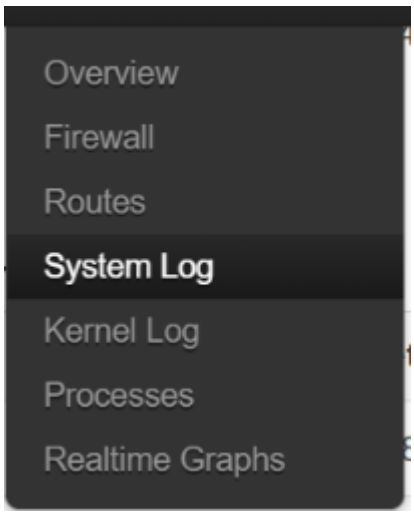
Active IPv6-Routes

Network	Target	Source	Metric	Table
lan	ff00::/8		256	local
wan6	ff00::/8		256	local
lan	ff00::/8		256	local
lan	ff00::/8		256	local

IPv6 Neighbours

IPv6-Address	MAC-Address	Interface

Select “System Log”:

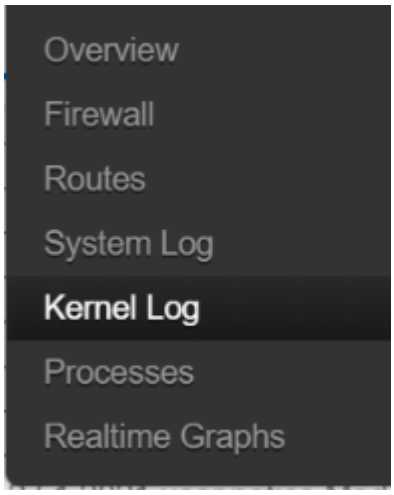


It will show:

System Log

```
Tue May 11 02:42:51 2021 user.notice ModemManager: hotplug: event reported: action=add, name=ipsecdummy, subsystem=net
Tue May 11 02:42:51 2021 daemon.emerg procd: sh: out of range
Tue May 11 02:42:51 2021 daemon.emerg procd: sh: 1: unknown operand
Tue May 11 02:42:51 2021 user.notice ModemManager: hotplug: error: parent device sysfspath not found
Tue May 11 02:42:51 2021 user.notice ModemManager: hotplug: cached event found: action=add, name=teql0, subsystem=net, sysfspath=/sys/devices/virtual/net/
Tue May 11 02:42:51 2021 user.notice ModemManager: hotplug: event reported: action=add, name=teql0, subsystem=net
Tue May 11 02:42:51 2021 user.notice ModemManager: hotplug: error: parent device sysfspath not found
Tue May 11 02:42:51 2021 user.notice ModemManager: hotplug: cached event found: action=add, name=wifi0, subsystem=net, sysfspath=/sys/devices/platform/sc
Tue May 11 02:42:51 2021 user.notice ModemManager: hotplug: event reported: action=add, name=wifi0, subsystem=net
Tue May 11 02:42:51 2021 daemon.emerg procd: sh: 0: unknown operand
Tue May 11 02:42:51 2021 daemon.emerg procd: sh: 0: unknown operand
Tue May 11 02:42:51 2021 daemon.emerg procd: sh: 0: unknown operand
Tue May 11 02:42:51 2021 user.notice ModemManager: hotplug: error: parent device sysfspath not found
Tue May 11 02:42:51 2021 user.notice ModemManager: hotplug: cached event found: action=add, name=wifi1, subsystem=net, sysfspath=/sys/devices/platform/sc
Tue May 11 02:42:51 2021 user.notice ModemManager: hotplug: event reported: action=add, name=wifi1, subsystem=net
Tue May 11 02:42:51 2021 user.notice ModemManager: hotplug: error: parent device sysfspath not found
Tue May 11 02:42:51 2021 user.notice ModemManager: hotplug: cached event found: action=add, name=soc0, subsystem=net, sysfspath=/sys/devices/platform/s
Tue May 11 02:42:51 2021 user.notice ModemManager: hotplug: event reported: action=add, name=soc0, subsystem=net
Tue May 11 02:42:51 2021 user.notice ModemManager: hotplug: error: parent device sysfspath not found
Tue May 11 02:42:51 2021 user.notice ModemManager: hotplug: cached event found: action=add, name=br-lan, subsystem=net, sysfspath=/sys/devices/virtual/ne
Tue May 11 02:42:51 2021 user.notice ModemManager: hotplug: event reported: action=add, name=br-lan, subsystem=net
Tue May 11 02:42:51 2021 daemon.emerg procd: sh: out of range
Tue May 11 02:42:51 2021 daemon.emerg procd: sh: auto: out of range
Tue May 11 02:42:51 2021 user.notice ModemManager: hotplug: error: parent device sysfspath not found
Tue May 11 02:42:51 2021 user.notice ModemManager: hotplug: cached event found: action=add, name=ath0, subsystem=net, sysfspath=/sys/devices/virtual/net/
Tue May 11 02:42:51 2021 daemon.emerg procd: wep40,wep104,tkip,aes-ocb,aes-ccmp-128,aes-ccmp-256,aes-gcmp-128,aes-gcmp-256,ckip,wapi,aes-cmac-12
Tue May 11 02:42:51 2021 user.notice ModemManager: hotplug: event reported: action=add, name=ath0, subsystem=net
```

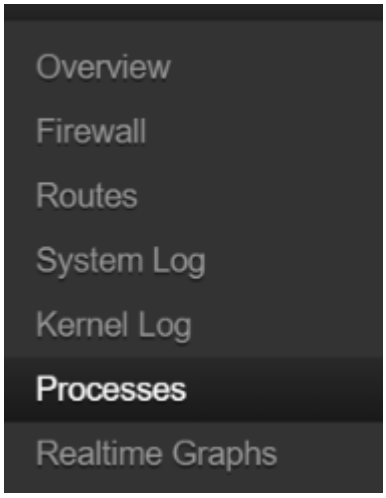
Kernel log:



Kernel Log

```
[    0.000000] Booting Linux on physical CPU 0x0
[    0.000000] Initializing cgroup subsys cpuset
[    0.000000] Initializing cgroup subsys cpu
[    0.000000] Initializing cgroup subsys cpuacct
[    0.000000] Linux version 4.4.60 (pdh0085@DONGHYUN-LQVM) (gcc version 5.2.0 (OpenWrt GCC 5.2.0 0784228+r49254) ) #113 SMP PREEMPT Tue May 4 (
[    0.000000] Boot CPU: AArch64 Processor [410fd034]
[    0.000000] Ignoring memory range 0x40000000 - 0x41000000
[    0.000000] Machine: Qualcomm Technologies, Inc. IPQ807x/AP-HK09
[    0.000000] efi: Getting EFI parameters from FDT:
[    0.000000] efi: UEFI not found.
[    0.000000] Reserved memory: OVERLAP DETECTED!
[    0.000000] wifi_dump@51100000 (0x0000000051100000--0x0000000051700000) overlaps with wigig_dump@51300000 (0x0000000051300000--0x000000005
[    0.000000] On node 0 totalpages: 228608
[    0.000000]   DMA zone: 3572 pages used for memmap
[    0.000000]   DMA zone: 0 pages reserved
[    0.000000]   DMA zone: 228608 pages, LIFO batch:31
[    0.000000] psci: probing for conduit method from DT.
[    0.000000] psci: PSCIv1.0 detected in firmware.
[    0.000000] psci: Using standard PSCI v0.2 function IDs
[    0.000000] psci: MIGRATE_INFO_TYPE not supported.
[    0.000000] PERCPU: Embedded 15 pages/cpu @ffffffc03ef47000 s20864 r8192 d32384 u61440
[    0.000000] pcpu-alloc: s20864 r8192 d32384 u61440 alloc=15*4096
[    0.000000] pcpu-alloc: [0] 0 [0] 1 [0] 2 [0] 3
[    0.000000] Detected VIPT I-cache on CPU0
[    0.000000] CPU features: enabling workaround for ARM erratum 845719
[    0.000000] Built 1 zonelists in Zone order, mobility grouping on.  Total pages: 225036
[    0.000000] Kernel command line: console=ttyMSM0,115200n8 ubi.mtd=rootfs root=mtd:ubi_rootfs rootfstype=squashfs rootwait swiotlb=1 coherent_pool=2M
```

Processes

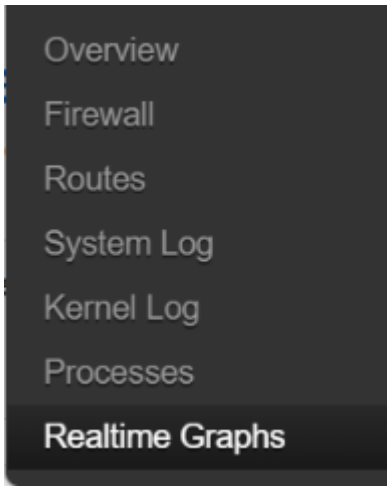


Processes

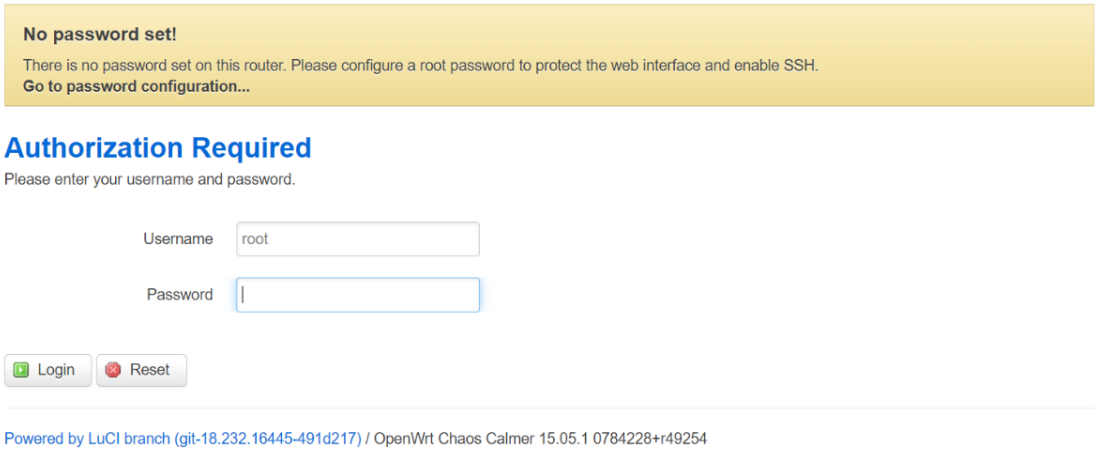
This list gives an overview over currently running system processes and their status.

PID	Owner	Command	CPU usage (%)	Memory usage (%)	Hang Up	Terminate	Kill
1	root	/sbin/procd	0%	0%	Hang Up	Terminate	Kill
2	root	[kthreadd]	0%	0%	Hang Up	Terminate	Kill
3	root	[ksoftirqd/0]	0%	0%	Hang Up	Terminate	Kill
5	root	[kworker/0:0H]	0%	0%	Hang Up	Terminate	Kill
6	root	[kworker/u8:0]	0%	0%	Hang Up	Terminate	Kill
7	root	[rcu_preempt]	0%	0%	Hang Up	Terminate	Kill
8	root	[rcu_sched]	0%	0%	Hang Up	Terminate	Kill

Realtime Graph



It shows login graphs.



3.3. System

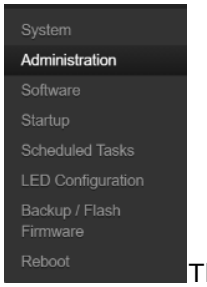
Select System, it will show currently running system processes & their status.

Processes

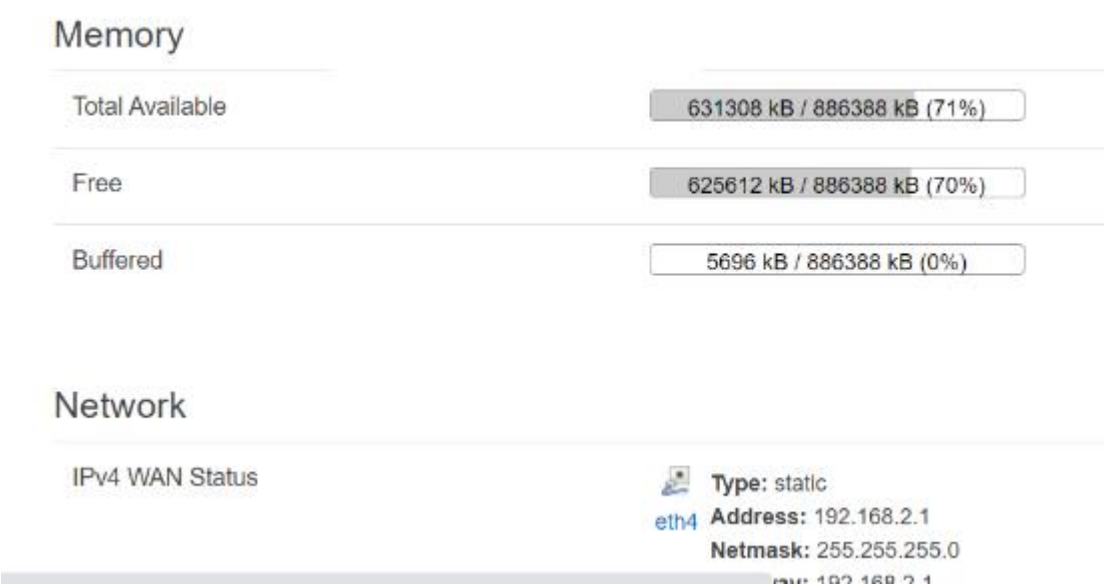
This list gives an overview over currently running system processes and their status.

