

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

Table of contents	2
FCC Warning Message:	3
Copyright	4
1. INTRODUCTION.....	5
2. BRIEF INFORMATION	6
3. SETTING YOUR PC ENVIRONMENT	15

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

This user manual describes features, especially usage of 5G gateway 500G including hardware and software. LIGHTSPEED has made best effort to ensure that the information contained in this document is accurate and reliable. This document is the property of LIGHTSPEED and implies no license under patents, copyrights, trade secrets. No part of this publication should be copied, reproduced, stored in a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photographic, or otherwise) without the prior permission of LIGHTSPEED.

Purpose

This manual includes how to use and configure the 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 perform wireless internet service between PC and wireless WAN via 5G 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 500G has some special function on wireless mobile internet like always on-line, demands on-line etc. It also provides IP filtering, Mac filtering for tight security application.

5G gateway 500G can 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/ax 2.5Gbps 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 are the 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 LEDWPS

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 LAN devices 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 500G as 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 by Modem router mode/Always On-line at 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.

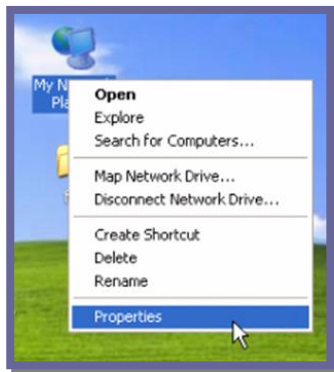


Figure 4: Step 1 of setting your PC's network environment.

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

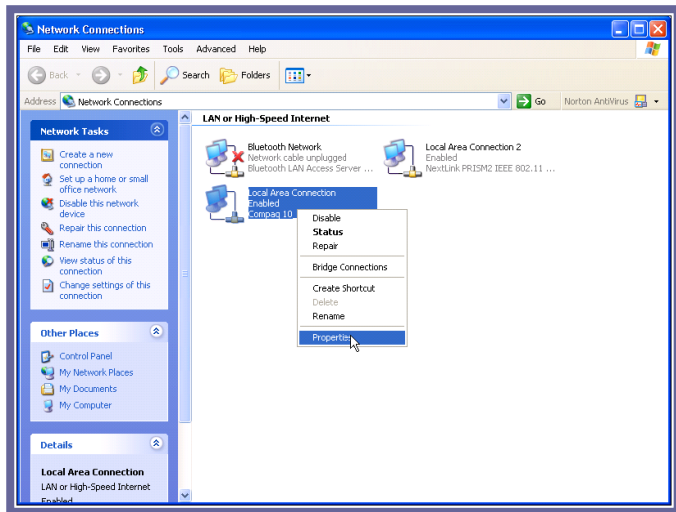


Figure 5: Step 2 of setting your PC's network environment

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

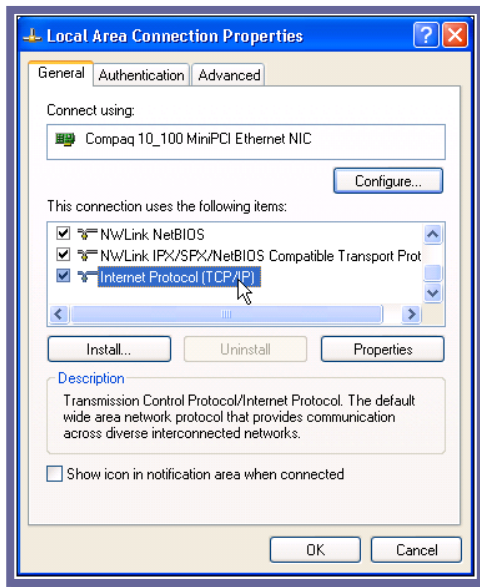


Figure 6: Step 3 of setting your PC’s network environment

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

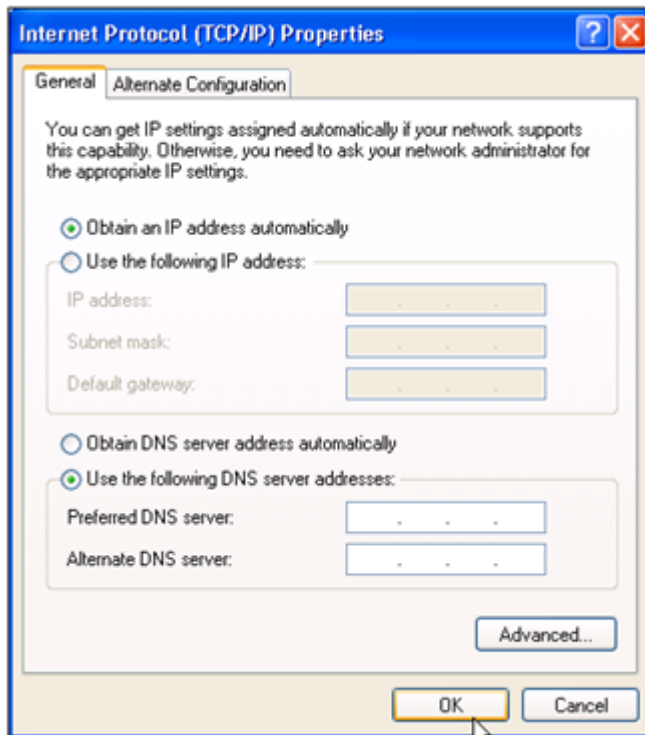


Figure 7: Step 4 of setting your PC’s network environment

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

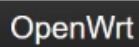
Lunch the web browser and put <http://192.168.1.1> on the address filed in browser than pop-up login page like follow

Default login credential is

User name: root

Password:

(No password)

The logo for OpenWrt, consisting of the text "OpenWrt" in white on a black rectangular background.

