Atop Technologies, Inc.

CWR5805
Industrial 5G-NR & Wi-Fi Mesh Router

User Manual

V1.2

7th June 2022

This PDF Document contains internal hyperlinks for ease of navigation.
For example, click on any item listed in the **Table of Contents** to go to that page.

Published by:

Atop Technologies, Inc.

2F, No. 146, Sec. 1, Tung-Hsing Rd,
30261 Chupei City,
Hsinchu County
Taiwan, R.O.C.

Tel: +886-3-550-8137
Fax: +886-3-550-8131
sales@atop.com.tw
www.atoponline.com

Important Announcement

Disclaimer

We have checked the contents of this manual for agreement with the hardware and the software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual is reviewed regularly and any necessary corrections will be included in subsequent editions.
Suggestions for improvement are welcome. All other product names referenced herein are registered trademarks of their respective companies.

Preface

This manual contains some advanced network management knowledge, instructions, examples, guidelines, and general theories. The contents are designed to help you manage the switch and use its software, a background in general theory is a must when reading it. Please refer to the Glossary for technical terms and abbreviations.

Who Should Use This User Manual

This manual is to be used by qualified network personnel or support technicians who are familiar with network operations and might be useful for system programmers or network planners as well. This manual also provides helpful and handy information for first-time. For any related problems, please contact your local distributor. If they are unable to assist you, please redirect your inquiries to www.atoponline.com.

Documentation Control

Author:	Sean Hong
Revision:	1.2
Revision History:	Fix incorrect information
Creation Date:	8 December 2021
Last Revision Date:	7 June 2022
Document Status:	Official Release

Table of Contents

List of Figures

List of Tables

1 Preface

1.1 Purpose of the Manual

This manual supports yous during the installation and the configuration of the advanced high-throughput wireless mesh access point (AP)/Router CWR5805. It explains the technical features available within the mentioned product. It also contains some general technical information to help you manage the devices, as well as various advanced network management information, such as instructions, examples, and guidelines. A background in general theory is necessary when reading it. Please refer to the Glossary for technical terms and abbreviations.

1.2 Supported Platform

This manual is solely designed for the CWR5805 Advanced High-Throughput AP/Router.

1.3 Compliance Information

1.3.1 Manufacturers' FCC Declaration of Conformity Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case you will be required to correct the interference at his/her own expense.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause an undesired operation

Note: all the figures herein are intended for illustration purposes only. This software and certain features work only on certain Atop devices.

2 Getting Started

2.1 Overview

The CWR5805 device is a cost-effective industrial-grade wireless access point (AP)/router with a high-throughput performance.

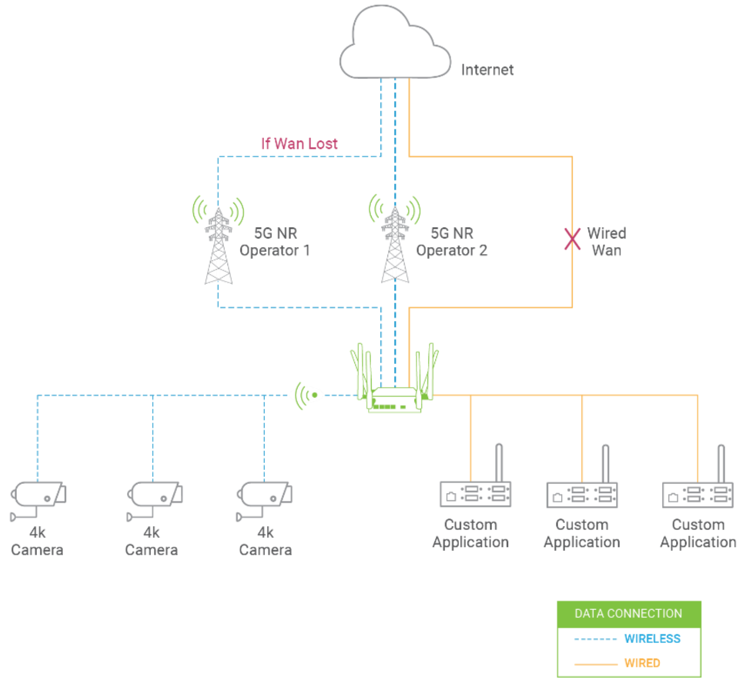
The CWR5805 support 5G NR and LTE network for the device through a wireless connection. And it has dual-SIM card backup to ensure a stable wireless network connection. The CWR5805 devices radiate signal in the dual-band (2.4GHz, 5GHz), while users' Wi-Fi devices can conveniently connect to them via any chosen band.

The device has also built-in full-duplex 10/100/1000 Mbps ports (WAN, LANs) to connect with users' wired Ethernet devices for the speed up to 1 Gbps. The Ethernet WAN and mobile module on the CWR5805 device provide a load balancing/failover mechanism for Internet connection. The router function combines traffic for all connected devices and let them share a high-speed cable or ADSL Internet connection.

Nowadays, some IoT infrastructure are require multiple connection interface which can be connected via wired (Ethernet) or wirless interfaces (Wi-Fi and/or Cellular 5G/LTE). For instance, the sensor is an inseparable part of efficient IoT plant and monitor its environment status. Such SCADA (Supervisory Control and Data Acquisition) system need an active Internet connection via Wi-Fi/LAN to reach the IoT plant.

Connectivity downtime can be easily resolved by adding a cellular 5G/LTE router between existing wired WAN. This way, it is possible to use the wired Internet option and share the connection to the IoT system via Ethernet and to a 4K monitor via Wi-Fi using a single compact Cellular Router CWR5805. Once it senses that wired WAN is lost or disrupted, it automatically switches to 5G/LTE as a source of the Internet to provide continuous Internet service to connected devices.

Figure 1. An Example of Wired and Wi-Fi Devices Connected to the Internet Via CWR5805 AP/Router



2.2 Features

Here are the main features of the CWR5805 series device:

- Industrial FWA solution for 4G & 5G NR networks
- Support 5G Non-standalone and standalone mode
- Selectable WWAN option for DL 5G NR 1.3Gbps/ Dual LTE 600Mbps/Single LTE 300 Mbps
- Wi-Fi 5 2x2 MU-MINO with 802.11ac peak speed 867 Mbps
- Easily Expandable Mesh WiFi System
- 1 x RJ45 for 10/100/1000Mbps BaseT WAN
- 4 x RJ45 for 10/100/1000Mbps BaseT LAN
- Integrated DHCP server with dynamic and static IP address assignment
- GPS option for location service
- Dual nano-SIM design
- Natural firewall using NAT technology
- 1x micro-SD slot for flexible use
- Firewall and VPN for security connection
- Backup WAN interfaces for connection reliability
- Industrial EMC protection, -40°C~75°C wide-range temperature operation
- Rugged metal case with a wall or DIN-Rail mount
- PoE PD support for flexible deployment
- Power supply input supporting 12~48VDC

Caution

Starting here, extreme caution must be exercised.

Never install or work with electricity or cabling during periods of lightning activity. Never connect or disconnect power when hazardous gases are present.

Warning: HOT!

WARNING: Disconnect the power and allow the unit to cool for 5 minutes before touching.

2.3 Installation

Before installing the device, please strictly follow all safety procedures described in the Hardware installation guide supplied inside the product. Atop will not be liable for any damages to the property or the personal injuries resulting from the installation or overall use of the device. Do not attempt to manipulate the product in any way if unsure of the steps described there. In such cases, please contact your dealer immediately.

1. First assemble your router by attaching all necessary antennas and inserting the SIM card.
2. To power up your router, please use the power adapter purchased from Atop. (IMPORTANT: Using a different power adapter can damage and void the warranty for this product.).
3. If you have a wired broadband connection you will also have to connect it to the WAN port of the router.

2.3.1 Packing List

Inside the delivery package, you will find the following items.

Table 1. Packing List

Item	Quantity	Description
CWR5805 Device	1	Industrial wireless access point/router device
5G/4G Antenna *	4	5G NR/4G LTE antenna (SMA male)
Wifi Antenna	2	Dual Band 2.4/5 Ghz antenna (SMA male)
Terminal Block	1	TB3 x 1: 2-pin 5.08mm lockable Terminal Block for power input
Documentation	1	Hardware installation guide

*4G model provides 2 antennas

2.3.2 Front Panel and Back Panel

Figure 2. Front Panel

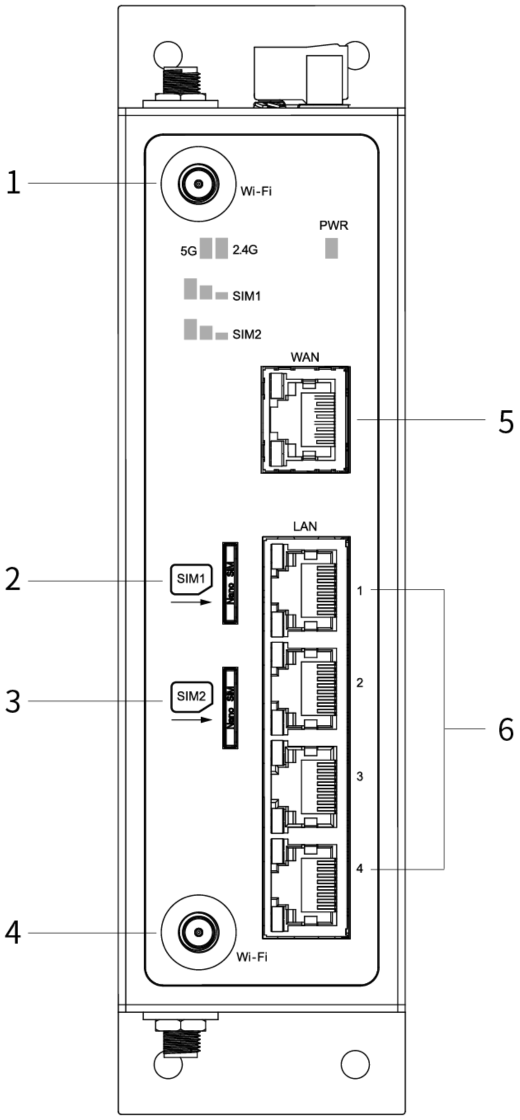


Table 2. Front Panel

No.	Description
1	Wi-Fi antenna connector (0)
2	SIM1 card holder
3	SIM2 card holder
4	Wi-Fi antenna connector (1)
5	WAN port
6	LAN port

Figure 3. Top View

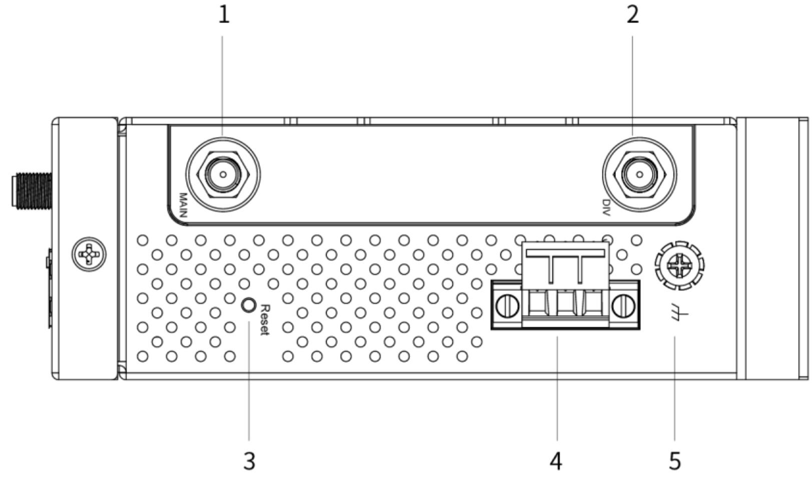


Table 3. Top View

No.	Description
1	Main 5G/LTE antenna connector (0)
2	Div (Diversity) 5G/LTE antenna connector (1)
3	Reset button
4	Power connector
5	Ground

Figure 4. Bottom view

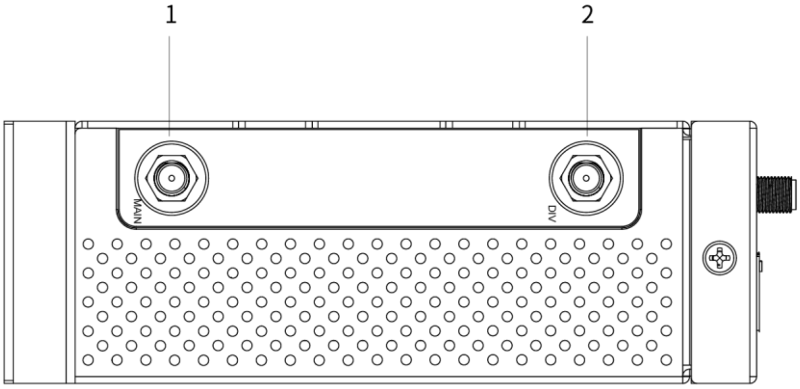


Table 4. Buttom view

No.	Description
1	Main 5G/LTE antenna connector (2)
2	Div (Diversity) 5G/LTE/GNSS antenna connector (3)

2.3.3 Power Connector

Figure 5. Power Connector on the Top

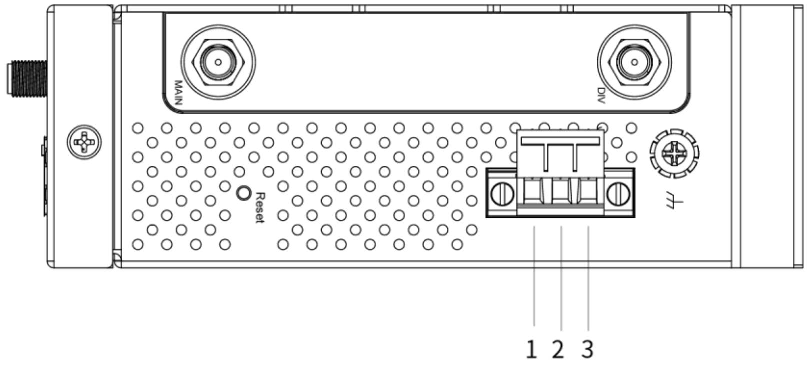


Table 5. Power Connector on the Top Panel

No.	Description
1	D-
2	D+
3	F.G.

2.3.4 Connection Status LED

Table 6. Color Interpretation of LED Indicators on the CWR5805 Device

Name	Color	Status	Description
PWR	●Green	On	Power connected
		Off	Power dis-connected
Wi-Fi 2.4GHz	●Green	On	Wi-Fi 2.4GHz activated
		Off	Wi-Fi 2.4GHz deactivated
Wi-Fi 5.0GHz	●Green	On	Wi-Fi 5GHz activated
		Off	Wi-Fi 5GHz deactivated
Ethernet LED (LAN/WAN)	●Orange	Blinking	10/100 Mbps. Data is transmitting
		Off	No data or speed is 1000 Mbps
	●Green	Blinking	1000 Mbps. Data is transmitting
		Off	No data or speed is 10/100 Mbps
SMI1/SMI2	●Green	On	5G NR/4G LTE Signal Strength 0-LED on (□□□) : No Signal 1-LED on (□□■) : Poor 2-LED on (□■■) : Good 3-LED on (■■■) : Excellent

2.3.5 SIM Card Installation

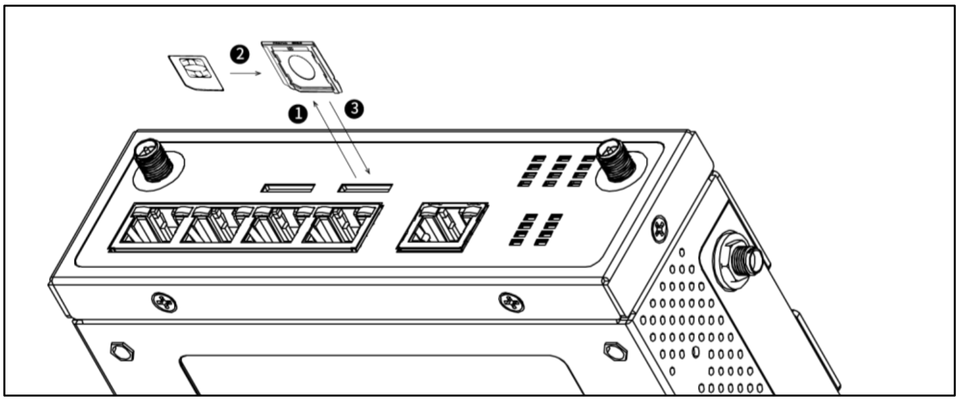
Follow these simple steps to install the SIM card for your 5G NR/4G LTE connectivities.

1. Pull out the SIM card tray

2. Insert the SIM card which was given by your ISP (Internet Service Provider) or cellular network operator. The correct SIM card's orientation is shown in the picture below.

3. Push the SIM card tray back into the chassis to close it.

Figure 6. SIM Card Installation



The device is compatible with **nano-SIM (4FF)** size card only. The latch will click into place when the nano-SIM is fully inserted.

Figure 7. 4 Latches on the 4FF SIM card tray

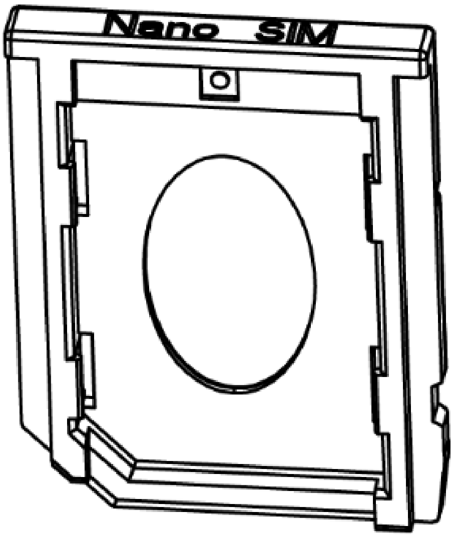


Table 7. 4FF SIM card tray format

SIM Card Format	Length (mm)	Width(mm)	Thickness (mm)
Nano-SIM (4FF)	12.30	8.80	0.67

2.4 Loggin in

Before installing the device, please strictly follow all safety procedures described in the Hardware installation guide supplied inside the product. Atop will not be liable for any damages to the property or the personal injuries resulting from the installation or overall use of the device. Do not attempt to manipulate the product in any way if unsure of the steps described there. In such cases, please contact your dealer immediately.

Specific installation instructions are not provided in this manual since they may differ considerably based on the purchased hardware.

2.4.1 Web Access and Network Interfaces Default Settings

The CWR5805 device is equipped with one WAN port, four LAN ports, Wi-Fi 2.4G/5G interfaces, and one 5G /LTE modem interface. The LAN interface and Wi-Fi interfaces are bridged together.

CWR5805 default network parameters are listed in the table below.

Table 8. Network Interfaces Default Settings

Interface	Device IP	Subnet Mask	Gateway IP	DNS
WAN	DHCP Client			
LAN/WiFi	192.168.1.1	255.255.255.0	None	None
5G NR/LTE	QMI Cellular			

Its WebUI login default Username and password are listed in the table below.

Table 9. Login Default Settings

Login Parameter	Default Values
Username	admin
Password	default

2.4.2 The Reset Button

If you forget the password or cannot access the Web Configurator of the device, you can use the RESET button to restore the factory default configuration file. This means you will lose all of your configurations after the resetting. The password will also be reset to the factory default setting (see the device label), and the LAN IP address will be “192.168.1.1”. To reset the device, follow these steps:

1. Make sure the POWER LED is on (not blinking).
2. Press the “Reset” button on the panel from the same side of the terminal bolck for **5** seconds to restore the factory default settings. When the Wi-Fi and Ethernet LED begin to blink, the device is starting to restore its factory default setting.

3 Configuration and Setup

CWR5805 is equipped with a built-in web server in its firmware. Thus, this device can be configured via a web browser by entering CWR5805 device's IP address.

The main WebUI menu of CWR5805 device contains four major categories:

- Status
- Network
- Services
- System

The detailed network functionalities of the above-mentioned categories will be described in the following Sections.

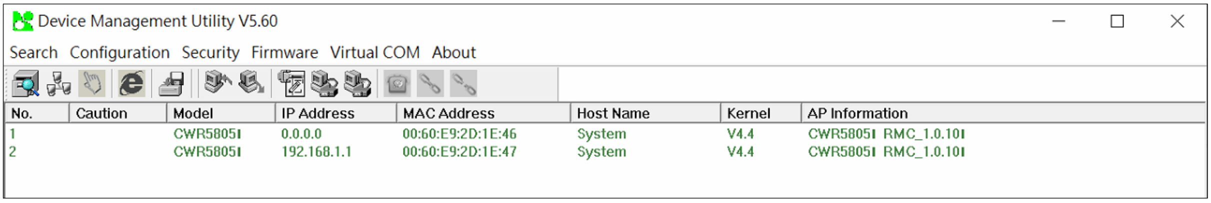
3.1 *Configuration Interface*

It is strongly recommended for you to set the Network Parameters through **Device Management Utility**© first. Other device-specific configurations can later be carried out via Atop's user-friendly Web-Interface.

3.1.1 Configuring through Management Utility

Please install Atop's configuration utility program called **Device Management Utility**® that can be downloaded from our website www.atoponline.com. For more information on how to install **Device Management Utility**®, please refer to the manual that is available online. After you start **Device Management Utility**®, if the CWR5805 Serial Device Server is already connected to the same subnet as your PC, the device can be accessed. **Device Management Utility**® will automatically detect your device and list it on **Device Management Utility**®'s window. Alternatively, if you did not see your device on your network, press "**Rescan**" icon, a list of devices, including your CWR5805 device currently connected to the network will be shown in the window of **Device Management Utility**® as shown in the Figure below.

Figure 8. List of Devices in Device Management Utility

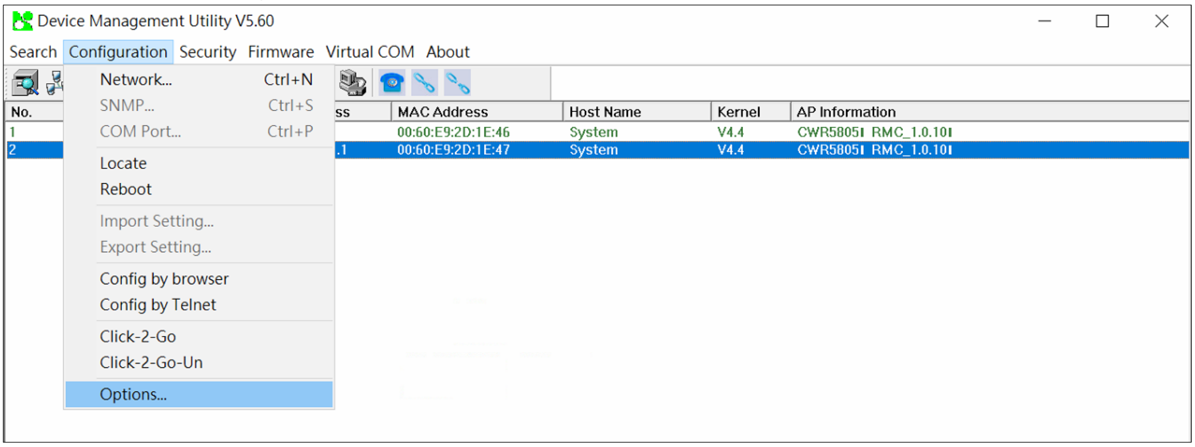


No.	Caution	Model	IP Address	MAC Address	Host Name	Kernel	AP Information
1		CWR5805I	0.0.0.0	00:60:E9:2D:1E:46	System	V4.4	CWR5805I RMC_1.0.10I
2		CWR5805I	192.168.1.1	00:60:E9:2D:1E:47	System	V4.4	CWR5805I RMC_1.0.10I

Note: This figure is for illustration purpose only. Actual values/settings may vary between devices.

Sometimes the CWR5805 device might not be in the same subnet as your PC; therefore, you will have to use Atop's utility to locate it in your virtual environment. To configure each device, first click to select the desired device (default IP: 192.168.1.1) in the list of **Device Management Utility**©, and then click "**Configuration** **Network**..." (or Ctrl+N) menu on **Device Management Utility**© as shown in the Figure below or click on the second icon called **Network** on the menu icon bar.

Figure 9. Pull-down Menu of Configuration and Network



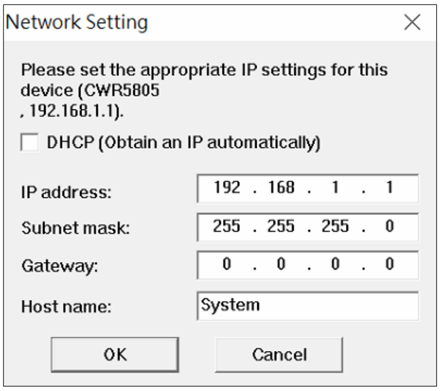
No.	ss	MAC Address	Host Name	Kernel	AP Information
1		00:60:E9:2D:1E:46	System	V4.4	CWR5805I RMC_1.0.10I
2	.1	00:60:E9:2D:1E:47	System	V4.4	CWR5805I RMC_1.0.10I

Then a pop-up window will appear as shown in the Figure below.

You may proceed then to change the IP address to avoid any IP address conflict with other hosts on your LAN or to connect the device to your existing one.

Please consult your system administrator if you do not know your network's subnet mask and gateway address.

Figure 10. Pop-up Window of Network Setting



Please set the appropriate IP settings for this device (CWR5805
, 192.168.1.1).

□ DHCP (Obtain an IP automatically)

IP address: 192 . 168 . 1 . 1

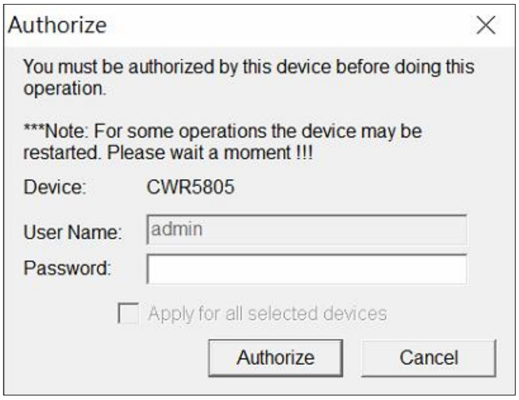
Subnet mask: 255 . 255 . 255 . 0

Gateway: 0 . 0 . 0 . 0

Host name: System

The system will prompt you for a credential to authorize the changes. It will ask you for the Username and the Password as shown in the Figure below.

Figure 11. Authorization for Change of Network Settings



You must be authorized by this device before doing this operation.

***Note: For some operations the device may be restarted. Please wait a moment !!!

Device: CWR5805

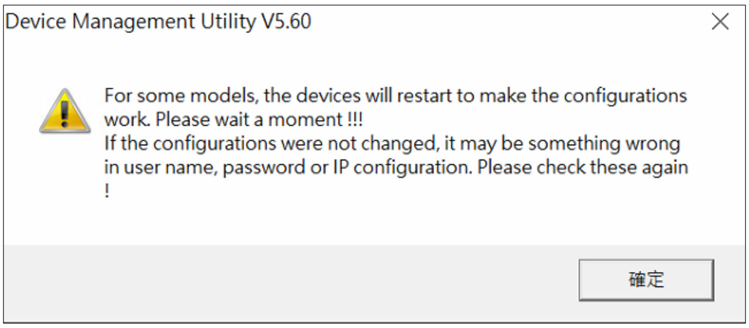
User Name: admin

Password:

□ Apply for all selected devices

The default Username is “admin”, while the default password is “default”. After clicking on the Authorize button, a notification window will pop-up as shown in the Figure below and some devices may be restarted.

Figure 12. Pop-up Notification Window after Authorization

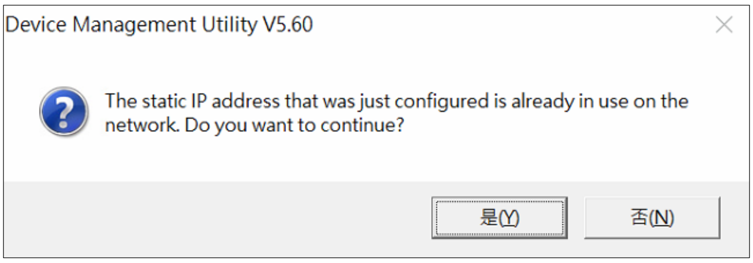


Device Management Utility V5.60

For some models, the devices will restart to make the configurations work. Please wait a moment !!!
If the configurations were not changed, it may be something wrong in user name, password or IP configuration. Please check these again
!

After the device is restarted (for some models), it will beep twice to indicate that the unit is running normally. Then, the device can be found on a new IP address. It may be listed automatically by the Device Management Utility© or it can be found by clicking on the “Rescan” icon. Note that if you did not change the IP address but changed another parameter, you may encounter another notification window as shown in the Figure below.

Figure 13. Pop-up Notification Window when there is the same IP address in the network



Device Management Utility V5.60

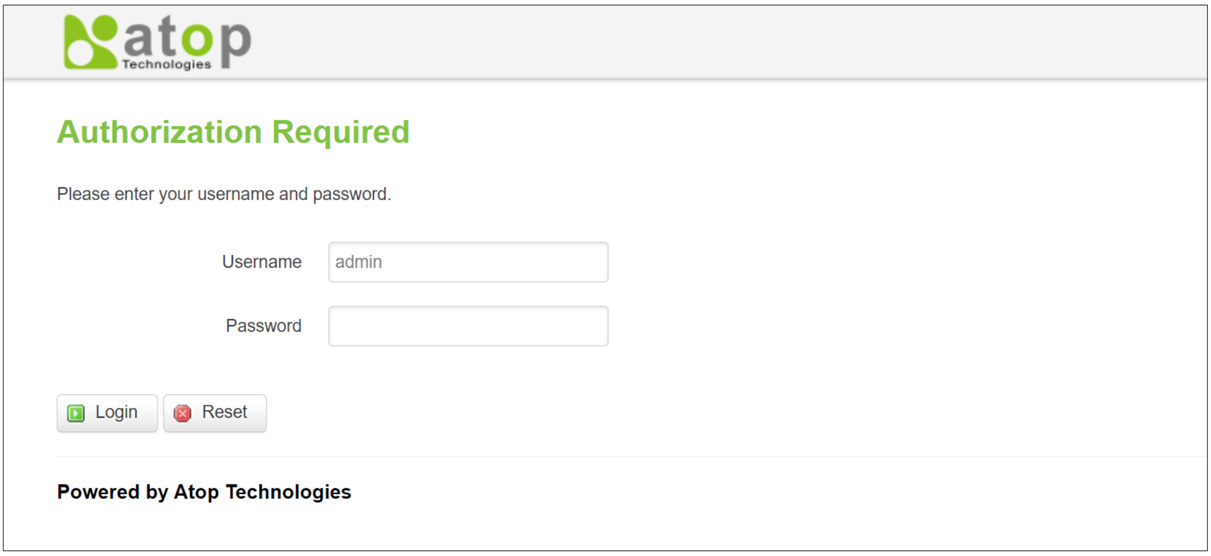
The static IP address that was just configured is already in use on the network. Do you want to continue?

3.1.2 Configuring through Web

A login authorization is required before a you can access to WebUI of the CWR5805 device. The default URL to access the device’s WebUI is https://192.168.1.1. It will be redirected to the login authorization webpage after pressing the enter key.

As shown in the Figure below, you need to enter the correct Username and Password to access the device’s WebUI. The default value for the Username is **admin** and for the Password is the **default**.

Figure 14. Authorization Required Webpage



Authorization Required

Please enter your username and password.

Username: admin

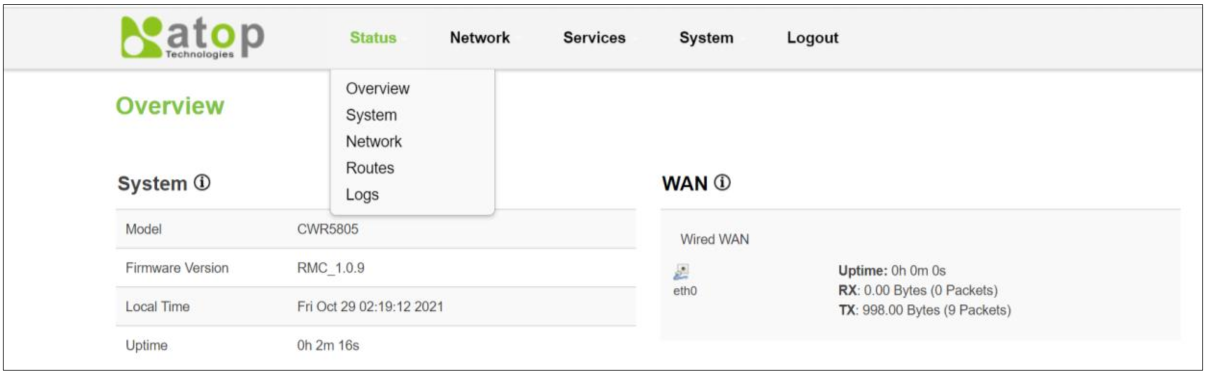
Password:

Powered by Atop Technologies

3.2 *Status Menu*

As shown in the Figure below, the Status menu contains the following sub-menus: Overview, System, Network, Routes and Logs. These sub-menus display the current network information, as well as real-time traffic statistics of each network interface.

Figure 15. Main page



Overview

System ⓘ

Model	CWR5805
Firmware Version	RMC_1.0.9
Local Time	Fri Oct 29 02:19:12 2021
Uptime	0h 2m 16s

WAN ⓘ

Wired WAN

eth0

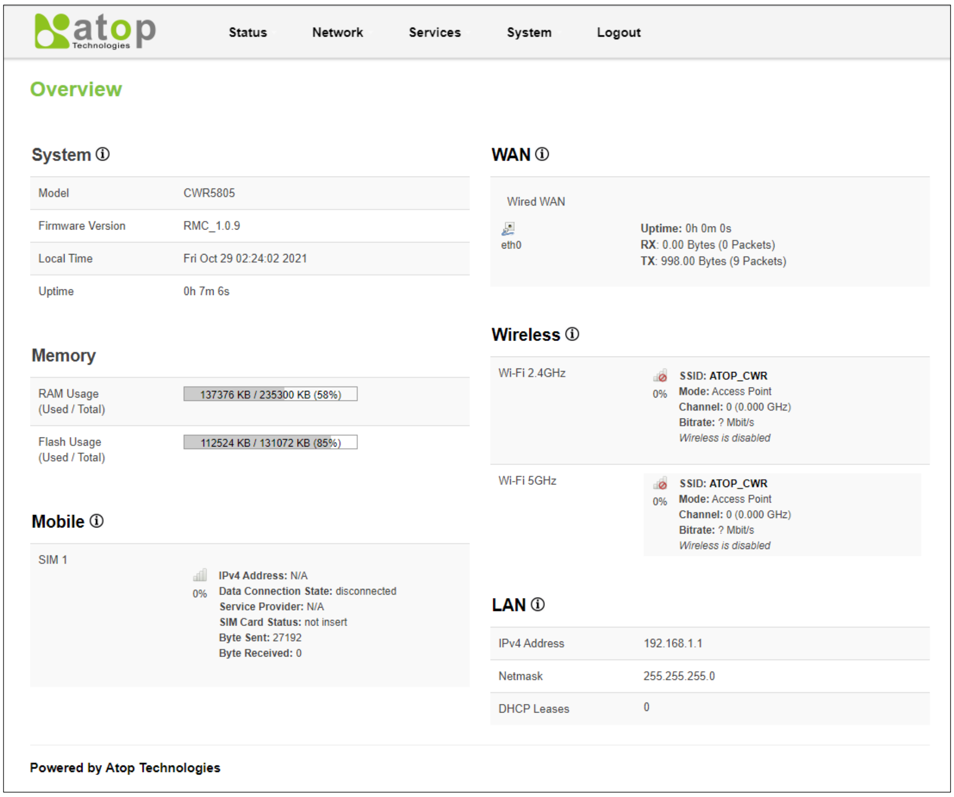
Uptime: 0h 0m 0s
RX: 0.00 Bytes (0 Packets)
TX: 998.00 Bytes (9 Packets)

3.2.1 Overview

The **Overview** sub-menu under the Status menu contains a summary of the device's information, i.e., System, Memory, Mobile, WAN, Wireless, and LAN interface live status.