PID	Owner	Command	CPU usage (%)	Memory usage (%)	Hang Up	Terminate	Kill
1	root	/sbin/procd	0%	0%	Hang Up	Terminate	Kill
2	root	[kthreadd]	0%	0%	Hang Up	Terminate	Kill
3	root	[ksoftirqd/0]	0%	0%	Hang Up	Terminate	Kill
5	root	[kworker/0:0H]	0%	0%	Hang Up	Terminate	Kill
6	root	[kworker/u8:0]	0%	0%	Hang Up	Terminate	Kill
7	root	[rcu_preempt]	0%	0%	Hang Up	Terminate	Kill
8	root	[rcu_sched]	0%	0%	Hang Up	Terminate	Kill

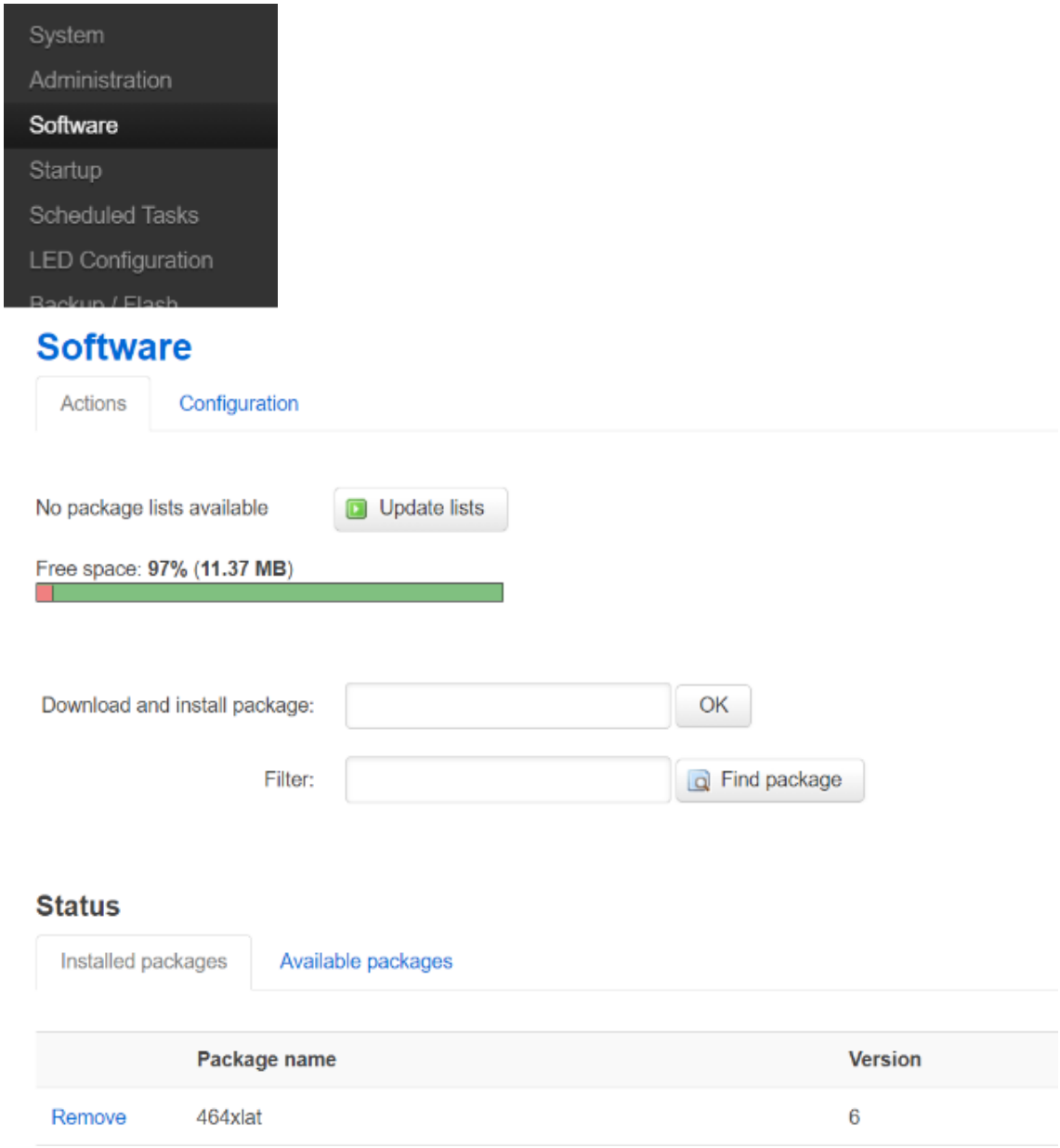
3.3.1. Administration



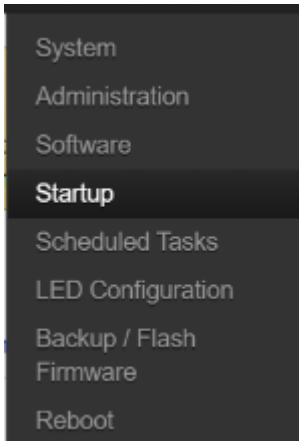
This shows current firmware version, memory size ..etc.

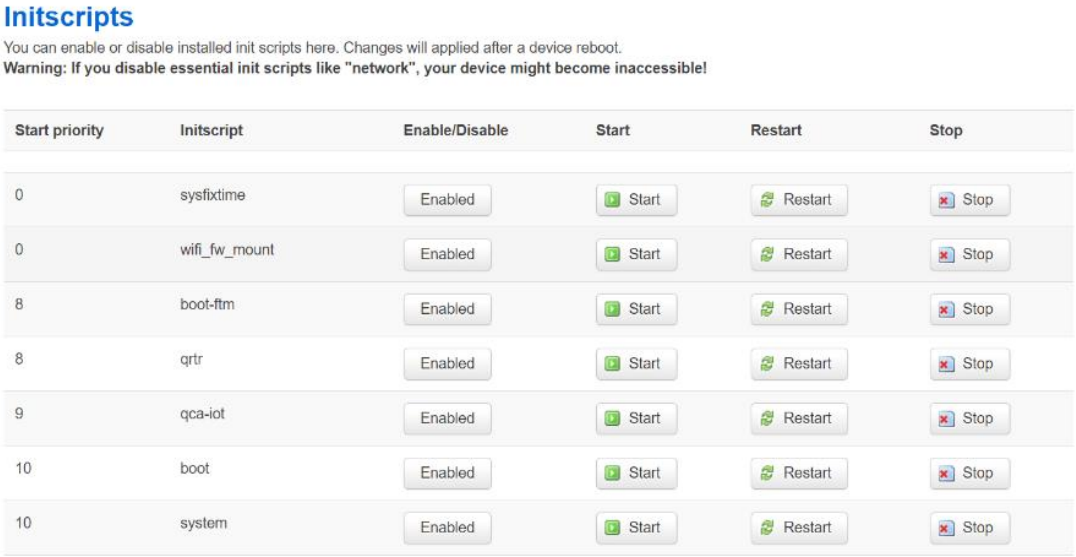


3.3.2 Software


System
Administration
Software
Startup
Scheduled Tasks
LED Configuration
Software
Actions
Configuration
No package lists available
Update lists
Free space: 97% (11.37 MB)
Download and install package:
OK
Filter:
Find package
Status
Installed packages
Available packages
Package name
Version
Remove
464xlat
6

3.3.2. Startup



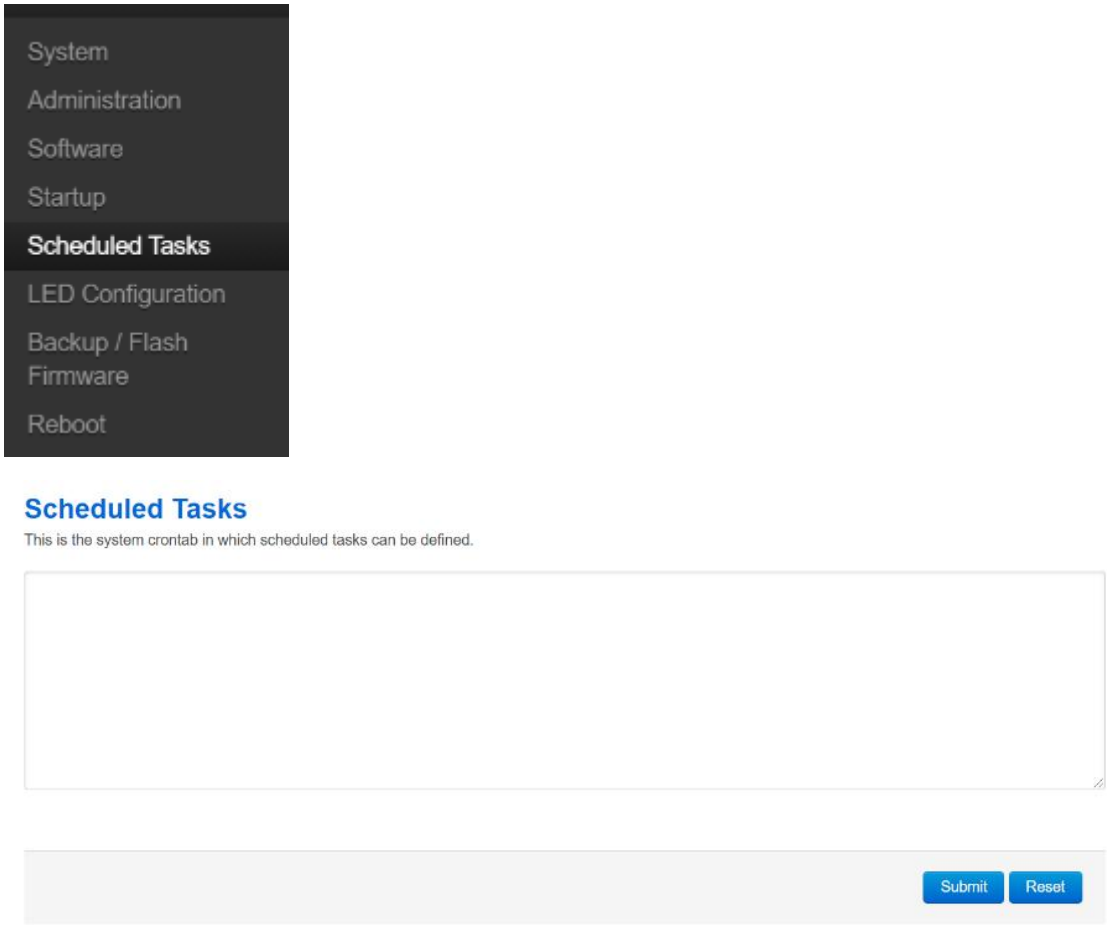


Initscripts

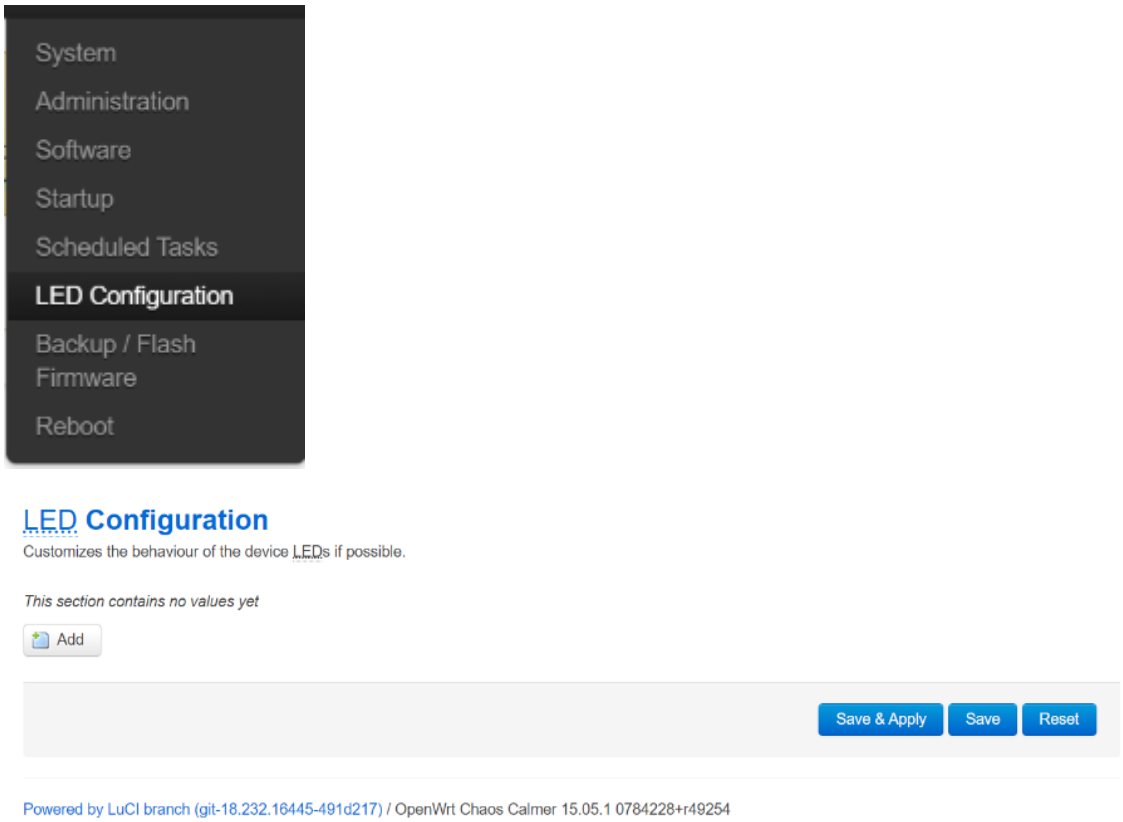
You can enable or disable installed init scripts here. Changes will applied after a device reboot.
Warning: If you disable essential init scripts like "network", your device might become inaccessible!