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...](#)

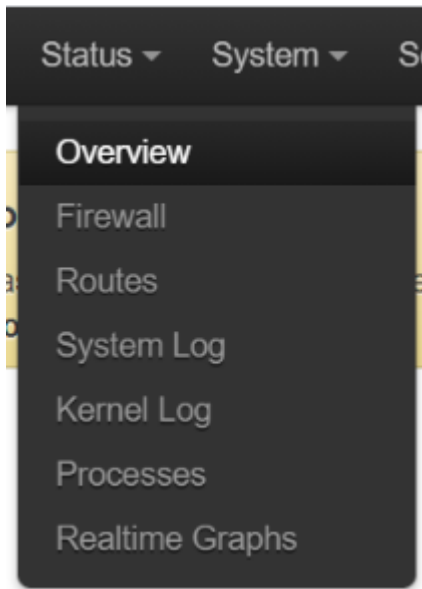
Authorization Required

Please enter your username and password.

Username

Password

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



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 (wif0)  **SSID:** LS5G500_5G_630A
 0% **Mode:** Master
Channel: 100 (5,500 GHz)
Bitrate: 2,401 Mbit/s


Generic 802.11axg Wireless Controller (wif1)  **SSID:** LS5G500_2G_630A
 0% **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

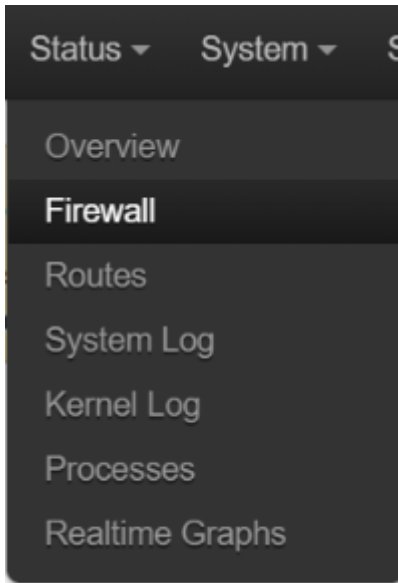
Multi-WAN Status

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	icmp type 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
--------	-------	---------	--------	-------	-------	----	-----	--------	-------------	---------

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)

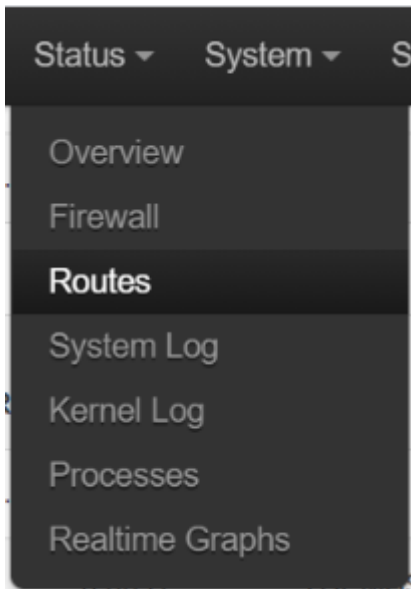
Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	0	0.00 B	TCPMSS	tcp	--	*	eth4	0.0.0.0/0	0.0.0.0/0	tcp flags:0x06/0x02 /* wan (mtu_fix) */ TCPMSS clamp to PMTU

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

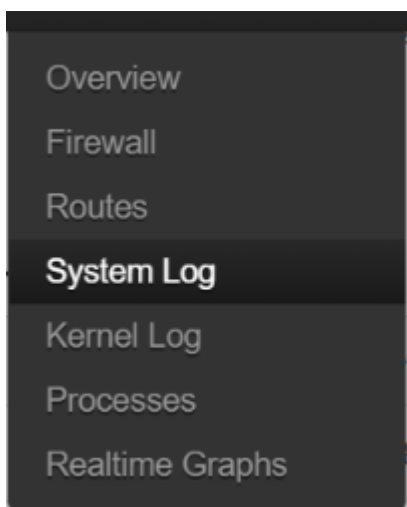
Active IPv6-Routes

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":

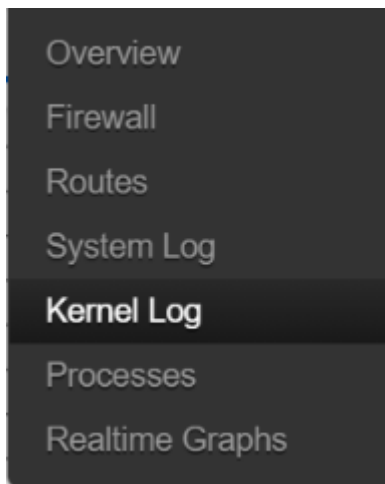


It will show:

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/sc
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-128
Tue May 11 02:42:51 2021 user.notice ModemManager: hotplug: event reported: action=add, name=ath0, subsystem=net
```

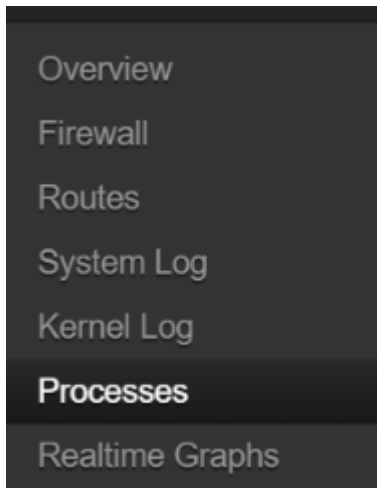
Kernel log:



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 cpufreq
[ 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 00:00:00 UTC 2016
[ 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 wigi_dump@51300000 (0x0000000051300000--0x0000000051700000)
[ 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 @ffffc03ef47000 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

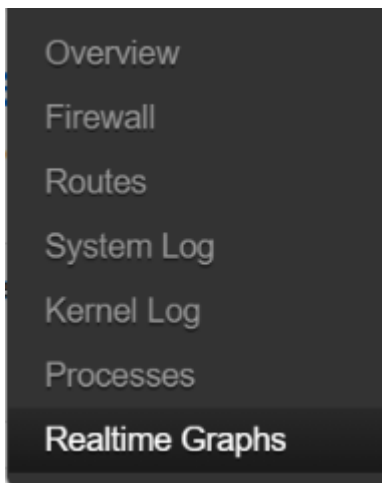


Processes

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.

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...](#)

Authorization Required

Please enter your username and password.

Username

Password

Login Reset

3.3. System

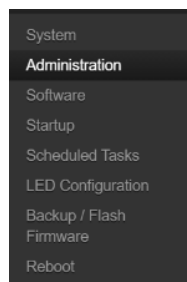
Select System, it will show currently running system processes & their status.

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	[kssoftirqd/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.

Memory

Total Available	631308 kB / 886388 kB (71%)
Free	625612 kB / 886388 kB (70%)
Buffered	5696 kB / 886388 kB (0%)

Network

IPv4 WAN Status	 Type: static
	 Address: 192.168.2.1
	Netmask: 255.255.255.0
	Gateway: 192.168.2.1

3.3.2 Software

- System
- Administration
- Software**
- Startup
- Scheduled Tasks
- LED Configuration
- Backup / Flash

Software

Actions Configuration

No package lists available

 Update lists

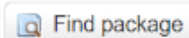
Free space: 97% (11.37 MB)



Download and install package:

OK

Filter:

 Find package

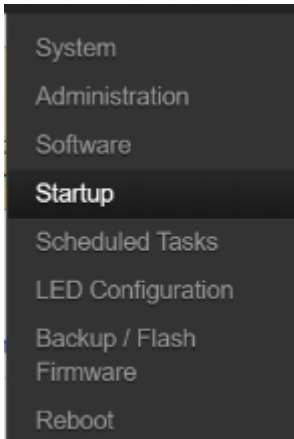
Status

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	qtr	Enabled	Start	Restart	Stop
9	qca-iot	Enabled	Start	Restart	Stop
10	boot	Enabled	Start	Restart	Stop
10	system	Enabled	Start	Restart	Stop

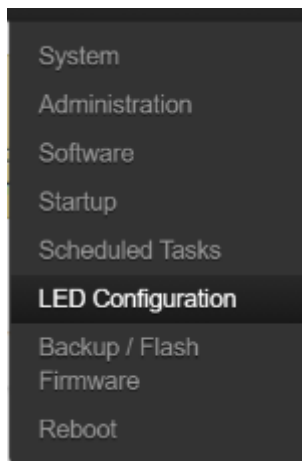
3.3.3. Scheduled Tasks

- System
- Administration
- Software
- Startup
- Scheduled Tasks**
- LED Configuration
- Backup / Flash
- Firmware
- Reboot

Scheduled Tasks

This is the system crontab in which scheduled tasks can be defined.

3.3.4. LED Configuration



LED Configuration

Customizes the behaviour of the device LEDs if possible.

This section contains no values yet

 Add

Save & Apply

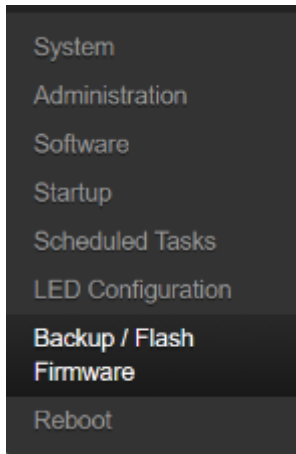
Save

Reset

Powered by LuCI branch ([git-18.232.16445-491d217](https://github.com/openwrt/lede)) / OpenWrt Chaos Calmer 15.05.1 0784228+rr49254

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



Flash operations

Actions Configuration

Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Download backup:

Reset to defaults:

To restore configuration files, you can upload a previously generated backup archive here.

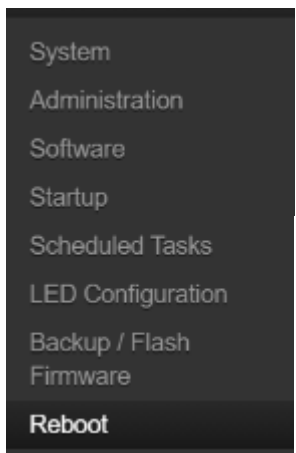
Restore backup:

Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an OpenWrt compatible firmware image).

Keep settings:

3.3.6. Reboot



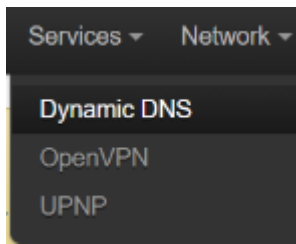
System

Reboot

Reboots the operating system of your device

[Perform reboot](#)

3.4.1 Under service, select Dynamic DNS



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 <i>No data</i>	<input type="checkbox"/>	Never Disabled	-----	Edit Delete
myddns_ipv6	yourhost.example.com <i>No data</i>	<input type="checkbox"/>	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 --

[Save & Apply](#) [Save](#) [Reset](#)

3.4.2 OpenVPN

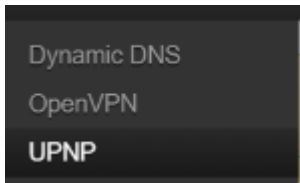
Overview » Instance "custom_config"

[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 --

3.4.3 Select UPnP



Universal Plug & Play

UPnP allows clients in the local network to automatically configure the router.

Active UPnP Redirects

Protocol	External Port	Client Address	Client Port
----------	---------------	----------------	-------------

There are no active redirects.

MiniUPnP settings

Start UPnP and NAT-PMP
service

MiniUPnP settings

General Settings

Advanced Settings

Start UPnP and NAT-PMP service

Enable UPnP functionality

Enable NAT-PMP functionality

Enable secure mode Allow adding forwards only to requesting ip addresses