This screen is the first thing you see when you log into the CWR5805. It also appears every time you click the **Status** icon in the navigation panel. The **Status** screen displays the CWR5805's connection information, wireless, mobile information, and traffic statistics.

Figure 16. Status > Overview



Overview

System ⓘ

Model	CWR5805
Firmware Version	RMC_1.0.9
Local Time	Fri Oct 29 02:24:02 2021
Uptime	0h 7m 6s

Memory

RAM Usage (Used / Total)	137376 KB / 235300 KB (58%)
Flash Usage (Used / Total)	112524 KB / 131072 KB (85%)

Mobile ⓘ

SIM 1

0%
IPv4 Address: N/A
Data Connection State: disconnected
Service Provider: N/A
SIM Card Status: not insert
Byte Sent: 27192
Byte Received: 0

WAN ⓘ

Wired WAN

eth0

Uptime: 0h 0m 0s
RX: 0.00 Bytes (0 Packets)
TX: 998.00 Bytes (9 Packets)

Wireless ⓘ

Wi-Fi 2.4GHz

0%
SSID: ATOP_CWR
Mode: Access Point
Channel: 0 (0.000 GHz)
Bitrate: ? Mbit/s
Wireless is disabled

Wi-Fi 5GHz

0%
SSID: ATOP_CWR
Mode: Access Point
Channel: 0 (0.000 GHz)
Bitrate: ? Mbit/s
Wireless is disabled

LAN ⓘ

IPv4 Address	192.168.1.1
Netmask	255.255.255.0
DHCP Leases	0

Powered by Atop Technologies

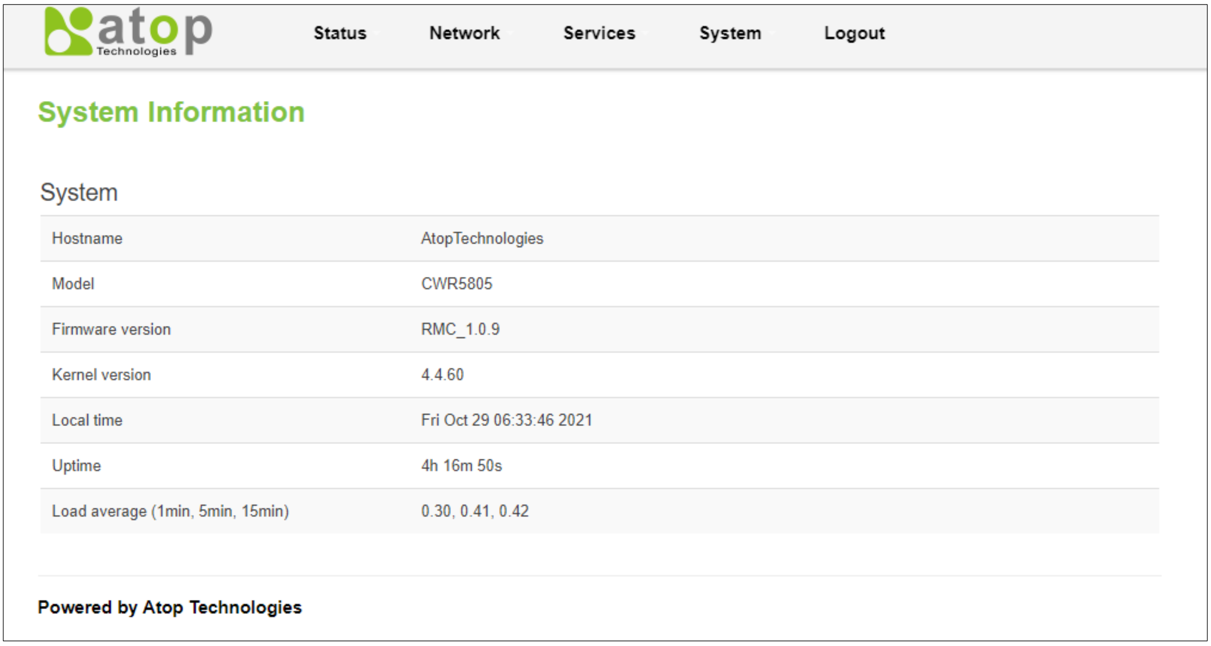
Table 10. Status > Overview

Field	Description
System	
Model	The model name of the device.
Firmware Version	The currently used firmware version on the device.
Local Time	Date and time information with timezone offset. The timezone offset can be selected on the Timezone field of the System webpage.
Uptime	Uptime measures the length of time a system has been running since it was booted.
Memory	
RAM Usage	Amount of random-access memory (RAM) that is currently in use by the device.
Flash Usage	Amount of Flash (storage) memory that is currently in use by the device.
Mobile	
SIM 1/2	The current Primary SIM card state.
WAN	
Wired WAN	The current WAN state.
Wireless	
Wi-Fi 2.4GHz	The current Wi-Fi 2.4GHz state.
Wi-Fi 5GHz	The current Wi-Fi 5GHz state.
LAN	
IPv4 Address	IPv4 address of the LAN interface.
Netmask	Netmask of the LAN interface.
DHCP Lease	The number of DHCP Clients connected.

3.2.2 System

This section shows the system status information of your router.

Figure 17. Status > System



System Information

System

Hostname	AtopTechnologies
Model	CWR5805
Firmware version	RMC_1.0.9
Kernel version	4.4.60
Local time	Fri Oct 29 06:33:46 2021
Uptime	4h 16m 50s
Load average (1min, 5min, 15min)	0.30, 0.41, 0.42

Powered by Atop Technologies

Table 11. Status > System

Field	Description
Hostname	This value can be modified on the Hostname field of the System webpage.
Model	The model name of the device.
Firmware Version	The currently used firmware version on the device
Kernel Version	The currently used kernel version of the device
Local Time	Date and time information with timezone offset. The timezone offset can be selected on the Timezone field of the System webpage.
Uptime	Uptime measures the length of time a system has been running since it was booted.
Load Average	It is the average system load calculated over a given period time of 1, 5 and 15 minutes.

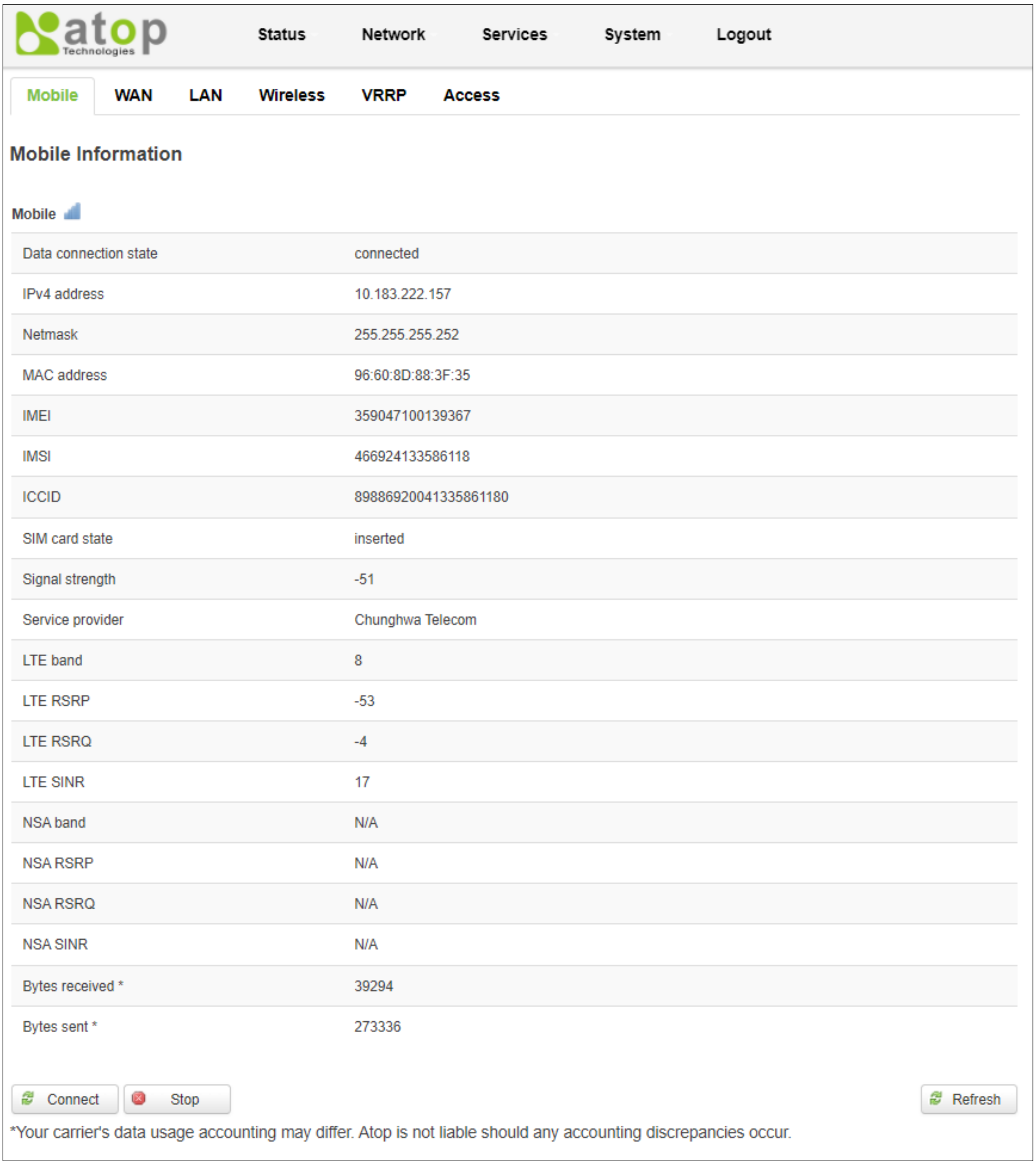
3.2.3 Network

3.2.3.1 Mobile

This section shows the Internet status information of the router. The status of the mobile interface. It contains information on the primary SIM card number, the data connection state, the service provider, the network type, the signal strength, the number of bytes sent, the number of bytes received, IMEI, IMSI, and ICCID.

Click **Connect** to connect to a 5G/LTE network, and click **Stop** to disconnect from a network.

Figure 18. Status > Network > Mobile



Mobile Information

Mobile

Data connection state	connected
IPv4 address	10.183.222.157
Netmask	255.255.255.252
MAC address	96:60:8D:88:3F:35
IMEI	359047100139367
IMSI	466924133586118
ICCID	89886920041335861180
SIM card state	inserted
Signal strength	-51
Service provider	Chunghwa Telecom
LTE band	8
LTE RSRP	-53
LTE RSRQ	-4
LTE SINR	17
NSA band	N/A
NSA RSRP	N/A
NSA RSRQ	N/A
NSA SINR	N/A
Bytes received *	39294
Bytes sent *	273336

*Your carrier's data usage accounting may differ. Atop is not liable should any accounting discrepancies occur.

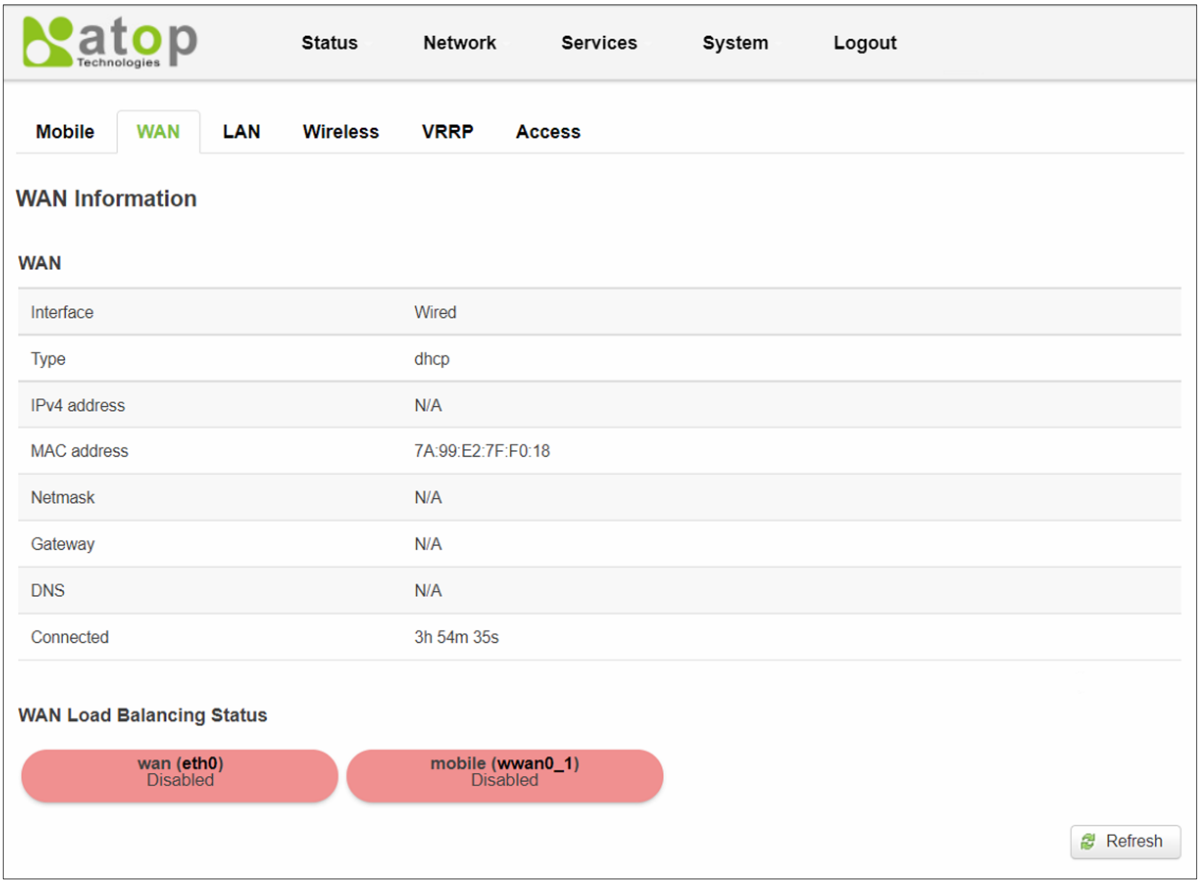
Table 12. Status > Network > Mobile

Field	Description
Data connection state	The Mobile data connection status.
IPv4 address	The IP address that the router uses to connect to the internet.
Netmask	Specifies a mask used to define how large the WAN network is.
Mac address	MAC (Media Access Control) address of the mobile module.
IMEI	IMEI (International Mobile Equipment Identity) number of the mobile module.
IMSI	IMSI (International Mobile Subscriber Identity) number of the current SIM.
ICCID	ICCID number of the current SIM.
SIM card state	SIM card's state, e.g. PIN required, Not inserted, etc.
Signal strength	The signal strength. Signal's strength measured in dBm.
Service provider	The name of ISP Network Provider.
LTE band	The band of the current network.
LTE RSRP	The signal of LTE Reference Signal Received Power.
LTE RSRQ	The signal of current LTE Reference Signal Received Quality.
LTE SINR	The Signal to Interference plus Noise Ratio.
NSA band	The current NSA frequency bands.
NSA RSRP	The signal of 5G NR Reference Signal Received Power.
NSA RSRQ	The signal of current LTE Reference Signal Received Quality.
NSA SINR	The Signal to Interference plus Noise Ratio.
Bytes received	The number of bytes were received via the mobile data connection.
Bytes sent	The number of bytes were sent via the mobile data connection.

3.2.3.2 WAN

This section shows the WAN status information of the router.

Figure 19. Status > Network > WAN



WAN Information

WAN

Interface	Wired
Type	dhcp
IPv4 address	N/A
MAC address	7A:99:E2:7F:F0:18
Netmask	N/A
Gateway	N/A
DNS	N/A
Connected	3h 54m 35s

WAN Load Balancing Status

wan (eth0) Disabled

mobile (wwan0_1) Disabled

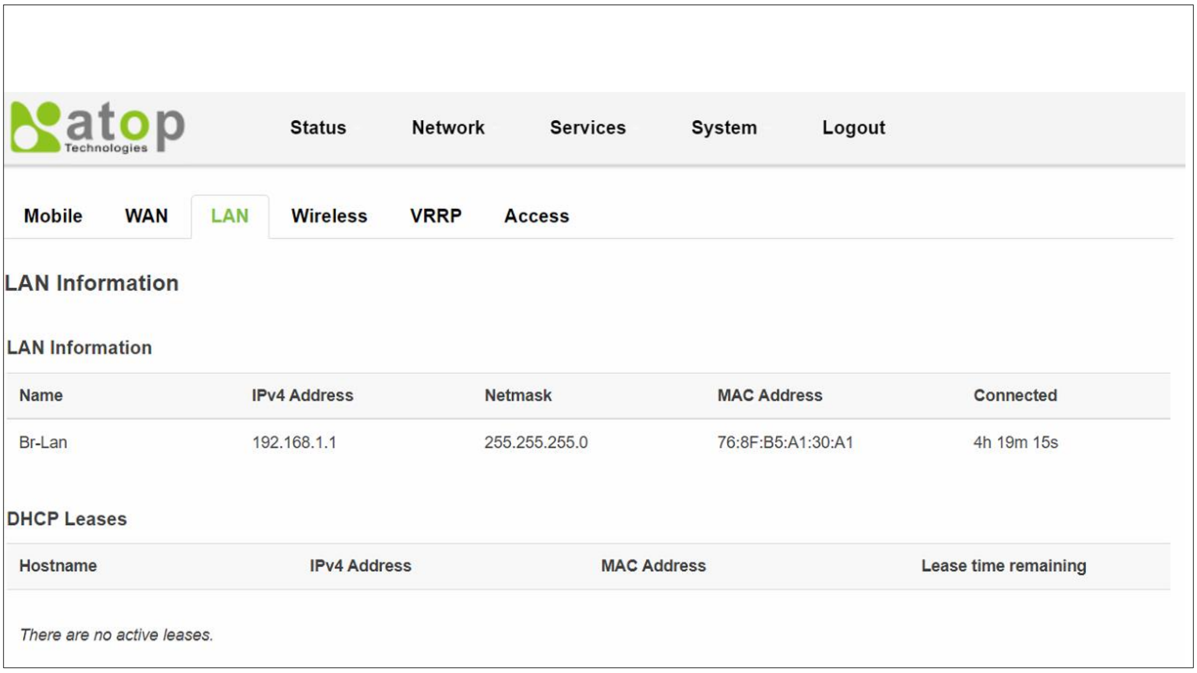
Table 13. Status > Network > WAN

Field	**Description**
Interface	Interface used for WAN connection.
Type	The current connection type status (DHCP/Static /PPPoE).
IPv4 address	The WAN IP address of the router.
MAC address	The WAN MAC address of the router.
Netmask	The WAN Netmask of the router.
Gateway	The WAN Gateway of the router.
DNS	The WAN DNS of the router.
Connected	The current amount of time which router has been connected.
wan (eth0)	The current wan status (Online/Offline/Disabled) of the WAN port interface.
mobile (wwan0_1)	The current wan status (Online/Offline/Disabled) of the mobile interface.

3.2.3.3 LAN

This section shows the LAN status information of the router.

Figure 20. Status > Network > LAN



LAN Information

LAN Information

Name	IPv4 Address	Netmask	MAC Address	Connected
Br-Lan	192.168.1.1	255.255.255.0	76:8F:B5:A1:30:A1	4h 19m 15s

DHCP Leases

Hostname	IPv4 Address	MAC Address	Lease time remaining

There are no active leases.

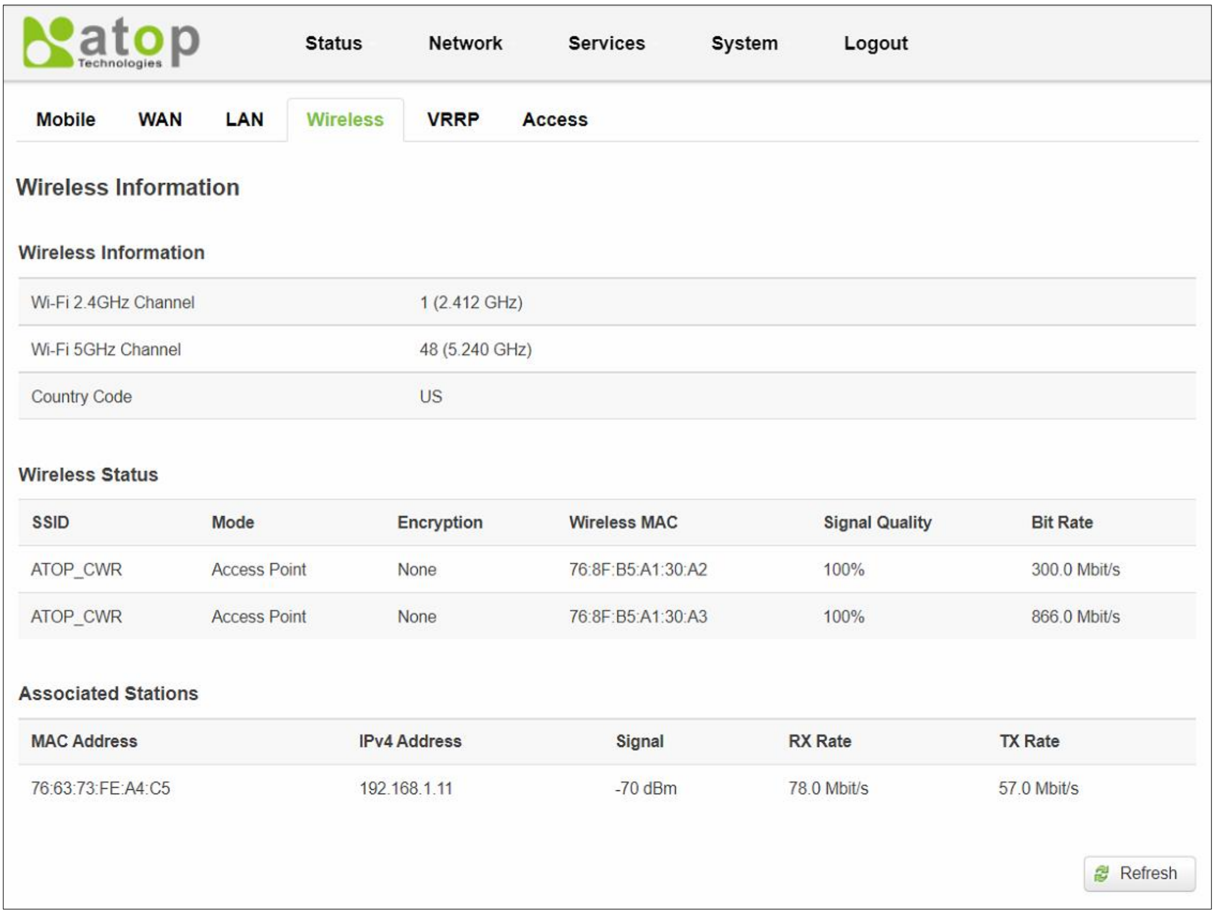
Table 14. Status > Network > LAN

Field	**Description**
Hostname	DHCP client’s hostname.
IPv4-Address	DHCP client’s IP address.
MAC-Address	DHCP client’s MAC address.
Leasetime remaining	The remaining lease time for a DHCP client. DHCP lease settings can be changed in the Network>Interface>LAN>DHCP Server section.

3.2.3.4 Wireless

This section shows the Wireless status information of the router.

Figure 21 Status > Network > Wireless



Wireless Information

Wireless Information

Wi-Fi 2.4GHz Channel	1 (2.412 GHz)
Wi-Fi 5GHz Channel	48 (5.240 GHz)
Country Code	US

Wireless Status

SSID	Mode	Encryption	Wireless MAC	Signal Quality	Bit Rate
ATOP_CWR	Access Point	None	76:8F:B5:A1:30:A2	100%	300.0 Mbit/s
ATOP_CWR	Access Point	None	76:8F:B5:A1:30:A3	100%	866.0 Mbit/s

Associated Stations

MAC Address	IPv4 Address	Signal	RX Rate	TX Rate
76:63:73:FE:A4:C5	192.168.1.11	-70 dBm	78.0 Mbit/s	57.0 Mbit/s

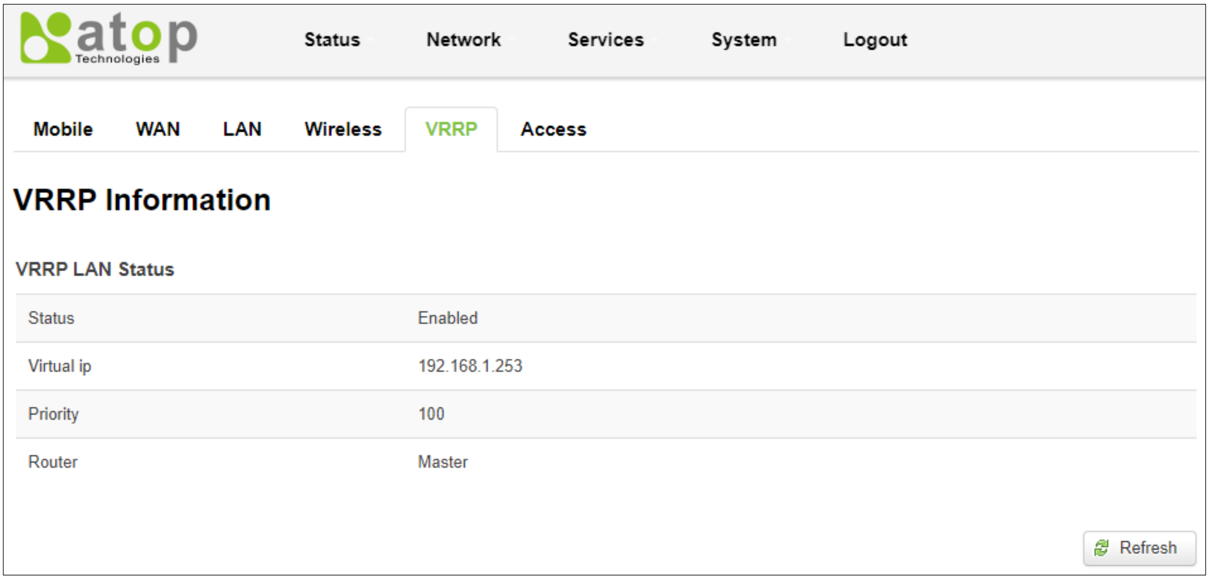
Table 15 Status > Network > Wireless

Field	Description
Wi-Fi 2.4GHz Channel	The display name of the Wi-Fi 2.4GHz interface on the CWR5805 device.
Wi-Fi 5GHz Channel	The display name of the Wi-Fi 5GHz interface on the CWR5805 device.
Country Code	Country code.
SSID	The broadcasted SSID of the wireless network that the client devices are connected to.
Mode	Access Point Mode.
Encryption	Type of Wi-Fi encryption that will be used.
Wireless MAC	Identify the basic service sets that are 48-bit labels and conform to the MAC-48 convention.
Signal Quality	The strength of the signal.
Bit Rate	The physical maximum possible throughput that the routers radio can handle. This value is cumulative. The bit rate will be shared between the router and other possible devices that connect to the local AP.
MAC Address	The MAC address of the associated station.
IPv4 Address	The IP address of the associated station.
Signal	The strength of the wireless between the CWR5805 and the associated station.
Rx Rate	The rate of the received packets from the associated station.
Tx Rate	The rate of the sent packets to the associated station.

3.2.3.5 VRRP

The **Virtual Router Redundancy Protocol** (**VRRP**) is a computer networking protocol used for automatic default gateway selection for clients on a **LAN network** in case the main router (Master) becomes unavailable. Another VRRP router (Backup) then assumes the role of Master; thus backing up the connection.

Figure 22. Status > Network > VRRP (Master)

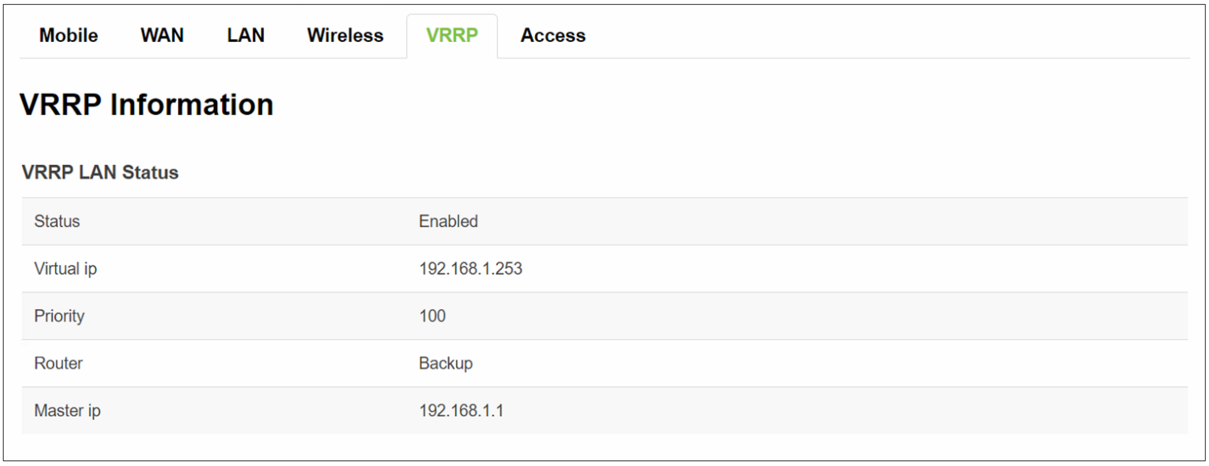


VRRP Information

VRRP LAN Status

Status	Enabled
Virtual ip	192.168.1.253
Priority	100
Router	Master

Figure 23. Status > Network > VRRP (Backup)



VRRP Information

VRRP LAN Status

Status	Enabled
Virtual ip	192.168.1.253
Priority	100
Router	Backup
Master ip	192.168.1.1

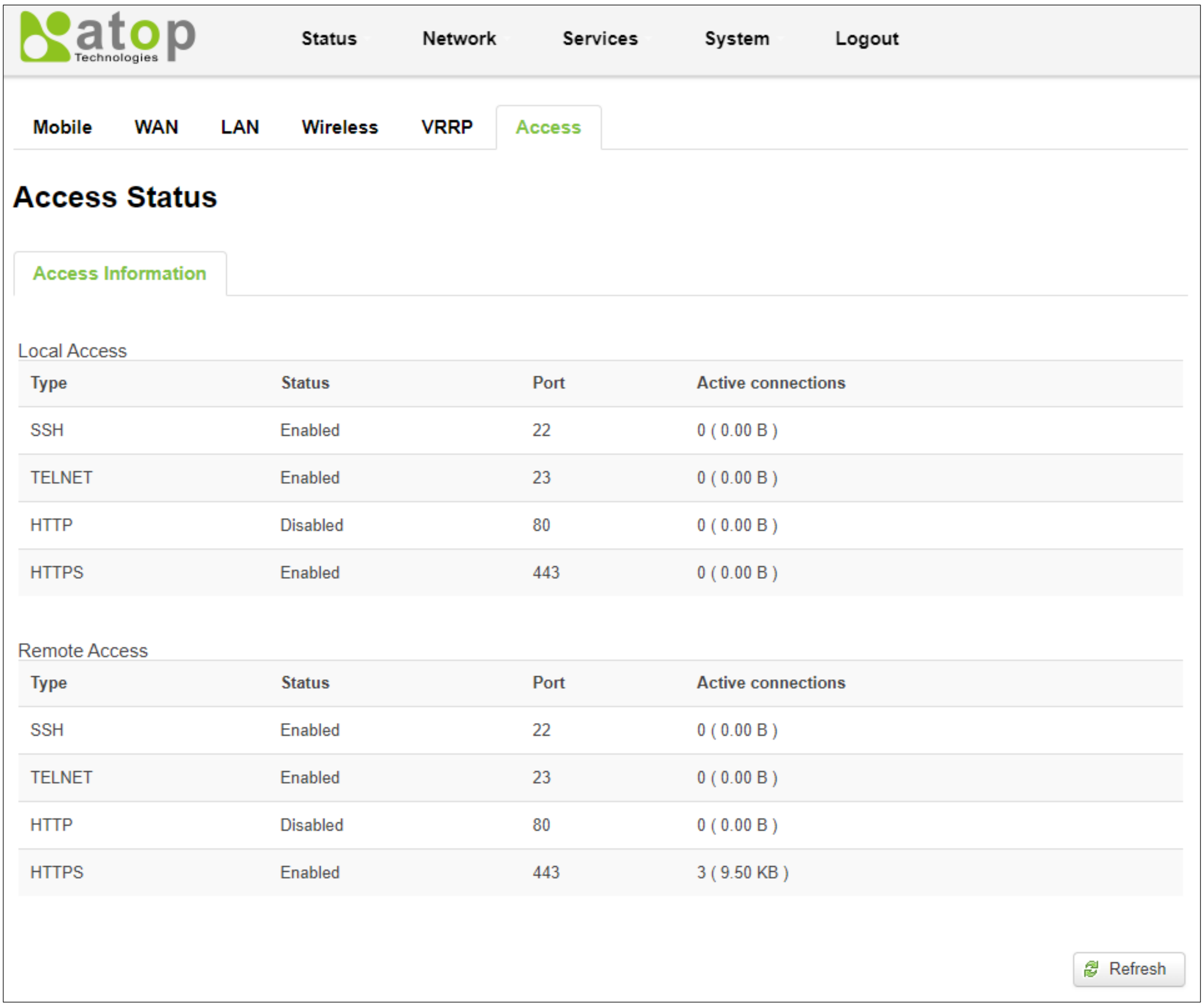
Table 16. Status > Network > VRRP

Field	Value	Description
Status	default: **disable**	VRRP status.
Virtual IP	default: **192.168.1.253**	Virtual IP address(-es) for LAN's VRRP (Virtual Router Redundancy Protocol) cluster.
Priority	integer [1 - 255]; default: **100**	The router with the highest priority value on the same VRRP cluster will act as a master.
Router	Master/Backup	Connection mode.
Master ip	ip	Master IP.