Start priority	Initscript	Enable/Disable	Start	Restart	Stop
0	sysfixtime	Enabled	Start	Restart	Stop
0	wifi_fw_mount	Enabled	Start	Restart	Stop
8	boot-ftm	Enabled	Start	Restart	Stop
8	qrtr	Enabled	Start	Restart	Stop
9	qca-iot	Enabled	Start	Restart	Stop
10	boot	Enabled	Start	Restart	Stop
10	system	Enabled	Start	Restart	Stop

3.3.3. Scheduled Tasks

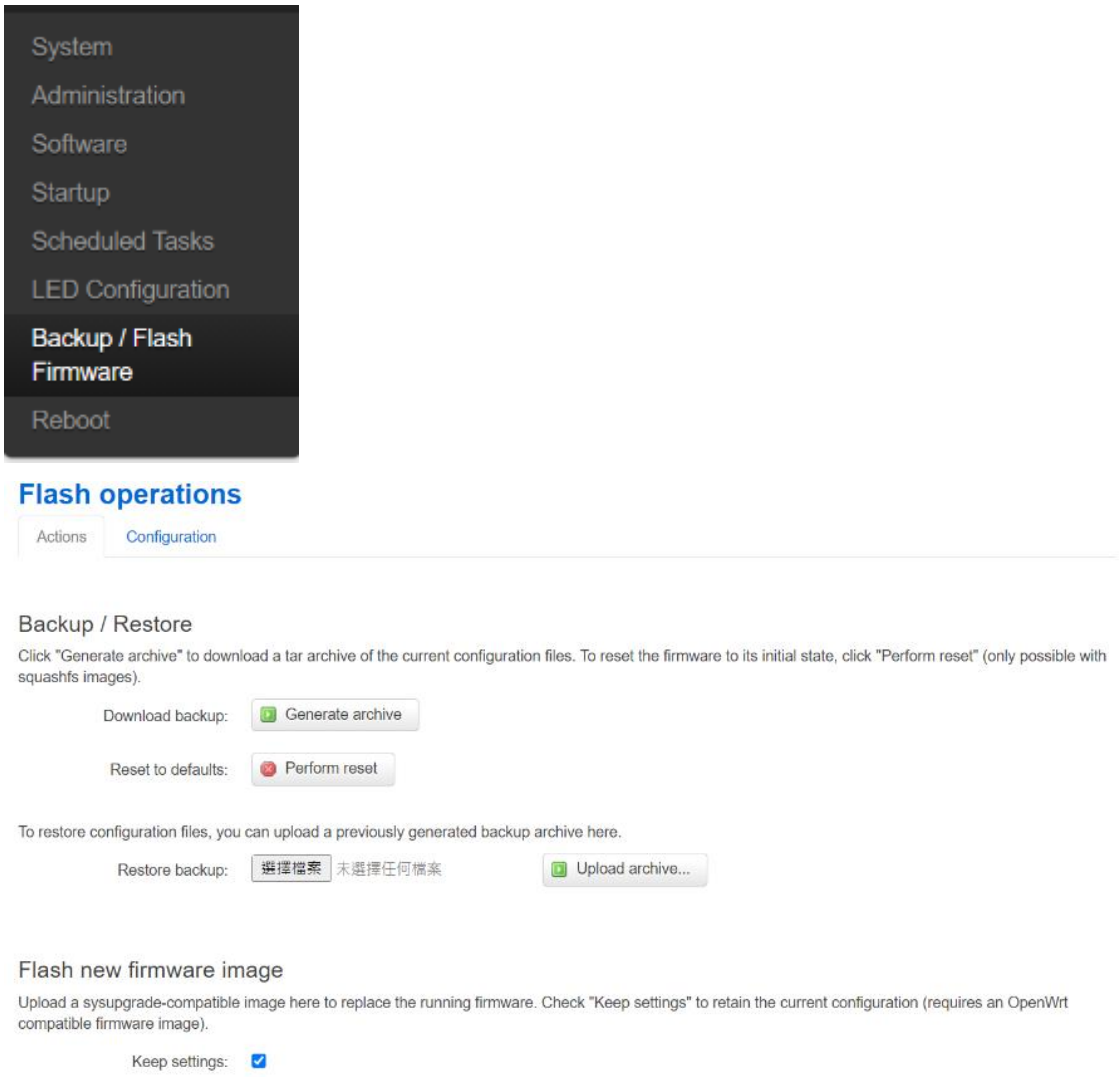


3.3.4. LED Configuration

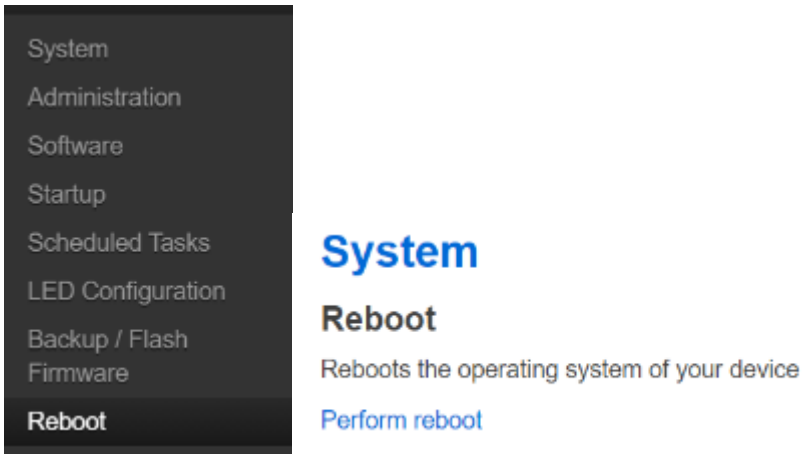


Please keep your PIN code in safe place. If it fails 3 times, SIM card will be block by Operator. Then you will need to ask service provider to give you PUK code to unlock SIM.

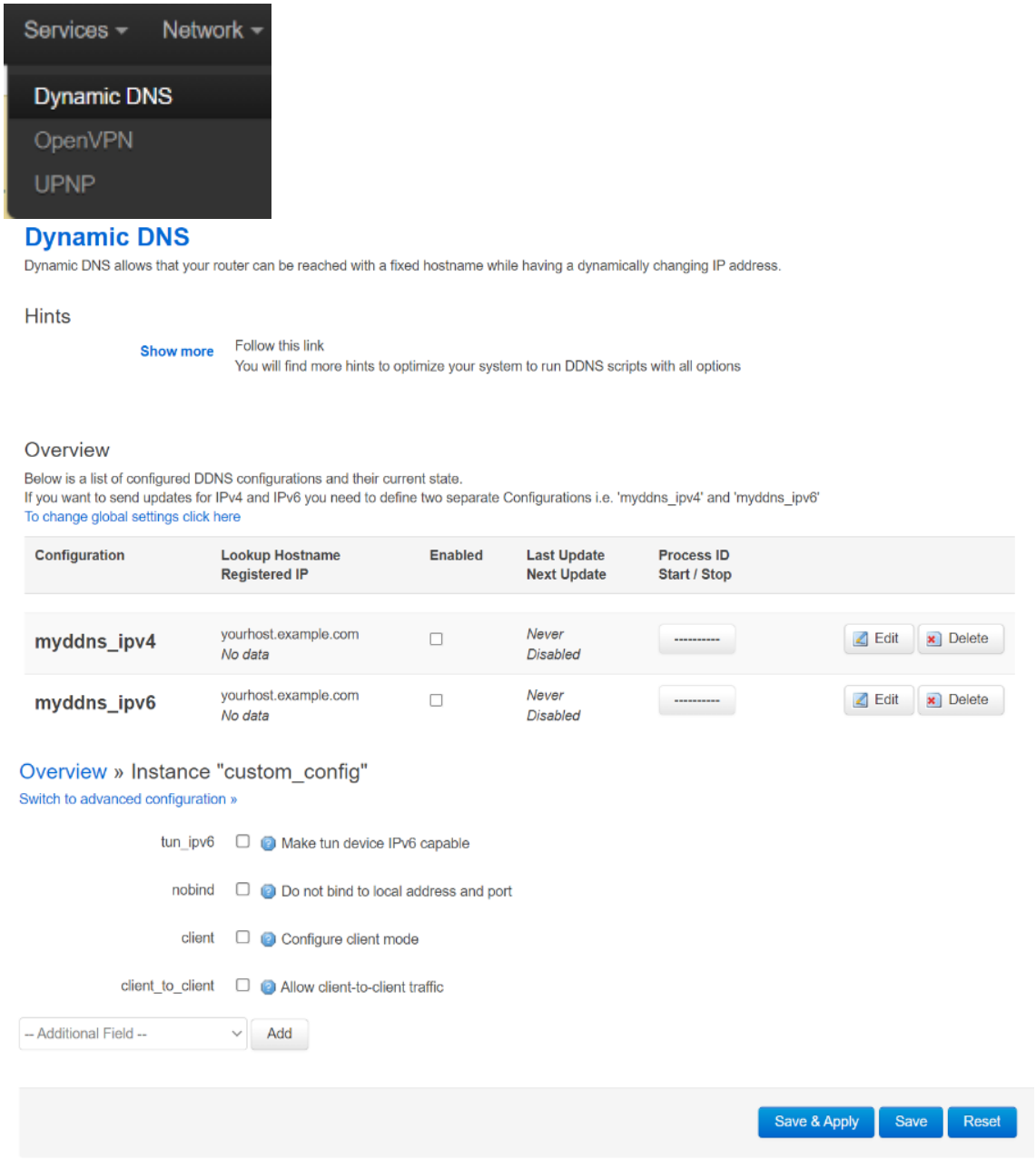
3.3.5. Backup/Flash Firmware



3.3.6. Reboot



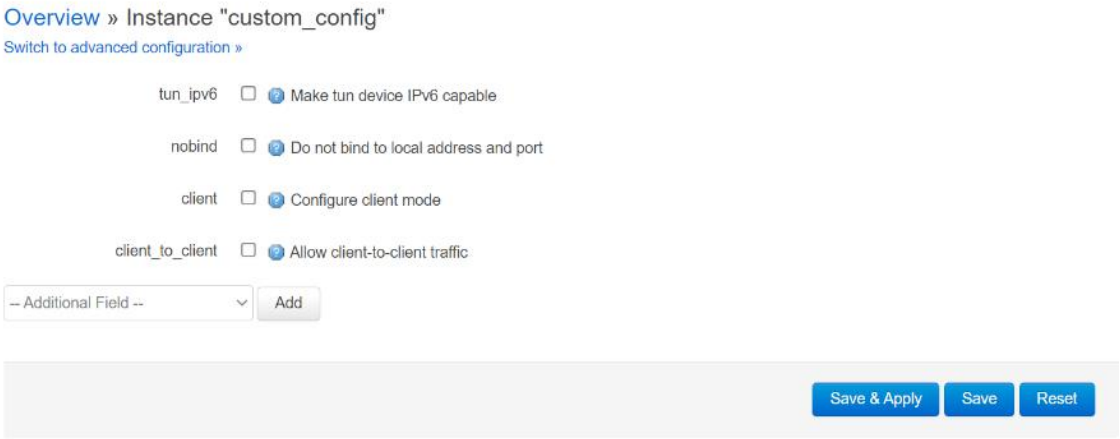
3.4.1 Under service, select Dynamic DNS


Services
Network
Dynamic DNS
OpenVPN
UPNP
Dynamic DNS
Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.
Hints
Show more
Follow this link
You will find more hints to optimize your system to run DDNS scripts with all options
Overview
Below is a list of configured DDNS configurations and their current state.
If you want to send updates for IPv4 and IPv6 you need to define two separate Configurations i.e. 'myddns_ipv4' and 'myddns_ipv6'
To change global settings click here
Configuration
Lookup Hostname
Registered IP
Enabled
Last Update
Next Update
Process ID
Start / Stop
myddns_ipv4
yourhost.example.com
No data
Never
Disabled

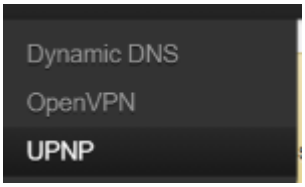
Edit
Delete
myddns_ipv6
yourhost.example.com
No data
Never
Disabled

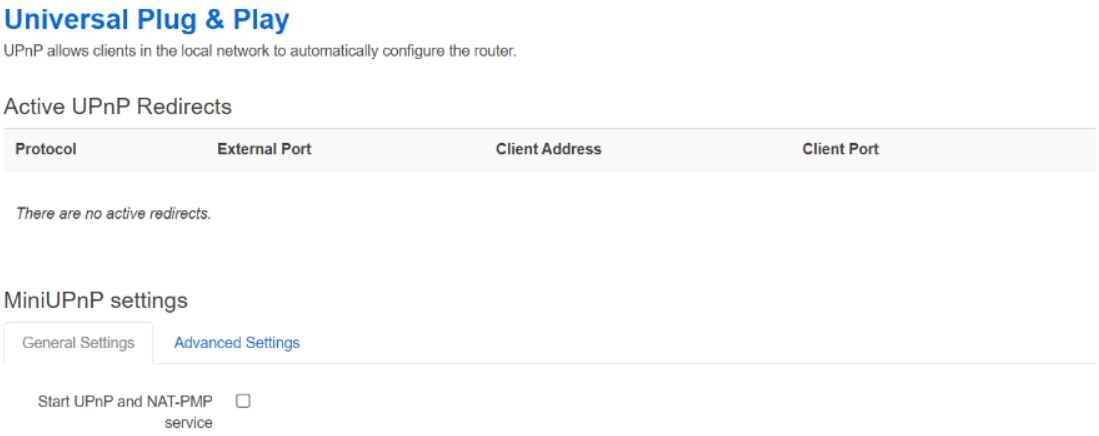
Edit
Delete
Overview » Instance "custom_config"
Switch to advanced configuration »
tun_ipv6
Make tun device IPv6 capable
nobind
Do not bind to local address and port
client
Configure client mode
client_to_client
Allow client-to-client traffic
-- Additional Field --
Add
Save & Apply
Save
Reset