Enable additional logging Puts extra debugging information into the system log

Downlink Value in KByte/s, informational only

Uplink Value in KByte/s, informational only

Port

Value in KBytes, informational only

Port

MiniUPnP ACLs
















ACLs specify which external ports may be redirected to which internal addresses and ports


Comment	External ports	Internal addresses	Internal ports	Action	Sort
<input type="text" value="Allow high ports"/>	<input type="text" value="1024-65535"/>	<input type="text" value="0.0.0.0/0"/>	<input type="text" value="1024-65535"/>	allow ▾	
<input type="text" value="Default deny"/>	<input type="text" value="0-65535"/>	<input type="text" value="0.0.0.0/0"/>	<input type="text" value="0-65535"/>	deny ▾	

Add

3.5 Under network, select Interface.




- Interfaces**
- Wifi
- Switch
- DHCP and DNS
- Hostnames
- Static Routes
- Firewall
- Diagnostics
- Whole Home Coverage
- HyFi Network
- Multi-WAN
- HyFi Security
- SQM QoS

Network	Status	Actions
LAN  ?	Collecting data...	 Connect  Stop  Edit  Delete
WAN  ?	Collecting data...	 Connect  Stop  Edit  Delete
WAN6  ?	Collecting data...	 Connect  Stop  Edit  Delete

 Add new interface...

Global network options

IPv6 ULA-Prefix

3.6 Select WiFi.

No password set!
There is no password set on this router. Please configure a password to protect the web interface and enable SSH.
[Go to password configuration...](#)

Interfaces

Interface Overview

Network	Status	Actions
LAN br-lan	Uptime: 0h 0m 2s MAC-Address: () RX: 21.41 KB (22 Pkts.) TX: 73.57 KB (18 Pkts.) IPv4: 192.168.1.1	Connect Stop Edit Delete
WAN carrier-wan	MAC-Address: 00:00:00:00:00:00 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	Connect Stop Edit Delete
WAN6 eth4	Uptime: 0h 0m 28s MAC-Address: 46:E7:C5:C8:05:35 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	Connect Stop Edit Delete

- Interfaces
- Wifi**
- Switch
- DHCP and DNS
- Hostnames
- Static Routes
- Firewall
- Diagnostics
- Whole Home Coverage
- HyFi Network
- Multi-WAN
- HyFi Security
- SQM QoS

Wireless Overview

Generic Atheros 802.11axa (wifi0)
Channel: 161 (5.805 GHz) | Bitrate: 2.401 Gbit/s
 Scan Add
 SSID: LS5G500_5G_630A | Mode: Master
 0% BSSID: 00:03:7F:12:1E:03 | Encryption: WPA2 PSK (CCMP)
 Disable Edit Remove

Generic Atheros 802.11axg (wifi1)
Channel: 11 (2.462 GHz) | Bitrate: 0.573 Gbit/s
 Scan Add
 SSID: LS5G500_2G_630A | Mode: Master
 0% BSSID: 00:03:7F:12:02:F7 | Encryption: WPA2 PSK (CCMP)
 Disable Edit Remove

Associated Stations

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
LS5G500_5G_630A	00:00:00:00:00:00	?	-95 dBm	-93 dBm	0.0 Mbit/s	0.0 Mbit/s
LS5G500_2G_630A	00:00:00:00:00:00	?	-95 dBm	-93 dBm	0.0 Mbit/s	0.0 Mbit/s

3.7 Select Switch.

No password set!
There is no password set on this router. Please configure a password to protect the web interface and enable SSH.
[Go to password configuration...](#)

Switch
The network ports on this device can be combined to several VLANs in which computers can communicate directly with each other. VLANs are often used to separate different network segments. Often there is by default one Uplink port for a connection to the next greater network like the internet and other ports for a local network.

Switch "switch0"
Enable VLAN functionality

VLANs on "switch0"

VLAN ID	CPU	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7
Port status:	1000baseT full-duplex	no link	no link	no link	1000baseT full-duplex	no link	no link	10baseT full-duplex

The network ports on this device can be combined to several VLANs in which computers can communicate directly with each other. VLANs are often used to separate different network segments. Often there is by default one Uplink port for a connection to the next greater network like the internet and other ports for a local network.

Switch "switch0"
Enable VLAN functionality

VLANs on "switch0"

VLAN ID	CPU	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7
Port status:	1000baseT full-duplex	no link	no link	no link	1000baseT full-duplex	no link	no link	10baseT full-duplex

This section contains no values yet

[Add](#)

[Save & Apply](#) [Save](#) [Reset](#)

3.8 Select DHCP & DNS

OpenWrt Status System Services Network Logout AUTO REFRESH ON