3.2.3.6 Access

Display information about local and remote active connections status.

Figure 24. Status > Network > Access



Access Status

Local Access

Type	Status	Port	Active connections
SSH	Enabled	22	0 (0.00 B)
TELNET	Enabled	23	0 (0.00 B)
HTTP	Disabled	80	0 (0.00 B)
HTTPS	Enabled	443	0 (0.00 B)

Remote Access

Type	Status	Port	Active connections
SSH	Enabled	22	0 (0.00 B)
TELNET	Enabled	23	0 (0.00 B)
HTTP	Disabled	80	0 (0.00 B)
HTTPS	Enabled	443	3 (9.50 KB)

Table 17. Status > Network > Access

Field	Value	Description
Type	SSH/HTTP/HTTPS	Type of connection protocol.
Status	disabled/enabled	Connection status.
Port	22/80/443	Connection port used.
Active connections	integer/data usage	Count of active connections and the amount of data transmitted.

3.2.4 Routes

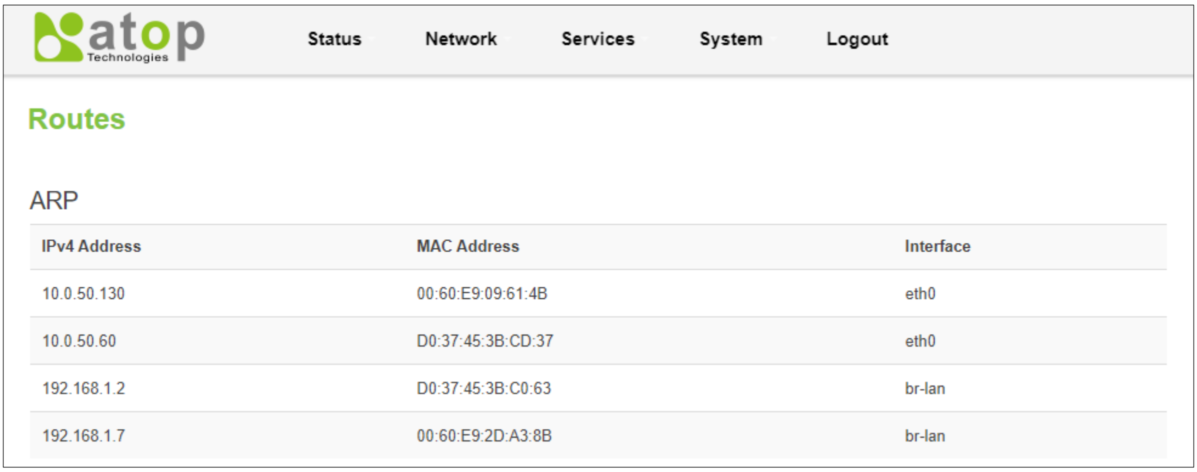
The **Routes** sub-menu under the Status menu provides information such as an ARP table and a table of active IPv4 routes of the CWR5805 device.

3.2.4.1 ARP

The ARP section shows the router’s active ARP table. An ARP table contains recently cached MAC addresses of every immediate device that was communicating with the router. This section also shows the router’s routing table.

The description of each field in the ARP section is shown in the table below.

Figure 25. Status > Routes - ARP



Routes

ARP

IPv4 Address	MAC Address	Interface
10.0.50.130	00:60:E9:09:61:4B	eth0
10.0.50.60	D0:37:45:3B:CD:37	eth0
192.168.1.2	D0:37:45:3B:C0:63	br-lan
192.168.1.7	00:60:E9:2D:A3:8B	br-lan

Table 18. Status > Routes - ARP

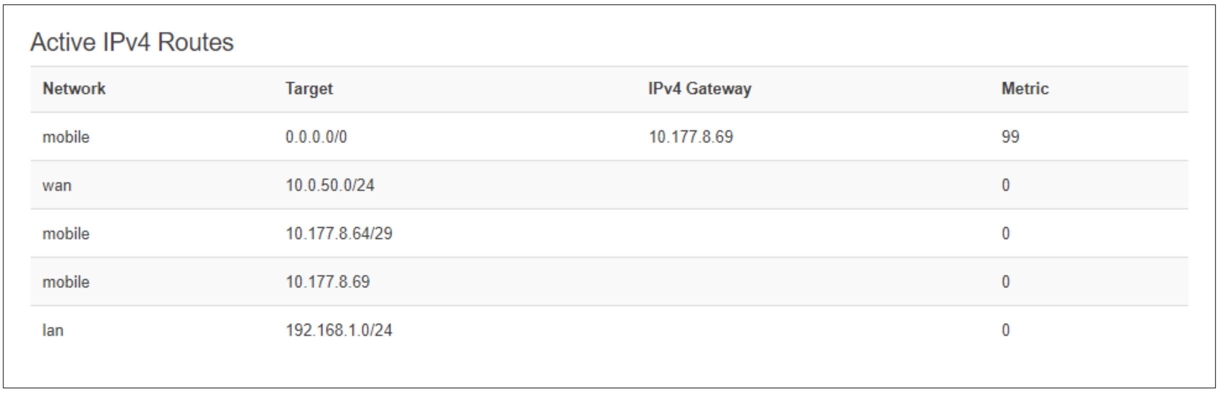
Field	Description
IPv4 Address	Recently cached IP addresses of every immediate device that was communicating with the router.
MAC-Address	Recently cached MAC addresses of every immediate device that was communicating with the router.
Interface	Interface used for the connection.

3.2.4.2 Active IPv4-Routes Section

The Active IPv4 Routes section indicates where a TCP/IP packet, with a specific IP address, should be directed to.

The description of each field is shown in the table below.

Figure 26. Status > Routes – Active IPv4 Routes



Active IPv4 Routes

Network	Target	IPv4 Gateway	Metric
mobile	0.0.0.0/0	10.177.8.69	99
wan	10.0.50.0/24		0
mobile	10.177.8.64/29		0
mobile	10.177.8.69		0
lan	192.168.1.0/24		0

Table 19. Status > Routes – Active IPv4 Routes

Field	Description
Network	Interface to be used to transmit TCP/IP packets through.
Target	IP address and mask of the destination network. It is used to determine the actual IP addresses which the routing rule is applied. This field is represented by Classless Inter Domain Routing (CIDR) notation.
IPv4-Gateway	An IP address where the CWR5805 device should send all the traffic to.
Metric	A metric number indicating interface priority of usage. This value is used as a sorting method. If a routing packet falls into the category of two rules, the one with the lower metric is applied.

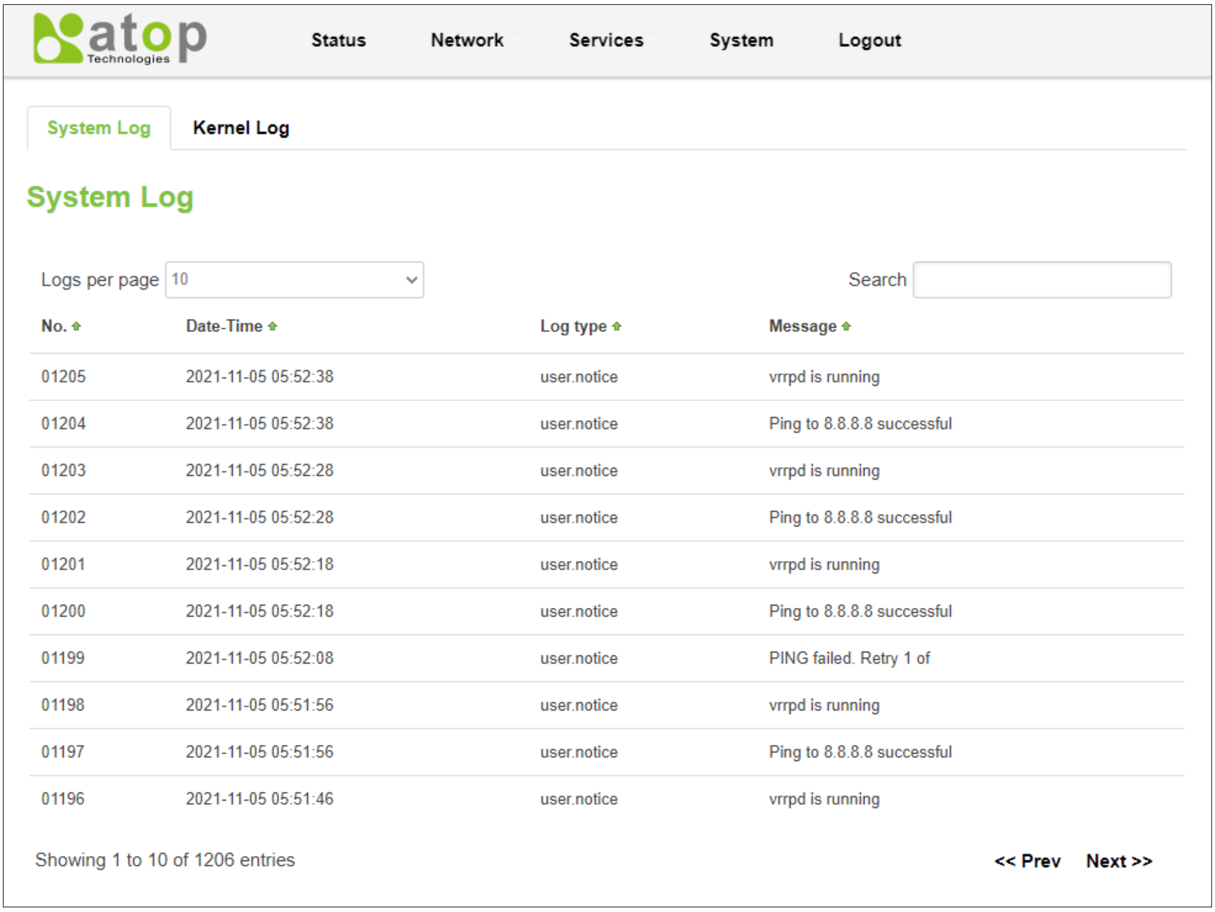
3.2.5 Logs

3.2.5.1 System Log

The **System Log** sub-menu under the Status menu follows a Message Logging standard. System Log collects data from most applications on the CWR5805 device, such as status, events, and diagnostics. The system Log message is categorized into 3 levels: Debug, Normal, and Warning.

This webpage substitute troubleshooting file that can be published to the external system log server.

Figure 27. Status > System > System Log



System Log

Logs per page 10

Search

No.	Date-Time	Log type	Message
01205	2021-11-05 05:52:38	user.notice	vrrpd is running
01204	2021-11-05 05:52:38	user.notice	Ping to 8.8.8.8 successful
01203	2021-11-05 05:52:28	user.notice	vrrpd is running
01202	2021-11-05 05:52:28	user.notice	Ping to 8.8.8.8 successful
01201	2021-11-05 05:52:18	user.notice	vrrpd is running
01200	2021-11-05 05:52:18	user.notice	Ping to 8.8.8.8 successful
01199	2021-11-05 05:52:08	user.notice	PING failed. Retry 1 of
01198	2021-11-05 05:51:56	user.notice	vrrpd is running
01197	2021-11-05 05:51:56	user.notice	Ping to 8.8.8.8 successful
01196	2021-11-05 05:51:46	user.notice	vrrpd is running

Showing 1 to 10 of 1206 entries

<< Prev Next >>

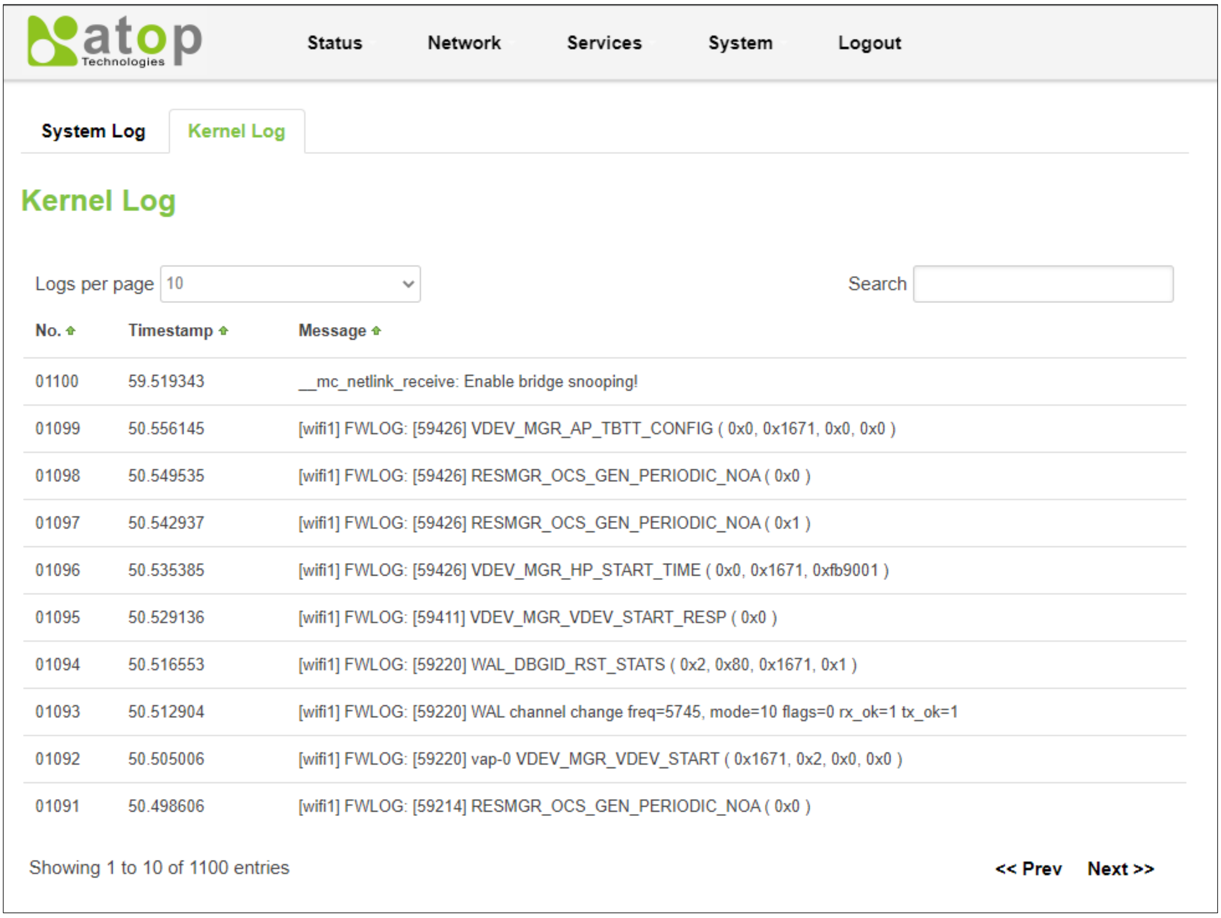
Table 20. Status > System > System Log

Field	Description
Date-Time	The time format: YYYY-MM-DD HH-MM-SS.
Log Type	Log type.
Message	The description of the System log.

3.2.5.2 Kernel Log

The Kernel Log Provides on-screen Kernel logging information.

Figure 28. Status > System > Kernel Log



Kernel Log

Logs per page 10

Search

No.	Timestamp	Message
01100	59.519343	__mc_netlink_receive: Enable bridge snooping!
01099	50.556145	[wifi1] FWLOG: [59426] VDEV_MGR_AP_TBTT_CONFIG (0x0, 0x1671, 0x0, 0x0)
01098	50.549535	[wifi1] FWLOG: [59426] RESMGR_OCS_GEN_PERIODIC_NOA (0x0)
01097	50.542937	[wifi1] FWLOG: [59426] RESMGR_OCS_GEN_PERIODIC_NOA (0x1)
01096	50.535385	[wifi1] FWLOG: [59426] VDEV_MGR_HP_START_TIME (0x0, 0x1671, 0xfb9001)
01095	50.529136	[wifi1] FWLOG: [59411] VDEV_MGR_VDEV_START_RESP (0x0)
01094	50.516553	[wifi1] FWLOG: [59220] WAL_DBGID_RST_STATS (0x2, 0x80, 0x1671, 0x1)
01093	50.512904	[wifi1] FWLOG: [59220] WAL channel change freq=5745, mode=10 flags=0 rx_ok=1 tx_ok=1
01092	50.505006	[wifi1] FWLOG: [59220] vap-0 VDEV_MGR_VDEV_START (0x1671, 0x2, 0x0, 0x0)
01091	50.498606	[wifi1] FWLOG: [59214] RESMGR_OCS_GEN_PERIODIC_NOA (0x0)

Showing 1 to 10 of 1100 entries

<< Prev Next >>

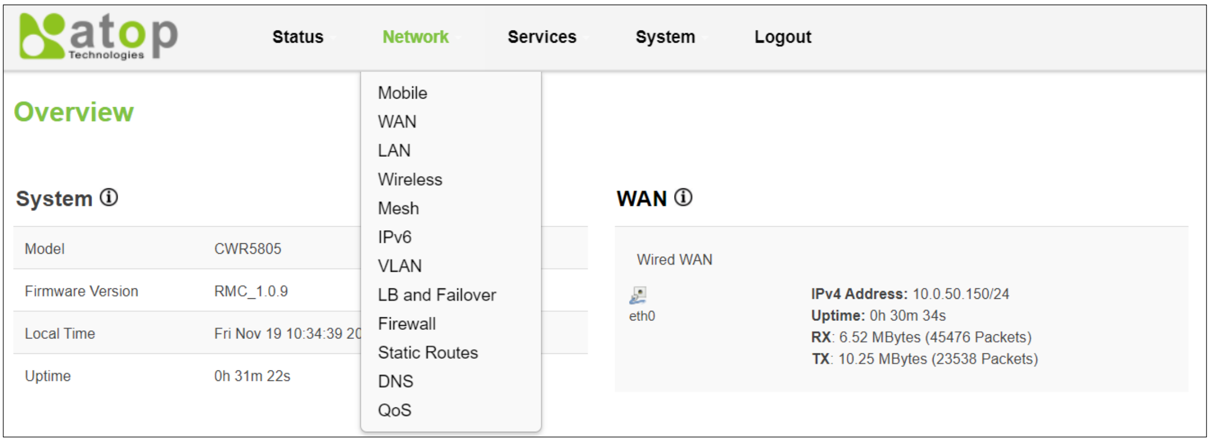
Table 21. Status > System > Kernel Log

Field	Description
Timestamp	The kernel log timestamp.
Message	The description of the Kernel log.

3.3 Network Menu

The Network menu contains 12 sub-menu items which provide some useful network applications on the CWR5805 device. The sub-menus are as follows: Mobile, WAN, LAN, Wireless, Mesh, IPv6, VLAN, LB and Failover, Firewall, Static Routes, DNS, and QoS.

Figure 29. Network



Model	CWR5805
Firmware Version	RMC_1.0.9
Local Time	Fri Nov 19 10:34:39 20
Uptime	0h 31m 22s

IPv4 Address: 10.0.50.150/24
Uptime: 0h 30m 34s
RX: 6.52 MBytes (45476 Packets)
TX: 10.25 MBytes (23538 Packets)

3.3.1 Mobile

CWR5805 is also equipped with a 5G/LTE module. In the MOBILE tab of the Interfaces sub-menu of the Network menu, you can configure parameters related to the mobile data connection. The MOBILE tab consists of General Setup, Advanced Settings, and SIM Switch sub-tabs.

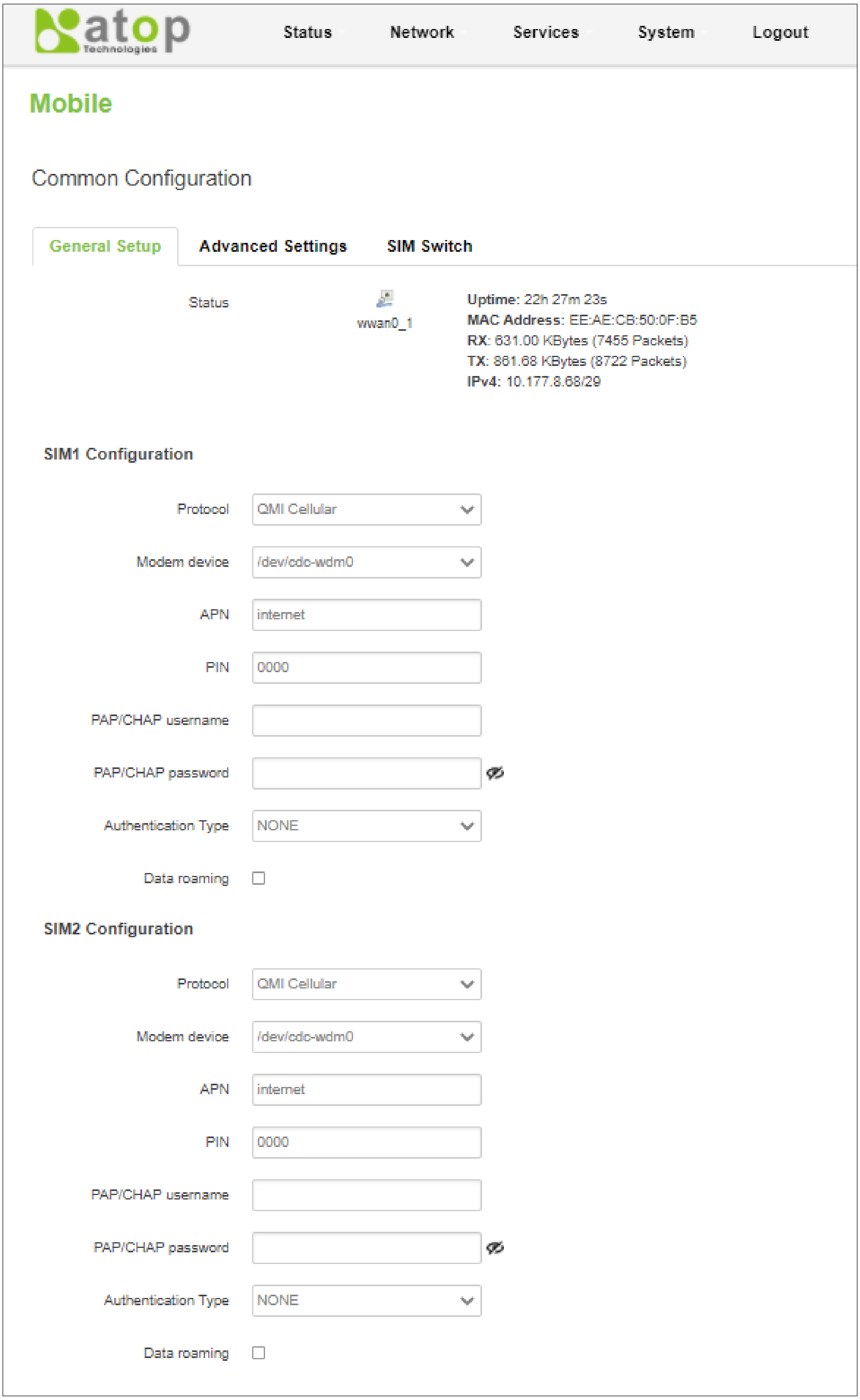
3.3.1.1 General Setup

In the **General Setup** sub-tab of Network-Interfaces-MOBILE tab, the **Status field** displays the current Mobile interface information of Uptime, MAC Address, RX, TX, and IPv4. You can configure QMI protocol parameters for the mobile interface, as shown in the Figure below.

You can modify these values in the General Setup tab except IP, which depends on their ISP SIM card information. For example, if the ISP SIM card supports public IP dial-up for Internet connection, then the value of the APN field can be set to public.

In the Mobile webpage, the default protocol is set as QMI (Qualcomm MSM Interface) Cellular, which is used for 5G/LTE dial-up to Internet connection. The default value of APN field is set to the Internet, and the default value of the PIN field is set to 0000. These default settings under the General Setup tab of the Interface-Mobile webpage apply to most ISP SIM card dial-up settings.

Figure 30. Network > Mobile > General Setup



Mobile

Common Configuration

Status: wwan0_1
Uptime: 22h 27m 23s
MAC Address: EE:AE:CB:50:0F:B5
RX: 631.00 KBytes (7455 Packets)
TX: 861.68 KBytes (8722 Packets)
IPv4: 10.177.8.68/29

SIM1 Configuration

Protocol	QMI Cellular
Modem device	/dev/cdc-wdm0
APN	internet
PIN	0000
PAP/CHAP username	
PAP/CHAP password	
Authentication Type	NONE
Data roaming	□

SIM2 Configuration

Protocol	QMI Cellular
Modem device	/dev/cdc-wdm0
APN	internet
PIN	0000
PAP/CHAP username	
PAP/CHAP password	
Authentication Type	NONE
Data roaming	□

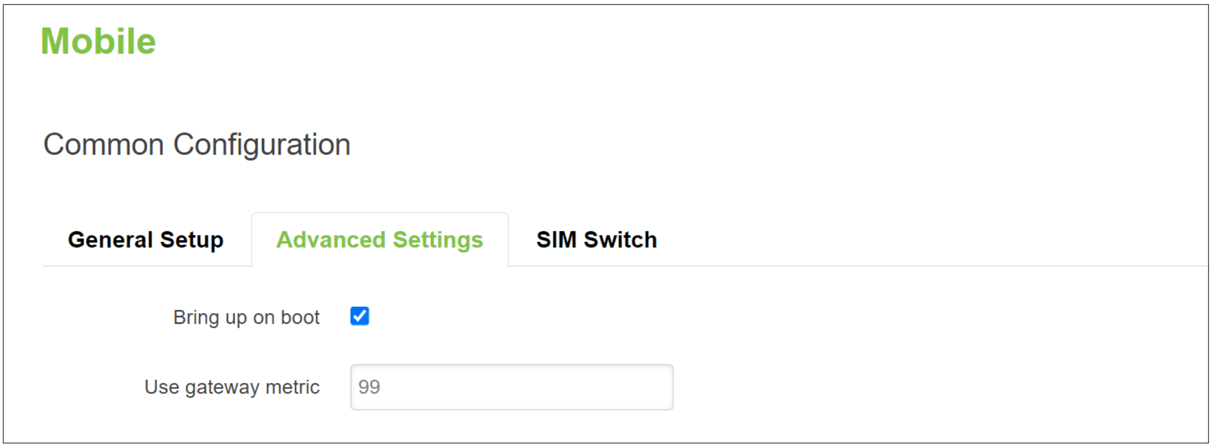
Table 22. Network > Mobile > General Setup

Field	Value	Description
Protocol	default: **QMI Cellular**	The protocol is used by the MOBILE interface.
Modem Device	default: **/dev/cdc-wdm0**	QMI device node.
APN	default: **internet**	An Access Point Name (APN) is the name of a gateway between a 5G/LTE mobile network. A mobile device making a data connection must be configured with an APN to present to the carrier. The carrier will then assign some connection parameters (e.g., security and priority level) based on the suitable type of network connection for that mobile device, depending on the contract with the operator.
PIN	default: **0000**	A password is used for authenticating the modem to the SIM card.
PAP/CHAP Username	default: **none**	Username for PAP/CHAP authentication.
PAP/CHAP Password	default: **none**	Password for PAP/CHAP authentication.
Authentication Type	PAP/CHAP(both)/ PAP/CHAP/None/Custom default: **none**	Authentication method that the 5G/LTE carrier uses to authenticate new connections on its network. If PAP or CHAP is selected, you will also be required to enter a Username and password.
Data Roaming	default: **disable**	By default, this option is unchecked to prevent the CWR5805 device from establishing a mobile data connection while not in the device's home network.

3.3.1.2 Advanced Settings Sub-Tab

In the **Advanced Setting** sub-tab of the Network-Interfaces-MOBILE tab, you can configure network functionalities in more detail based on your requirement for the mobile interface.

Figure 31. Network > Mobile > Advanced Settings


Mobile

Common Configuration

Bring up on boot ☑

Use gateway metric 99

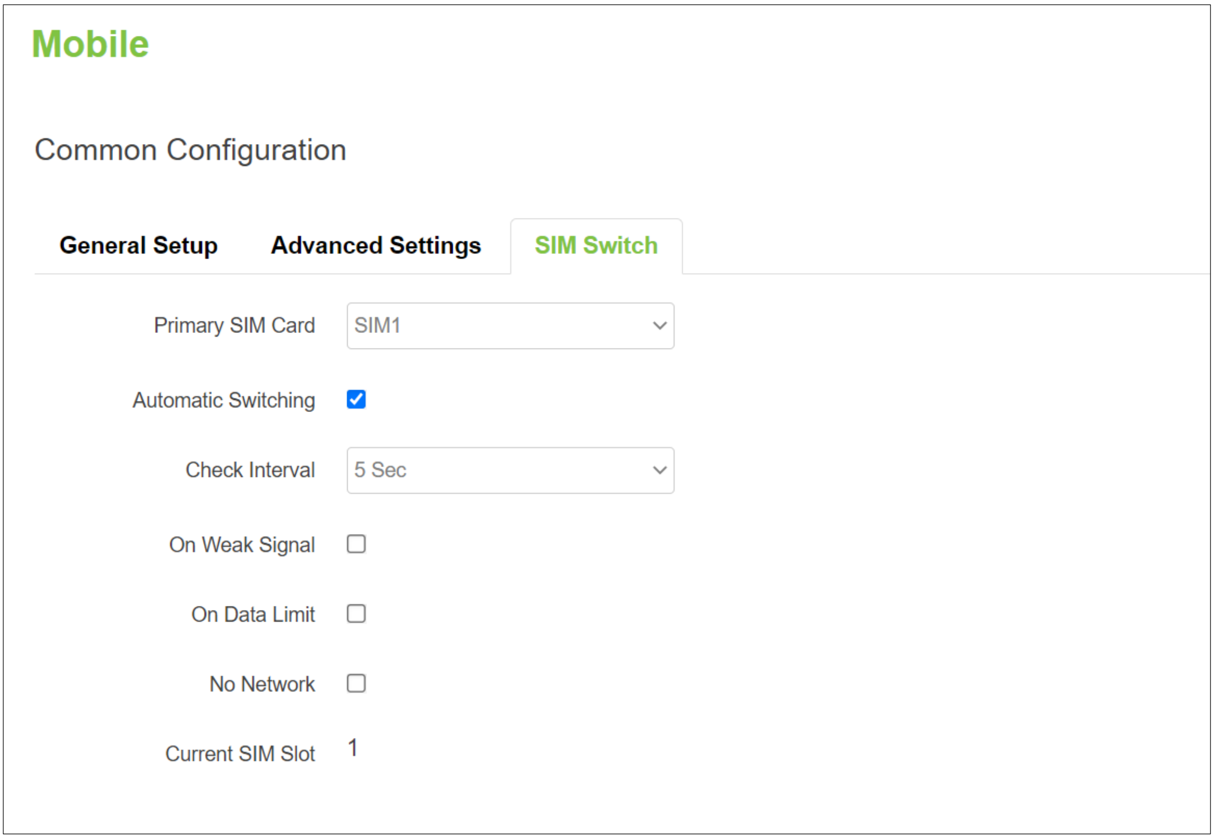
Table 23. Network > Mobile > Advanced Settings

Field	Value	Description
Bring Up on Boot	default: **enable**	Specify whether or not to bring up the WAN interface on the boot.
Use Gateway Metric	default: **99**	The priority of the gateway on the WAN interface. By default, a routing table entry is generated. You can alter the metric of that entry in this field.

3.3.1.3 SIM Switch

In the **SIM Switch** sub-tab of the Network-Interfaces-MOBILE tab, you can configure switching the current SIM card to the other SIM card when the 5G/LTE network conditions are proper.

Figure 32. Network > Mobile > SIM Switch



Mobile

Common Configuration

Primary SIM Card: SIM1

Automatic Switching: ☑

Check Interval: 5 Sec

On Weak Signal: ☐

On Data Limit: ☐

No Network: ☐

Current SIM Slot: 1

Table 24. Network > Mobile > SIM Switch

Field	Values	Description
Primary SIM Card	SIM1/SIM2; default: **SIM1**	Specify the SIM card slot that is used for 5G/LTE dial-up as the primary SIM card.
Automatic Switching	Enable/Disable; default: **disable**	If checked, the 5G/LTE network status will be monitored regularly. When the switch mechanism is matched one of the conditions from On Weak Signal/On Data Limit/No Network, then the Current SIM will be the non-primary SIM Slot.
Check Interval	5/15/30/60/120 Sec; default: **5**	Duration time for checking whether the 5G/LTE network status is matched with what you specified.
On Weak Signal	Disable, 10%, 20%, 30%, 40%, 50%; Default: **disable**	If checked, detect whether the current 5G/LTE signal status is weak or not.
On Data Limit	Enable/Disable; default: **disable**	If checked, detect whether the current 5G/LTE data traffic is reached the data limit size or not.
No Network	Enable/Disable; default: **disable**	If checked, detect whether the current 5G/LTE network is unavailable or not.
Current SIM Slot	1/2; default: **1**	Display the current primary SIM card slot which is used for 5G/LTE dial-up.

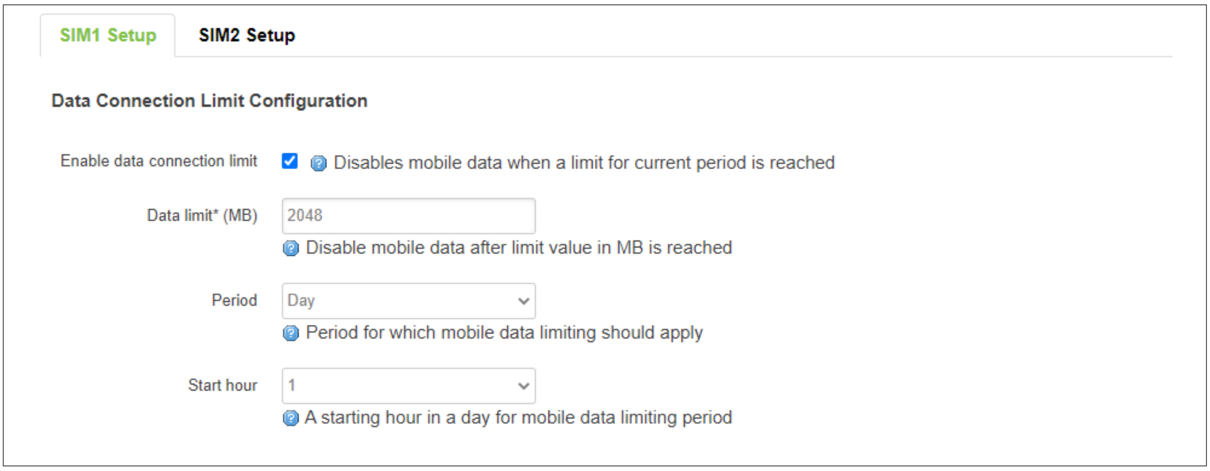
3.3.1.4 *Data Limit Configuration*

In the **Data Limit Configuration** section within all sub-tabs of the MOBILE tab, you can configure the data usage limit to avoid unwanted data charges. The limit on the data connections can be pre-selected for each SIM card. When the limit is later reached, the data usage warnings will be sent to notify you via SMS messages.