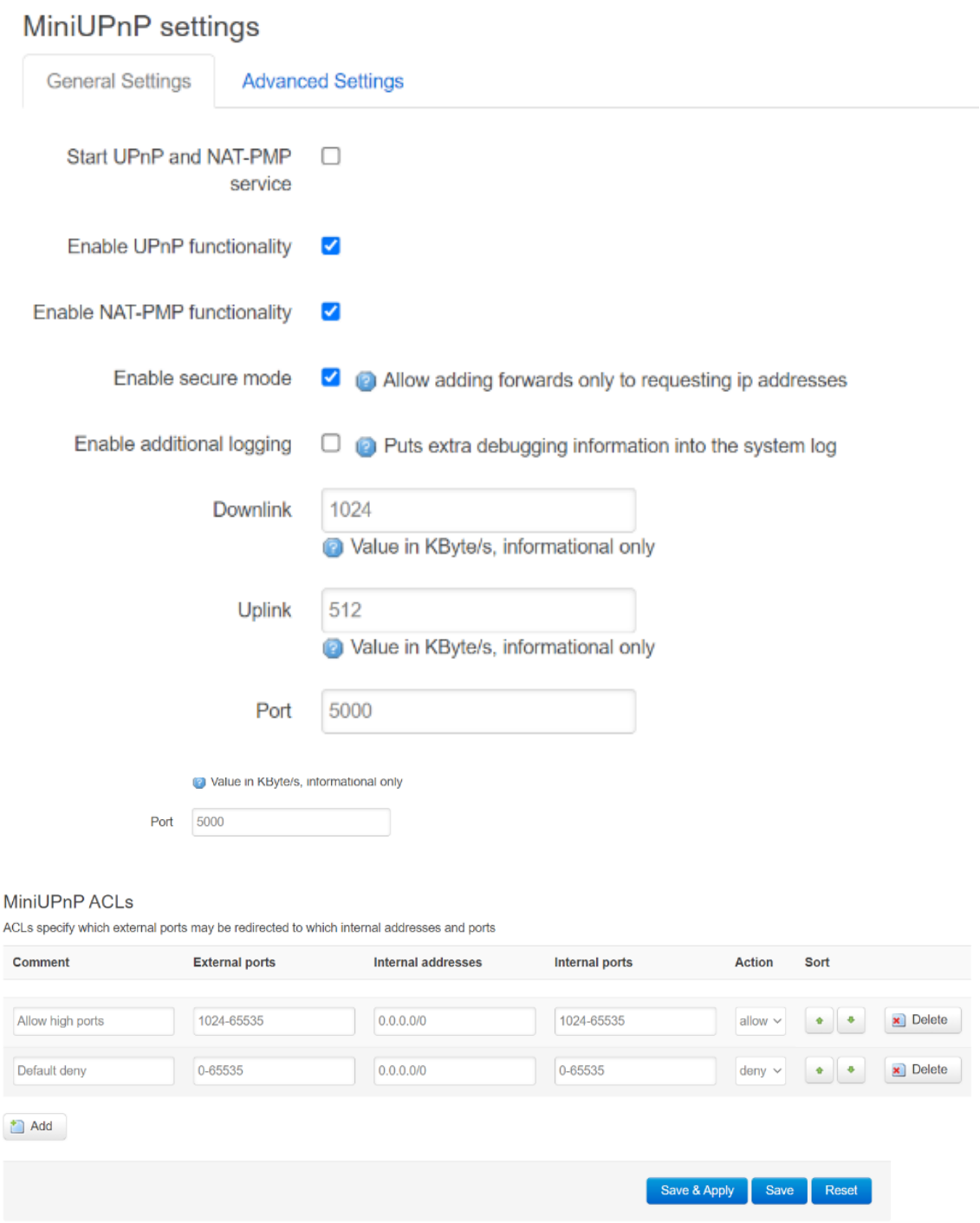
3.4.2 OpenVPN



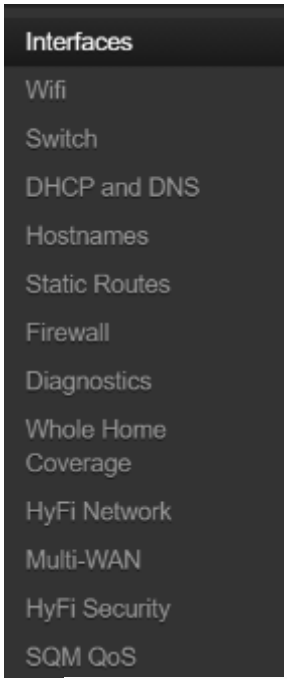
3.4.3 Select UPnP

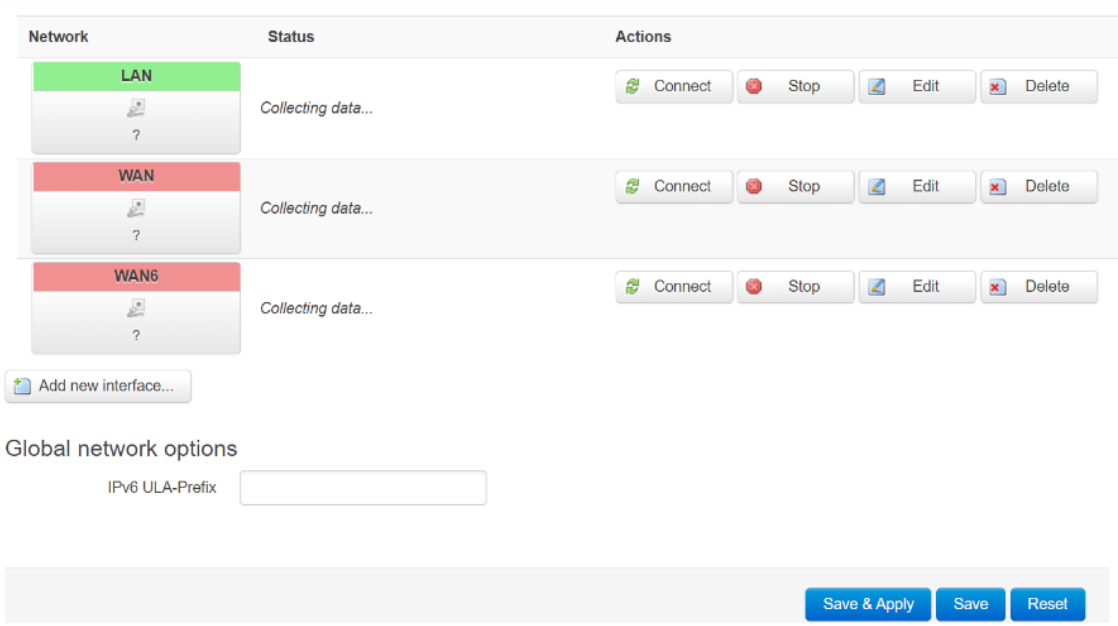




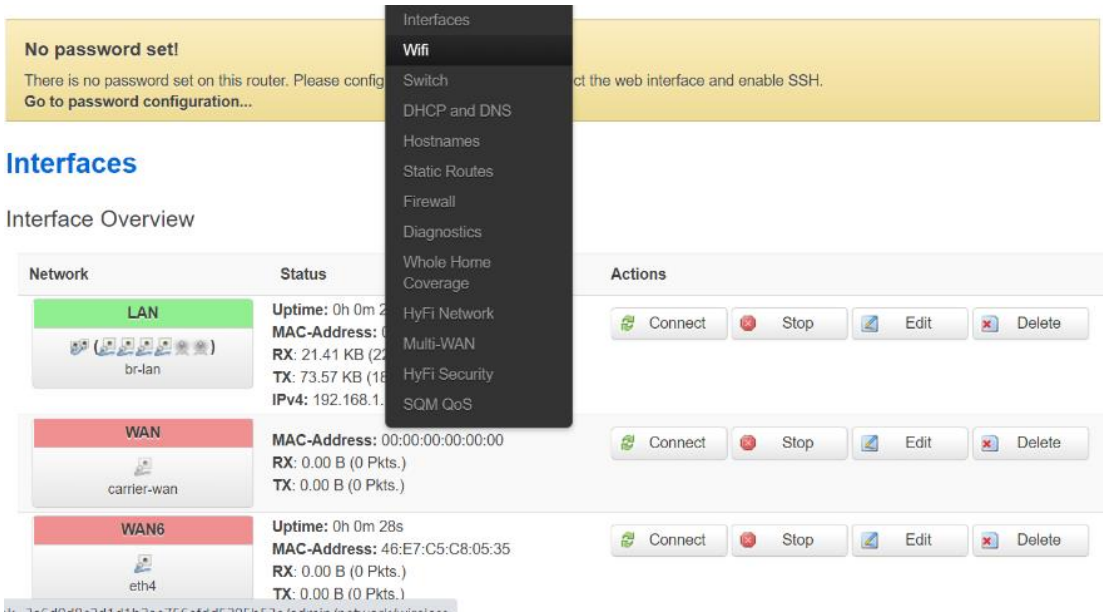


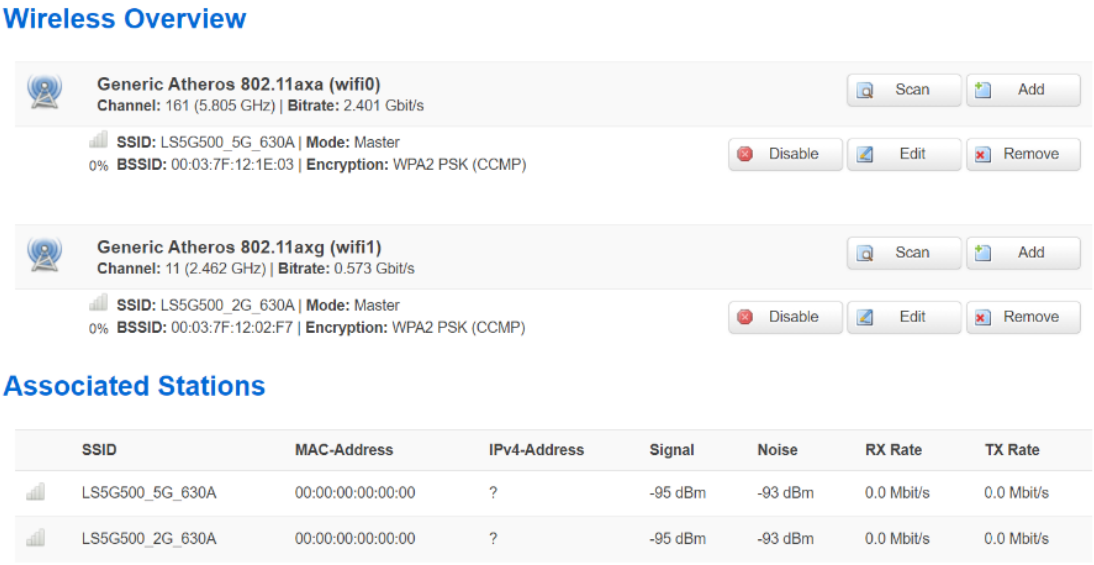
3.5 Under network, select Interface.



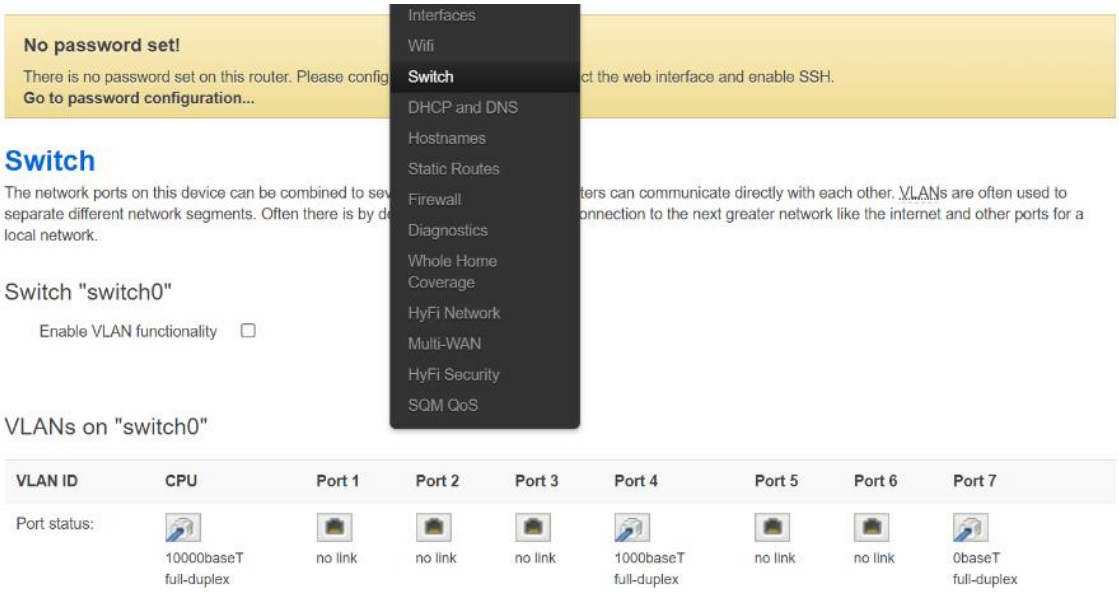


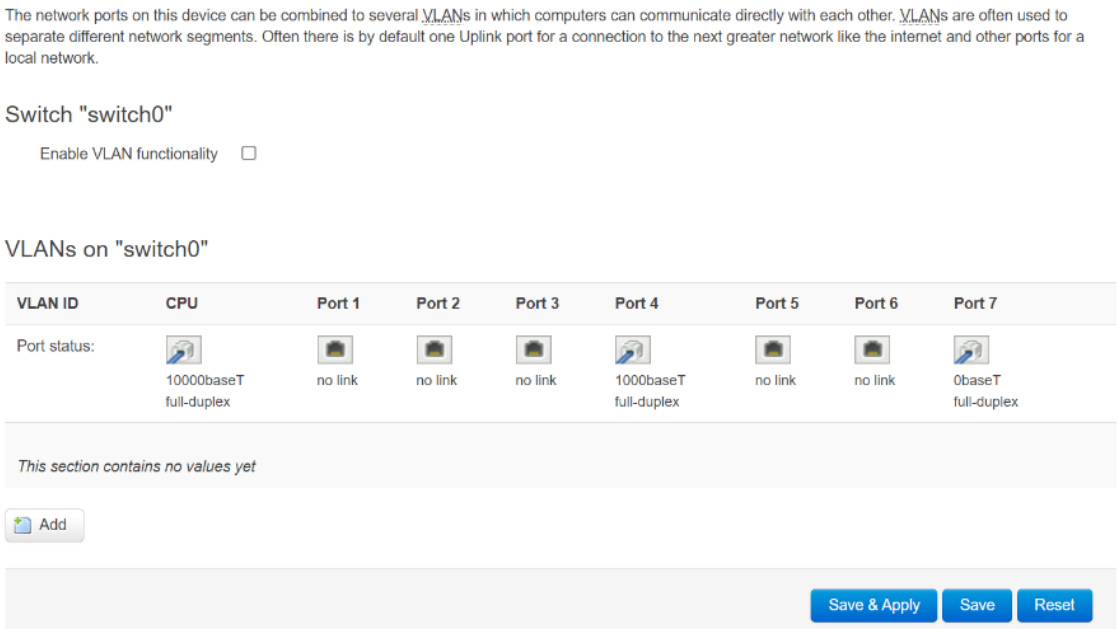
3.6 Select WiFi.