No password set!
There is no password set on this router. Please configure a password to protect the web interface and enable SSH.
[Go to password configuration...](#)

DHCP and DNS

Dnsmasq is a combined [DHCP-Server](#) and [DNS-Forwarder](#).

Server Settings

General Settings **Resolv and Hosts Files** [DNS Settings](#)

Domain required [Don't forward](#) Name

Authoritative [This is the only authoritative DNS server in the local network](#)

Local server
[Local domain specification. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only](#)

Local domain

Rebind protection [Discard upstream RFC1918 responses](#)

Allow localhost [Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services](#)

Domain whitelist [List of domains to allow RFC1918 responses for](#)

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

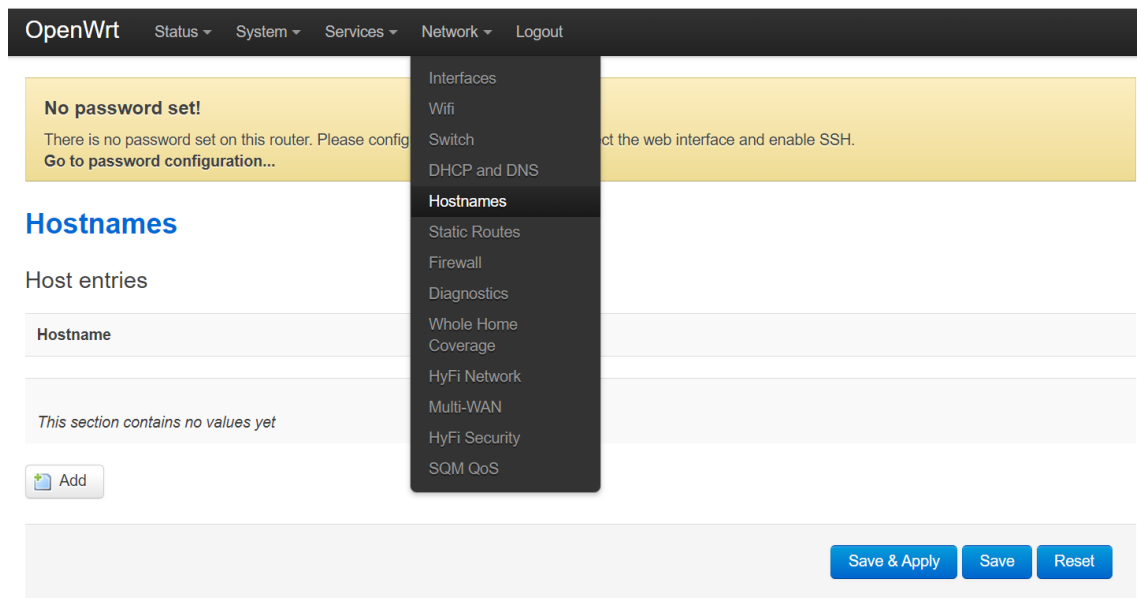
Hostname	IPv6-Address	DUID	Leasetime remaining
<i>There are no active leases.</i>			

Static Leases

Static leases are used 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. Use the *Add* Button to add a new lease entry. The *MAC-Address* identifies the host, the *IPv4-Address* specifies to the fixed address to use and the *Hostname* is assigned as symbolic name to the requesting host.

Hostname	MAC-Address	IPv4-Address	IPv6-Suffix (hex)
<i>This section contains no values yet</i>			
			
  			

3.9 Select Hostname



The screenshot shows the OpenWrt web interface. At the top, there is a navigation bar with 'OpenWrt' and several menu items: 'Status', 'System', 'Services', 'Network', and 'Logout'. Below the navigation bar, there is a yellow warning box that says 'No password set! There is no password set on this router. Please configure the web interface and enable SSH. Go to password configuration...'. The main content area is titled 'Hostnames' and has a sub-section 'Host entries'. Below this, there is a table with a single header 'Hostname' and a body containing the text 'This section contains no values yet'. An 'Add' button is located below the table. At the bottom right, there are three buttons: 'Save & Apply', 'Save', and 'Reset'. A dark grey dropdown menu is open over the 'Network' menu item, listing various configuration options: 'Interfaces', 'Wifi', 'Switch', 'DHCP and DNS', 'Hostnames' (which is highlighted), 'Static Routes', 'Firewall', 'Diagnostics', 'Whole Home Coverage', 'HyFi Network', 'Multi-WAN', 'HyFi Security', and 'SQM QoS'.

3.10 Select Static Rules

OpenWrt Status System Services Network Logout

No password set!
There is no password set on this router. Please configure a password to protect the web interface and enable SSH.
[Go to password configuration...](#)

Static Routes
Routes specify over which interface and gateway a certain destination is reached.

Static IPv4 Routes

Interface	Target	IPv4-Gateway	Metric	MTU
	Host-IP or Network			

This section contains no values yet

[Add](#)

Static IPv6 Routes

Interface	Target	IPv6-Gateway	Metric	MTU
	Host-IP or Network			if target is a network

This section contains no values yet

[Add](#)

Static IPv6 Routes

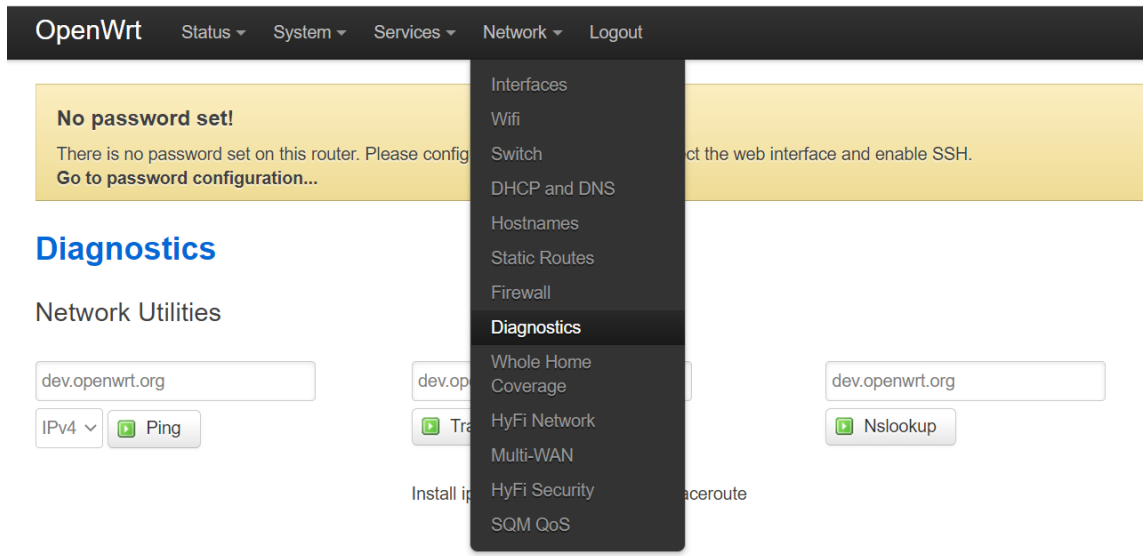
Interface	Target	IPv6-Gateway	Metric	MTU
	IPv6-Address or Network (CIDR)			

This section contains no values yet

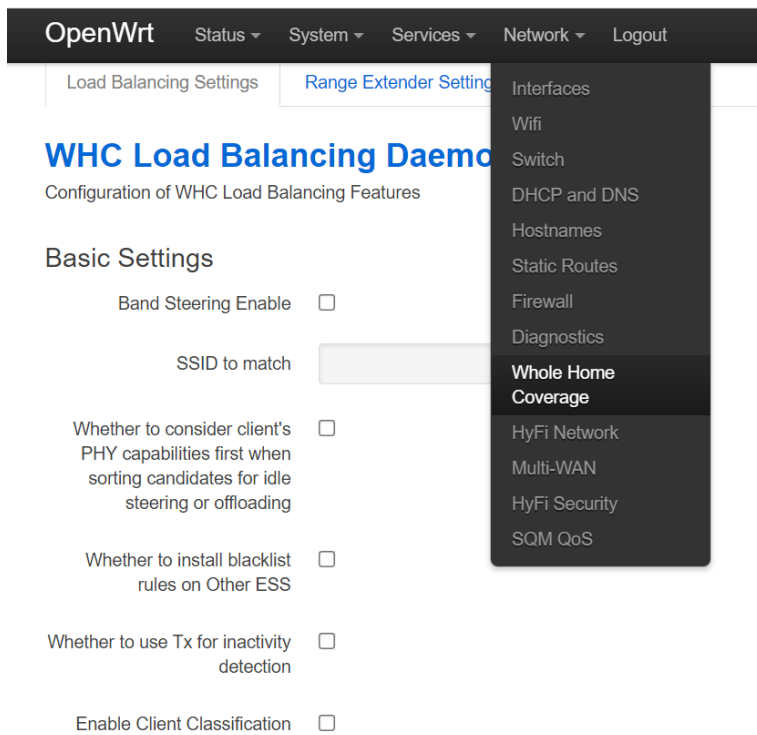
[Add](#)

[Save & Apply](#) [Save](#) [Reset](#)

3.10 Select Firewall



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

Active Steering Settings

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

Offloading Settings

- Time to average before generating a new utilization

Offloading Settings

Time to average before generating a new utilization report (s)

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

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

Medium utilization safety threshold for active steering to 2.4 GHz (%)

Medium utilization safety threshold for active steering to 5 GHz (%)

Uplink RSSI (in dB) above which association will be considered safe

AP Steering Settings

DisableSteeringInactiveLegacyClients

DisableSteeringActiveLegacyClient

DisableSteering11kUnfriendlyClient

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

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