3.3.1.4.1 Data Connection Limit Configuration

The **Data Connection Limit Configuration** section is used to configure custom mobile data limits for your SIM card. When the mobile data limit set for the SIM card is reached, the CWR5805 device will no longer use the mobile connection to establish a data connection until the limitation period is over or the limit is reset by you.

Figure 33. Network > Mobile > General Setup > Data Limit Configuration > Data Connection Limit Configuration



Data Connection Limit Configuration

Enable data connection limit ☑ Disables mobile data when a limit for current period is reached

Data limit* (MB) 2048
Disable mobile data after limit value in MB is reached

Period Day
Period for which mobile data limiting should apply

Start hour 1
A starting hour in a day for mobile data limiting period

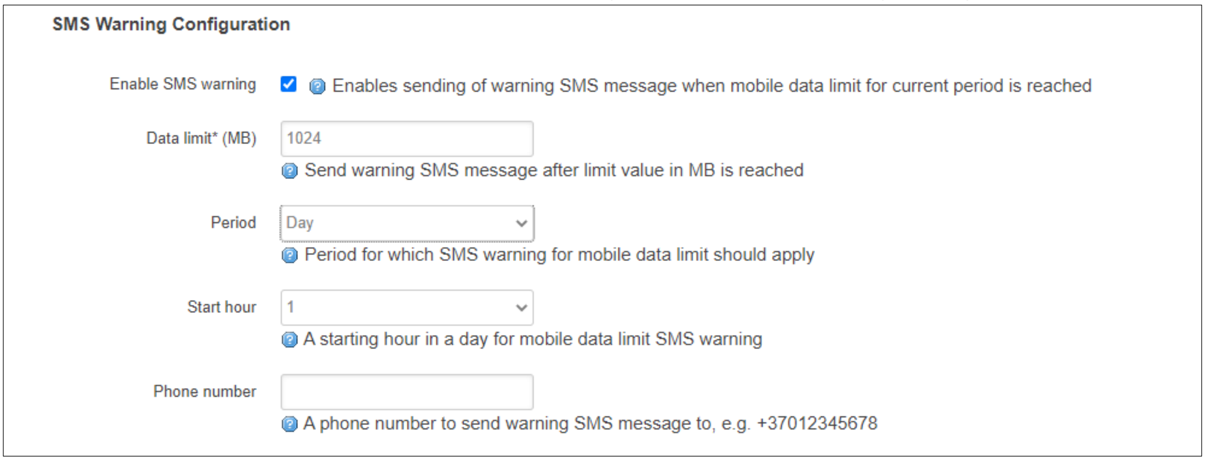
Table 25. Network > Mobile > General Setup > Data Limit Configuration > Data Connection Limit Configuration

Field	Values	Description
Enable Data Connection Limit	default: **disable**	Turns mobile data limitations on/off.
Data Limit (MB)	default: **none**	The amount of data that can be downloaded/uploaded over the specified period. When the limit is reached, the CWR5805 device will no longer be able to establish any data connection until the period is over or the data limit is reset.
Period	Day/Week/Month; default: **Month**	Length of time to monitor the data usage.
Start Hour	integer [1 – 24]; default: **1**	Specify the hour that the monitoring period begins. After the period is over, the data usage is reset before the monitoring process restarts.

3.3.1.4.2 SMS Warning Configuration

In the **SMS Warning Configuration** section, you can configure a rule to send SMS messages after the data connection sent/received through the CWR5805 device's SIM card is reached the specified limit.

Figure 34. Network > Mobile > General Setup > Data Limit Configuration > SMS Warning Configuration



SMS Warning Configuration

Enable SMS warning ☑ Enables sending of warning SMS message when mobile data limit for current period is reached

Data limit* (MB) 1024
Send warning SMS message after limit value in MB is reached

Period Day
Period for which SMS warning for mobile data limit should apply

Start hour 1
A starting hour in a day for mobile data limit SMS warning

Phone number
A phone number to send warning SMS message to, e.g. +37012345678

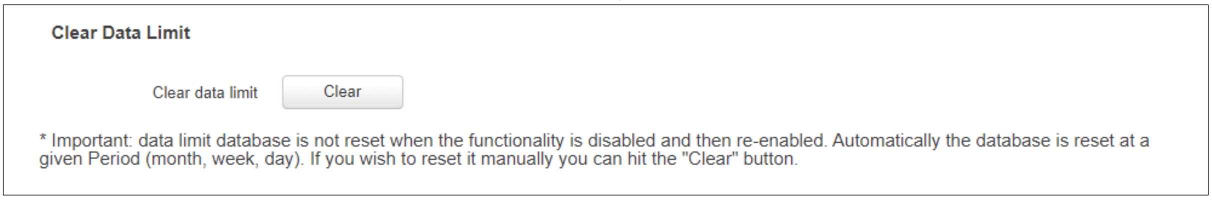
Table 26. Network > Mobile > General Setup > Data Limit Configuration > SMS Warning Configuration

Field	Description
Enable SMS Warning	Turns SMS warning on/off.
Data Limit (MB)	The amount of the limit data usage in Mbytes before the CWR5805 device will send SMS warnings to the specified phone number.
Period	Length of time to monitor the data usage. Currently, the field supports the monitoring period monthly, weekly, and daily.
Start Day/ Start Hour	Specify the day that the monitoring period begins. After the period is over, the data usage is reset before the monitoring process restarts.
Phone Number	The recipient's phone number that the SMS messages will be sent.

3.3.1.4.3 Clear Data Limit

The **Clear Data Limit** section contains only one button - 'Clear data limit'. When clicked, the button resets the data limit counter for the selected SIM card. Thus, the count is started over again regardless of the specified period.

Figure 35. Network > Mobile > General Setup > Data Limit Configuration > Clear Data Limit



Clear Data Limit

Clear data limit

* Important: data limit database is not reset when the functionality is disabled and then re-enabled. Automatically the database is reset at a given Period (month, week, day). If you wish to reset it manually you can hit the "Clear" button.

Figure 36. Network > Mobile > General Setup > Data Limit Configuration > Clear Data Limit

Field	Description
Clear Data Limit	When clicked, the data limit counter for the selected SIM card is reset. The count is started at 0 regardless of when it occurred in the specified period.

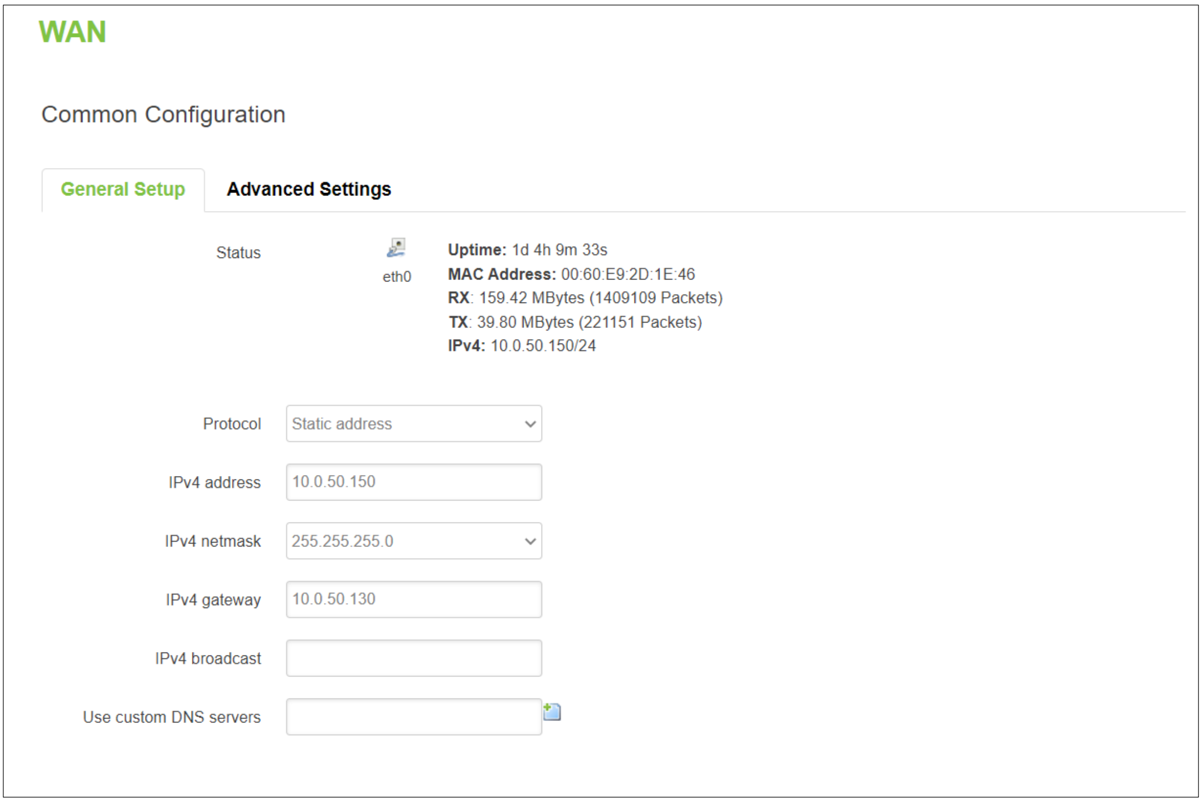
3.3.2 WAN

A **Wide Area Network** (WAN) is a telecommunications network or computer network that extends over a large geographical distance. For example, the Internet is a wide area network.

3.3.2.1 General Setup

In the General Setup sub-tab of the Network-Interfaces-WAN tab, different protocols for the WAN interface can be configured.

Figure 37. Network > WAN > General Setup



Status

Uptime: 1d 4h 9m 33s
MAC Address: 00:60:E9:2D:1E:46
RX: 159.42 MBytes (1409109 Packets)
TX: 39.80 MBytes (221151 Packets)
IPv4: 10.0.50.150/24

Protocol: Static address
IPv4 address: 10.0.50.150
IPv4 netmask: 255.255.255.0
IPv4 gateway: 10.0.50.130
IPv4 broadcast:
Use custom DNS servers:

You can switch between Static, DHCP, or PPPoE protocol by selecting the protocol that you want to use and then pressing **Switch Protocol.**

In the **WAN** webpage, the default protocol is set to **DHCP client**. It means that the WAN interface can get a dynamic IPv4 address from its connected Ethernet port of a Cable/ADSL modem.

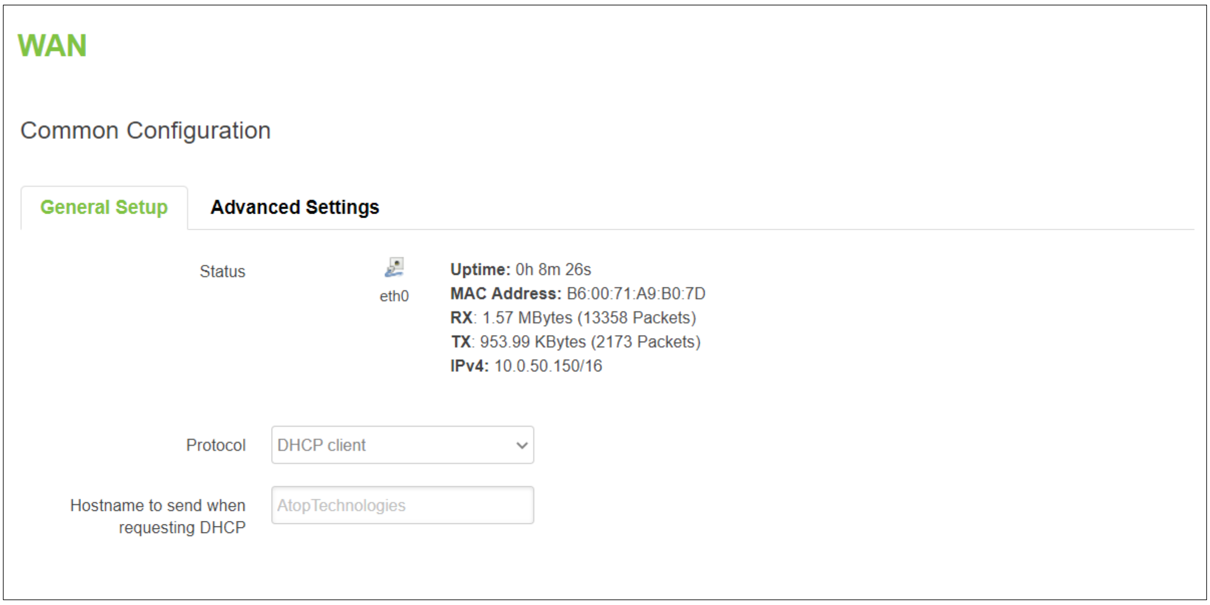
As shown in the Figure above, the **Status** field currently displays the WAN interface (eth0) information of Uptime, MAC Address, RX, TX, and IPv4. If the connected Cable/ADSL modem can provide an Internet service, CWR5805 also has an Internet service available via its WAN interface.

In addition, there are two other protocols supported by the WAN interface which are **Static address** and **PPPoE**. The setting of the protocol option for the WAN interface depends on the protocol requirement of the connected frontend Cable/ADSL modem.

3.3.2.2 DHCP Client

3.3.2.2.1 General Setup

Figure 38. Network > WAN > General Setup – DHCP Client



WAN

Common Configuration

Status eth0

Uptime: 0h 8m 26s
MAC Address: B6:00:71:A9:B0:7D
RX: 1.57 MBytes (13358 Packets)
TX: 953.99 KBytes (2173 Packets)
IPv4: 10.0.50.150/16

Protocol: DHCP client

Hostname to send when requesting DHCP: AtopTechnologies

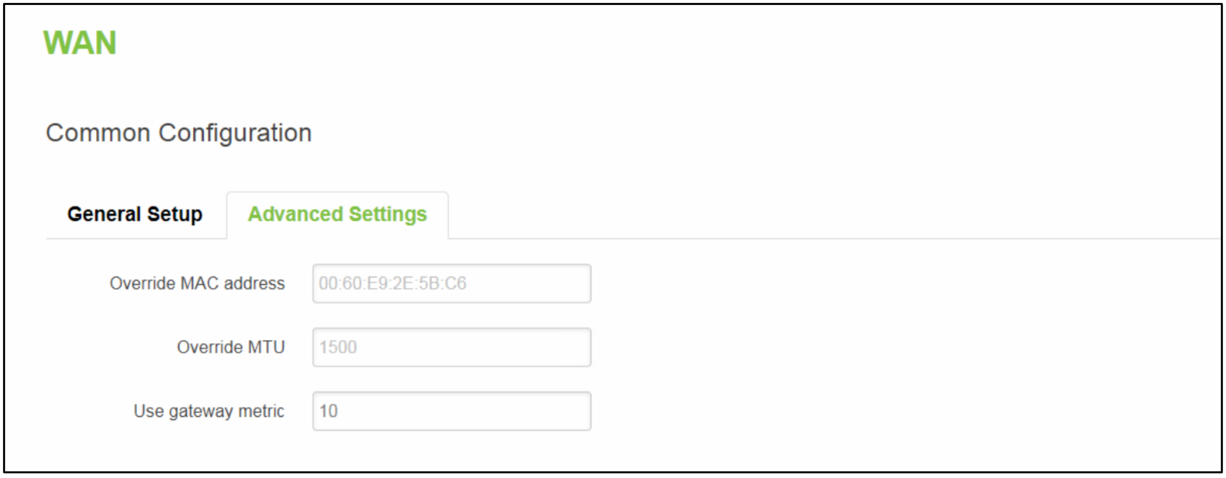
Table 27. Network > WAN > General Setup – DHCP Client

Field	Value	Description
Protocol	Static, DHCP and PPPoE; default: **DHCP**	The protocol is used by the WAN interface.
Hostname to send when requesting DHCP	ip/hostname; default: **none**	Hostname to which the DHCP request will be sent.

3.3.2.2.2 Advanced Settings

In the General Setup sub-tab of the Network-Interfaces-WAN tab, you can configure the WAN interface in more detail.

Figure 39. Network > WAN > Advanced Settings – DHCP Client



WAN

Common Configuration

Override MAC address: 00:60:E9:2E:5B:C6

Override MTU: 1500

Use gateway metric: 10

Table 28. Network > WAN > Advanced Settings – DHCP Client

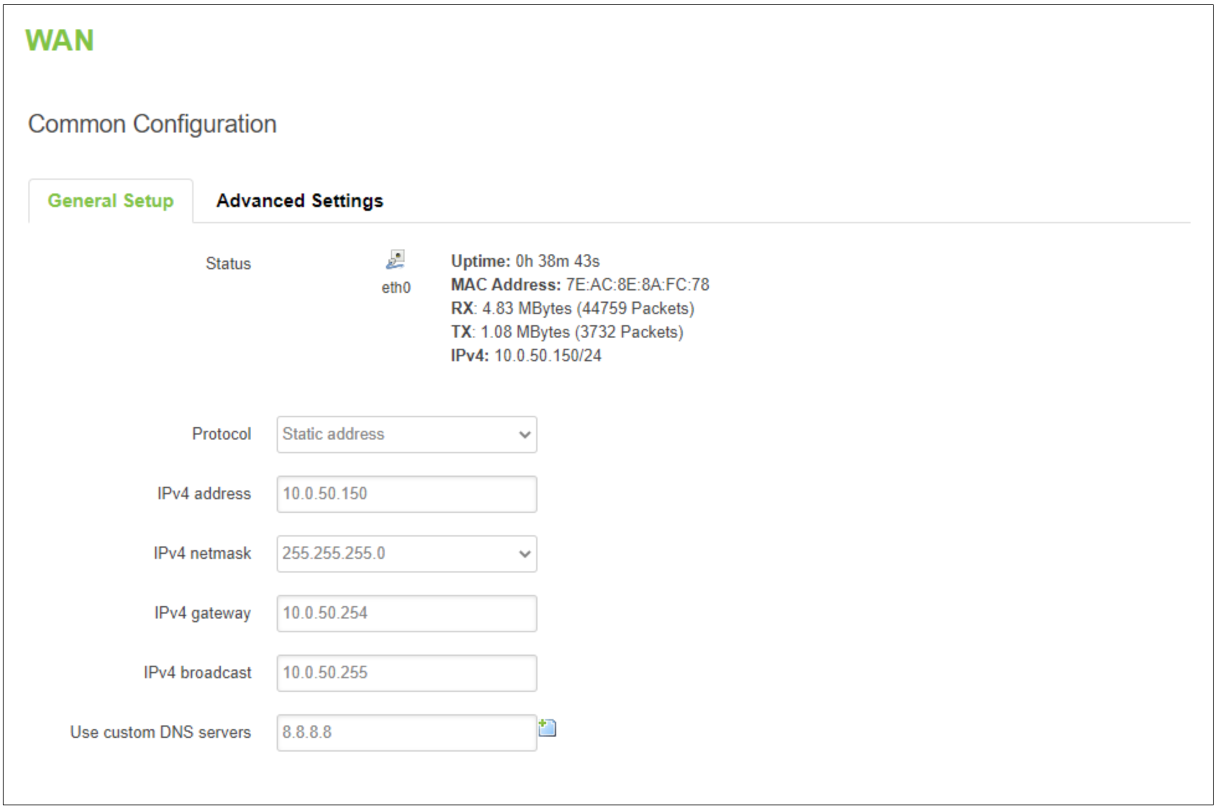
Field	Value	Description
Override MAC address	default: **CWR's MAC**	To override the MAC address of the WAN interface. For example, your ISP (Internet Service Provider) gives you a static IP address and it might also bind it to your computers' MAC address. In this field, you can enter

		the computer’s MAC address and fool the gateway into thinking that it is communicating with your computer.
Override MTU	integer [1 – 1500]; default: **1500**	Specify the maximum transferred size of a data packet.
Use Gateway Metric	default: **0**	By default, the WAN configuration generates a routing table entry. You can change the metric of that entry here.

3.3.2.3 Static address

3.3.2.3.1 General Setup

Figure 40. Network > WAN > General Setup – Static Address



Status
eth0
Uptime: 0h 38m 43s
MAC Address: 7E:AC:8E:8A:FC:78
RX: 4.83 MBytes (44759 Packets)
TX: 1.08 MBytes (3732 Packets)
IPv4: 10.0.50.150/24

Protocol: Static address

IPv4 address: 10.0.50.150

IPv4 netmask: 255.255.255.0

IPv4 gateway: 10.0.50.254

IPv4 broadcast: 10.0.50.255

Use custom DNS servers: 8.8.8.8

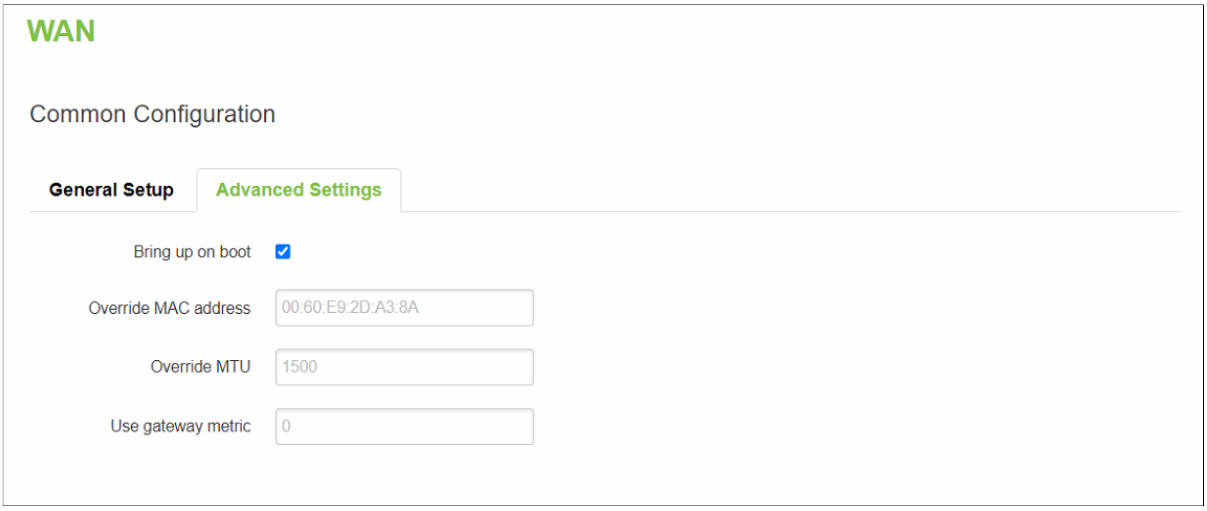
Table 29. Network > WAN > General Setup – Static Address

Field	Value	Description
Protocol	Static/DHCP/PPPoE; default: **DHCP**	The protocol is used by the WAN interface. This field currently supports DHCP clients, static address, and PPPoE.
IPv4 address	ip4; default: **none**	Your router’s address on the WAN network.
IPv4 netmask	netmask; default: **none**	Netmask defines how "large" a network is.
Ipv4 gateway	ip4; default: **none**	The IPv4 address gateway of this interface. An interface's gateway is the default next-hop address to access other networks.
IPv4 broadcast	ip4; default: none	IP broadcasts are used by BOOTP and DHCP clients to find and send requests to their respective servers.
Use custom DNS servers	ip4; default: **none**	By entering custom DNS servers, the router will take care of the hostname resolution. You can enter multiple DNS servers to provide redundancy in case one of the servers fails.

3.3.2.3.2 Advanced Settings

These are the advanced settings for each of the protocols. If you are unsure of how to alter these attributes it is highly recommended to leave them to a trained professional:

Figure 41. Network > WAN > Advanced Settings – Static Address



WAN

Common Configuration

Bring up on boot ☑

Override MAC address 00:60:E9:2D:A3:8A

Override MTU 1500

Use gateway metric 0

Table 30. Network > WAN > Advanced Settings – Static Address

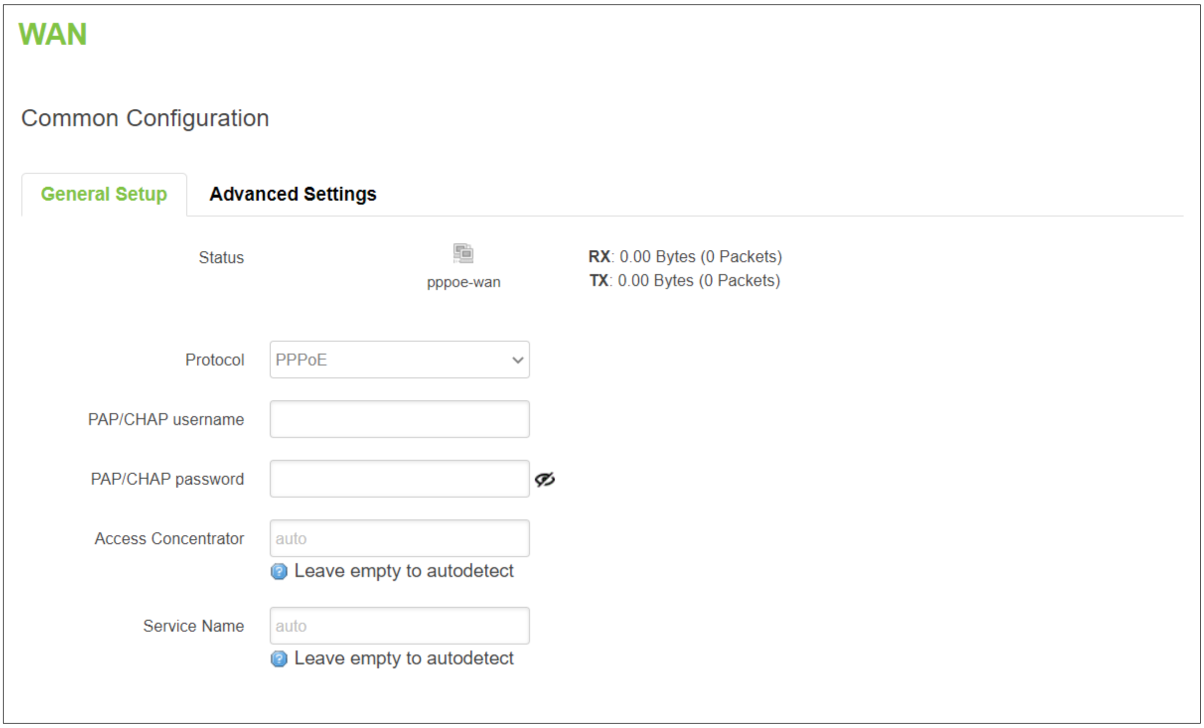
Field	Value	Description
Bring up on boot	default: **enable**	Specify whether to bring up the LAN interface on boot or not.
Override MAC address	default: **Device's MAC**	Override the MAC address of the LAN interface.
Override MTU	default: **1500**	Specify the maximum transferred size of a data packet.
Use gateway metric	default: **0**	The WAN configuration by default generates a routing table entry. With this field, you can alter the metric of that entry.

3.3.2.4 PPPoE

3.3.2.4.1 General Setup

This protocol is mainly used by DSL providers.

Figure 42. Network > WAN > General Setup – PPPoE



WAN

Common Configuration

Status: pppoe-wan — RX: 0.00 Bytes (0 Packets) TX: 0.00 Bytes (0 Packets)

Protocol: PPPoE

PAP/CHAP username:

PAP/CHAP password:

Access Concentrator: auto
Leave empty to autodetect

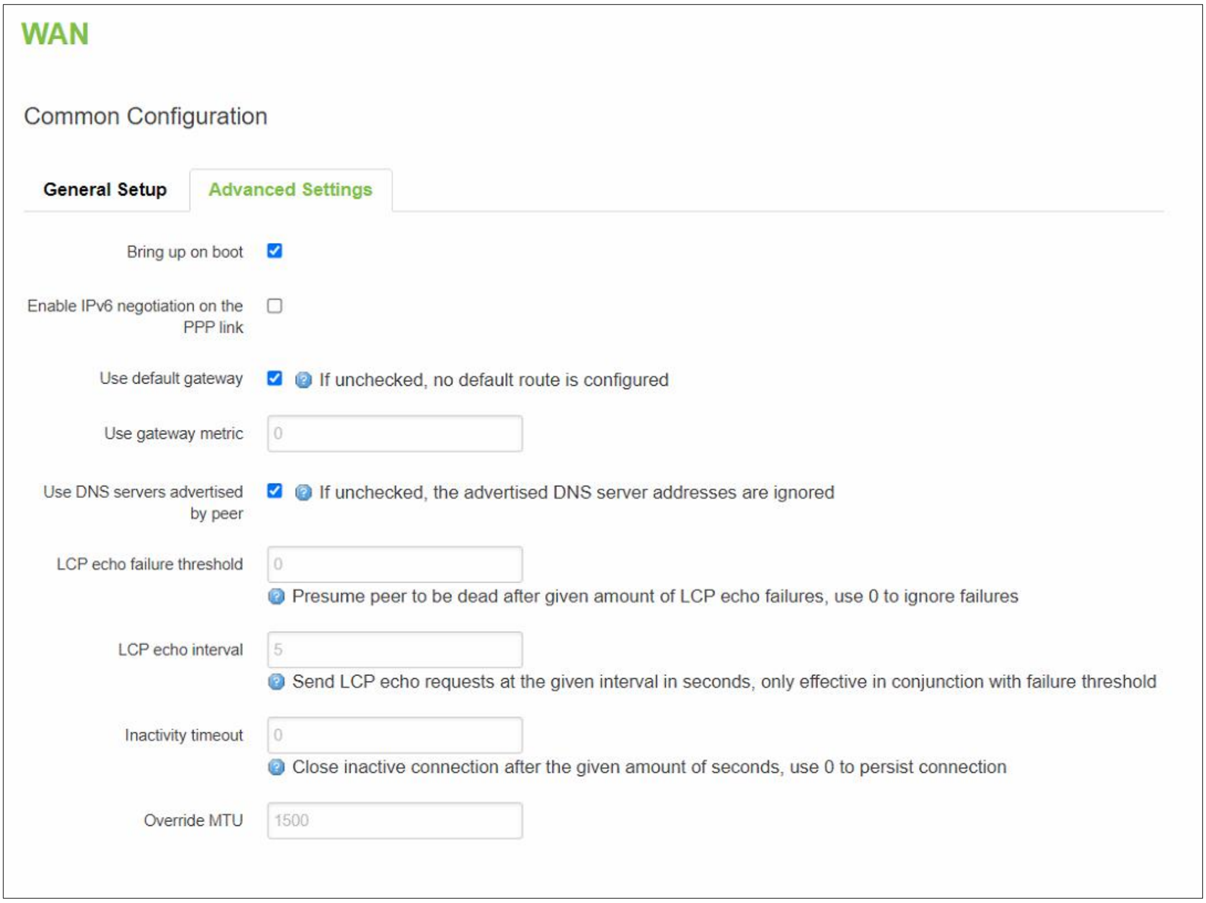
Service Name: auto
Leave empty to autodetect

Table 31. Network > WAN > General Setup – PPPoE

Field	Value	Description
Protocol	Static /DHCP /PPPoE default: DHCP	The protocol is used by the WAN interface. This field currently supports DHCP client, static address, and PPPoE.
PAP/CHAP Username	default: **non**	The username used in PAP/CHAP authentication.
PAP/CHAP password	default: **none**	The password used in PAP/CHAP authentication.
Access Concentrator	default: **auto**	The Access Concentrator to connect to ISPs used Access Concentrators to route their PPPoE connections. Usually, the settings are received automatically, however, in some cases, it is required to specify the name for an Access Concentrator. Leave this field empty to detect Access Concentrators automatically.
Service Name	default: **auto**	The Service Name to connect to. Leave this field empty to detect the Service name automatically.

3.3.2.4.2 Advanced Settings

Figure 43. Network > WAN > Advanced Setting – PPPoE



WAN

Common Configuration

Bring up on boot ☑

Enable IPv6 negotiation on the PPP link □

Use default gateway ☑ If unchecked, no default route is configured

Use gateway metric 0

Use DNS servers advertised by peer ☑ If unchecked, the advertised DNS server addresses are ignored

LCP echo failure threshold 0
Presume peer to be dead after given amount of LCP echo failures, use 0 to ignore failures

LCP echo interval 5
Send LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold

Inactivity timeout 0
Close inactive connection after the given amount of seconds, use 0 to persist connection

Override MTU 1500

Table 32. Network > WAN > Advanced Setting – PPPoE

Field	Value	Description
Bring up on boot	default: **enable**	Specify whether to bring up the WAN interface on boot or not.
Enable IPv6 negotiation on the PPP link	default: **disable**	Point-to-point protocol.
Use default gateway	default: **enable**	If unchecked, no default route is configured.
Use gateway metric	default: **0**	The WAN configuration by default generates a routing table entry. With this field, you can alter the metric of that entry.
Use DNS servers advertised by peer	default: **enable**	If unchecked, the advertised DNS server addresses are ignored.
LCP echo failure threshold	default: **0**	Presume peer to be dead after the given amount of LCP echo failures, use 0 to ignore failures.
LCP echo interval	default: **6**	Send LCP echo requests at the given interval in seconds, only effective in conjunction with the failure threshold.
Inactivity timeout	default: **0**	Close inactive connection after the given number of seconds, use 0 to persist connection.
Override MTU	default: **1500**	Specify the maximum transferred size of a data packet.

3.3.3 LAN

A **local area network** (LAN) is a computer network that interconnects computers within a limited area such as a residence, a school, a laboratory, a university campus, or an office building.

In the **Interface-LAN** webpage, the default protocol is set to a **Static address** with a default IPv4 address of 192.168.1.1.

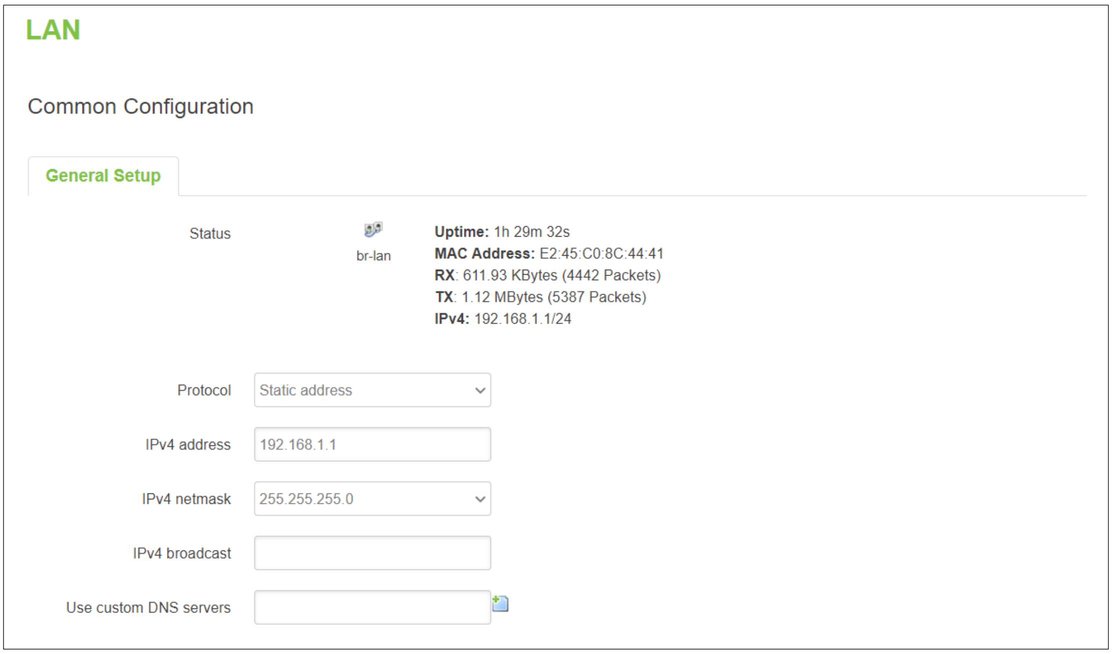
The IPv4 DHCP server is also enabled by default on this interface. It means that any device with IPv4 DHCP client enabled in its Ethernet interface will be assigned a dynamic IP address from the LAN port interface of CWR5805. The default IP address of the IPv4 DHCP server is 192.168.1.1, and the dynamic IP address range starts from 192.168.1.100 to 192.168.1.250.