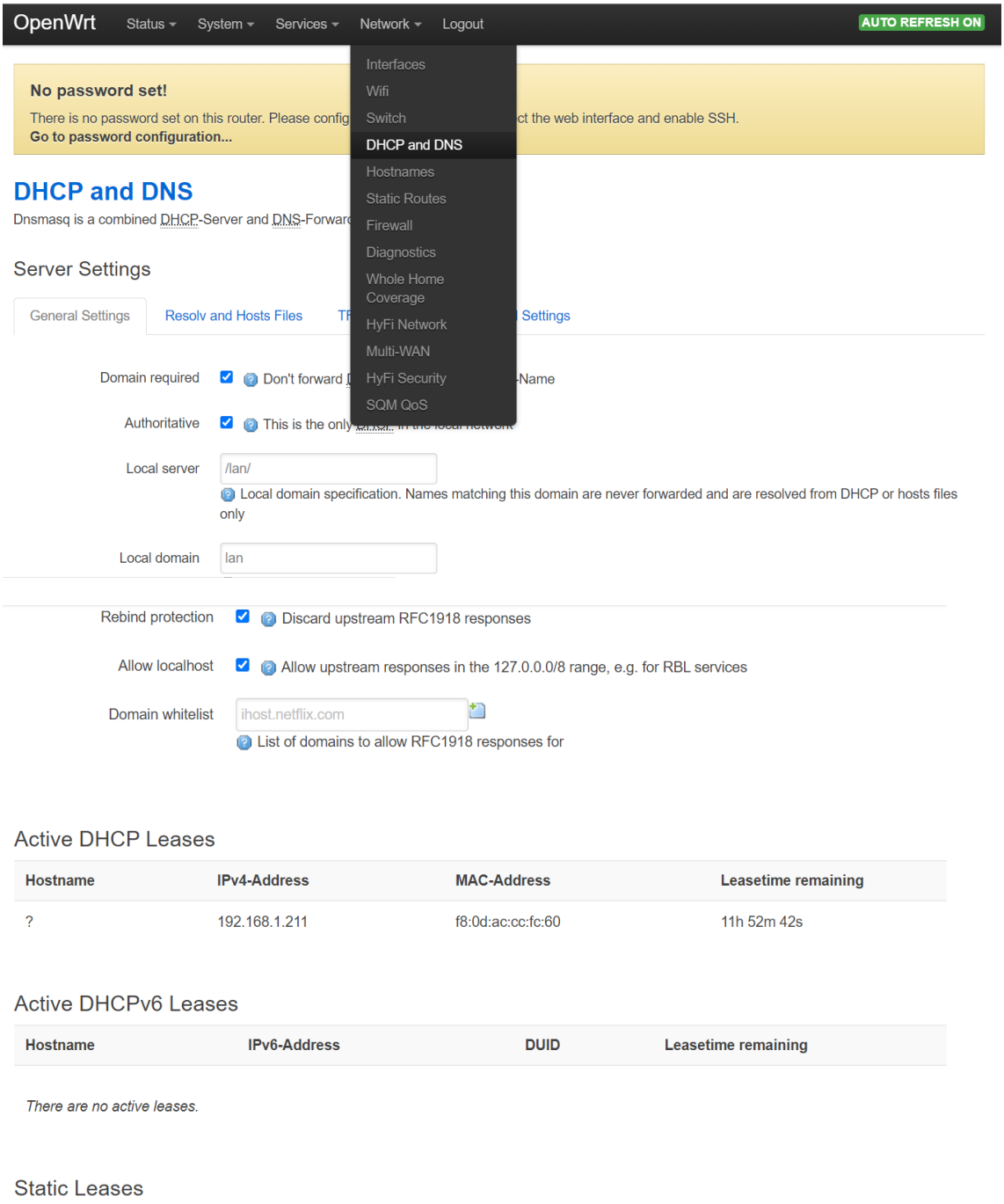


3.7 Select Switch.





3.8 Select DHCP & DNS



Active DHCP Leases

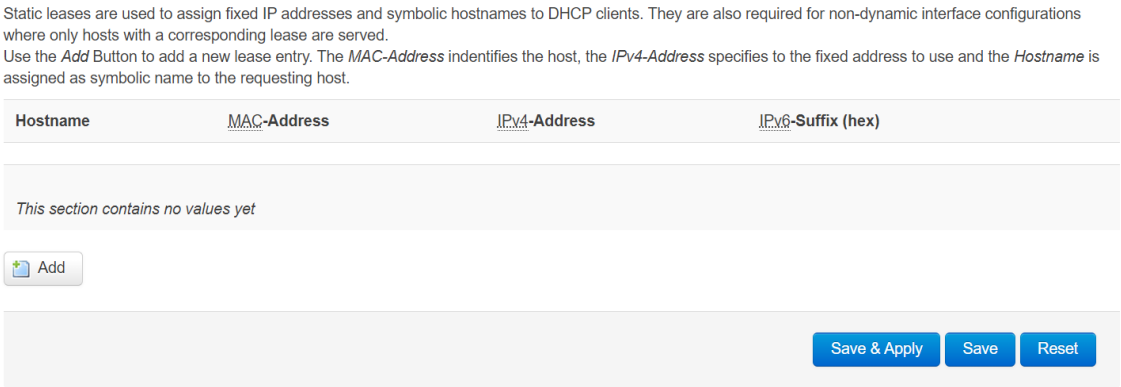
Hostname	IPv4-Address	MAC-Address	Leasetime remaining
?	192.168.1.211	f8:0d:ac:cc:fc:60	11h 52m 42s

Active DHCPv6 Leases

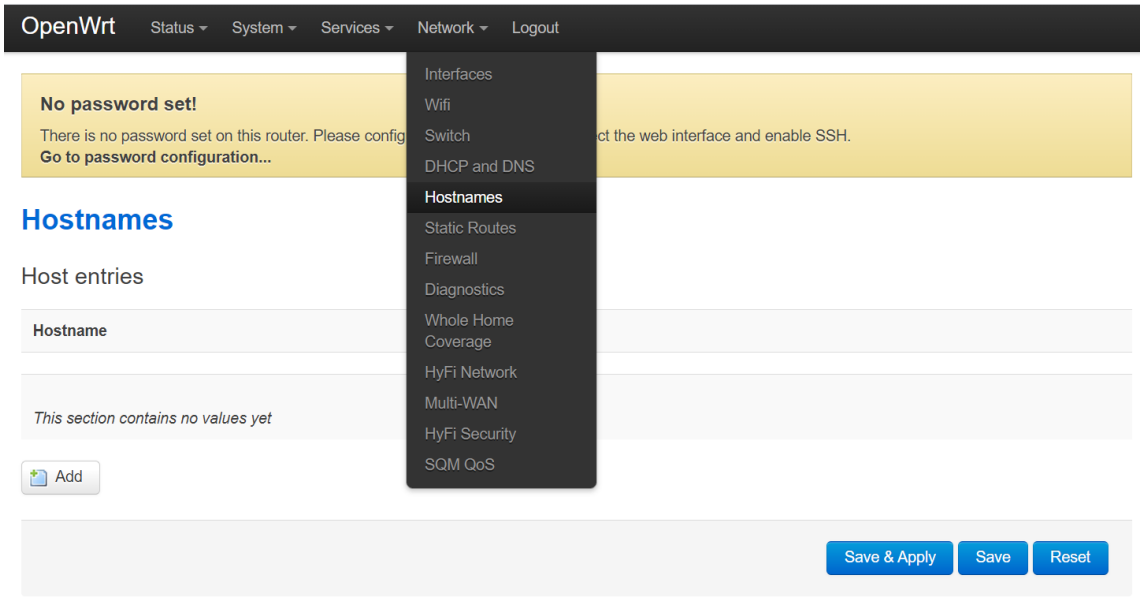
Hostname	IPv6-Address	DUID	Leasetime remaining

There are no active leases.