The RSSI value (in dB) the target AP should exceed the serving AP to be considered for AP steering towards leaf

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

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

Interference Avoidance Steering Settings

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

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

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

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

Steering Executor Settings

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

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

Show Advanced Settings

Show Diagnostic Log Settings

Basic Advanced

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

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

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

Whether running with 0 AP interfaces is permitted

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

Primary device purpose

Mode when connected to gateway

Method of range extension

Interoperable RE mode to use

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)

Enable multi-ssid and traffic separation in SON mode

Guest network bridge name

Guest network's backhaul interface

Multi-AP Basic Settings

Enable Multi-AP Topology Optimization Algorithm

Create all VAPs from scratch

wspclcd Template that controls how BSSes are instantiated

SSID to use for fronthaul BSSes

PSK to use for fronthaul BSSes (or empty for open mode)

SSID to use for backhaul BSSes

PSK to use for backhaul BSSes (or empty for open mode)

Suffix to append when generating backhaul SSID

Create smart monitor VAPs

Show Advanced Settings

Gateway Link Monitoring

ARPs to send to GW over Ethernet to confirm connectivity

Number of times the GW must reply to the reachability confirmation ARPs

Number of lost GW pings before declaring it unreachable

Save & Apply Save Reset

3.13 HiFy Network

OpenWrt Status System Services Network Logout

Go to password configuration...

HyFi Network Settings

Configuration of HyFi networks

Basic Hy-Fi Settings

Hy-Fi Feature

Hy-Fi Auto Configuration

Hy-Fi Configuration Mode

- Interfaces
- Wifi
- Switch
- DHCP and DNS
- Hostnames
- Static Routes
- Firewall
- Diagnostics
- Whole Home Coverage
- HyFi Network**
- Multi-WAN
- HyFi Security
- SQM QoS

Advanced Hy-Fi Settings

Load-balancing seamless path switching

Max LB reordering timeout

Strict IEEE 1905.1 Mode

Generate LLDP packets

Avoid Duplicate Renew packets Upstream

Avoid Duplicate Topology Notification packets Upstream

Hy-Fi 1.0 Compatibility Mode

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

Advanced Auto-Configuration Settings

Interval Between DHCP Discovery Messages (sec)	<input type="text" value="2"/>
HR Number of Seconds Between DHCP Retries	<input type="text" value="3"/>
HR Maintenance Interval Between DHCP Discovery	<input type="text" value="15"/>
Constrain TCP-ACK streams to the same medium as their primary TCP-DATA stream	<input type="text" value="Disable"/>
Maximum age of a H-Active entry before it will be aged out (ms)	<input type="text" value="120000"/>
Hy-Fi Netfilter forwarding mode	<input type="text" value="APS"/>
IGMP Extra Query response time	<input type="text"/>

Advanced Auto-Configuration Settings

Interval Between DHCP Discovery Messages (sec)	<input type="text" value="2"/>
HR Number of Seconds Between DHCP Retries	<input type="text" value="3"/>
HR Maintenance Interval Between DHCP Discovery	<input type="text" value="15"/>

General WLAN Path Characterization Setting

Use the WHC algorithm to calculate link capacity	<input type="text" value="1"/>
Number of capacity updates to receive after link change before considered valid	<input type="text" value="3"/>

WLAN 5G Path Characterization Setting

UpdatedStatsInterval	<input type="text" value="1"/>
StatsAgedOutInterval	<input type="text" value="30"/>
MaxMediumUtilization	<input type="text" value="70"/>
MediumChangeThreshold	<input type="text" value="10"/>
LinkChangeThreshold	<input type="text" value="10"/>
MaxMediumUtilizationForLC	<input type="text" value="70"/>
CPUlimitedTCPThroughput	<input type="text" value="0"/>
CPUlimitedUDPThroughput	<input type="text" value="0"/>