3.3.3.1 General Setup

In the **General Setup** sub-tab of the Network-Interfaces-LAN tab, you can configure the CWR5805 device's network settings e.g., IP address, IP netmask, IP gateway, and DNS server.

As shown in the Figure below, the Status field currently displays LAN port interface (br-lan) information of Uptime, MAC Address, RX, TX, and IPv4. For a DHCP client, a device connected to a LAN port interface will be assigned an IPv4 address.

Figure 44. Network > LAN > Common Configuration – Static Address



LAN

Common Configuration

General Setup

Status — br-lan

Uptime: 1h 29m 32s
MAC Address: E2:45:C0:8C:44:41
RX: 611.93 KBytes (4442 Packets)
TX: 1.12 MBytes (5387 Packets)
IPv4: 192.168.1.1/24

Protocol: Static address

IPv4 address: 192.168.1.1

IPv4 netmask: 255.255.255.0

IPv4 broadcast:

Use custom DNS servers:

Table 33. Network > LAN > Common Configuration – Static Address

Field	**Value**	**Description**
Protocol	Static address	The protocol is used by the LAN interface. This field currently supports DHCP client and Static address.
IPv4 Address	default: **192.168.1.1**	IPv4 that the router uses on the LAN network.
IPv4 Netmask	default: **255.255.255.0**	IPv4 netmask is used to define how "large" the LAN network is.
IPv4 Gateway	default: **none**	Default IPv4 gateway for LAN network.
IPv4 Broadcast	default: **none**	IP broadcast is used by BOOTP and DHCP clients to find and send requests to their respective servers.
Use Custom DNS servers	ip; default: **none**	Specify DNS server for LAN network.

3.3.3.2 DHCP Server

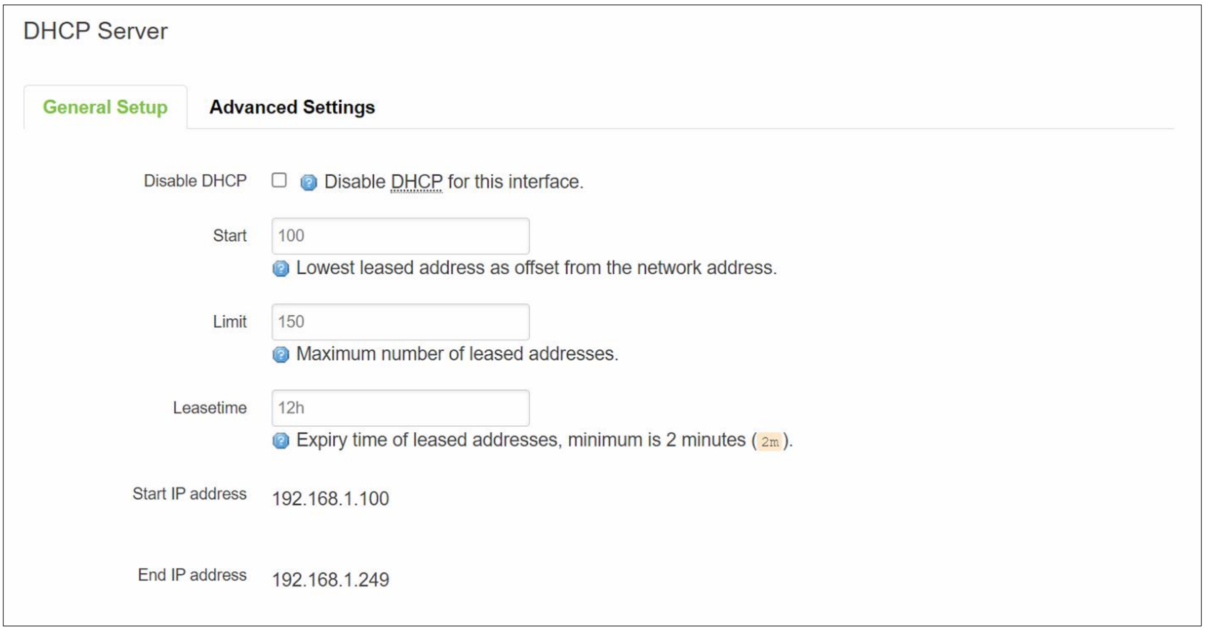
A **DHCP server** is a service that can automatically configure the TCP/IP settings of any device that requests such a service (i.e., connects to the device with the operational DHCP server). If you connect a device that has been configured to obtain an IP address automatically, the DHCP server will lease out an IP address from the available IP pool and the device will be able to communicate within the private network.

The physical network interfaces of Ethernet Adapter (eth1), Wi-Fi 2.4GHz (ATOP_CWR), and Wi-Fi 5GHz (ATOP_CWR) are bridged together. In another word, any IPv4 DHCP client devices connected to a LAN port interface, wireless 2.4GHz/5GHz AP can be assigned a dynamic IPv4 address in the same network domain of 192.168.1.x. This means that these IPv4 DHCP client devices can communicate with each other via the bridged interface (br-lan).

3.3.3.2.1 General Setup

In the **General Setup** inner sub-tab of the DHCP Server section within the Network-Interface-LAN tab. Sub-tabs in the basic setting of the DHCP server service is available.

Figure 45. Network > LAN > DHCP Server > General Setup



DHCP Server

Disable DHCP □ Disable DHCP for this interface.

Start 100
Lowest leased address as offset from the network address.

Limit 150
Maximum number of leased addresses.

Leasetime 12h
Expiry time of leased addresses, minimum is 2 minutes (2m).

Start IP address 192.168.1.100

End IP address 192.168.1.249

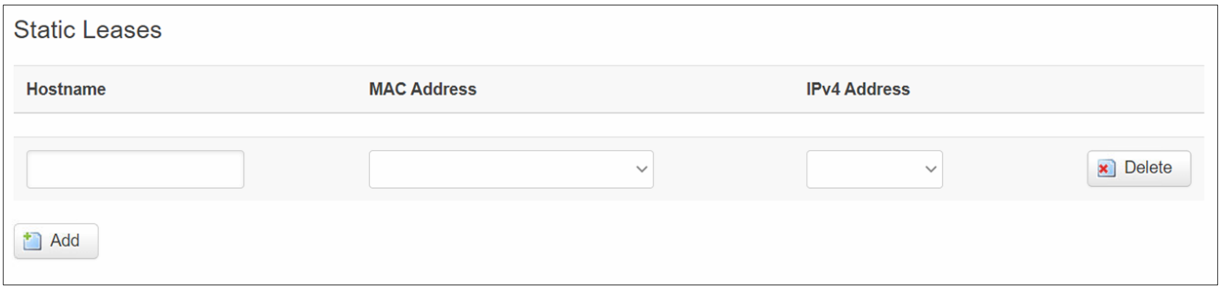
Table 34. Network > LAN > DHCP Server > General Setup

Field	Value	Description
Disable DHCP	default: **disable**	To enable/disable DHCP server for LAN interface.
Start	default: **100**	The starting IP address value.
Limit	default: **150**	Maximum numbers of IP addresses the DHCP server can lease out.
Leasetime	default: **12h**	The duration of an IP address lease. Leased out addresses will expire after the amount of time specified in this field and the device that was using the lease will have to request a new DHCP lease.

3.3.3.2.2 Static Leases

The **Static Leases** section is used to reserve specific IP addresses for specific client devices by binding them to their MAC address. This is useful when you have a stationary device connected to a network that needs to be reached frequently, e.g., printer, IP phone, etc.

Figure 46. Network > LAN > DHCP Server > Static Leases



Static Leases

Hostname	MAC Address	IPv4 Address	
			Delete

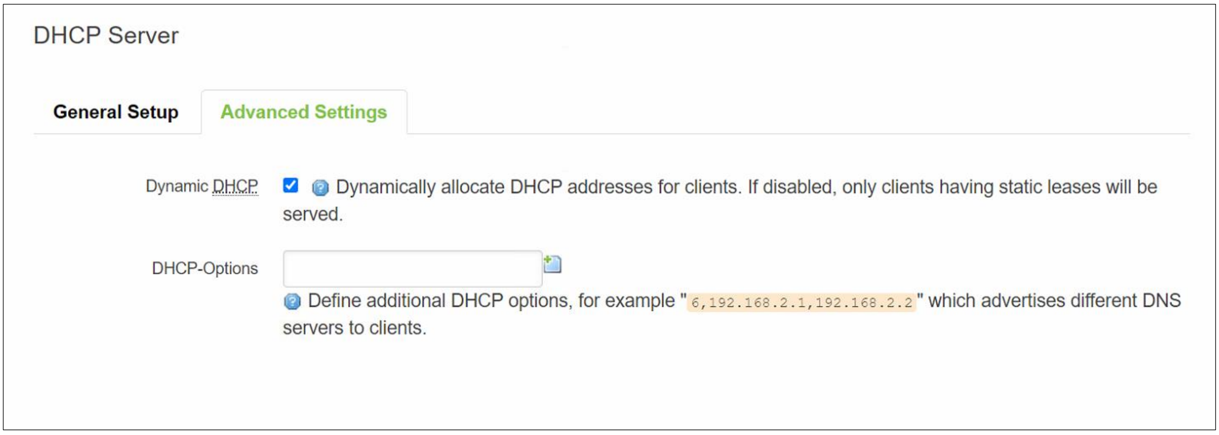
Table 35. Network > LAN > DHCP Server > Static Leases

Field	Description
Hostname	A custom name that will be linked with the device.
MAC-Address	Device's MAC address.
IPv4-Address	The desirable IP address will be reserved for the specified device.
Add	To add a new static IP leased entry.

3.3.3.2.3 Advanced Settings

In the **Advanced Settings** inner sub-tab of the DHCP Server section within Network-Interface-LAN tap-All sub taps, you can configure more complicated settings of the DHCP server service.

Figure 47. Network > LAN > DHCP Server > Advanced Settings



DHCP Server

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

DHCP-Options

Define additional DHCP options, for example "`6,192.168.2.1,192.168.2.2`" which advertises different DNS servers to clients.

Table 36. Network > LAN > DHCP Server > Advanced Settings

Field	Description
Dynamic DHCP	If checked, dynamically allocate DHCP addresses for clients. If not checked, only provides service to static IP address clients.
DHCP-Options	Define additional DHCP options, for example, "192.168.2.1,192.168.2.2" which advertises different DNS servers to clients.

3.3.4 Wireless

In the **Wireless Overview** section within the Network-Wifi sub-menu, you can configure wireless access points and choose the method to scan wireless stations. Here, you can disable or enable WiFi interfaces, or configure each WiFi interface in detail by pressing the Edit button. The configuration webpage of the selected WiFi interface will be initialized.

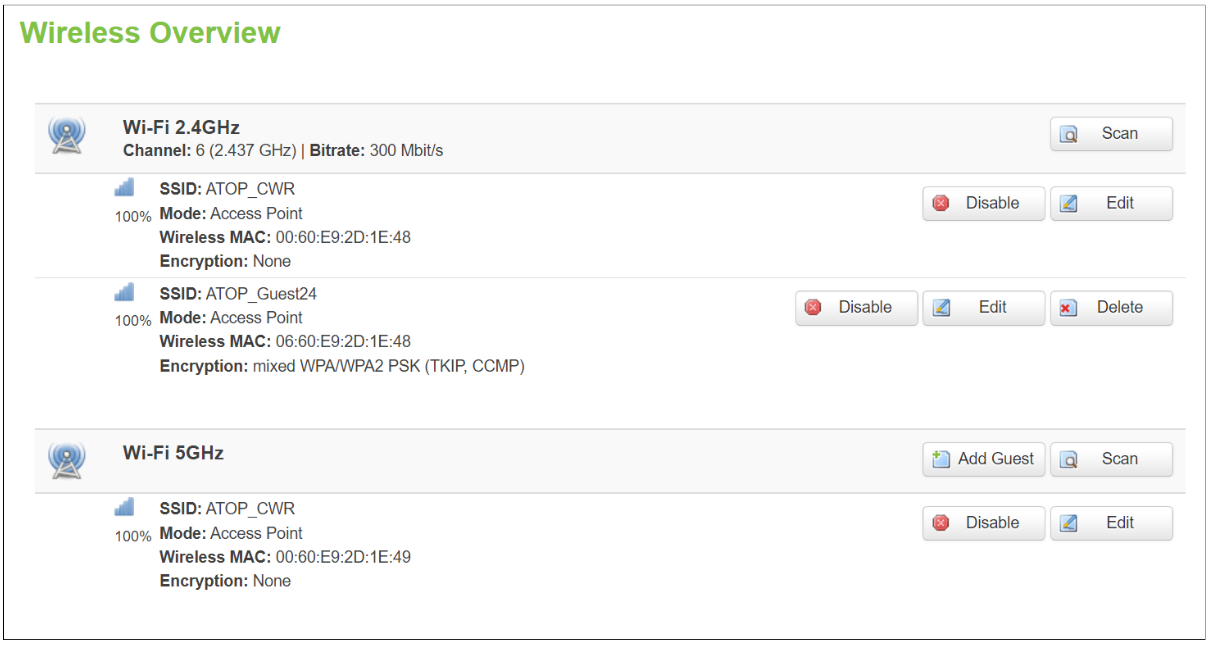
In the **Wifi** sub-menu within the Network menu, you can manage and configure Wi-Fi Access Points (AP) and Wi-Fi Stations (STA). The CWR5805 device supports **IEEE802.11 a/b/g/n/ac** wireless technologies.

3.3.4.1 Wireless Overview

The Wi-Fi 2.4GHz field indicates the status of the Wi-Fi 2.4GHz port interface (wifi0). It contains information about SNR, SSID, mode, bit rate, BSSID, and encryption.

The Wi-Fi 5GHz field indicates the status of the Wi-Fi 5GHz port interface (wifi1). It contains information about SNR, SSID, mode, bit rate, BSSID, and encryption.

Figure 48. Network > Wireless > Wireless Overview



Wireless Overview

Wi-Fi 2.4GHz
Channel: 6 (2.437 GHz) | **Bitrate:** 300 Mbit/s

100%
SSID: ATOP_CWR
Mode: Access Point
Wireless MAC: 00:60:E9:2D:1E:48
Encryption: None

100%
SSID: ATOP_Guest24
Mode: Access Point
Wireless MAC: 06:60:E9:2D:1E:48
Encryption: mixed WPA/WPA2 PSK (TKIP, CCMP)

Wi-Fi 5GHz

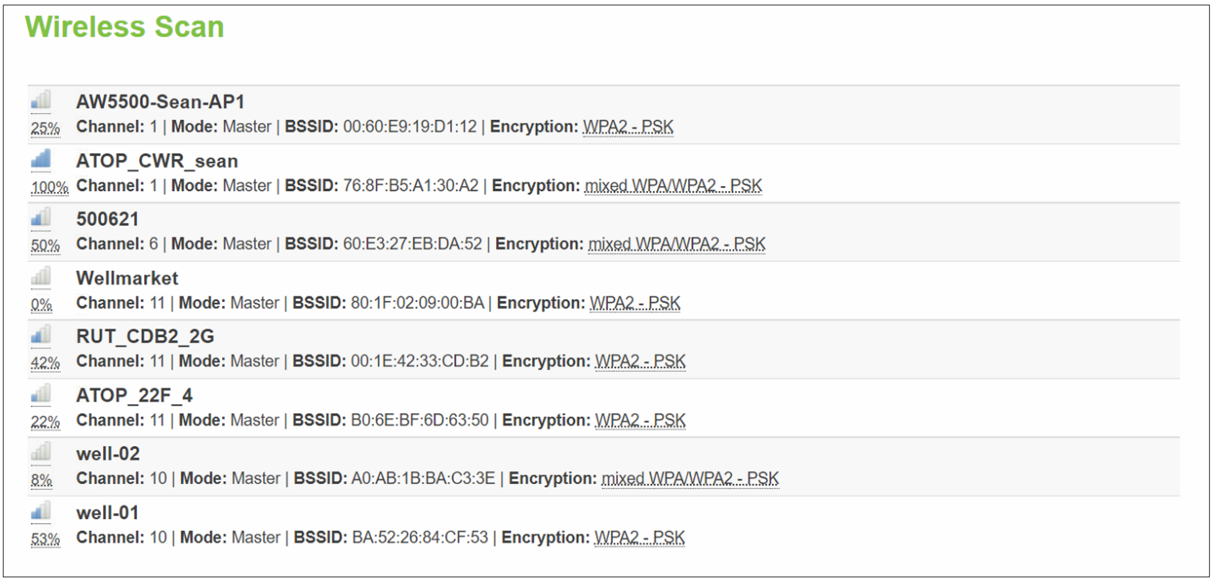
100%
SSID: ATOP_CWR
Mode: Access Point
Wireless MAC: 00:60:E9:2D:1E:49
Encryption: None

Table 37. Network > Wireless > Wireless Overview

Field	Description
Scan	To scan for available wireless stations within the surrounding area.
Enable/Disable	To enable/disable Wi-Fi 2.4GHz/5GHz access point.
Edit	To configure Wi-Fi 2.4GHz/5GHz access point in detail.

Click the **Scan** button to scan the currently available Wi-Fi Access Points in the surrounding area is displayed, as shown in the Figure below. This section will be initialized with you click the “Scan” button in the Wireless Overview section.

Figure 49. Network > Wireless > Wireless Scan



Wireless Scan

AW5500-Sean-AP1
25% **Channel:** 1 | **Mode:** Master | **BSSID:** 00:60:E9:19:D1:12 | **Encryption:** WPA2 - PSK

ATOP_CWR_sean
100% **Channel:** 1 | **Mode:** Master | **BSSID:** 76:8F:B5:A1:30:A2 | **Encryption:** mixed WPA/WPA2 - PSK

500621
50% **Channel:** 6 | **Mode:** Master | **BSSID:** 60:E3:27:EB:DA:52 | **Encryption:** mixed WPA/WPA2 - PSK

Wellmarket
0% **Channel:** 11 | **Mode:** Master | **BSSID:** 80:1F:02:09:00:BA | **Encryption:** WPA2 - PSK

RUT_CDB2_2G
42% **Channel:** 11 | **Mode:** Master | **BSSID:** 00:1E:42:33:CD:B2 | **Encryption:** WPA2 - PSK

ATOP_22F_4
22% **Channel:** 11 | **Mode:** Master | **BSSID:** B0:6E:BF:6D:63:50 | **Encryption:** WPA2 - PSK

well-02
8% **Channel:** 10 | **Mode:** Master | **BSSID:** A0:AB:1B:BA:C3:3E | **Encryption:** mixed WPA/WPA2 - PSK

well-01
53% **Channel:** 10 | **Mode:** Master | **BSSID:** BA:52:26:84:CF:53 | **Encryption:** WPA2 - PSK

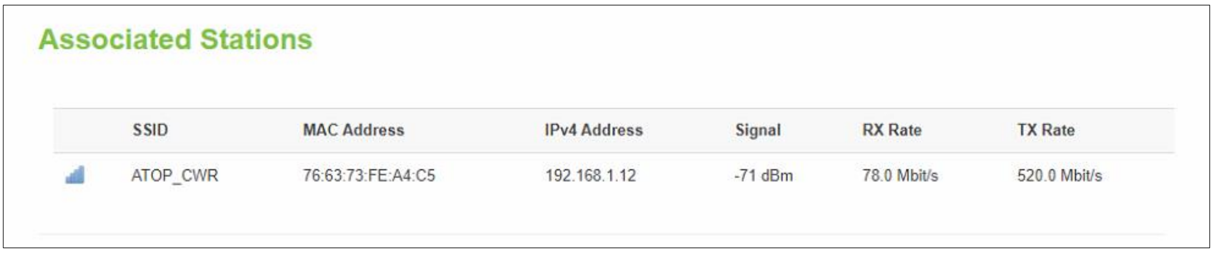
Table 38. Network > Wireless > Wireless Scan

Field	**Description**
Signal Level	Received Signal Strength Indicator (RSSI) level measured in percentage.
SSID	The broadcasted SSID of the wireless network that clients will be connected to.
Channel	Currently used Wi-Fi channel by the access point.
Mode	Current only support Master (access point) mode.
BSSID	MAC address. Identify the basic service sets that are 48-bit labels. It conforms to the MAC-48 convention.
Encryption	Encryption type that Wi-Fi access point use.

3.3.4.2 Associated Stations

The section displays a list of all devices and their MAC address that are maintaining connections with your router right now.

Figure 50. Network > Wireless > Associated Stations



Associated Stations

	SSID	MAC Address	IPv4 Address	Signal	RX Rate	TX Rate
	ATOP_CWR	76:63:73:FE:A4:C5	192.168.1.12	-71 dBm	78.0 Mbit/s	520.0 Mbit/s

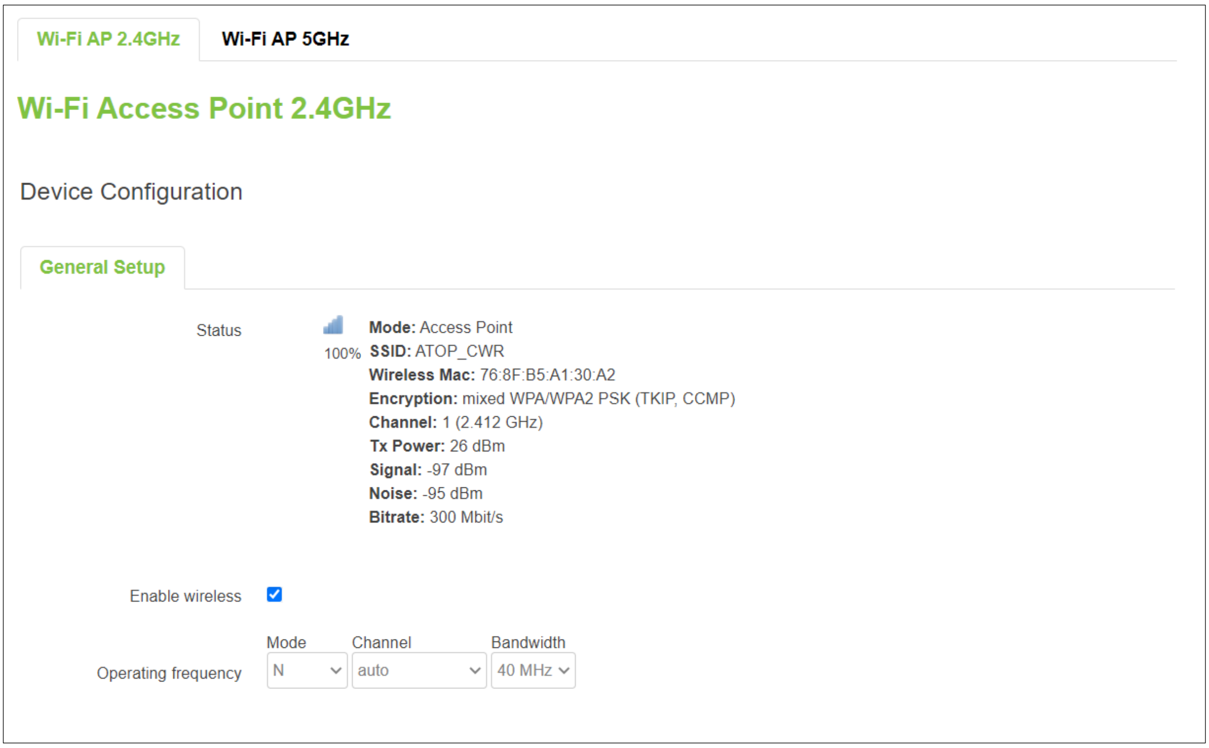
Table 39. Network > Wireless > Associated Stations

Field	**Description**
MAC Address	The MAC address of the associated station.
IPv4 Address	The IP address of the associated station.
Signal	The strength of the wireless between the the CWR5805 and associated station.
Rx Rate	The rate of the received packets from the associated station.
Tx Rate	The rate of the sent packets to the associated station.

3.3.4.3 Device Configuration

In the **Device Configuration** webpage of the Wireless Overview section within the Network-Wifi sub-menu, you can configurethe hardware parameters of the Wi-Fi 2.4GHz/5GHz access point, as shown in the Figure below. This section will be initialized when you click on the “Edit” button in the Wireless Overview section.

Figure 51. Network > Wireless > Edit Wi-Fi AP 2.4GHz



Wi-Fi Access Point 2.4GHz

Device Configuration

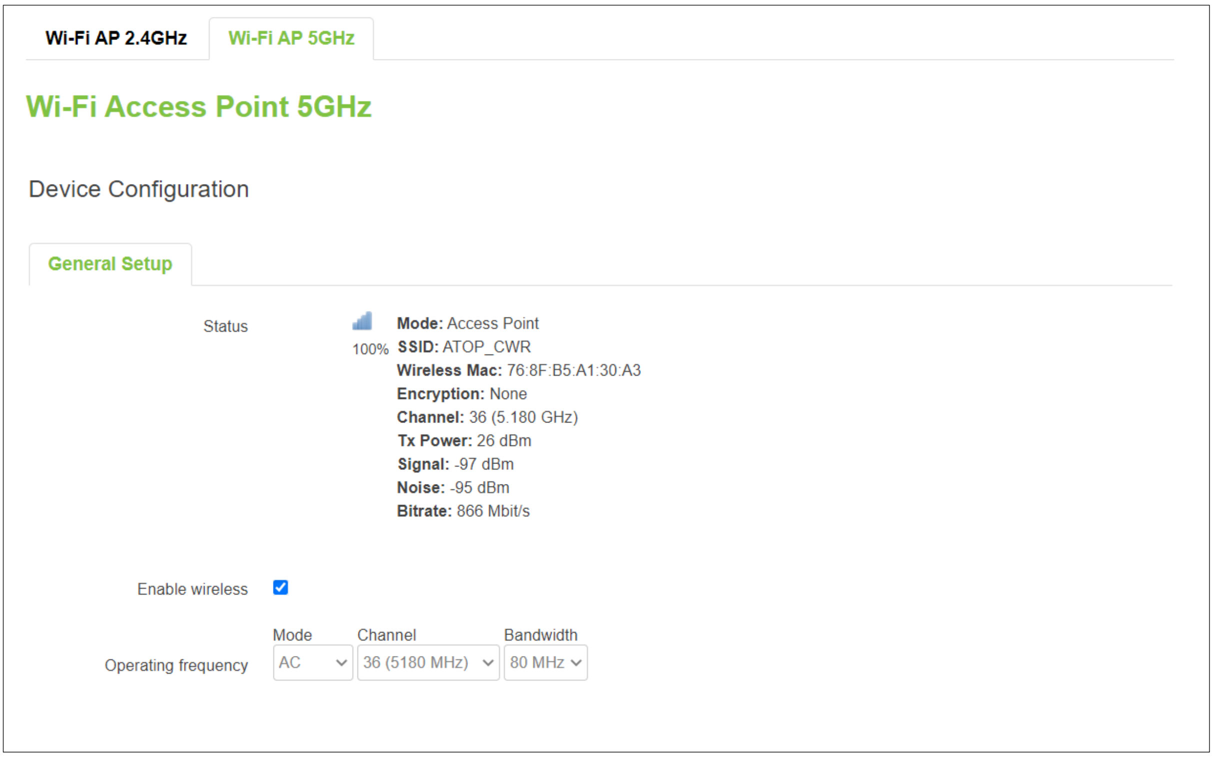
General Setup

Status 100%
Mode: Access Point
SSID: ATOP_CWR
Wireless Mac: 76:8F:B5:A1:30:A2
Encryption: mixed WPA/WPA2 PSK (TKIP, CCMP)
Channel: 1 (2.412 GHz)
Tx Power: 26 dBm
Signal: -97 dBm
Noise: -95 dBm
Bitrate: 300 Mbit/s

Enable wireless ☑

Operating frequency — Mode: N; Channel: auto; Bandwidth: 40 MHz

Figure 52. Network > Wireless > Edit Wi-Fi AP 5GHz



Wi-Fi Access Point 5GHz

Device Configuration

General Setup

Status 100%
Mode: Access Point
SSID: ATOP_CWR
Wireless Mac: 76:8F:B5:A1:30:A3
Encryption: None
Channel: 36 (5.180 GHz)
Tx Power: 26 dBm
Signal: -97 dBm
Noise: -95 dBm
Bitrate: 866 Mbit/s

Enable wireless ☑

Operating frequency — Mode: AC; Channel: 36 (5180 MHz); Bandwidth: 80 MHz

Table 40. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz

Field		Value	Description
Status		-	The status of Wi-Fi 2.4GHz/5GHz access point, which contains signal level, mode, BSSID, encryption, channel, tx-power, SNR, and bitrate info.
Enable Wireless		disable/enable; default: **disable**	To enable/disable Wi-Fi 2.4GHz/5GHz access point.
Operating Frequency -Mode	**2.4GHz**	legacy (b/g) mode and N mode	The wireless protocol is used by the access point.
	5GHz	legacy (a) mode, N mode, and AC mode	
Operating Frequency -Channel	**2.4GHz**	Auto/1/2/3/4/5/6/7/8/9/10/11; default: Auto	
	5GHz	Auto/36/40/44/48/149/153/157/161/165; default: Auto	
Operating Frequency -Width	**2.4GHz**	20/40MHz in N mode	
	5GHz	20/40 MHz in N mode, and 20/40/80/160 MHz in AC mode	

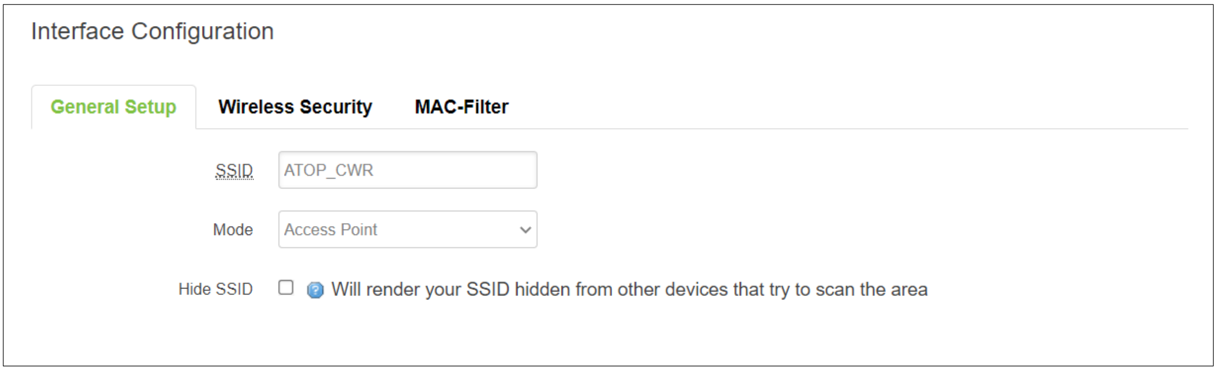
3.3.4.4 Interface Configuration

In the **Interface Configuration** webpage of the Wireless Overview section within the Network-Wifi sub-menu, you can configure the software parameters of the Wi-Fi 2.4GHz/5GHz access point. This section will be initialized with you click the "Edit" button in the Wireless Overview section.

3.3.4.4.1 General Setup

In the **General Setup** sub-tab within the Interface Configuration webpage, you can configure the SSID of Wi-Fi 2.4GHz/5GHz Access Points, as shown in the Figure below.

Figure 53. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > General Setup



Interface Configuration

SSID: ATOP_CWR

Mode: Access Point

Hide SSID: □ Will render your SSID hidden from other devices that try to scan the area

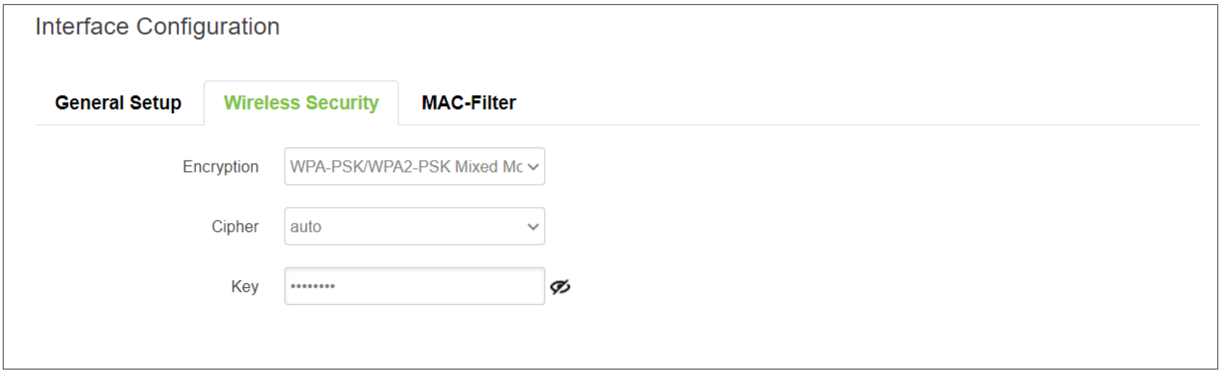
Table 41. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > General Setup

Field	Value	Description
SSID	default: **ATOP_CWR**	The broadcast SSID of the wireless network that clients will be connected to.
Mode	default: **Access Point**	Access Point mode only.
Hide SSID	default: **disable**	Will render your SSID hidden from other devices that try to scan the area.

3.3.4.4.2 Wireless Security

In the **Wireless Security** sub-tab within the Interface Configuration webpage, you can configure the encryption type that will be used in Wi-Fi Access Point 2.4GHz/5GHz, as shown in the Figure below.