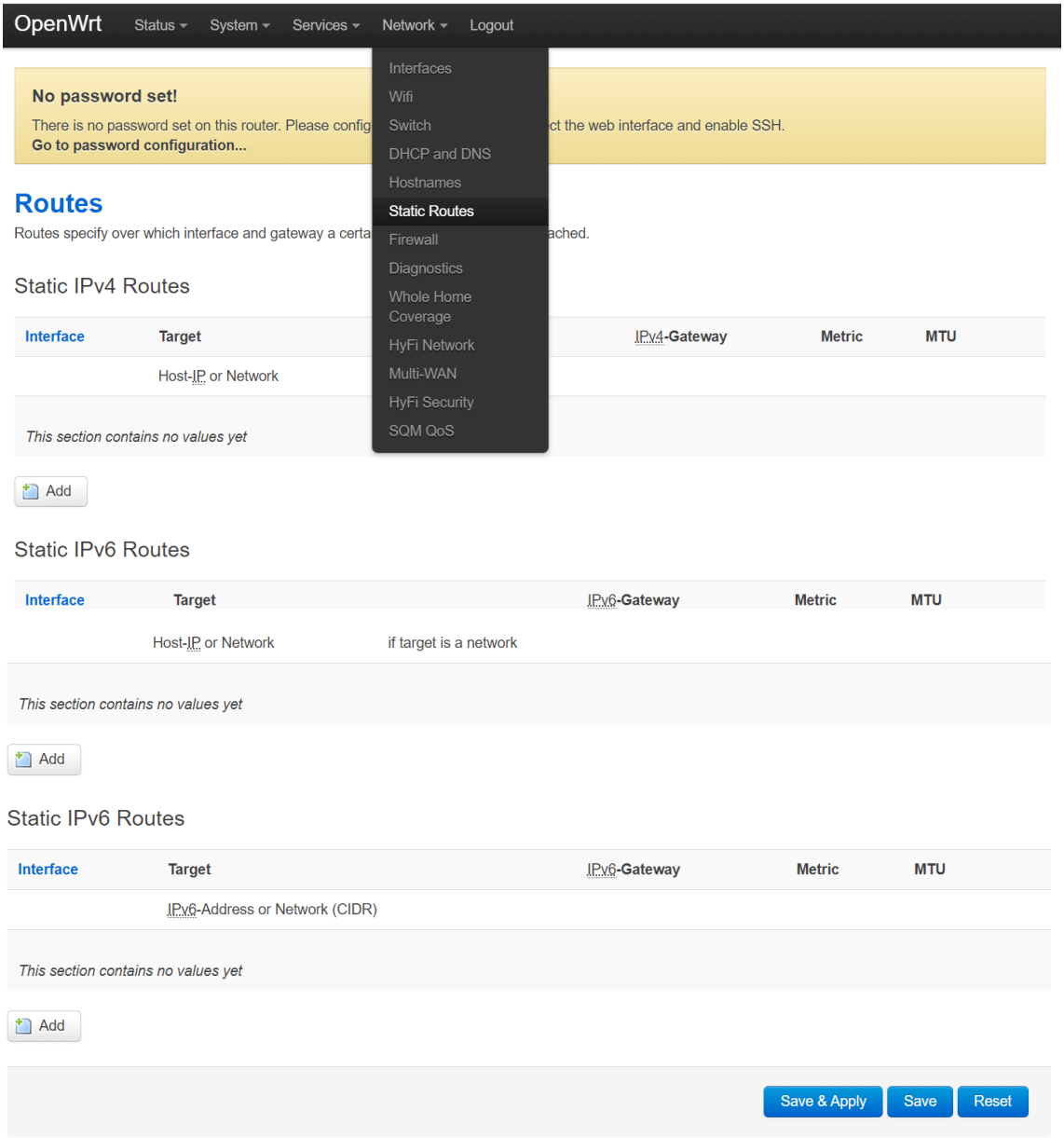
Static Leases



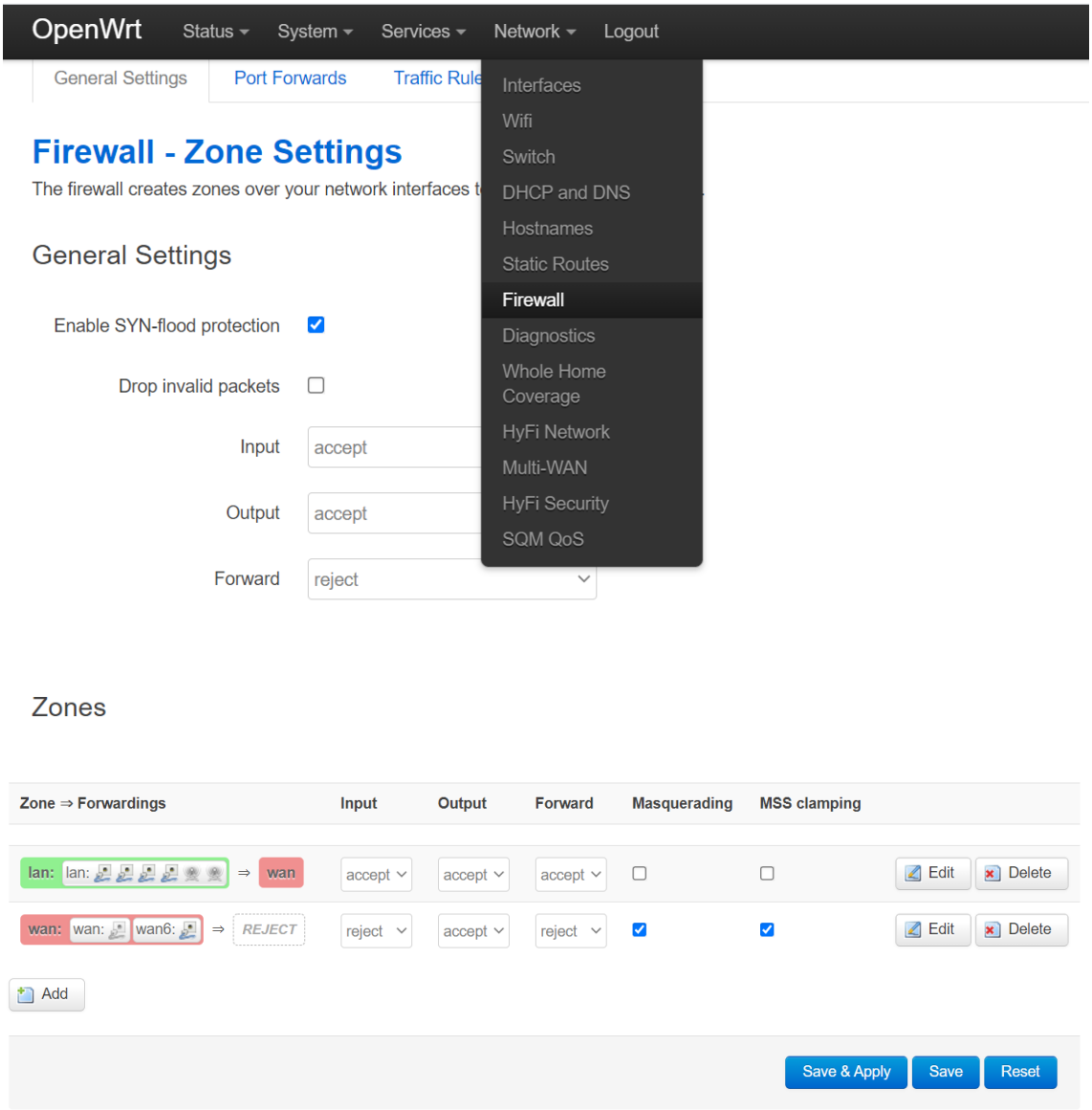
3.9 Select Hostname



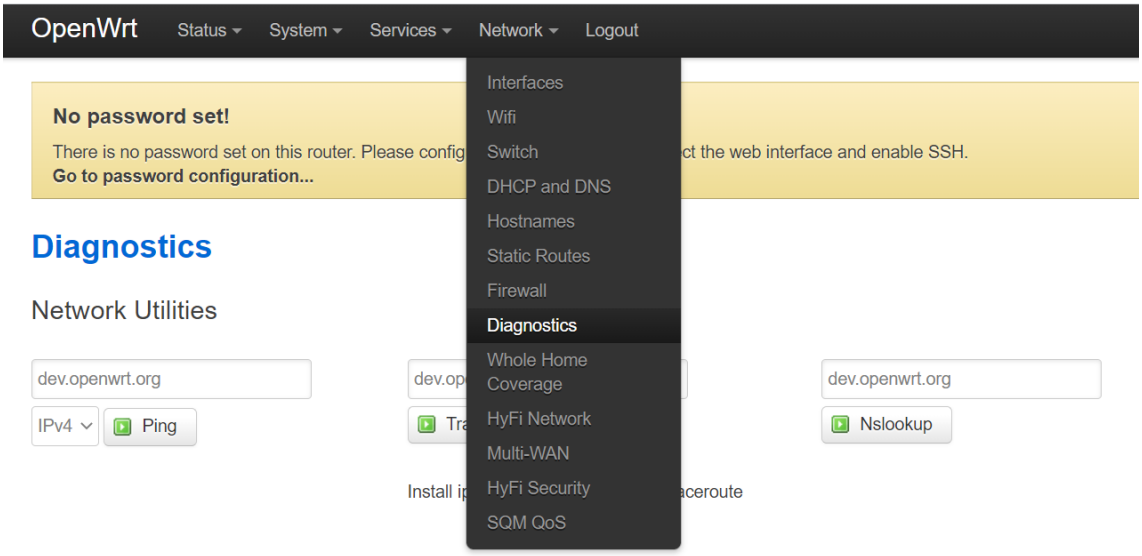
3.10 Select Static Rules



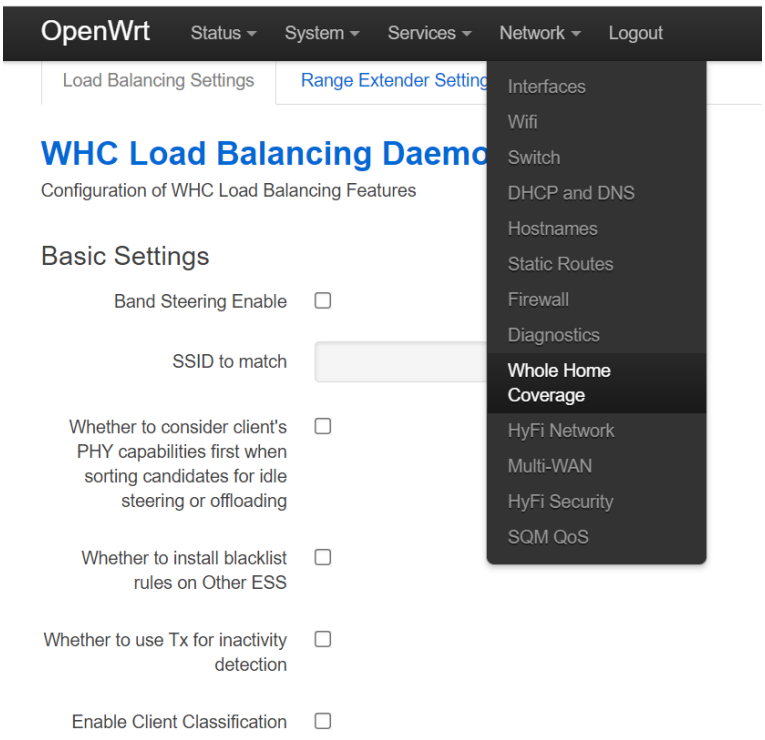
3.10 Select Firewall



3.11 Select Diagnostics



3.12 Whole Home Coverage



Station Database

Include out-of-network devices ☑

Track remote associations ☑

Mark 11k/v capable devices as dual band ☐

Idle Steering Settings

RSSI value indicating a node associated on 5 GHz should be steered to 2.4 GHz (dB)	5
RSSI value indicating a node associated on 2.4 GHz should be steered to 5 GHz (dB)	20
Normal Inactive timer (s)	10
Overload Inactive timer (s)	10
Inactive Check Frequency (s)	1

Active Steering Settings

When the client Tx rate increases beyond this threshold, generate an indication (Kbps)	50000
When evaluating a STA for rate-based upgrade steering, the RSSI must also be above this threshold (dB)	30
When the client Tx rate decreases beyond this threshold, generate an indication (Kbps)	6000
When the client RSSI decreases beyond this threshold, generate an indication (dB)	0

Offloading Settings

Time to average before generating a new utilization	60

Offloading Settings

Time to average before generating a new utilization report (s)	60
Medium utilization threshold for an overload condition on 2.4 GHz (%)	70
Medium utilization threshold for an overload condition on 5 GHz (%)	70
Medium utilization safety threshold for active steering to 2.4 GHz (%)	50
Medium utilization saftey threshold for active steering to 5 GHz (%)	60
Uplink RSSI (in dB) above which association will be considered safe	20

AP Steering Settings

DisableSteeringInactiveLegacyClie☑s

DisableSteeringActiveLegacyClien☑

DisableSteering11kUnfriendlyClien☑

RSSI value indicating a node associated on CAP is far enough to be steered to another AP	20
RSSI value indicating a node associated on RE is far enough to be steered to another AP	45
The RSSI value (in dB) the target AP should exceed the serving AP to be considered for AP steering towards root	5
The RSSI value (in dB) the target AP should exceed the serving AP to be considered for AP steering towards leaf	10

The RSSI value (in dB) the target AP should exceed the serving AP to be considered for AP steering between peers: 10

The value (in dB) the target AP downlink should exceed to be considered to steer to 5 GH: -65

Interference Avoidance Steering Settings

If cleared, will not perform any Interference Avoidance Steering from the 2.4GHz band: 0

If cleared, will not perform any Interference Avoidance Steering from the 5GHz band: 0

Maximum time (in seconds) a BSS can be considered polluted with no further updates: 1200

If set, use best-effort mode (failures do not mark a STA as unfriendly) for IAS steering: 0

Steering Executor Settings

Time to wait before steering a legacy client again after completing steering (s): 300

Time to wait before steering a client via BTM again after completing steering without sending an auth reject (s): 30

Show Advanced Settings

Show Diagnostic Log Settings

Basic Advanced

Maximum number of seconds elapsed allowed for a 'recent' measurement: 5

Maximum number of seconds elapsed allowed for a 'recent' backhaul capacity measurement: 60

Maximum number of seconds elapsed allowed for a 'recent' measurement for a legacy Client: 20

Whether running with 0 AP interfaces is permitted: ☐

Save & Apply | Save | Reset

Load Balancing Settings | Range Extender Settings

WHC - Range Extender Placement and Auto-configuration Daemon Settings

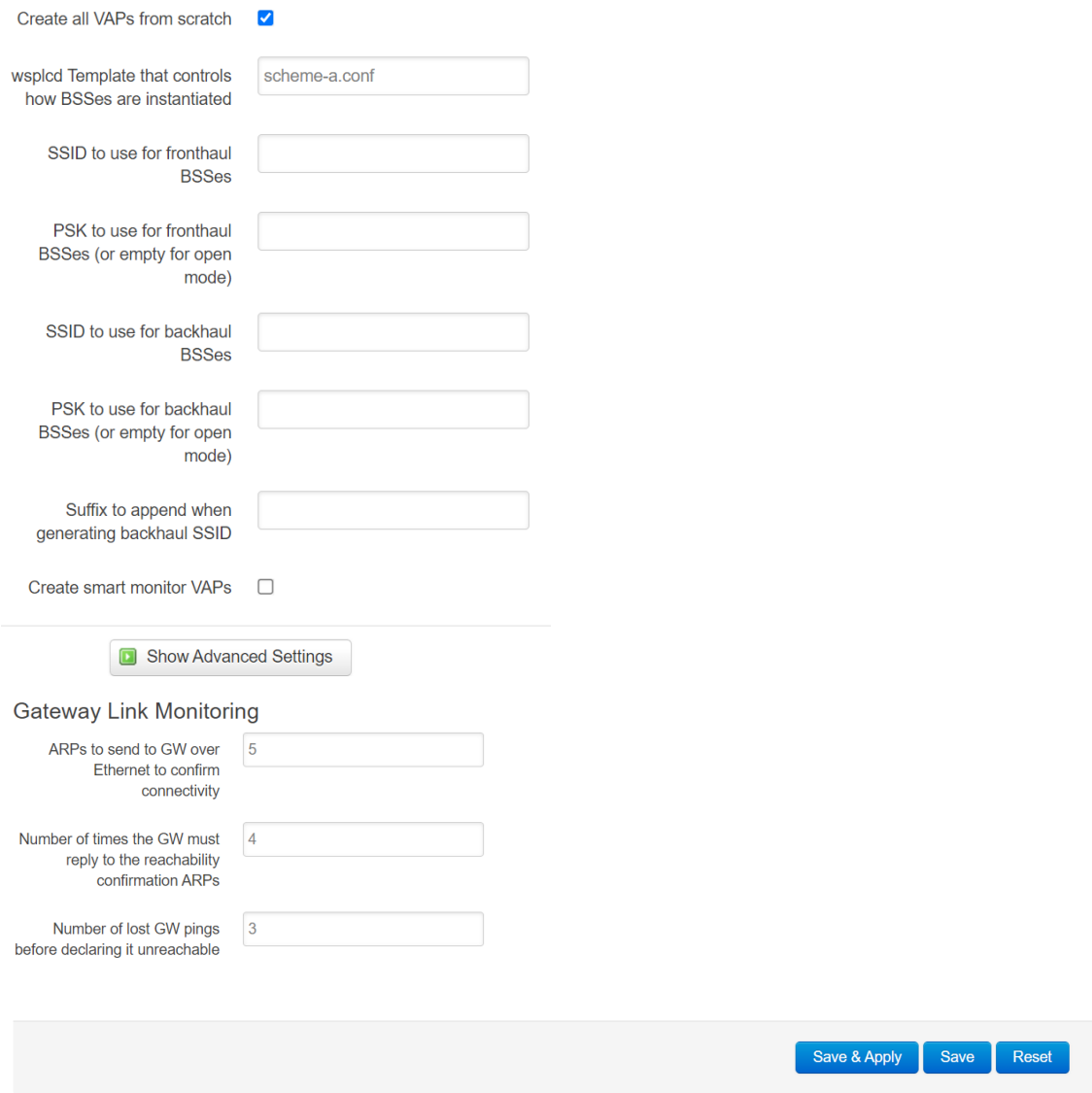
Configuration of WHC Range Extender Features