PHYRateThresholdForMU	<input type="text" value="2000"/>
ProbePacketInterval	<input type="text" value="1"/>
ProbePacketSize	<input type="text" value="64"/>
EnableProbe	<input type="text" value="1"/>
AssocDetectionDelay	<input type="text" value="5"/>
Rate above which ScalingFactorHigh is used	<input type="text"/>

WLAN 2.4G Path Characterization Setting

WLAN 2.4G Path Characterization Setting

UpdatedStatsInterval	<input type="text" value="1"/>
StatsAgedOutInterval	<input type="text" value="30"/>
MaxMediumUtilization	<input type="text" value="70"/>
MediumChangeThreshold	<input type="text" value="10"/>
LinkChangeThreshold	<input type="text" value="10"/>
MaxMediumUtilizationForLC	<input type="text" value="70"/>
CPULimitedTCPThroughput	<input type="text" value="0"/>
CPULimitedUDPThroughput	<input type="text" value="0"/>
PHYRateThresholdForMU	<input type="text" value="2000"/>
ProbePacketInterval	<input type="text" value="1"/>
ProbePacketInterval	<input type="text" value="1"/>
ProbePacketSize	<input type="text" value="64"/>
EnableProbe	<input type="text" value="1"/>
AssocDetectionDelay	<input type="text" value="5"/>
Rate above which ScalingFactorHigh is used	<input type="text"/>

PLC Path Characterization Setting

MaxMediumUtilization	<input type="text" value="80"/>
MediumChangeThreshold	<input type="text" value="10"/>
LinkChangeThreshold	<input type="text" value="10"/>

EntryExpirationInterval	<input type="text" value="120"/>
MaxMediumUtilizationForLC	<input type="text" value="80"/>
LCThresholdForUnreachable	<input type="text" value="5"/>
LCThresholdForReachable	<input type="text" value="10"/>
HostPLCInterfaceSpeed	<input type="text" value="0"/>

Stream Estimation Setting

UpdateHSPECInterval	<input type="text" value="1"/>
NotificationThresholdLimit	<input type="text" value="10"/>
NotificationThresholdPercentage	<input type="text" value="20"/>
AlphaNumerator	<input type="text" value="3"/>
LocalFlowRateThreshold	<input type="text" value="2000000"/>
LocalFlowRatioThreshold	<input type="text" value="5"/>
Maximum number of H-Active entries supported in user-space	<input type="text" value="8192"/>

Topology Discovery Setting

ND_UPDATE_INTERVAL	<input type="text" value="15"/>
BD_UPDATE_INTERVAL	<input type="text" value="3"/>
HOLDING_TIME	<input type="text" value="190"/>
TIMER_LOW_BOUND	<input type="text" value="7"/>
TIMER_UPPER_BOUND	<input type="text" value="11"/>

MSGID_DELTA	<input type="text" value="64"/>
HA_AGING_INTERVAL	<input type="text" value="120"/>
ENABLE_TD3	<input type="text" value="1"/>
ENABLE_BD_SPOOFING	<input type="text" value="1"/>
NOTIFICATION_THROTTLING_W	<input type="text" value="1"/>
PERIODIC_QUERY_INTERVAL	<input type="text" value="60"/>
ENABLE_NOTIFICATION_UNICA	<input checked="" type="checkbox"/>

Path Selection Setting

UpdateHDInterval	<input type="text" value="10"/>
LinkCapacityThreshold	<input type="text" value="20"/>
NonUDPInterfaceOrder	<input type="text" value="EP52"/>
SerialflowIterations	<input type="text" value="10"/>
DeltaLCThreshold	<input type="text" value="10"/>
EnableBadLinkStatsSwitchFlow	<input checked="" type="checkbox"/>

WLAN Manager Settings

WlanCheckFreqInterval	<input type="text" value="10"/>
WlanALDNLNumOverride	<input type="text" value="0"/>

LOG settings

EnableLog	<input type="text" value="0"/>
-----------	--------------------------------

Port range that source port number in packet header.

3.14 Select Multi-WAN

OpenWrt Status System Services Network Logout

Multi-WAN

Multi-WAN allows for the use of multiple uplinks for load balancing.

Enable

WAN Interfaces

Health Monitor detects and corrects network changes and failures.

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 Recovery: 5

- Interfaces
- Wifi
- Switch
- DHCP and DNS
- Hostnames
- Static Routes
- Firewall
- Diagnostics
- Whole Home Coverage
- HyFi Network
- Multi-WAN**
- HyFi Security
- SQM QoS

Attempts Before WAN Recovery

Failover Traffic Destination

DNS Server(s)

Multi-WAN Traffic Rules

Configure rules for directing outbound traffic through specified WAN Uplinks.

Source Address	Destination Address	Protocol	Ports	WAN Uplink	
<input type="text" value="192.168.1.0/24"/>	<input type="text" value="ftp.netlab7.com"/>	<input type="text" value="TCP"/>	<input type="text" value="21"/>	<input type="text" value="lan"/>	<input type="button" value="Delete"/>