Figure 54. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > Wireless Security



Interface Configuration

Encryption: WPA-PSK/WPA2-PSK Mixed Mc

Cipher: auto

Key: ••••••••

Table 42. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > General Setup

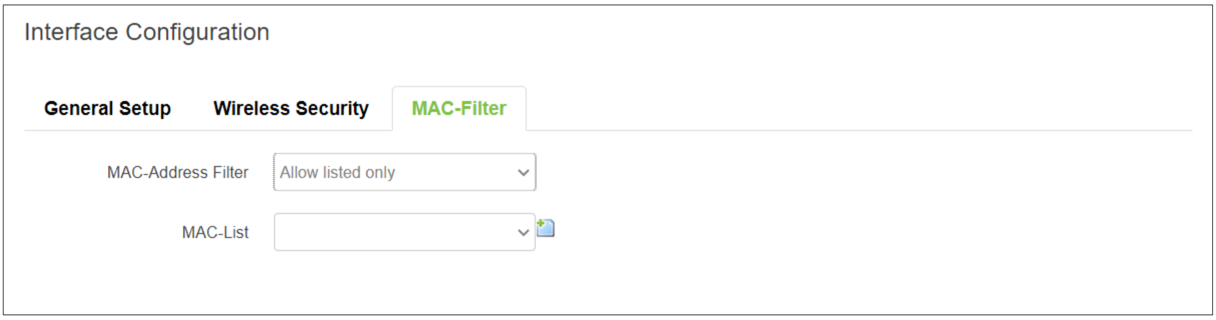
Field	**Value**	**Description**
Encryption	No Encryption/WPA2- /WPA &WPA2/WPA3 default: **No Encryption**	Type of Wi-Fi encryption used.
Cipher*	Auto/Force CCMP/Force TKIP and CCMP default: **auto**	An algorithm for performing encryption or decryption.
Key	default: **none**	A custom passphrase is used for authentication (at least 8 characters long).

*: WPA&WPA2 only

3.3.4.4.3 MAC-Filter

You can define a rule for what to do with the MAC list you have defined. You can either allow only the listed MACs or allow “ALL” but forbid the listed ones.

Figure 55. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > MAC-Filter



Interface Configuration

MAC-Address Filter: Allow listed only

MAC-List:

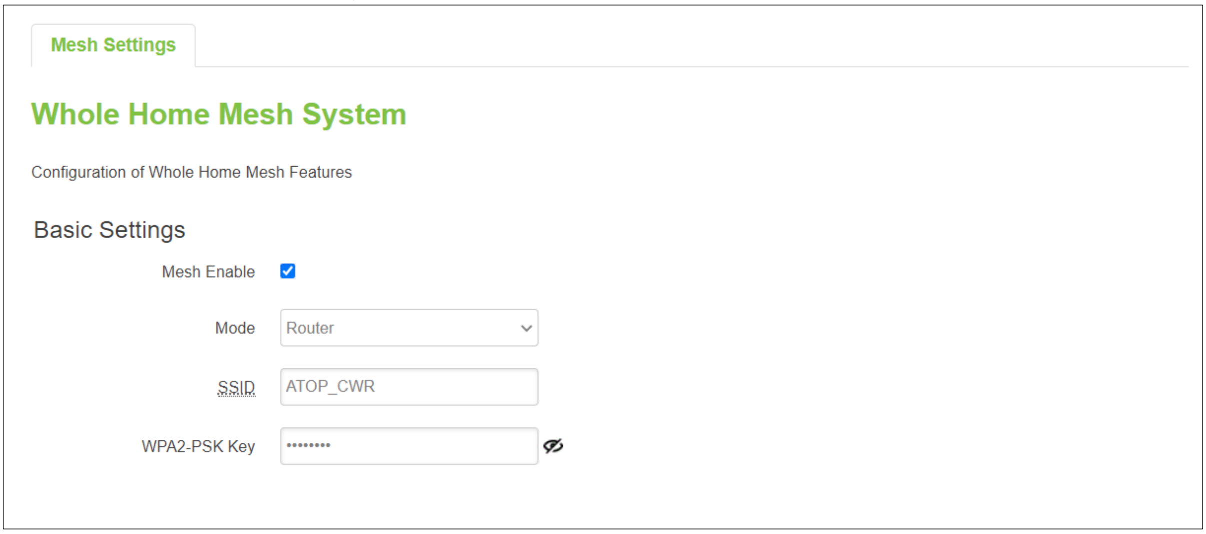
Table 43. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > MAC-Filter

Field	**Value**	**Description**
MAC-Address Filter	disable/Allow listed only/Allow all except listed; default: **disable**	Select MAC address Filter mode.
MAC-List	MAC; default: **none**	Input MAC list.

3.3.5 Mesh

On the **Whole Home Mesh System** webpage, you can build the mesh network with another CWR5805 device. The mesh network must have at least one Central Access Point (CAP) mode CWR5805 device and one Access Point mode CWR5805 device connecting. These settings can be configured on this webpage for CAP mode and AP mode, respectively.

Figure 56. Network > Mesh > Basic Settings



Whole Home Mesh System

Configuration of Whole Home Mesh Features

Basic Settings

Mesh Enable ☑

Mode: Router

SSID: ATOP_CWR

WPA2-PSK Key: ••••••••

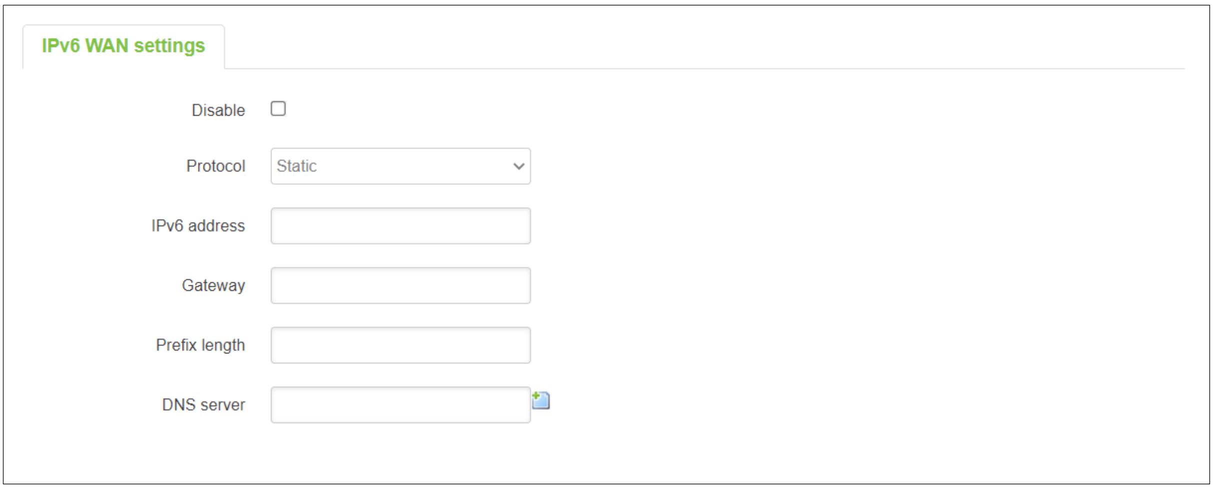
Table 44. Network > Mesh > Basic Settings

Field	Value	Description
Mesh Enable	Disable/Enable; default: **disable**	To enable/disable the mesh feature.
Mode	Router/Satellite; default: Router	Select mesh mode of Central Access Point or Access Point.
SSID	default: **ATOP_CWR**	The broadcasted SSID of the mesh network. Both CAP mode and AP mode CWR5805 devices must be set to the same ESSID.
WPA2-PSK Key	default: **ATOP_CWR**	Specifies the encryption key of WPA2-PSK. Both CAP mode and AP mode CWR5805 devices must use the same WPA2-PSK key.

3.3.6 IPv6

In the **IPv6** webpage, you can manage the IPv6 IP settings.

Figure 57. Network > IPv6



Disable ☐

Protocol: Static

IPv6 address:

Gateway:

Prefix length:

DNS server:

Table 45. Network > IPv6

Field	Value	Description
Disable	Disable/Enable; default: **Enable**	Check Disable box to disable IPv6.
Protocol	DHCPv6/Static; default: DHCPv6	The protocol is used by the WAN interface.
IPv6 address	ip6; default: **none**	Your router's address on the WAN network.
Gateway	ip6; default: **none**	The IPv6 address gateway of this interface. An interface's gateway is the default next-hop address to access other networks.
Prefix length	integer [1 - 64]; default: **none**	Like an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address.
DNS server	ip6; default: **none**	By entering custom DNS servers the router will take care of the hostname resolution. You can enter multiple DNS servers to provide redundancy in case one of the servers fails.

3.3.7 VLAN

On this page, you can configure your Virtual LAN settings.

3.3.7.1 Interface Based

Figure 58. Network > VLAN > Interface Based

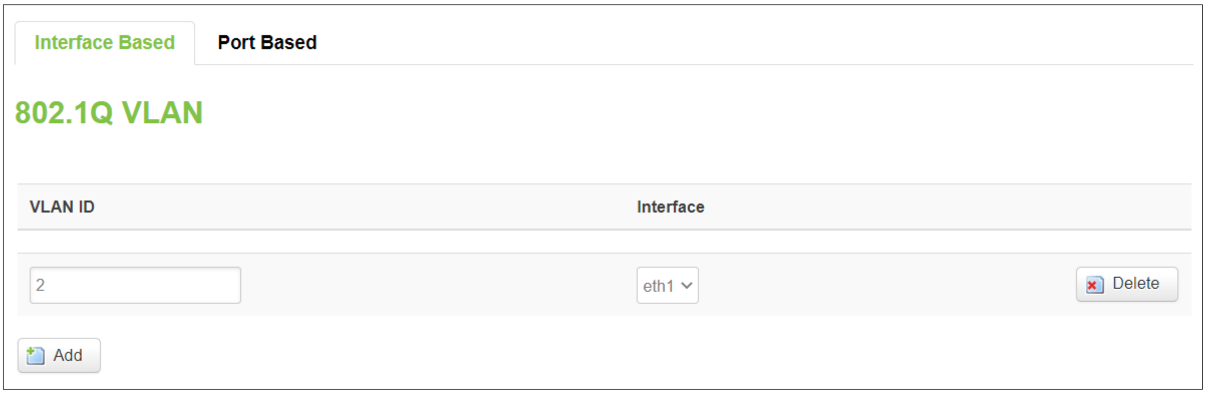


Table 46. Network > VLAN > Interface Based

Field	Value	Description
VLAN ID	integer [1 - 4094]; default: **none**	VLAN identification number.
Interface	eth0/eth1 default: **none**	Select to which interface will be applied.

3.3.8 LB (Load Balancing) and Failover

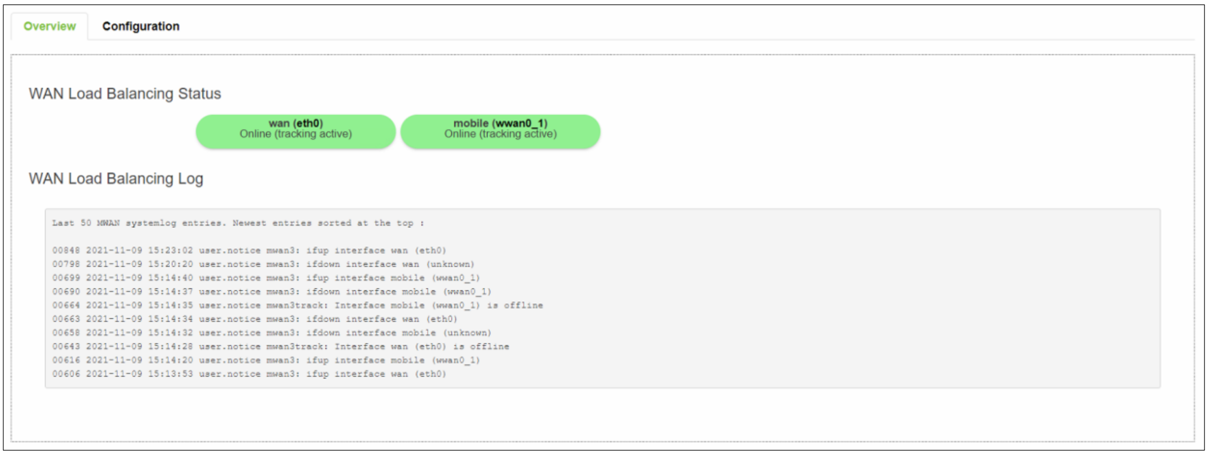
Load balancing (LB) lets yous create rules that divide the traffic between different interfaces. In this case, there are the WAN and the Mobile interfaces. The LB mechanism provides the data traffic balancing control between WAN and 5G/LTE connections.

The **Failover** mechanism provides the data traffic redirection to the Mobile port interface while the WAN interface is disconnected, and versa.

3.3.8.1 Overview Tab

The **Overview** tab contains the Interface Status and Detailed Status sub-tabs which shows the current status info of each configured Multi-WAN interfaces.

Figure 59. Network > LB and Failover > Overview



WAN Load Balancing Status

wan (eth0)
Online (tracking active)

mobile (wwan0_1)
Online (tracking active)

WAN Load Balancing Log

```
Last 50 MWAN systemlog entries. Newest entries sorted at the top :

00848 2021-11-09 15:23:02 user.notice mwan3: ifup interface wan (eth0)
00798 2021-11-09 15:20:20 user.notice mwan3: ifdown interface wan (unknown)
00699 2021-11-09 15:14:40 user.notice mwan3: ifup interface mobile (wwan0_1)
00690 2021-11-09 15:14:37 user.notice mwan3: ifdown interface mobile (wwan0_1)
00664 2021-11-09 15:14:35 user.notice mwan3track: Interface mobile (wwan0_1) is offline
00663 2021-11-09 15:14:34 user.notice mwan3: ifdown interface wan (eth0)
00658 2021-11-09 15:14:32 user.notice mwan3: ifdown interface mobile (unknown)
00643 2021-11-09 15:14:28 user.notice mwan3track: Interface wan (eth0) is offline
00616 2021-11-09 15:14:20 user.notice mwan3: ifup interface mobile (wwan0_1)
00606 2021-11-09 15:13:53 user.notice mwan3: ifup interface wan (eth0)
```

Table 47. Network > LB and Failover > Overview

Field	Description
wan (eth0)	Current multi-wan status (Online/Offline/Disabled) of the WAN port interface.
mobile (wwan0)	Current multi-wan status (Online/Offline/Disabled) of the mobile interface.

The WAN Interface Syslog (System log) section shows recent Multi-WAN interface log messages.

In the Detailed Status sub-tab, the Multi-WAN interfaces status, configured policies, activated rules, and local connected networks information are displayed.

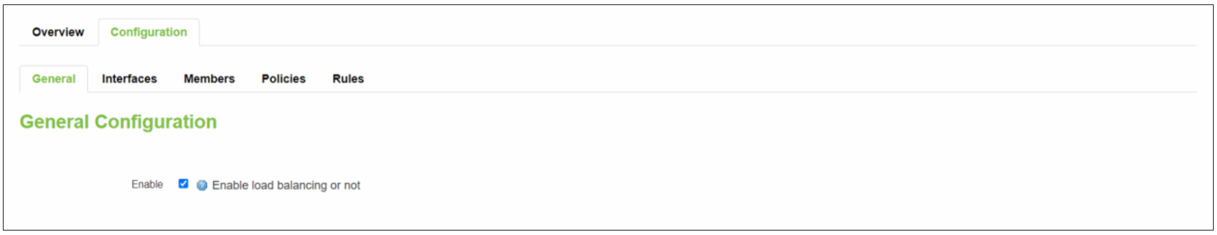
3.3.8.2 Configuration

The **Configuration** tab consists of five sub-tabs, which are General, Interfaces, Members, Policies, and rules.

3.3.8.2.1 General

In **General** sub-tab, the load balancing feature is disabled by default. You can check the Enable field to start the load balancing service.

Figure 60. Network > LB and Failover > Configuration > General



General Configuration

Enable ☑ Enable load balancing or not

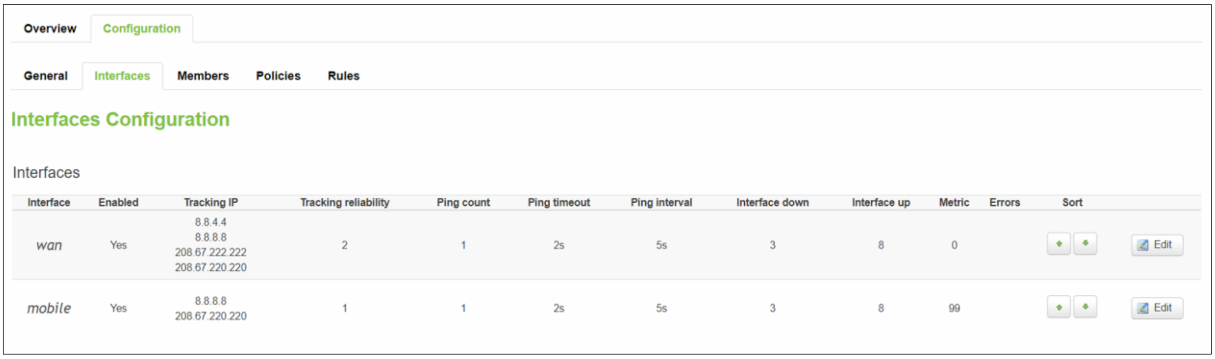
Table 48. Network > LB and Failover > Configuration > General

Field	Value	Description
Enabled	default: **disable**	Enable/Disable load balancing service.

3.3.8.2.2 Interfaces - Overivew

In **Interfaces** sub-tab, you can configure each WAN/Mobile interface uder Interfaces section and defines how each WAN/Mobile interface is tested for up/down status. Each interface section must have a name that corresponds with the interface name in you's network configuration.

Figure 61. Network > LB and Failover > Configuration > Interfaces



Interfaces Configuration

Interfaces

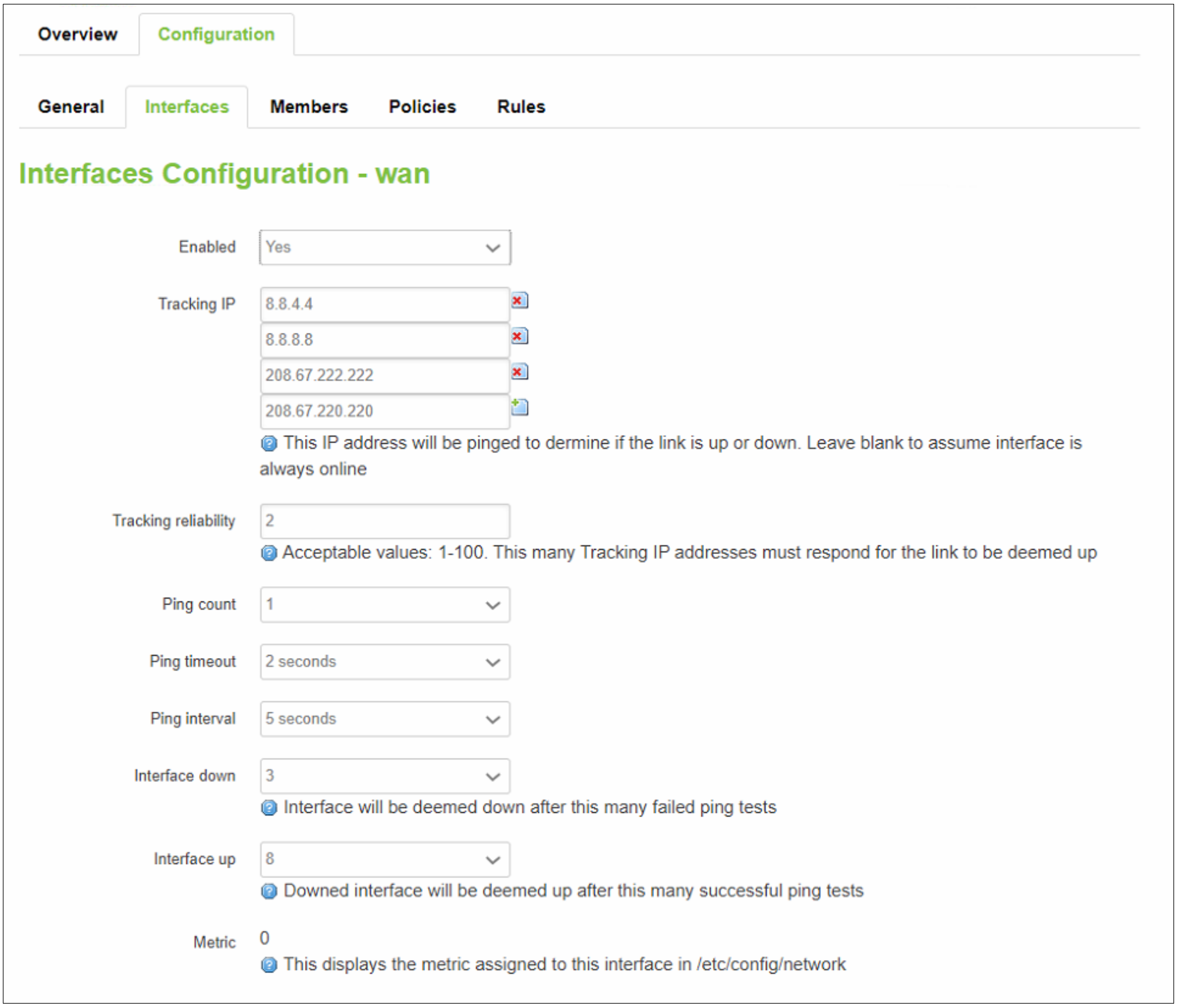
Interface	Enabled	Tracking IP	Tracking reliability	Ping count	Ping timeout	Ping interval	Interface down	Interface up	Metric	Errors	Sort	
wan	Yes	8.8.4.4 8.8.8.8 208.67.222.222 208.67.220.220	2	1	2s	5s	3	8	0		↑ ↓	Edit
mobile	Yes	8.8.8.8 208.67.220.220	1	1	2s	5s	3	8	99		↑ ↓	Edit

Table 49. Network > LB and Failover > Configuration > Interfaces

Field	Description
Interface	The interface name as shown in Network -> Interfaces list (if using a PPPoE interface, the interface name specified here should be the underlying interface name, not the "pppoe-…" interface name).
Enabled	Enable/Disable load balancing service on this interface.
Tracking IP	The hosts to test if the interface is still alive. If this value is missing the interface is always considered up.
Tracking Reliability	A number of tracking IP hosts that must reply for the test to be considered as successful. Ensure that there are at least these many tracking IP hosts defined, or the interface will always be considered down.
Ping Count	The number of checks to send to each host with each test.
Ping Timeout	The number of seconds to wait for an echo-reply after an echo-request.
Ping Interval	The number of seconds between each test.
Interface down	The number of failed tests to considered link as dead.
Interface Up	The number of successful tests to considered link as alive.
Metric	The metric value of this interface.
Sort	To sort the port forward rules. The top classification rule means highest priority.

3.3.8.2.3 Interfaces - Configuration

Figure 62. Network > LB and Failover > Configuration > Interfaces > Edit



Interfaces Configuration - wan

Enabled: Yes

Tracking IP: 8.8.4.4; 8.8.8.8; 208.67.222.222; 208.67.220.220

This IP address will be pinged to dermine if the link is up or down. Leave blank to assume interface is always online

Tracking reliability: 2

Acceptable values: 1-100. This many Tracking IP addresses must respond for the link to be deemed up

Ping count: 1

Ping timeout: 2 seconds

Ping interval: 5 seconds

Interface down: 3

Interface will be deemed down after this many failed ping tests

Interface up: 8

Downed interface will be deemed up after this many successful ping tests

Metric: 0

This displays the metric assigned to this interface in /etc/config/network

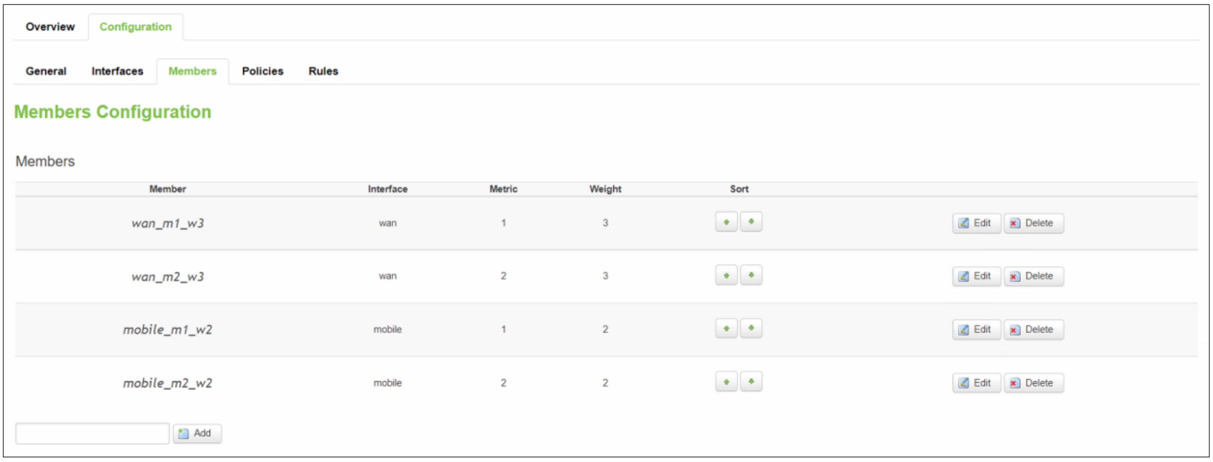
Table 50. Network > LB and Failover > Configuration > Interfaces > Edit

Field	Value	Description
Enabled*	no/yes; default: **no**	Enable/Disable load balancing service on this nterface.
Tracking IP	ip; default: **8.8.8.8/8.8.4.4**	The hosts to test if the interface is still alive. If this value is missing the interface is always considered up.
Tracking Reliability	integer [1 – 100]; default: **1**	The number of tracking IP hosts that must reply for the test to be considered as successful. Ensure that there are at least these many tracking IP hosts defined, or the interface will always be considered down.
Ping Count	integer [1 – 5]; default: **1**	The number of checks to send to each host with each test.
Ping Timeout	intger [1 – 10]; default: **1**	The number of seconds to wait for an echo-reply after an echo-request.
Ping Interval	1/3/5/10/20/30 seconds 1/5/10/15/30 minitues 1 hour default: **2 seconds**	The number of seconds between each test.
Interface down	integer [1 – 10]; default: **3**	The number of failed tests to considered link as dead.
Interface Up	integer [1 – 10]; default: **8**	The number of successful tests to considered link as alive.
Metric	Same as configured	The metric value of this interface.

3.3.8.2.4 Members – Overview

Each member represents an interface with a metric and a weight value. Members are referenced in policies to define a pool of interfaces with corresponding metric and load-balancing weight. Members can not be used for rules directly.

Figure 63. Network > LB and Failover > Configuration > Members



Members Configuration

Members

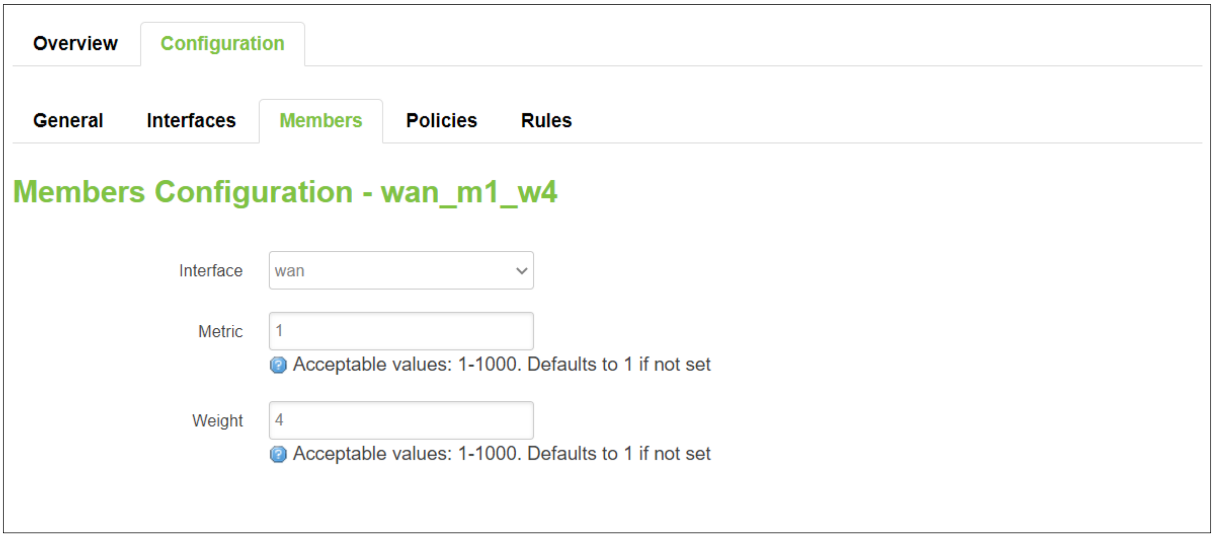
Member	Interface	Metric	Weight	Sort	
wan_m1_w3	wan	1	3		Edit Delete
wan_m2_w3	wan	2	3		Edit Delete
mobile_m1_w2	mobile	1	2		Edit Delete
mobile_m2_w2	mobile	2	2		Edit Delete

Table 51. Network > LB and Failover > Configuration > Members

Field	Description
Member	A name to define this member profile.
Interface	Member applies to this interface (use the same interface name as used in the Interface Configuration section, above).
Metric	Members within one policy with a lower metric have precedence over higher metric members.
Weight	Members with same metric will distribute the load based on this weight value.

3.3.8.2.5 Member – Configuration

Figure 64. Network > LB and Failover > Configuration > Members > Edit



Members Configuration - wan_m1_w4

Interface: wan

Metric: 1

Acceptable values: 1-1000. Defaults to 1 if not set

Weight: 4

Acceptable values: 1-1000. Defaults to 1 if not set

Table 52. Network > LB and Failover > Configuration > Members > Edit

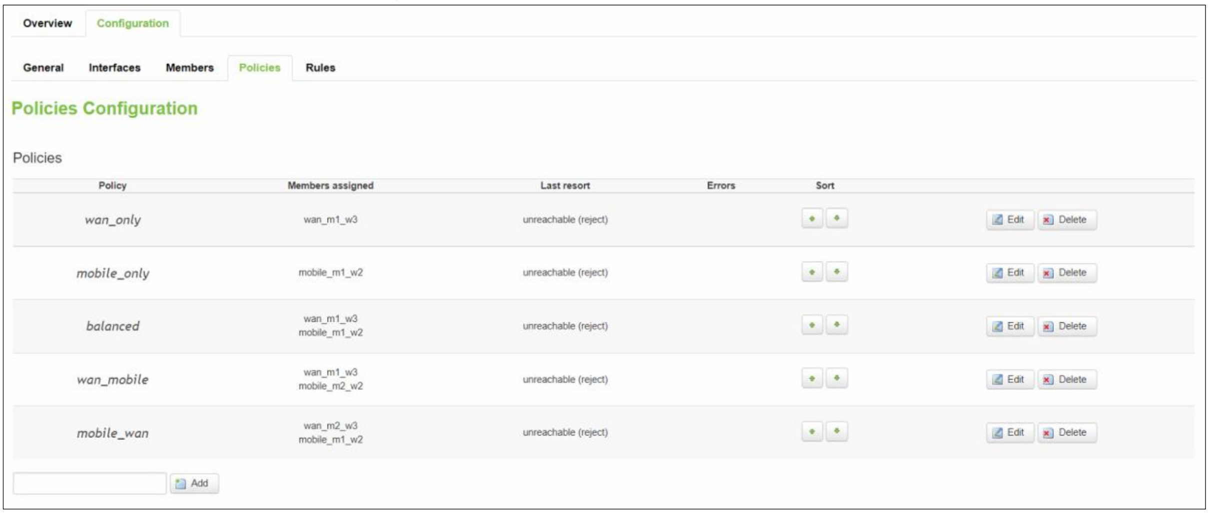
Field	Value	Description
Interface	wan/mobile; default: **wan**	The VRRP interface.
Metric	integer [1 – 1000]; default: **1**	The metric value of this interface. A larger number means higher priority. Used as a sorting measure. If a packet is routed with two rules, the higher metric will be chosen first.
Weight	integer [1 – 1000]; default: 4	A smaller number means lower weight.

3.3.8.2.6 Policies - Overview

Policies define how traffic is routed through different WAN interfaces. Every policy has at least one or more members assigned to it, which defines the policy's traffic behavior. If a policy has a single member, traffic will only go out through that member. If a policy has more than one member, it wills either load-balance among members or uses one member as a primary but fail-over to another, depending on how the members are configured.

If there is more than one member assigned to a policy, members within the policy with a lower metric have precedence over higher metric members. Members with the same metric will load-balance. Load-balancing members (with the same metric) will distribute the load based on assigned weight values.

Figure 65. Network > LB and Failover > Configuration > Policies



Policies Configuration

Policies

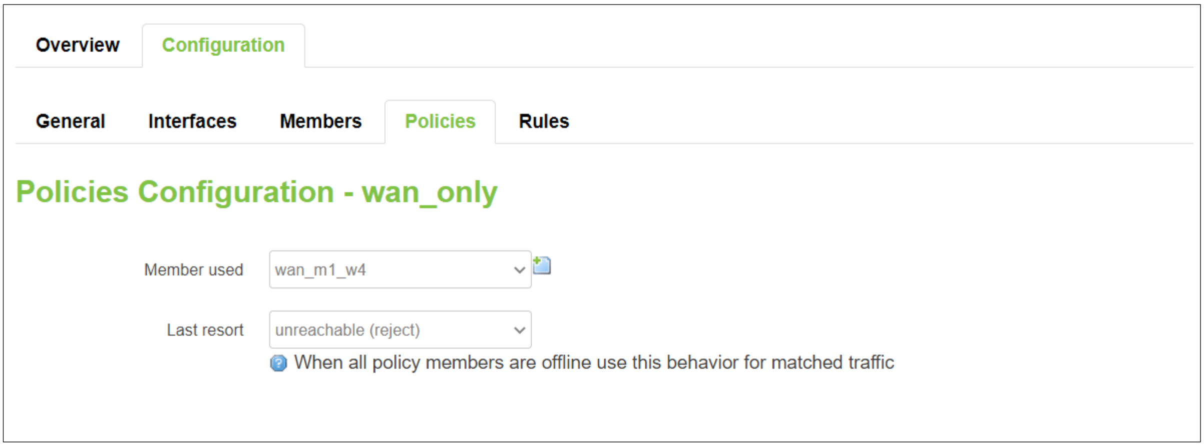
Policy	Members assigned	Last resort	Errors	Sort	
wan_only	wan_m1_w3	unreachable (reject)			Edit Delete
mobile_only	mobile_m1_w2	unreachable (reject)			Edit Delete
balanced	wan_m1_w3 mobile_m1_w2	unreachable (reject)			Edit Delete
wan_mobile	wan_m1_w3 mobile_m2_w2	unreachable (reject)			Edit Delete
mobile_wan	wan_m2_w3 mobile_m1_w2	unreachable (reject)			Edit Delete

Table 53. Network > LB and Failover > Configuration > Policies

Field	Description
Policy	A name to define this policy profile.
Member Assigned	Member's name is assigned to this policy.
Last Resort	If a traffic rule matches a policy, but all the members (interfaces) for that policy are down, the exit strategy for that policy will default to “unreachable”. Valid values are blackhole, unreachable, or default.