Basic Settings

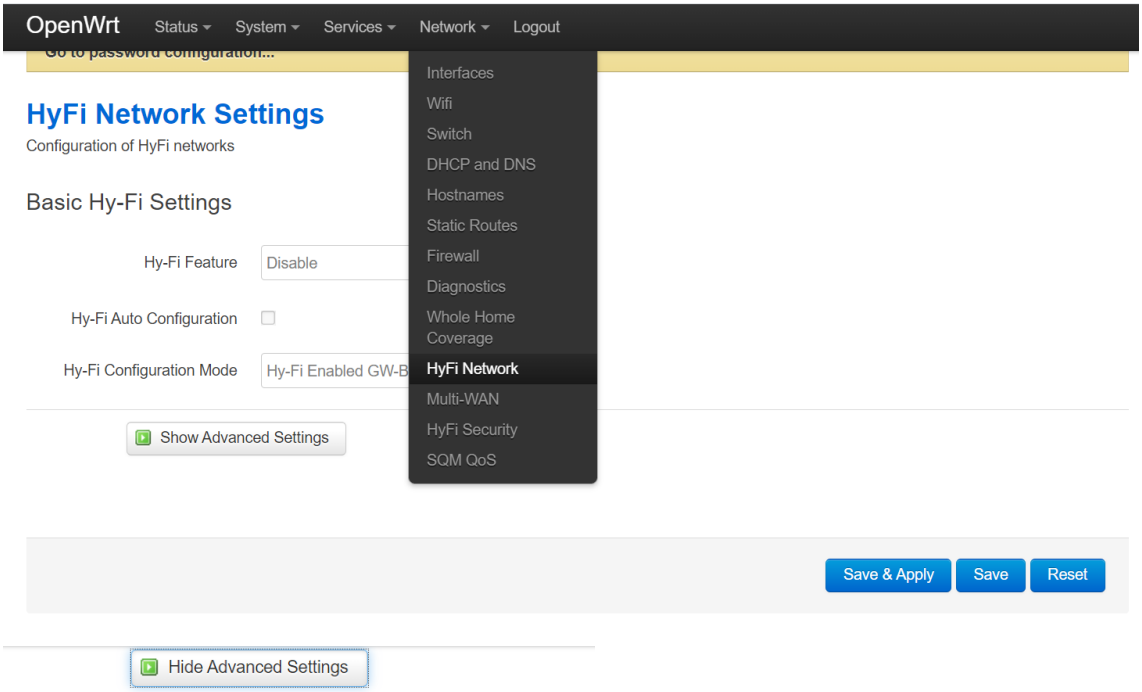
RE Placement and Auto-Configuration Enable	☐
Network to extend	lan
Primary device purpose	Range extender
Mode when connected to gateway	Access Point
Method of range extension	Automatic selection
Interoperable RE mode to use	QWRAP
Enable steering in WDS mode	☑
Enable switching into full Wi-Fi SON mode	☑
Manage the Multicast Services Daemon (mcsd)	☑
Do not operate on DFS channels	☐
Link check delay (s)	2
Enable multi-ssid and traffic separation in SON mode	☐
Guest network bridge name	guest
Guest network's backhaul interface	Both

Multi-AP Basic Settings

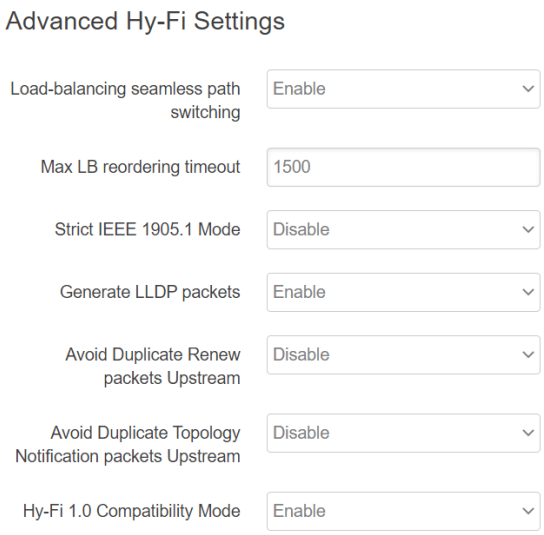
Enable Multi-AP Topology Optimization Algorithm	☐



3.13 HiFy Network


OpenWrt
Status
System
Services
Network
Logout
Interfaces
Wifi
Switch
DHCP and DNS
Hostnames
Static Routes
Firewall
Diagnostics
Whole Home Coverage
HyFi Network
Multi-WAN
HyFi Security
SQM QoS
HyFi Network Settings
Configuration of HyFi networks
Basic Hy-Fi Settings
Hy-Fi Feature
Disable
Hy-Fi Auto Configuration
Hy-Fi Configuration Mode
Hy-Fi Enabled GW-B
Show Advanced Settings
Save & Apply
Save
Reset

Hide Advanced Settings


Advanced Hy-Fi Settings
Load-balancing seamless path switching
Enable
Max LB reordering timeout
1500
Strict IEEE 1905.1 Mode
Disable
Generate LLDP packets
Enable
Avoid Duplicate Renew packets Upstream
Disable
Avoid Duplicate Topology Notification packets Upstream
Disable
Hy-Fi 1.0 Compatibility Mode
Enable

Constrain TCP-ACK streams to the same medium as their primary TCP-DATA stream	Disable
Maximum age of a H-Active entry before it will be aged out (ms)	120000
Hy-Fi Netfilter forwarding mode	APS
IGMP Extra Query response time	

Advanced Auto-Configuration Settings

Interval Between DHCP Discovery Messages (sec)	2
HR Number of Seconds Between DHCP Retries	3
HR Maintenance Interval Between DHCP Discovery	15

Constrain TCP-ACK streams to the same medium as their primary TCP-DATA stream	Disable
Maximum age of a H-Active entry before it will be aged out (ms)	120000
Hy-Fi Netfilter forwarding mode	APS
IGMP Extra Query response time	

Advanced Auto-Configuration Settings

Interval Between DHCP Discovery Messages (sec)	2
HR Number of Seconds Between DHCP Retries	3
HR Maintenance Interval Between DHCP Discovery	15

General WLAN Path Characterization Setting

Use the WHC algorithm to calculate link capacity	1
Number of capacity updates to receive after link change before considered valid	3

WLAN 5G Path Characterization Setting

UpdatedStatsInterval	1
StatsAgedOutInterval	30
MaxMediumUtilization	70
MediumChangeThreshold	10
LinkChangeThreshold	10
MaxMediumUtilizationForLC	70
CPULimitedTCPThroughput	0
CPULimitedUDPThroughput	0
PHYRateThresholdForMU	2000
ProbePacketInterval	1
ProbePacketSize	64
EnableProbe	1
AssocDetectionDelay	5
Rate above which ScalingFactorHigh is used	

WLAN 2.4G Path Characterization Setting

WLAN 2.4G Path Characterization Setting

UpdatedStatsInterval	1
StatsAgedOutInterval	30
MaxMediumUtilization	70
MediumChangeThreshold	10
LinkChangeThreshold	10
MaxMediumUtilizationForLC	70
CPULimitedTCPThroughput	0
CPULimitedUDPThroughput	0
PHYRateThresholdForMU	2000
ProbePacketInterval	1

ProbePacketInterval	1
ProbePacketSize	64
EnableProbe	1
AssocDetectionDelay	5
Rate above which ScalingFactorHigh is used	

PLC Path Characterization Setting

MaxMediumUtilization	80
MediumChangeThreshold	10
LinkChangeThreshold	10

EntryExpirationInterval	120
MaxMediumUtilizationForLC	80
LCThresholdForUnreachable	5
LCThresholdForReachable	10
HostPLCInterfaceSpeed	0

Stream Estimation Setting

UpdateHSPECInterval	1
NotificationThresholdLimit	10
NotificationThresholdPercentage	20
AlphaNumerator	3
LocalFlowRateThreshold	2000000
LocalFlowRatioThreshold	5
Maximum number of H-Active entries supported in user-space	8192

Topology Discovery Setting

ND_UPDATE_INTERVAL	15
BD_UPDATE_INTERVAL	3
HOLDING_TIME	190
TIMER_LOW_BOUND	7
TIMER_UPPER_BOUND	11

MSGID_DELTA	64
HA_AGING_INTERVAL	120
ENABLE_TD3	1
ENABLE_BD_SPOOFING	1
NOTIFICATION_THROTTLING_W	1
PERIODIC_QUERY_INTERVAL	60
ENABLE_NOTIFICATION_UNICAS	☑

Path Selection Setting

UpdateHDInterval	10
LinkCapacityThreshold	20
NonUDPInterfaceOrder	EP52
SerialflowIterations	10
DeltaLCThreshold	10
EnableBadLinkStatsSwitchFlow	☑

WLAN Manager Settings

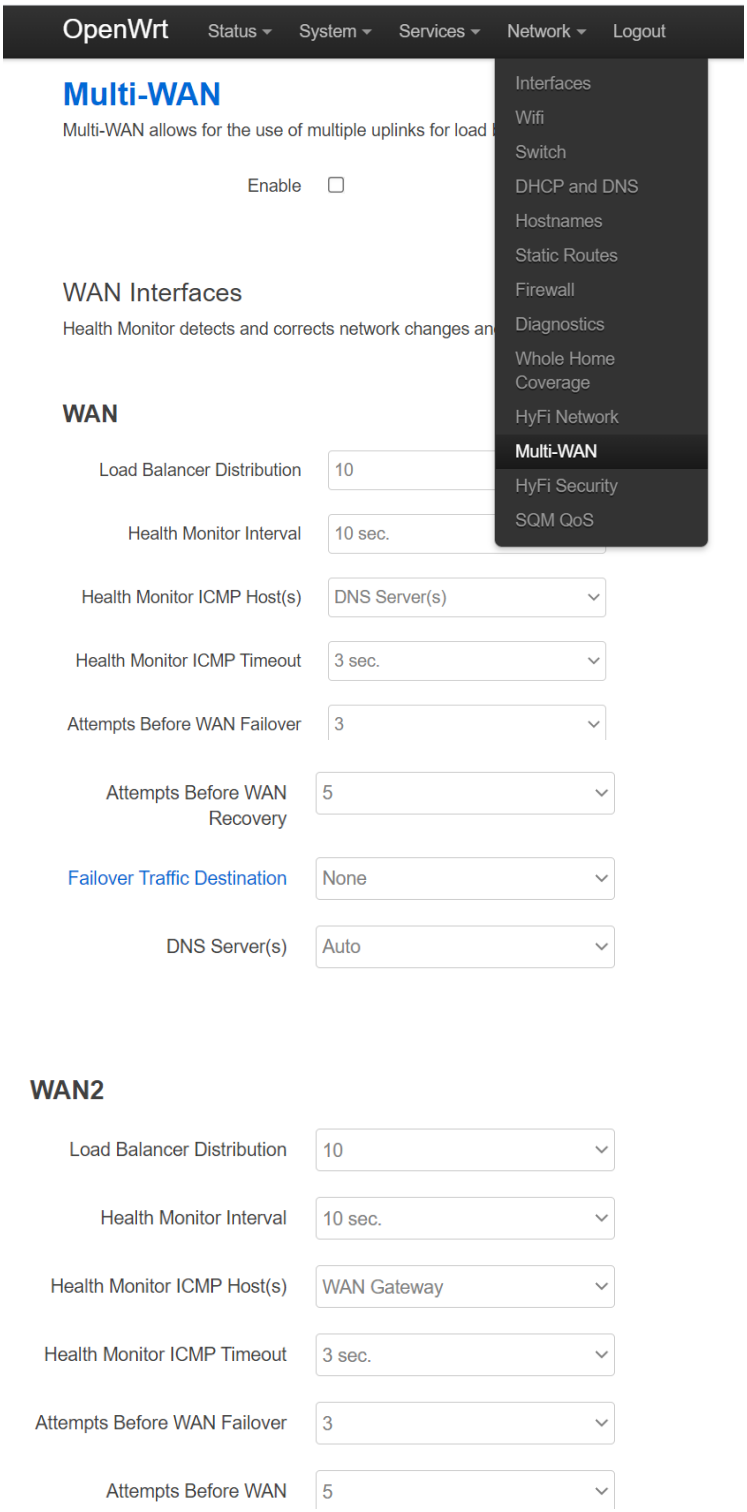
WlanCheckFreqInterval	10
WlanALDNLNumOverride	0