<input type="text" value="192.168.0.3"/>	<input type="text" value="all"/>	<input type="text" value="ICMP"/>	<input type="text" value="all"/>	<input type="text" value="Load Balancer(Compatibility)"/>	<input type="button" value="Delete"/>
<input type="text" value="all"/>	<input type="text" value="www.whatismyip.com"/>	<input type="text" value="all"/>	<input type="text" value="all"/>	<input type="text" value="Load Balancer(Performance)"/>	<input type="button" value="Delete"/>

Multi-WAN Traffic Rules

Configure rules for directing outbound traffic through specified WAN Uplinks.

Source Address	Destination Address	Protocol	Ports	WAN Uplink	
<input type="text" value="192.168.1.0/24"/>	<input type="text" value="ftp.netlab7.com"/>	<input type="text" value="TCP"/>	<input type="text" value="21"/>	<input type="text" value="lan"/>	<input type="button" value="Delete"/>
<input type="text" value="192.168.0.3"/>	<input type="text" value="all"/>	<input type="text" value="ICMP"/>	<input type="text" value="all"/>	<input type="text" value="Load Balancer(Compatibility)"/>	<input type="button" value="Delete"/>
<input type="text" value="all"/>	<input type="text" value="www.whatismyip.com"/>	<input type="text" value="all"/>	<input type="text" value="all"/>	<input type="text" value="Load Balancer(Performance)"/>	<input type="button" value="Delete"/>

Default Route

3.15 Select HiFy Security

HyFi Security Settings

Security configuration of HyFi networks

Enable

Multi-AP SIG Enable

1905.1 Configuration Role

Designated Push Button AP

AL MAC-specific Multi-AP BSS Instantiation Policy File

Generic Multi-AP BSS Instantiation Policy File

Maximum supported BSSes per radio in Multi-AP Mode

1905.1 UCPK

1905.1 UCPK Salt

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

The screenshot displays the OpenWrt web interface for configuring Smart Queue Management (SQM). The main heading is "Smart Queue Management". Below it, there is a description: "With SQM you can enable traffic shaping, better mixing (with AQM) and prioritisation on one network interface." The "Queues" section has three tabs: "Basic Settings", "Queue Discipline", and "Link Layer". The "Queue Discipline" tab is active. It contains several configuration options:

- Enable this SQM instance.**
- Interface name:** eth1
- Download speed (kbit/s) (ingress) set to 0 to selectively disable ingress shaping:** 85000
- Upload speed (kbit/s) (egress) set to 0 to selectively disable egress shaping:** 10000
- Create log file for this SQM instance under**
- Download speed (kbit/s) (ingress) set to 0 to selectively disable ingress shaping:** 85000
- Upload speed (kbit/s) (egress) set to 0 to selectively disable egress shaping:** 10000
- Create log file for this SQM instance under** `/var/run/sqm/${Interface_name}.debug.log`. Make sure to delete log files manually.
- Verbosity of SQM's output into the system log.** info (default)

A dropdown menu is open, showing the following options: Interfaces, Wifi, Switch, DHCP and DNS, Hostnames, Static Routes, Firewall, Diagnostics, Whole Home Coverage, HyFi Network, Multi-WAN, HyFi Security, and **SQM QoS** (highlighted). A "Delete" button is visible in the top right corner of the configuration area.

At the bottom of the page, there are three buttons: "Save & Apply", "Save", and "Reset".

3.17 Select Logout

OpenWrt [Status](#) [System](#) [Services](#) [Network](#) [Logout](#)

Smart Queue Management

With [SQM](#) you can enable traffic shaping, better mixing (Fair Queueing), active queue length management (AQM) and prioritisation on one network interface.

Queues

[Delete](#)

[Basic Settings](#) [Queue Discipline](#) [Link Layer Adaptation](#)

Enable this SQM instance.

Interface name

Download speed (kbit/s) (ingress) set to 0 to selectively disable ingress shaping:

Upload speed (kbit/s) (egress) set to 0 to selectively disable egress shaping:

Create log file for this SQM instance under

3.18 After logout, re-login again.

OpenWrt

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...](#)

Authorization Required

Please enter your username and password.

Username

Password

-----End-----