3.3.8.2.7 Policies – Configuration

Figure 66. Network > LB and Failover > Configuration > Policies > Edit/Add



Policies Configuration - wan_only

Member used: wan_m1_w4

Last resort: unreachable (reject)

When all policy members are offline use this behavior for matched traffic

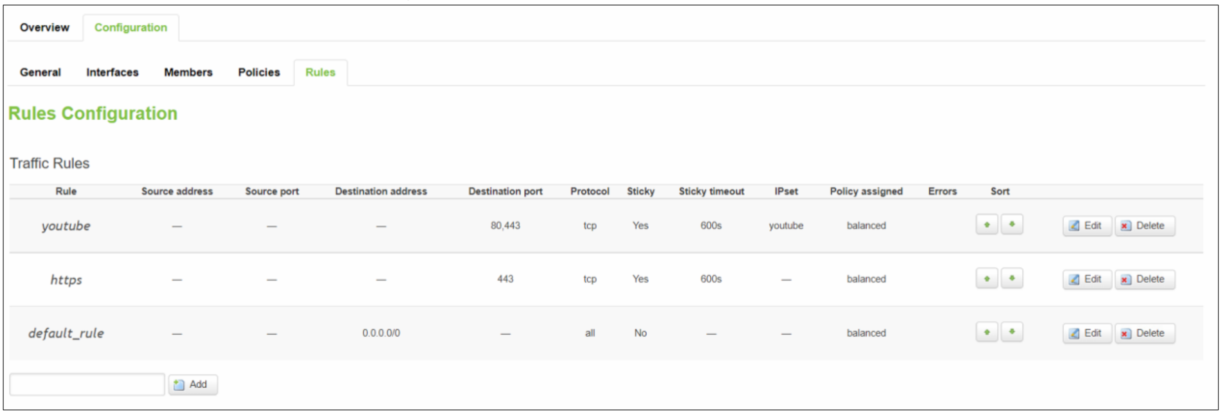
Table 54. Network > LB and Failover > Configuration > Policies > Edit/Add

Field	Description
Member used	The member assigned to this policy.
Last resort	Determine the fallback routing behavior if all WAN members in the policy are down.

3.3.8.2.8 Rules - Overview

A r**ule** describes what traffic to match and what policy to assign for that traffic.

Figure 67. Network > LB and Failover > Configuration > Rules



Rules Configuration

Traffic Rules

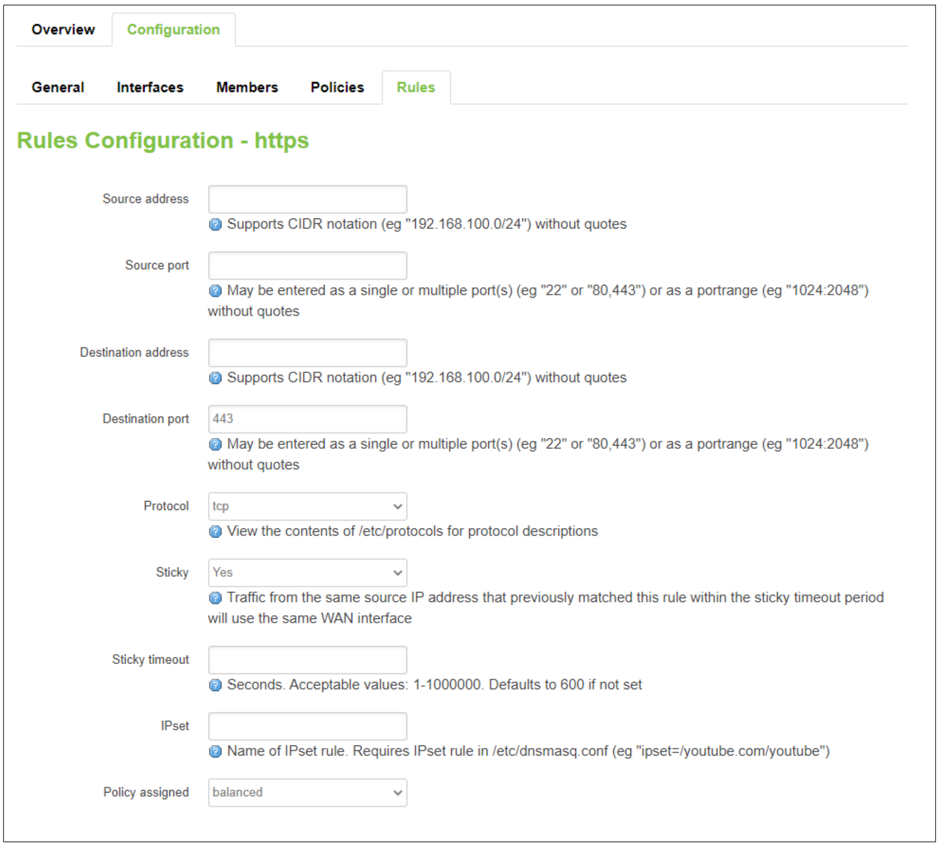
Rule	Source address	Source port	Destination address	Destination port	Protocol	Sticky	Sticky timeout	IPset	Policy assigned	Errors	Sort	
youtube	—	—	—	80,443	tcp	Yes	600s	youtube	balanced			Edit Delete
https	—	—	—	443	tcp	Yes	600s	—	balanced			Edit Delete
default_rule	—	—	0.0.0.0/0	—	all	No	—	—	balanced			Edit Delete

Table 55. Network > LB and Failover > Configuration > Rules

Field	Description
Rule	A name to define this rule profile.
Source Address	Match traffic from the specified source IP address.
Source Port	Match traffic from the specified source port or port range, if the relevant protocol is specified.
Source Address	Match traffic from the specified source IP address.
Source Port	Match traffic from the specified source port or port range, if the relevant protocol is specified.
Dest. Address	Match traffic directed to the specified destination IP address.
Dest. Port	Match traffic directed to the given destination port or port range, if the relevant protocol is specified.
Protocol	Match traffic using the given protocol. Can be one of TCP, UDP, ICMP, or all or it can be a numeric value, representing one of these protocols or a different one.
Sticky	Allow traffic from the same source IP address within the timeout limit to use the same WAN interface as a prior session.
Sticky Timeout	Stickiness timeout value in seconds.

3.3.8.2.9 Rules – Configuration

Figure 68. Network > LB and Failover > Configuration > Rules > Edit/Add



Rules Configuration - https

Source address:
Supports CIDR notation (eg "192.168.100.0/24") without quotes

Source port:
May be entered as a single or multiple port(s) (eg "22" or "80,443") or as a portrange (eg "1024:2048") without quotes

Destination address:
Supports CIDR notation (eg "192.168.100.0/24") without quotes

Destination port: 443
May be entered as a single or multiple port(s) (eg "22" or "80,443") or as a portrange (eg "1024:2048") without quotes

Protocol: tcp
View the contents of /etc/protocols for protocol descriptions

Sticky: Yes
Traffic from the same source IP address that previously matched this rule within the sticky timeout period will use the same WAN interface

Sticky timeout:
Seconds. Acceptable values: 1-1000000. Defaults to 600 if not set

IPset:
Name of IPset rule. Requires IPset rule in /etc/dnsmasq.conf (eg "ipset=/youtube.com/youtube")

Policy assigned: balanced

Table 56. Network > LB and Failover > Configuration > Rules > Edit/Add

Field	**Value**	**Description**
Source Address	IP/submask; default: **none**	Match traffic from the specified source IP address.
Source Port	port; default: **none**	Match traffic from the specified source port or port range, if the relevant protocol is specified.
Destination Address	IP/submask; default: **none**	Match traffic directed to the specified destination IP address.
Destination Port	port; default: **none**	Match traffic directed to the given destination port or port range, if the relevant protocol is specified.
Protocol	TCP/UDP/ICMP; default: **TCP**	Match traffic using the given protocol. Can be one of TCP, UDP, ICMP, or all or it can be a numeric value, representing one of these protocols or a different one.
Sticky	default: yes	Allow traffic from the same source IP address within the timeout limit to use the same WAN interface as a prior session.
Sticky Timeout	integer [1 - 1000000]; default: **600**	Stickiness timeout value in seconds.
IPset	string; default: **none**	Match traffic directed at the given destination domain name address to an ipset.
Policy assigned	default: **balanced**	Type of the policy assigned.

3.3.9 Firewall

The CWR5805 device uses a standard Linux **iptables** package as its firewall, which uses routing chains and policies to facilitate control over inbound and outbound traffic.

3.3.9.1 General Settings

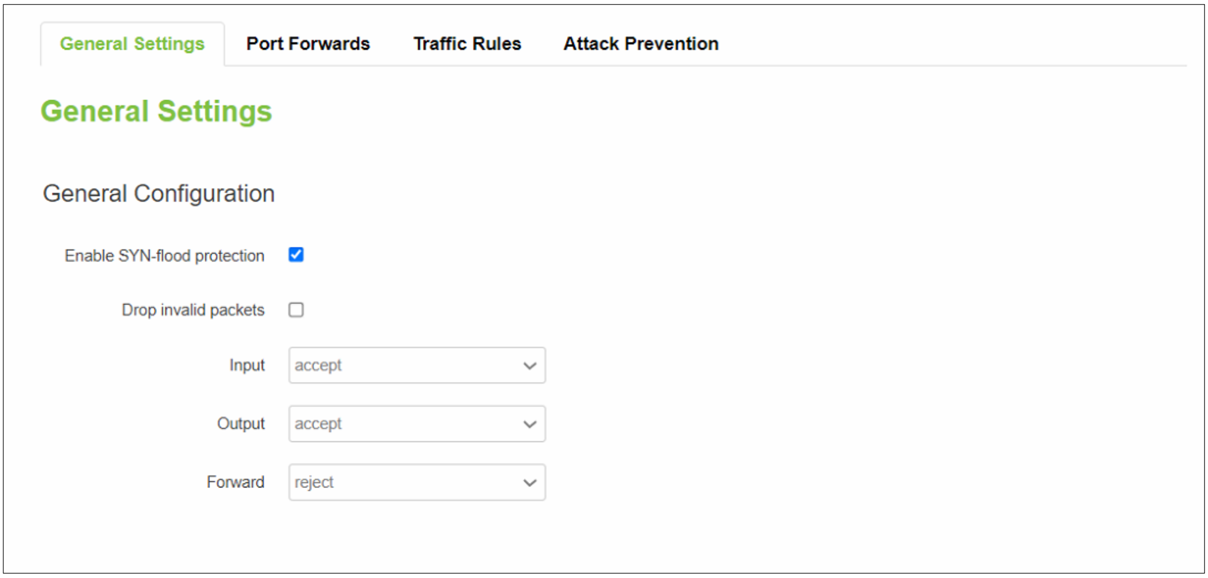
3.3.9.1.1 General Configuration

The **General Settings** tab is used to configure the main policies of the CWR5805 device's firewall. The firewall creates zones over network interfaces to control network traffic flow.

The value’s explanation of Input, Output, and Forward fields is as below:

- Accept - packet gets to continue down to the next chain.
- Drop - packet is stopped and deleted.
- Reject - packet is stopped, deleted and, and differently from Drop, an ICMP packet containing a message.

Figure 69. Network > Firewall > General Settings



General Settings

General Configuration

Enable SYN-flood protection ☑

Drop invalid packets □

Input: accept

Output: accept

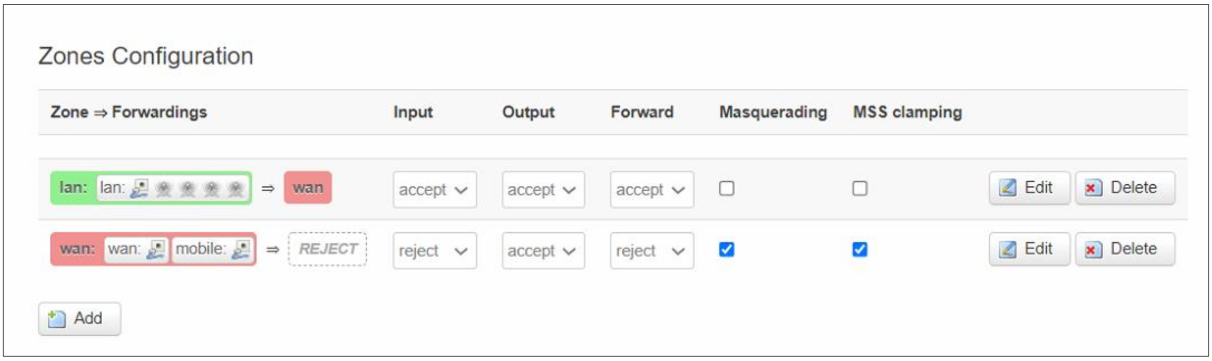
Forward: reject

Table 57. Network > Firewall > General Settings

Field	Value	Description
Enable SYN-flood Protection	default: enable	To enable/disable SYN-flood protection.
Drop Invalid Packets	default: disable	A “Drop” action is performed on a packet that is determined to be invalid.
Input	default: accept	Action that is to be performed for packets that pass through the Input chain.
Output	default: accept	Action that is to be performed for packets that pass through the Output chain.
Forward	default: reject	Action that is to be performed for packets that pass through the Forward chain.

3.3.9.1.2 Zones Configuration

Figure 70. Network > Firewall > General Settings > Zone Configuration



Zones Configuration

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping		
lan: lan: ⇒ wan	accept	accept	accept	□	□	Edit	Delete
wan: wan: mobile: ⇒ REJECT	reject	accept	reject	☑	☑	Edit	Delete

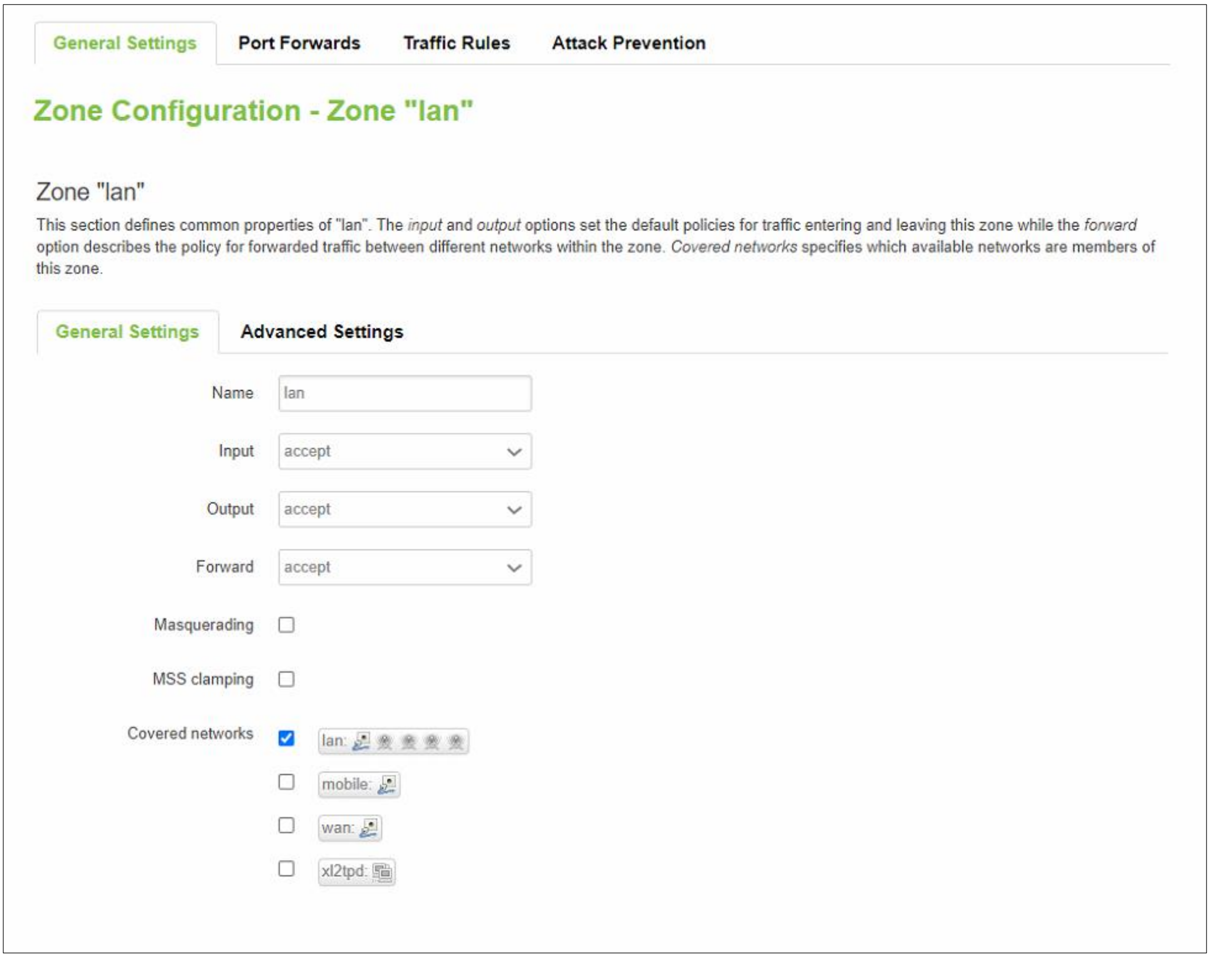
Table 58. Network > Firewall > General Settings > Zone Configuration

Field	Description
Zone➔Forwardings	The zone forwarding contains the source zone from which data packets will redirect and the destination zone to which data packets will be redirected.
Input	Action that is to be performed for packets that pass through the Input chain.
Output	Action that is to be performed for packets that pass through the Output chain.
Forward	Action that is to be performed for packets that pass through the Forward chain.
Masquerading	Specifies whether outgoing zone traffic should be masqueraded. This is typically enabled on the WAN zone.
MSS Clamping	To enable/disable MSS clamping for outgoing zone traffic.

3.3.9.1.3 Zones Configuration - Zone "lan”

Choose the firewall zone that you want to assign to the LAN interface or select “unspecified” to remove the LAN interface from the associated zone, or fill out the create field to define a new zone and attach it to the LAN interface.

Figure 71. Network > Firewall > General Settings > Zone Configuration > Zone “Lan”



Zone Configuration - Zone "lan"

Zone "lan"

This section defines common properties of "lan". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are members of this zone.

Name: lan

Input: accept

Output: accept

Forward: accept

Masquerading: □

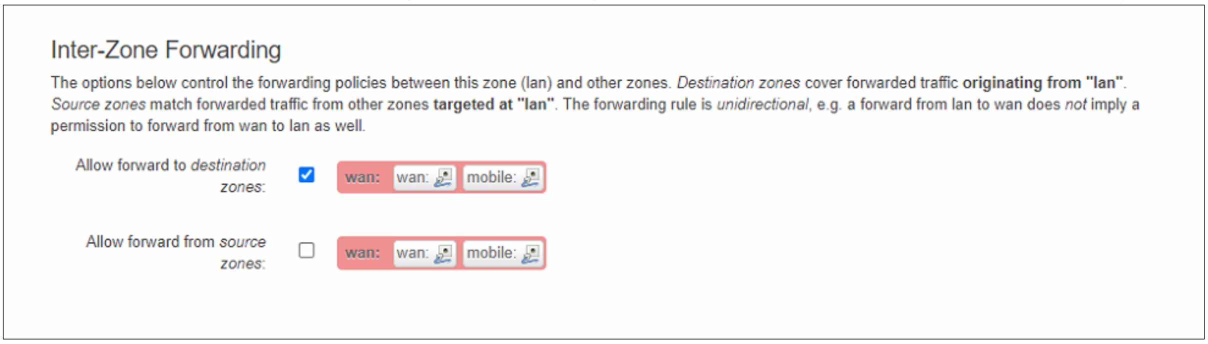
MSS clamping: □

Covered networks: ☑ lan: □ mobile: □ wan: □ xl2tpd:

Table 59. Network > Firewall > General Settings > Zone Configuration > Zone “Lan”

Field	Description
Zone➔Forwardings	The zone forwarding contains the source zone from which data packets will redirect and the destination zone to which data packets will be redirected.
Input	Action that is to be performed for packets that pass through the Input chain.
Output	Action that is to be performed for packets that pass through the Output chain.
Forward	Action that is to be performed for packets that pass through the Forward chain.
Masquerading	Specifies whether outgoing zone traffic should be masqueraded. This is typically enabled on the WAN zone.
MSS Clamping	To enable/disable MSS clamping for outgoing zone traffic.

Figure 72. Network > Firewall > General Settings > Zone Configuration > Zone “Lan” > Inter-Zone Forwarding



Inter-Zone Forwarding

The options below control the forwarding policies between this zone (lan) and other zones. *Destination zones* cover forwarded traffic **originating from "lan"**. *Source zones* match forwarded traffic from other zones **targeted at "lan"**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

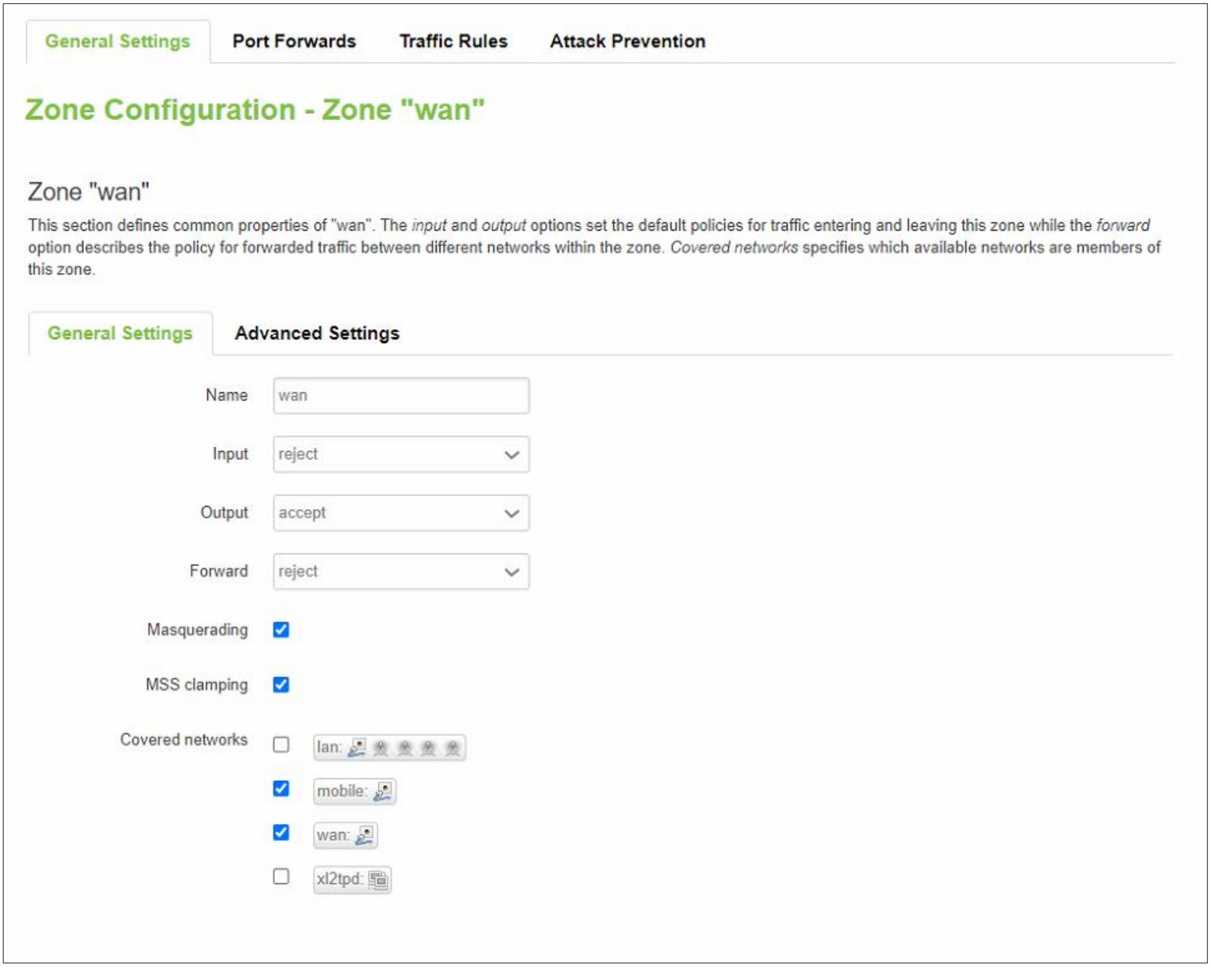
Allow forward to *destination zones*: ☑ wan: wan: mobile:

Allow forward from *source zones*: □ wan: wan: mobile:

3.3.9.1.4 Zone Configuration-WAN

In the Firewall Setting sub-tab of the Network-Interfaces-WAN tab, you can assign a firewall zone to the WAN interface.

Figure 73. Network > Firewall > General Settings > Zone “wan”



Zone Configuration - Zone "wan"

Zone "wan"

This section defines common properties of "wan". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are members of this zone.

Name: wan

Input: reject

Output: accept

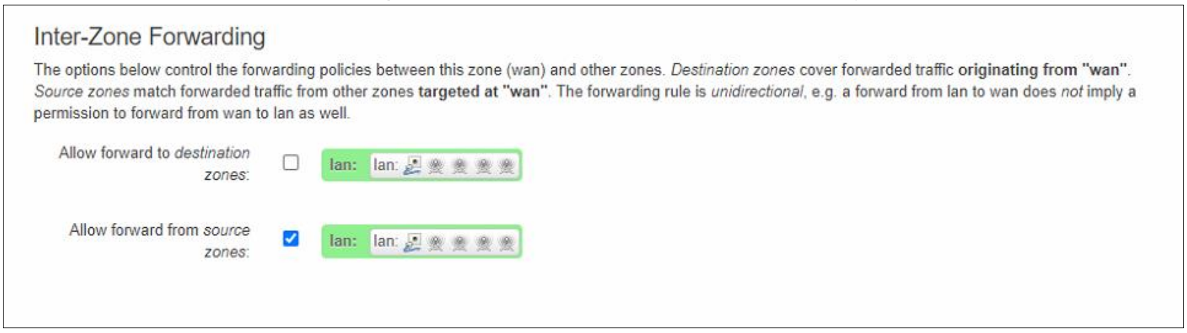
Forward: reject

Masquerading ☑

MSS clamping ☑

Covered networks
□ lan:
☑ mobile:
☑ wan:
□ xl2tpd:

Table 60. Network > Firewall > General Settings > Zone “wan” > Inter-Zone Forwarding



Inter-Zone Forwarding

The options below control the forwarding policies between this zone (wan) and other zones. *Destination zones* cover forwarded traffic **originating from "wan"**. *Source zones* match forwarded traffic from other zones **targeted at "wan"**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

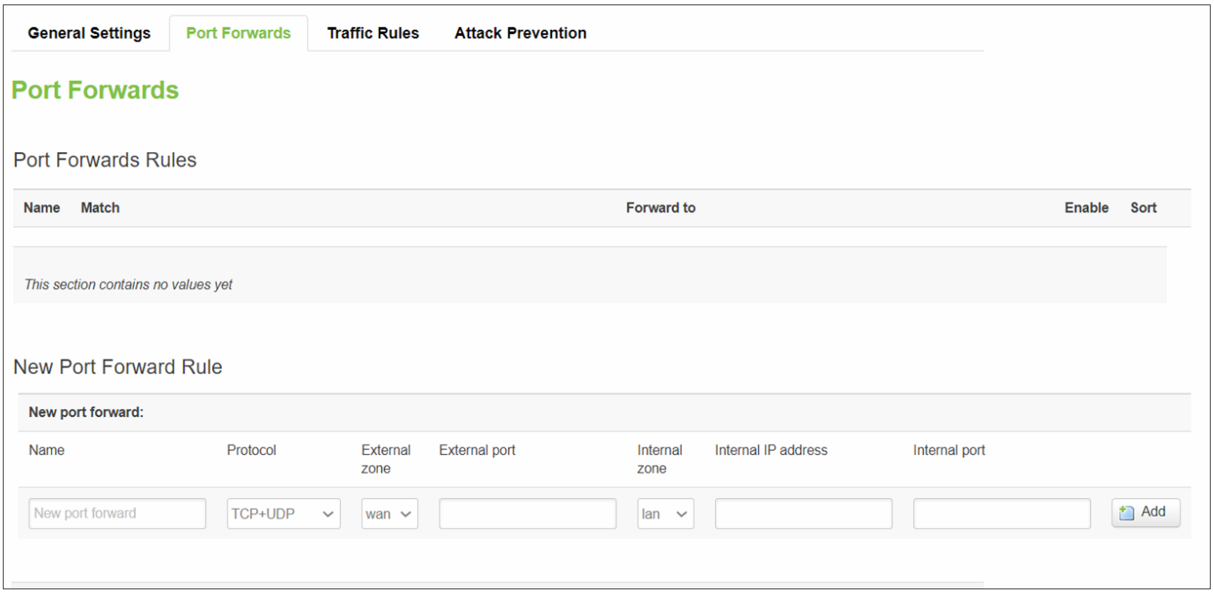
Allow forward to *destination* zones: □ lan: lan:

Allow forward from *source* zones: ☑ lan: lan:

3.3.9.2 Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN. It is a way of redirecting an incoming connection to another IP address, port. or a combination of both.

Figure 74. Network > Firewall > Port Forwards > Port Forwards Rules



Port Forwards

Port Forwards Rules

Name	Match	Forward to	Enable	Sort

This section contains no values yet

New Port Forward Rule

New port forward:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port	
New port forward	TCP+UDP	wan		lan			Add

Table 61. Network > Firewall > Port Forwards > Port Forwards Rules

Field	Description
Name	Name of the port forward rule, used only for easier management purposes.
Match	Display matched conditions of the port forwarding rule.
Forward to	Display the port forward destination info when matched with the conditions.

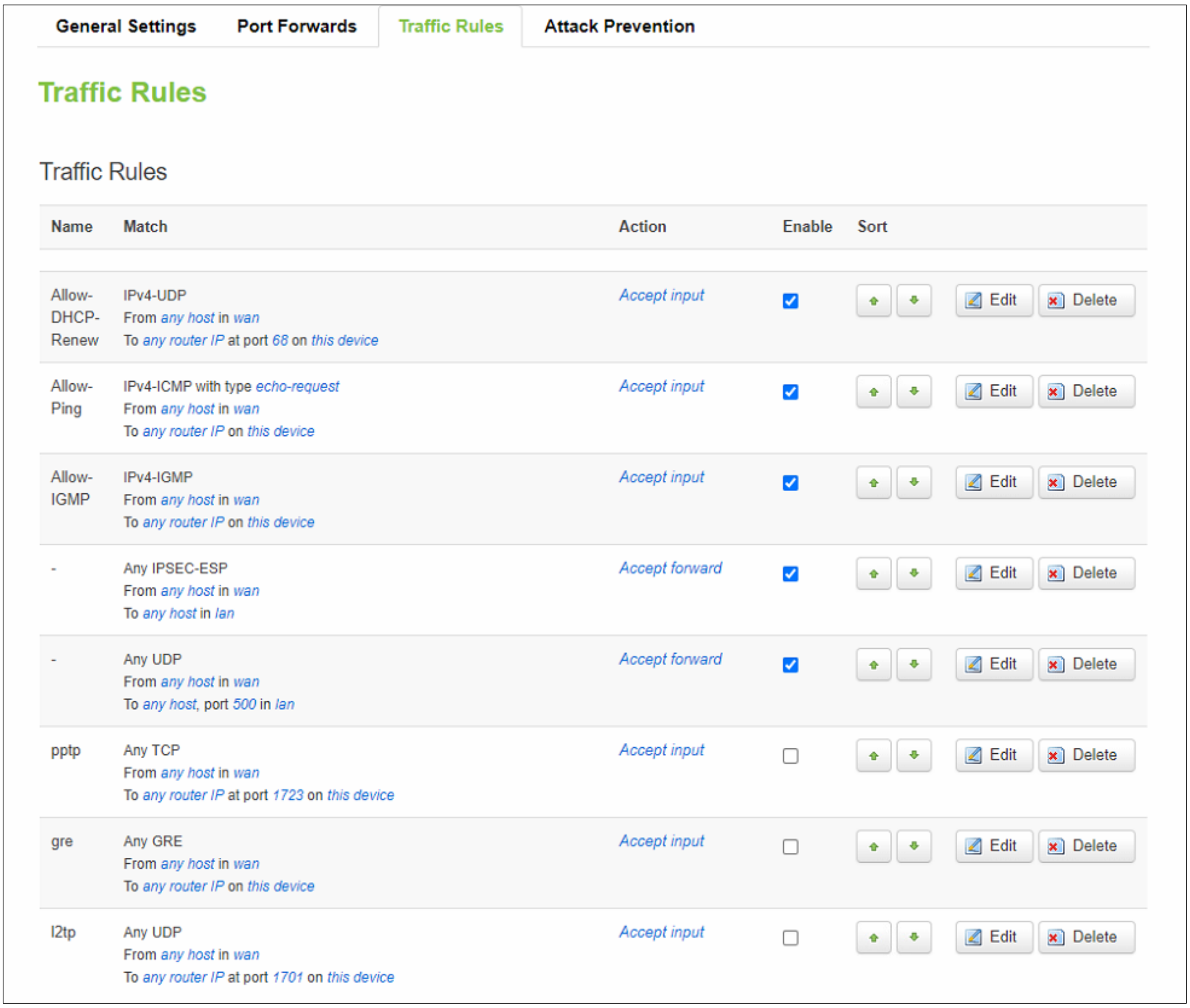
Table 62. Network > Firewall > Port Forwards > New Port Forwards Rules

Field	Value	Description
Name	-	Name of the port forward rule, used only for easier management purposes.
Protocol	default: **TCP+UDP**	Type of protocol of the incoming packet.
External Zone	default: **wan**	The WAN network that data traffic will be redirected from.
External Port	integer [0-65535] | range of integers [0-65534] - [1-65535]; default: **none**	Traffic will be forwarded from this port on the WAN network. The rule will match the source port used by the connecting host with the port number(s) specified in this field. Leave empty to make the rule skip source port matching.
Internal Zone	integer [0-65535] | range of integers [0-65534] - [1-65535]; default: **none**	The LAN network that data traffic will be redirected to.
Internal IP Address	-	The IP address of the internal machine that hosts some services that you want to access from the outside.
Internal Port	default: **lan**	The rule will redirect the data traffic to this port on the internal machine.