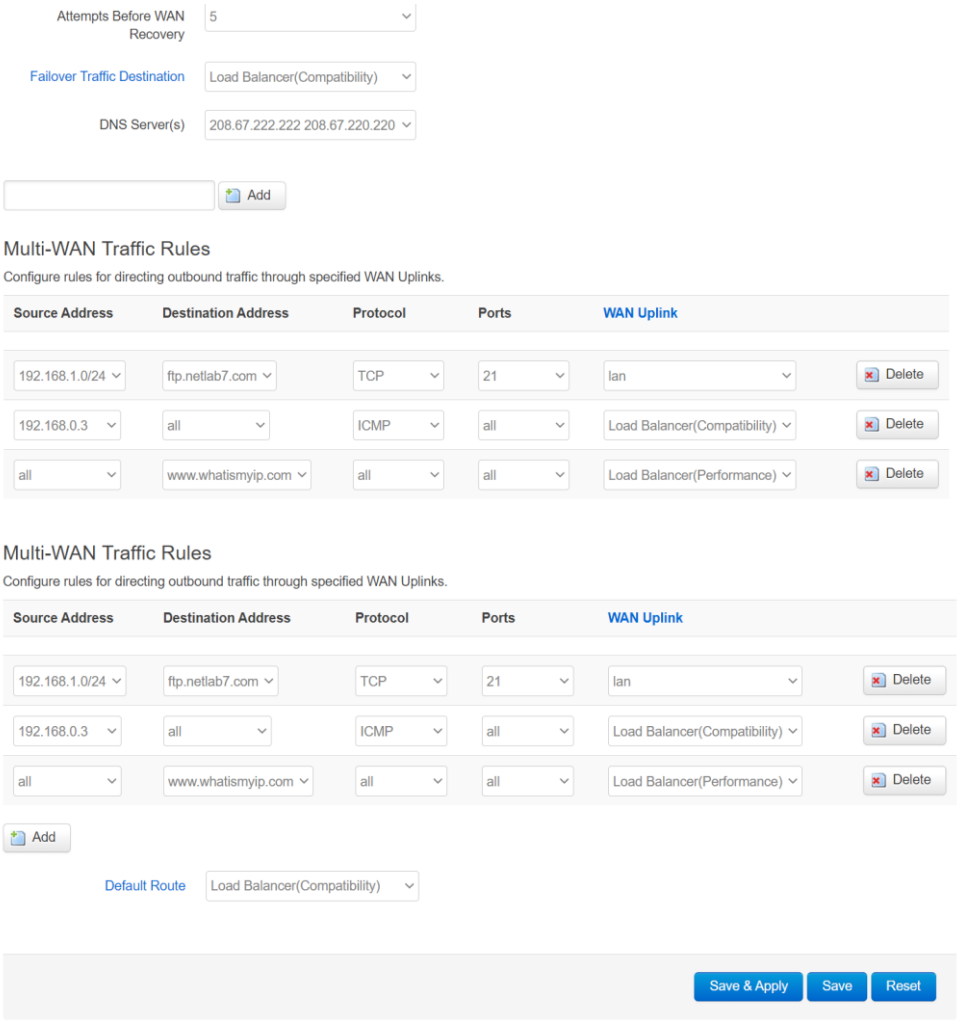
LOG settings

EnableLog	0

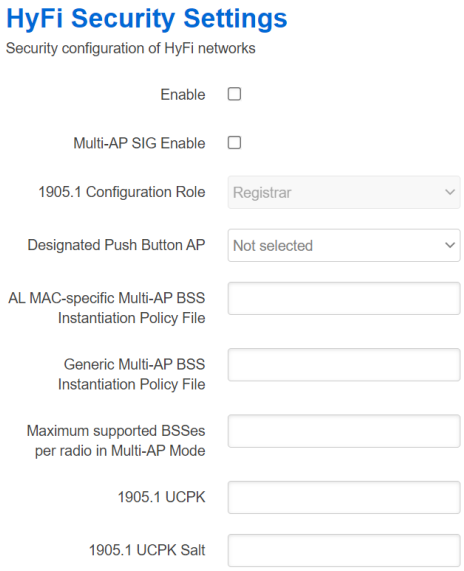
Port range that source port number in packet header.

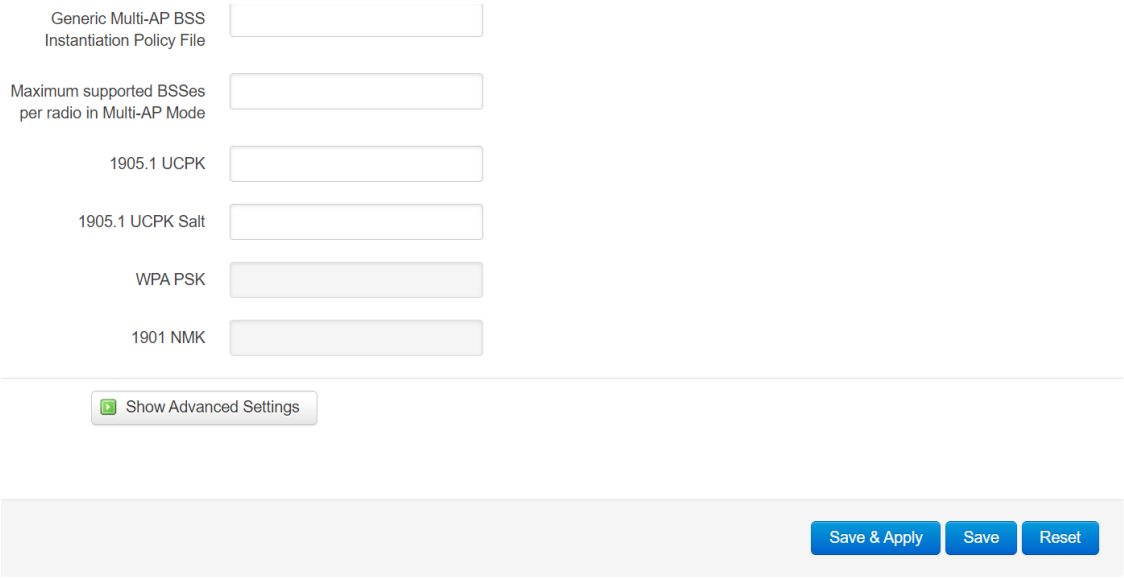
3.14 Select Multi-WAN


OpenWrt
Status
System
Services
Network
Logout
Interfaces
Wifi
Switch
DHCP and DNS
Hostnames
Static Routes
Firewall
Diagnostics
Whole Home Coverage
HyFi Network
Multi-WAN
HyFi Security
SQM QoS
Multi-WAN
Multi-WAN allows for the use of multiple uplinks for load
Enable
WAN Interfaces
Health Monitor detects and corrects network changes an
WAN
Load Balancer Distribution
10
Health Monitor Interval
10 sec.
Health Monitor ICMP Host(s)
DNS Server(s)
Health Monitor ICMP Timeout
3 sec.
Attempts Before WAN Failover
3
Attempts Before WAN Recovery
5
Failover Traffic Destination
None
DNS Server(s)
Auto
WAN2
Load Balancer Distribution
10
Health Monitor Interval
10 sec.
Health Monitor ICMP Host(s)
WAN Gateway
Health Monitor ICMP Timeout
3 sec.
Attempts Before WAN Failover
3
Attempts Before WAN
5

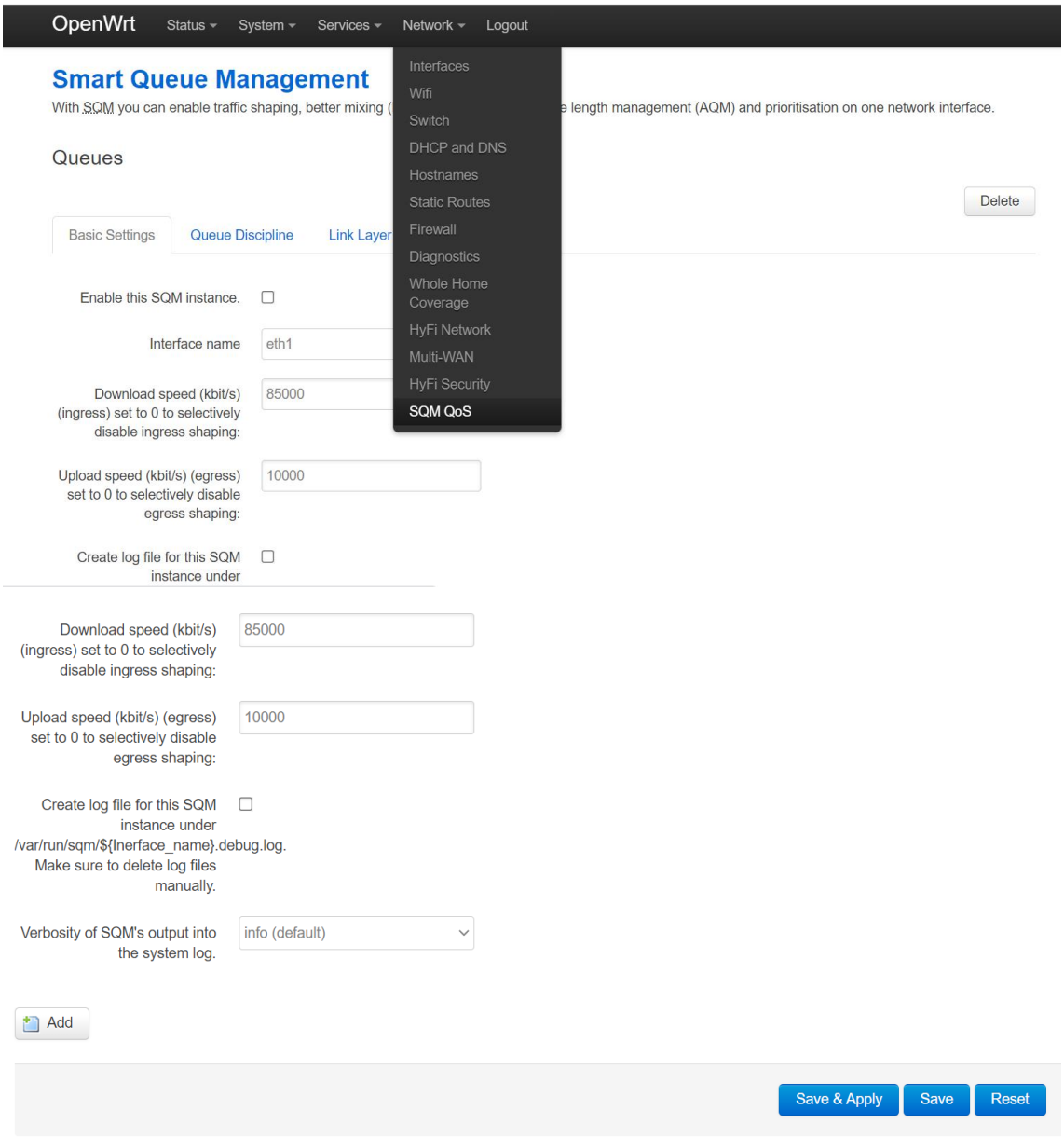


3.15 Select HiFy Security

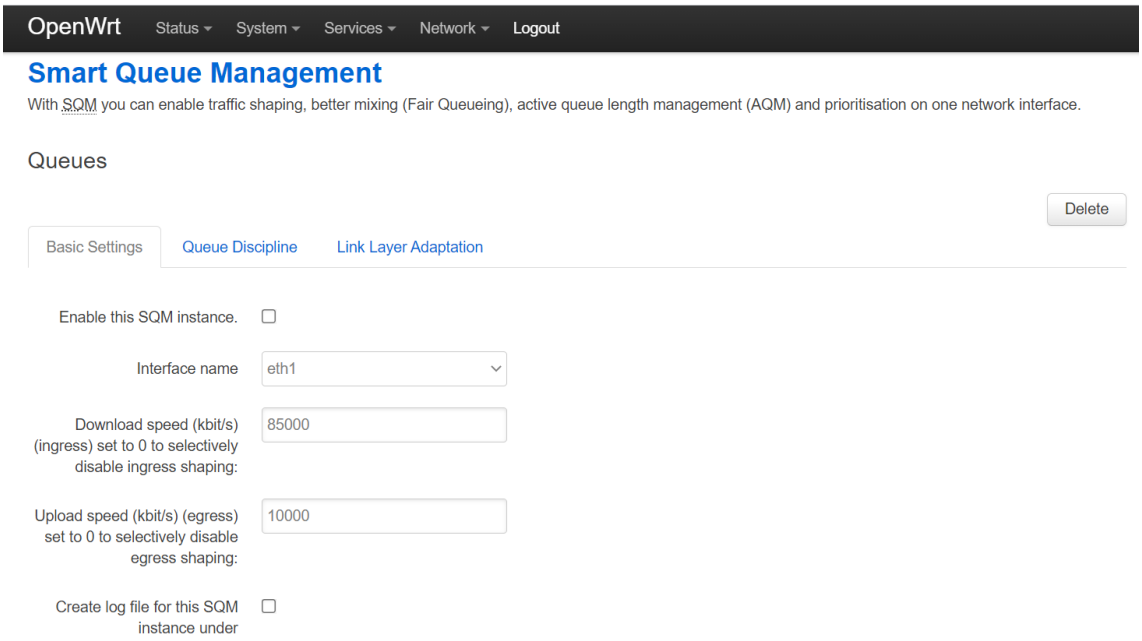



Generic Multi-AP BSS Instantiation Policy File
Maximum supported BSSes per radio in Multi-AP Mode
1905.1 UCPK
1905.1 UCPK Salt
WPA PSK
1901 NMK
Show Advanced Settings
Save & Apply
Save
Reset

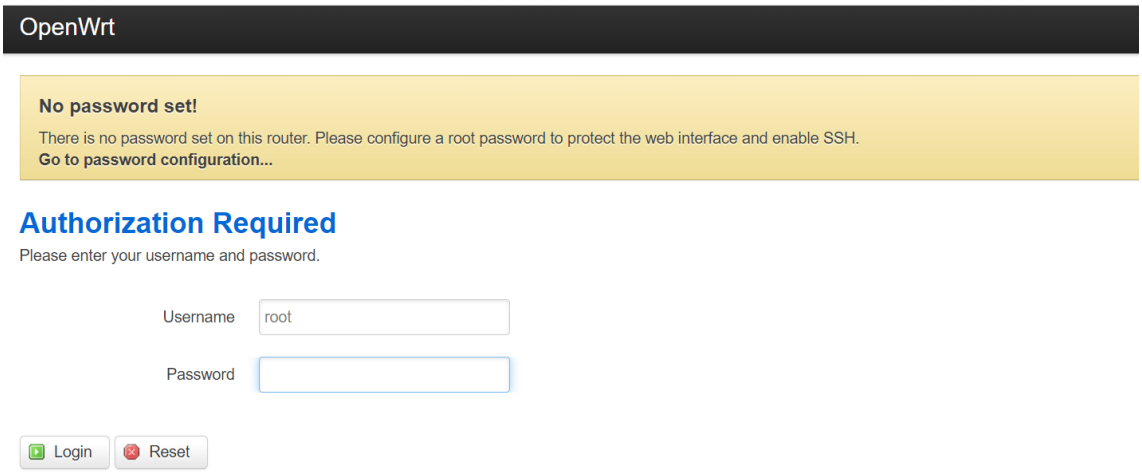
3.16 Select SQM QoS



3.17 Select Logout



3.18 After logout, re-login again.



----------End----------