3.3.9.3 Traffic Rule

The **Traffic Rules** tab contains a more generalized rule definition. You can block or open ports, alter how traffic is forwarded between LAN and WAN, and many other things.Traffic Rules

Figure 75. Network > Firewall > Traffic Rules > Traffic Rules



Traffic Rules

Traffic Rules

Name	Match	Action	Enable	Sort		
Allow-DHCP-Renew	IPv4-UDP From *any host* in *wan* To *any router IP* at port *68* on *this device*	*Accept input*	☑	↑ ↓	Edit	Delete
Allow-Ping	IPv4-ICMP with type *echo-request* From *any host* in *wan* To *any router IP* on *this device*	*Accept input*	☑	↑ ↓	Edit	Delete
Allow-IGMP	IPv4-IGMP From *any host* in *wan* To *any router IP* on *this device*	*Accept input*	☑	↑ ↓	Edit	Delete
-	Any IPSEC-ESP From *any host* in *wan* To *any host* in *lan*	*Accept forward*	☑	↑ ↓	Edit	Delete
-	Any UDP From *any host* in *wan* To *any host*, port *500* in *lan*	*Accept forward*	☑	↑ ↓	Edit	Delete
pptp	Any TCP From *any host* in *wan* To *any router IP* at port *1723* on *this device*	*Accept input*	☐	↑ ↓	Edit	Delete
gre	Any GRE From *any host* in *wan* To *any router IP* on *this device*	*Accept input*	☐	↑ ↓	Edit	Delete
l2tp	Any UDP From *any host* in *wan* To *any router IP* at port *1701* on *this device*	*Accept input*	☐	↑ ↓	Edit	Delete

Table 63. Network > Firewall > Traffic Rules > Traffic Rules

Field	Description
Name	Name of the traffic rule, used only for simplified management purposes.
Match	Display matched conditions of the traffic rule.
Action	Action to be performed with the packet if it matches the rule.
Enable	To enable/disable this traffic rule.
Sort	To sort the traffic rules. The top classification rule means the highest priority.
Edit	To configure selected traffic rule.
Delete	To remove selected traffic rule.

3.3.9.3.1 Open Ports on Router

Open Ports on Router rules can open certain ports and redirect hosts connecting to the router from specified zones to specified ports.

Figure 76. Network > Firewall > Traffic Rules > Open ports on router

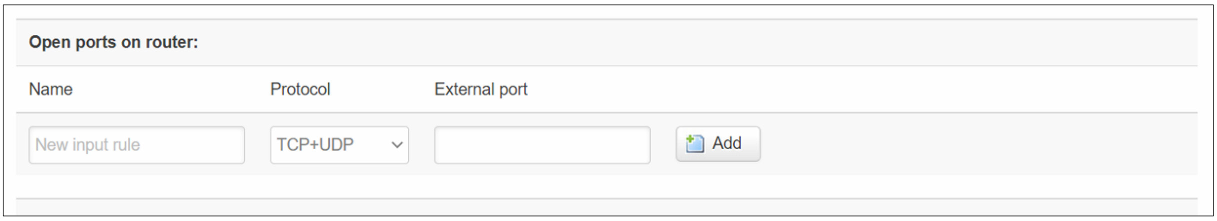


Table 64. Network > Firewall > Traffic Rules > Open ports on router

Field	Description
Name	Name of the traffic rule, used only for easier management purposes.
Protocol	Specifies to which protocols the rule should apply.
External Port	Specifies which port should be opened.
Add	Add a new open port on the router rule.

3.3.9.3.2 New Forward Rule

New Forward Rules enable you to create custom zone forwarding rules. This is used to create firewall rules that control traffic on the FORWARD chain.

Figure 77. Network > Firewall > Traffic Rules > New forward rule

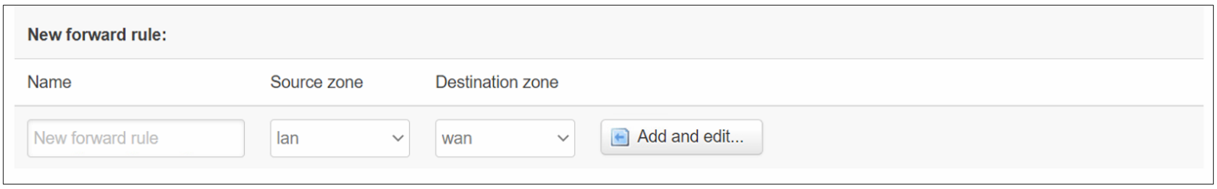


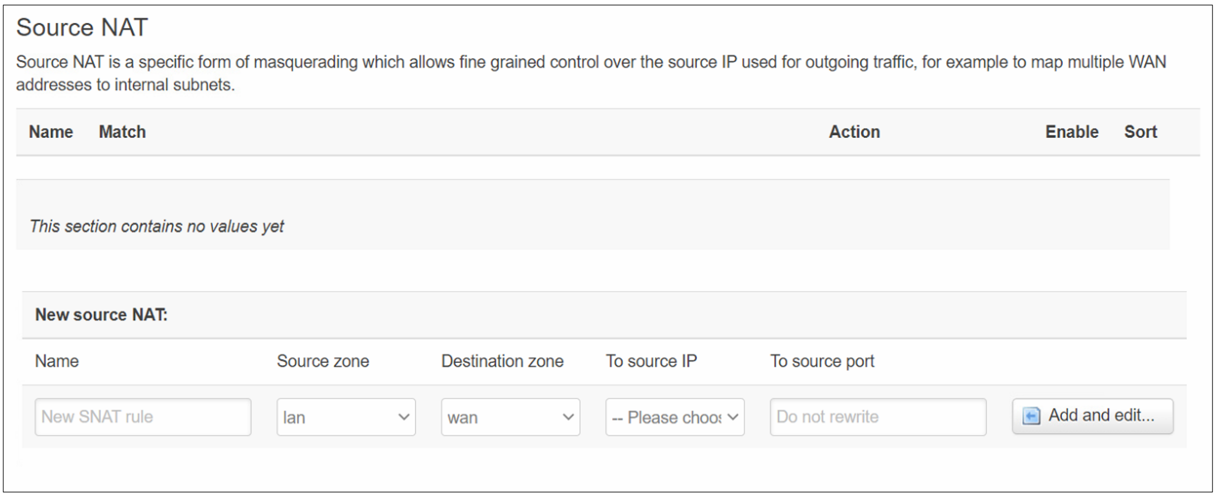
Table 65. Network > Firewall > Traffic Rules > New forward rule

Field	Description
Name	Name of the traffic rule, used only for easier management purposes.
Source Zone	Match incoming traffic from selected address family only.
Destination Zone	Forward incoming traffic to selected address family only.

3.3.9.3.3 Source NAT

SNAT is a form of masquerading used to change a packet's source address and/or port number to a static, user-defined value. It is performed in the POST ROUTING chain, just before a packet leaves the device. For example, it enables the mapping of multiple WAN addresses to internal subnets.

Figure 78. Network > Firewall > Traffic Rules > Source NAT



Source NAT

Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.

Name	Match	Action	Enable	Sort

This section contains no values yet

New source NAT:

Name	Source zone	Destination zone	To source IP	To source port	
New SNAT rule	lan	wan	-- Please choos	Do not rewrite	Add and edit...

Table 66. Network > Firewall > Traffic Rules > Source NAT

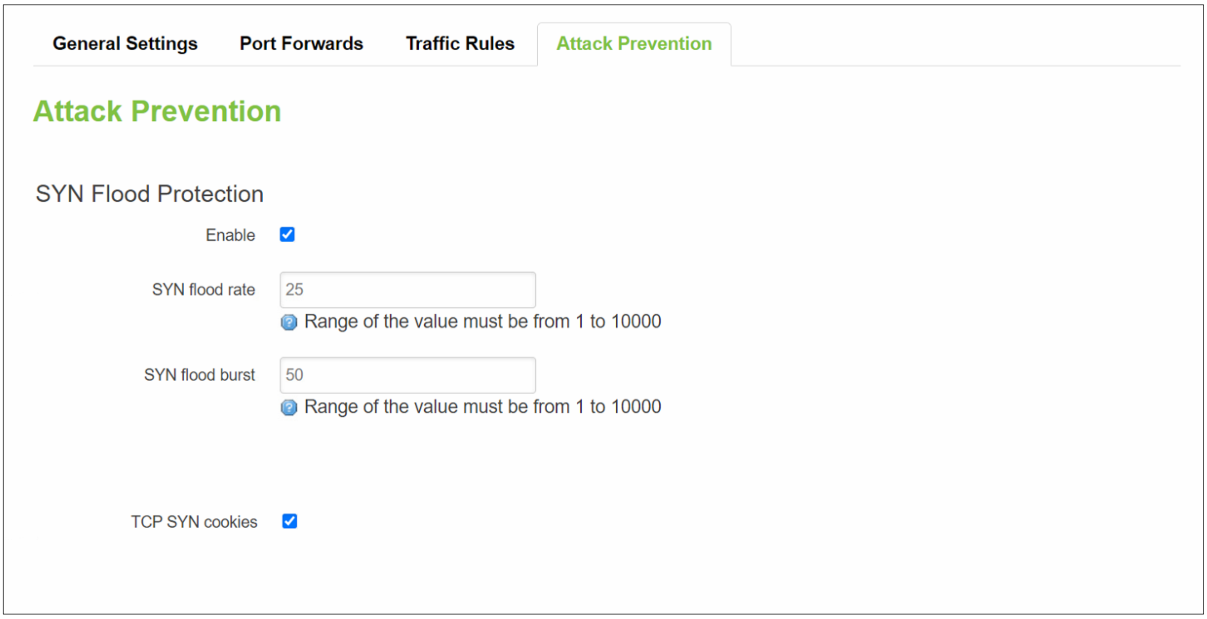
Field	Description
Name	Name of the traffic rule, used only for easier management purposes.
Source Zone	Match incoming traffic from selected address family only.
Destination Zone	Forward incoming traffic to selected address family only.
To Source IP	Match incoming traffic from the specified source IP address.
To Source Port	Match incoming traffic originating from the given source port or port range on the client host.

3.3.9.4 Attack Prevention

3.3.9.4.1 SYN Flood Protection

SYN Flood Protection allows you to protect your router from attacks that exploit part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive. Essentially, with SYN flood DDoS, the offender sends TCP connection requests faster than the targeted machine can process them, causing network saturation.

Figure 79. Network > Firewall > Attack Prevention > SYN Flood Protection



Attack Prevention

SYN Flood Protection

Enable ☑

SYN flood rate 25
Range of the value must be from 1 to 10000

SYN flood burst 50
Range of the value must be from 1 to 10000

TCP SYN cookies ☑

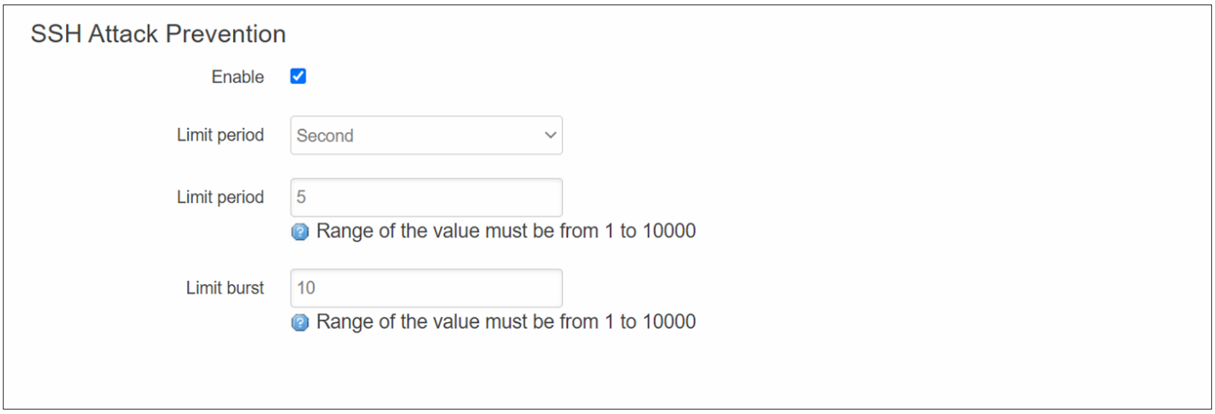
Table 67. Network > Firewall > Attack Prevention > SYN Flood Protection

Field	Value	Description
Enable	default: **enable**	Makes the router more resistant to SYN flood attacks.
SYN flood rate	integer [1 to 10000]; default: **25**	Set rate limit (packets/second) for SYN packets above which the traffic is considered flooding.
SYN flood burst	integer [1 to 10000]; default: **50**	Set burst limit for SYN packets above which the traffic is considered flooded if it exceeds the allowed rate.
TCP SYN cookies	default: **enable**	Enable the use of SYN cookies (particular choices of initial TCP sequence numbers by TCP servers).

3.3.9.4.2 SSH Attack Prevention

SSH Attack Prevention allows you to run commands on a machine's command prompt without them being physically present near the machine and attacks by limiting connections in a defined period.

Figure 80. Network > Firewall > Attack Prevention > SSH Attack Protection



SSH Attack Prevention

Enable ☑

Limit period: Second

Limit period: 5

Range of the value must be from 1 to 10000

Limit burst: 10

Range of the value must be from 1 to 10000

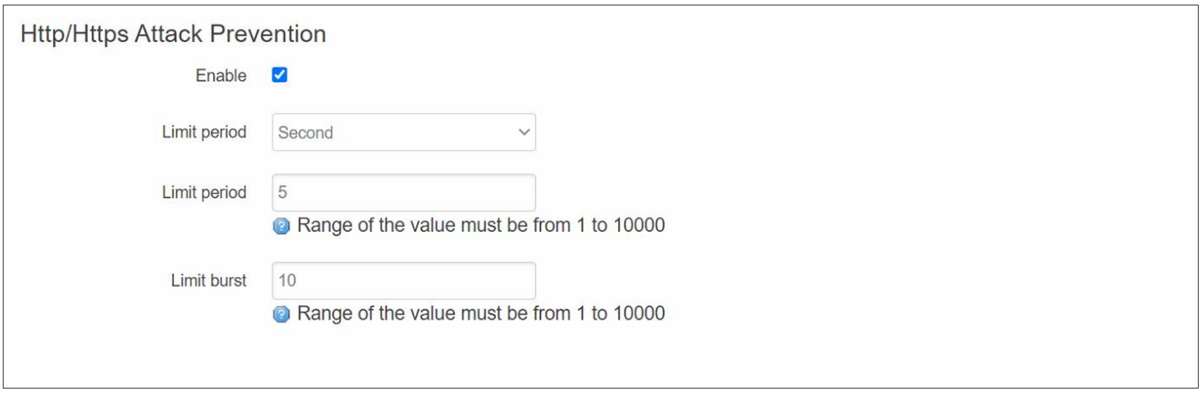
Table 68. Network > Firewall > Attack Prevention > SSH Attack Protection

Field	Value	Description
Enable	default: **enable**	Enable SSH connections to limit in the selected period.
Limit period	Second/Minute/Hour/Day; default: **Second**	Select in what period limit SSH connections.
Limit	integer [1 to 10000]; default: **5**	Maximum SSH connections during the period.
Limit burst	integer [1 to 10000]; default: **10**	Indicating the maximum burst before the above limit kicks in.

3.3.9.4.3 Http/Https Attack Prevention

HTTP attacks send a complete, legitimate HTTP header, which includes a 'Content-Length' field to specify the size of the message body to follow. However, the attacker then proceeds to send the actual message body at an extremely slow rate (i.e. 1 byte/110 seconds). Due to the entire message being correct and complete, the target server will attempt to obey the 'Content-Length' field in the header, and wait for the entire body of the message to be transmitted, hence slowing it down.

Figure 81. Network > Firewall > Attack Prevention > Http/Https Attack Protection



Http/Https Attack Prevention

Enable ☑

Limit period: Second

Limit period: 5

Range of the value must be from 1 to 10000

Limit burst: 10

Range of the value must be from 1 to 10000

Table 69. Network > Firewall > Attack Prevention > Http/Https Attack Protection

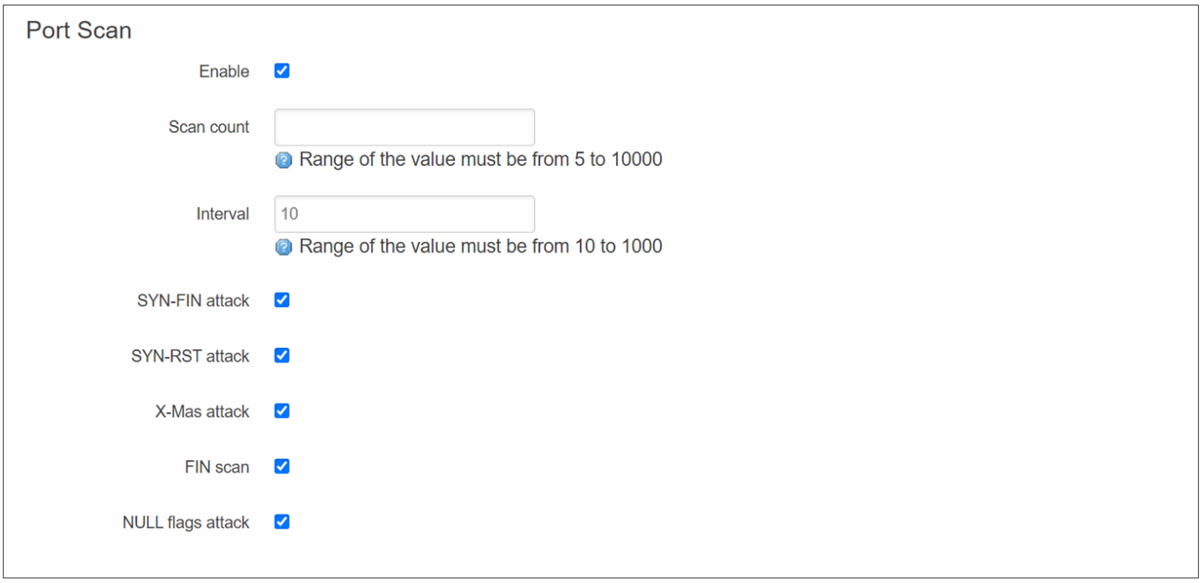
Field	Value	Description
Enable	default: **enable**	Enable HTTP connections to limit in the selected period.
Limit period	Second/Minute/Hour/Day; default: **Second**	Select in what period limit HTTP connections.
Limit	integer [1 to 10000]; default: **5**	Maximum HTTP connections during the period.
Limit burst	integer [1 to 10000]; default: **10**	Indicating the maximum burst before the above limit kicks in.

3.3.9.4.4 Port Scan

Port Scan attacks scan which of the targeted host's ports are open. Network ports are the entry points to a machine that is connected to the Internet. A service that listens on a port can receive data from a client application, process it and send a response back. Malicious clients can sometimes exploit vulnerabilities in the server code so they gain access to sensitive data or execute malicious code on the machine remotely.

Port scanning is usually done in the initial phase of a penetration test in order to discover all network entry points into the target system. The Port Scan section provides you with the possibility to enable protection against port scanning software. The Defending Type section provides the possibility for the user to enable protections from certain types of online attacks. These include **SYN-FIN**, **SYN-RST**, **X-Mas**, **FIN scan** and **NULLflags** attacks.

Figure 82. Network > Firewall > Attack Prevention > Port Scan



Port Scan

Enable ☑

Scan count

Range of the value must be from 5 to 10000

Interval 10

Range of the value must be from 10 to 1000

SYN-FIN attack ☑

SYN-RST attack ☑

X-Mas attack ☑

FIN scan ☑

NULL flags attack ☑

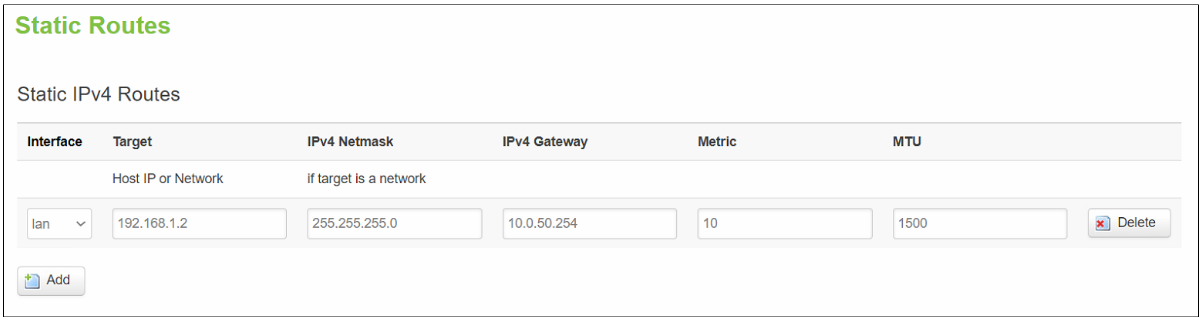
Table 70. Network > Firewall > Attack Prevention > Port Scan

Field	**Value**	**Description**
Enable	default: **enable**	Enable port scan prevention.
Scan count	integer [5 to 10000]; Default: **none**	The numbers port of scanned before blocked.
Interval	integer [10 to 1000]; default: **10**	Time interval in seconds counting the length of the scan (10 – 60 sec).
SYN-FIN attack	default: **enable**	Protect from SYN-FIN attack.
SYN-RST attack	default: **enable**	Protect from SYN-RST attack.
X-Mas attack	default: **enable**	Protect from X-Mas attack.
FIN scan	default: **enable**	Protect from FIN scan.
NULL flags attack	default: **enable**	Protect from NULLflags attack.

3.3.10 Static Routes

Static routes specify over which interface and gateway a certain host or network can be reached. You can configure the custom routes in this webpage.

Figure 83. Network > Static Routes



Static Routes

Static IPv4 Routes

Interface	Target	IPv4 Netmask	IPv4 Gateway	Metric	MTU	
	Host IP or Network	if target is a network				
lan	192.168.1.2	255.255.255.0	10.0.50.254	10	1500	Delete

Add

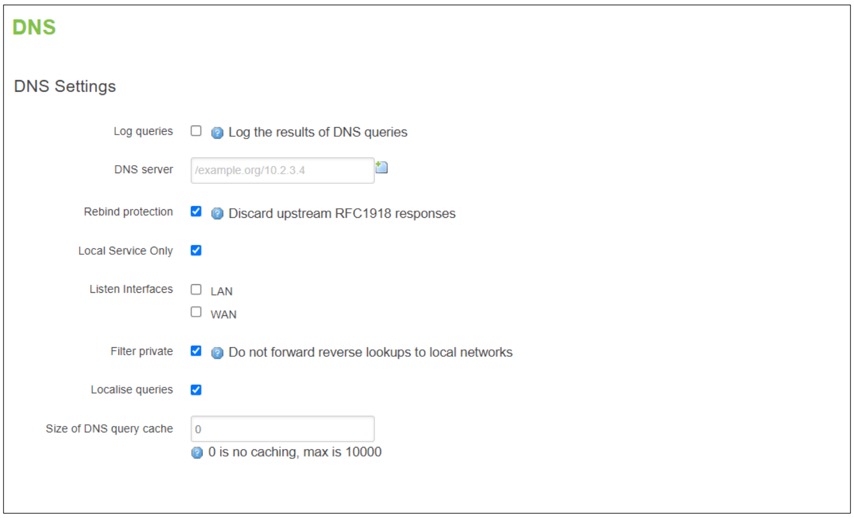
Table 71. Network > Static Routes

Field	Description
Interface	Interface which will be used for the route in IPv4 routing table.
Target	The IP address of the destination network or host.
IPv4 Netmask	A subnet mask that is applied to the Target field to determine to what actual IP addresses the routing rule applies.
IPv4 Gateway	Defines where the CWR5805 device should send all the traffic that applies to the rule.
Metric	The Metric value is used as a sorting measure. If a packet about to be routed fits two rules, the one with the lower metric is applied.
MTU	Specifies the largest possible size of a data packet.
Delete	To remove selected static IPv4 route entry.
Add	To add a new static IPv4 route entry.

3.3.11 DNS

The DNS page is used to set up the how the device utilized its own and other DNS servers.

Figure 84. Network > DNS



DNS

DNS Settings

Log queries ☐ Log the results of DNS queries

DNS server /example.org/10.2.3.4

Rebind protection ☑ Discard upstream RFC1918 responses

Local Service Only ☑

Listen Interfaces ☐ LAN
☐ WAN

Filter private ☑ Do not forward reverse lookups to local networks

Localise queries ☑

Size of DNS query cache 0

0 is no caching, max is 10000

Table 72. Network > DNS

Field	Value	Description
Log queries	enable/disable; default: **disable**	When enabled, write received DNS requests to syslog.
DNS server	default: none	List of DNS servers to forward requests to.
Rebind protection	enable/disable; default: **enable**	Discard upstream RFC1918 responses. When enabled, the device will not resolve domain names for internal hosts.
Local Service Only	enable/disable; default: **enable**	Limit DNS service to subnets and interfaces on which this device is serving as a DNS server.
Listen Interfaces	LAN/WAN; default: **none**	Limits listening for DNS queries to interfaces specified in the field and loopback. Leave empty to listen on all interfaces.
Filter private	enable/disable; default: **enable**	Do not forward reverse lookups for local networks.
Localise queries	enable/disable; default: **enable**	Localise hostname depending on the requesting subnet if multiple IPs are available.

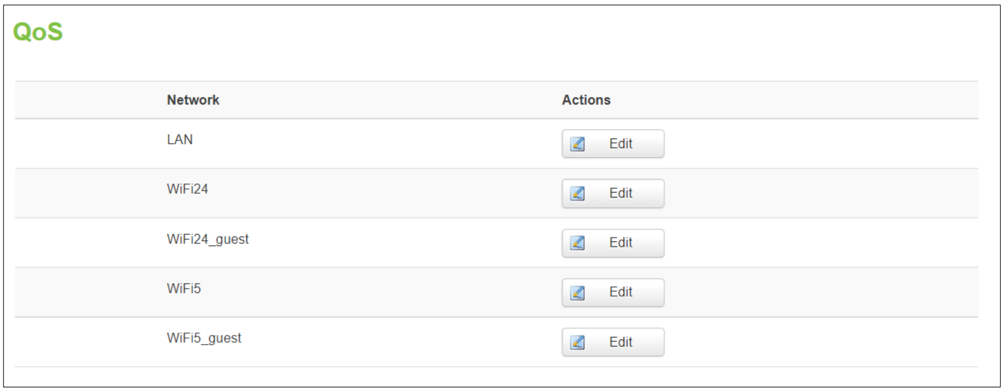
Size of DNS query cache	Integer [0 to 10000]; default: **none**	Number of cached DNS entries. Set to 0 for no caching.

3.3.12 QoS

The **QoS** (**Quality of Service**) page is used to set up Smart Queue Management (SQM) instances which can limit the download and upload speeds of selected network interfaces.

This manual page provides an overview of the QoS windows.

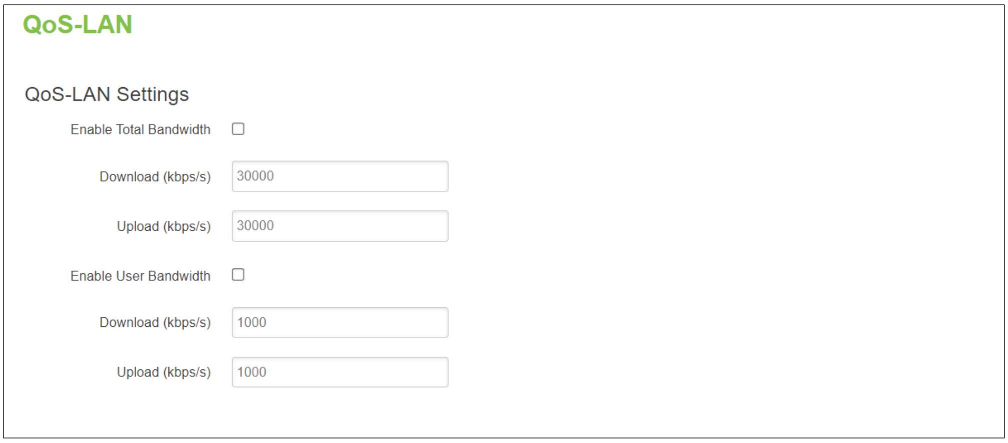
Figure 85. Network > QoS



QoS

Network	Actions
LAN	Edit
WiFi24	Edit
WiFi24_guest	Edit
WiFi5	Edit
WiFi5_guest	Edit

Figure 86. Network > QoS > QoS-LAN Settings



QoS-LAN

QoS-LAN Settings

Enable Total Bandwidth □
Download (kbps/s) 30000
Upload (kbps/s) 30000
Enable User Bandwidth □
Download (kbps/s) 1000
Upload (kbps/s) 1000

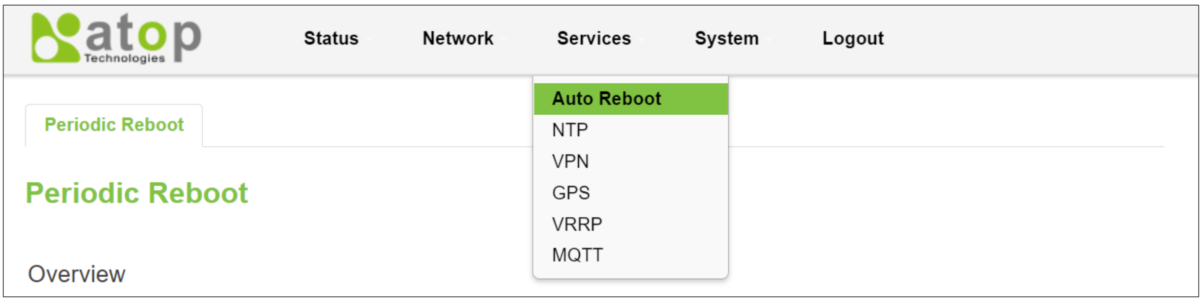
Table 73. Network > QoS > QoS-LAN Settings

Field	**Value**	**Description**
Enable Total Bandwidth	disable/enable; Default: **disable**	Overall Speed limits for all LANs.
Download (kbps/s)	integer [0 - 1000000]; default: **30000**	Limits the download speed (ingress) of the selected interface to the value specified in this field.
Upload (kbps/s)	integer [0 - 1000000]; default: **30000**	Limits the upload speed (egress) of the selected interface to the value specified in this field.
Enable User Bandwidth	disable/enable; Default: **disable**	Speed limits for each user.
Download (kbps/s)	integer [0 - 1000000]; default: **30000**	Limits the download speed (ingress) of the selected interface to the value specified in this field.
Upload (kbps/s)	integer [0 - 1000000]; default: **30000**	Limits the upload speed (egress) of the selected interface to the value specified in this field.

3.4 Services Menu

The **Services** menu as shown in the Figure below consists of the following sub-menus: Auto Reboot, NTP, VPN, GPS, VRRP and MQTT.

Figure 87. Service



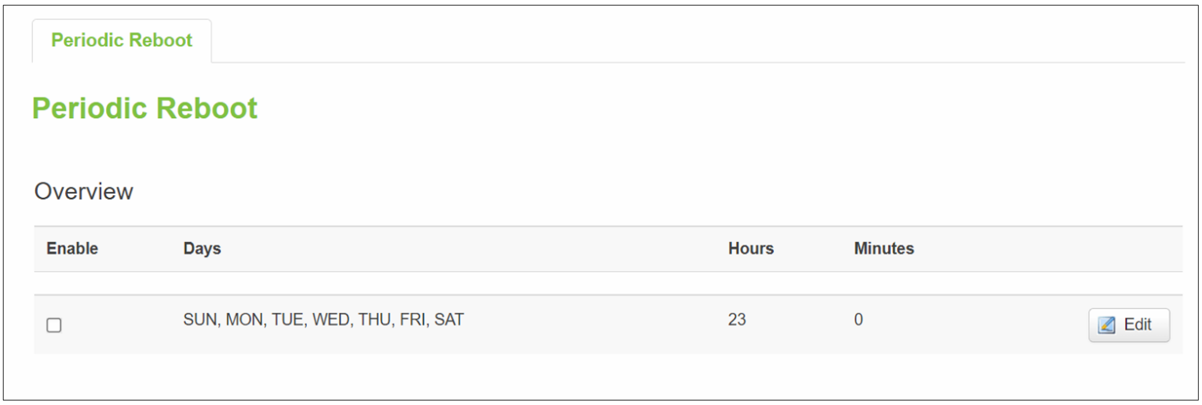
3.4.1 Auto Reboot

3.4.1.1 Overview

Various automatic device reboot scenarios can be configured in the **Auto Reboot** section. Automatic reboots can be used as a prophylactic or precautionary measure that ensures the device will self-correct some unexpected issues, especially related to connection downtime.

The **Periodic Reboot** is a function that reboots the device at a specified time interval regardless of other circumstances. It can be used as a prophylactic measure, for example, to reboot the device once at the end of every Monday.

Figure 88. Service > Auto Reboot



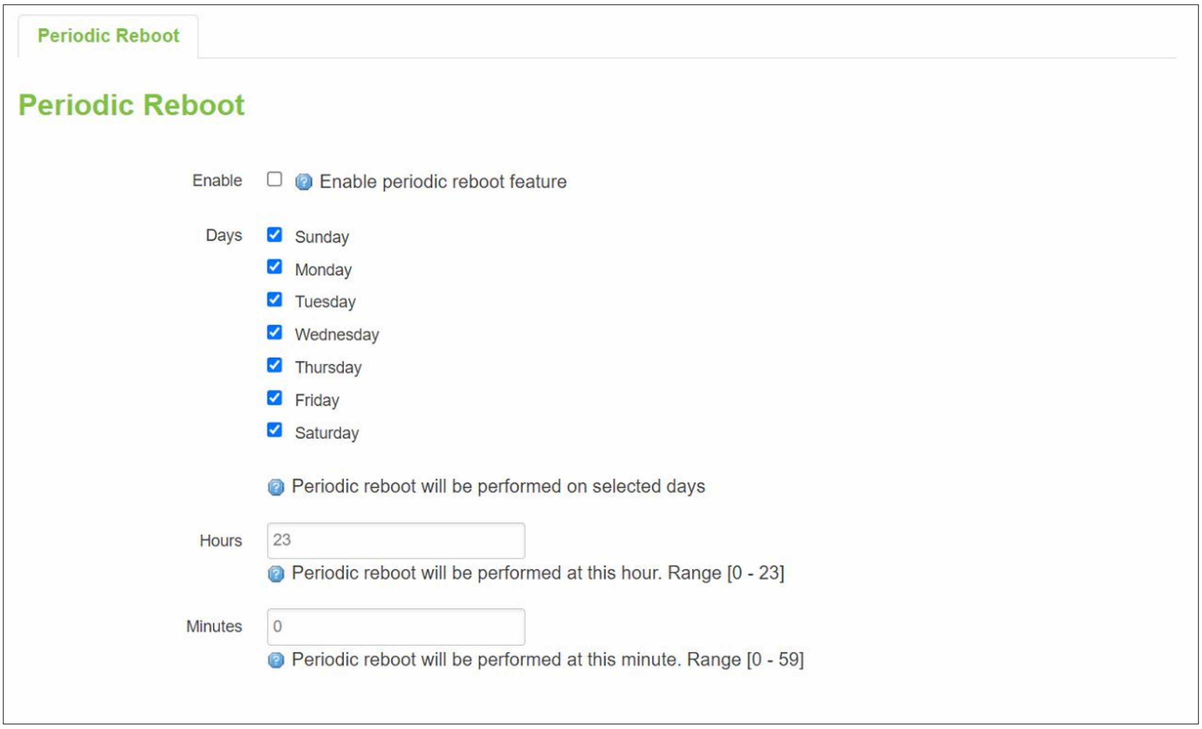
Periodic Reboot

Overview

Enable	Days	Hours	Minutes	
☐	SUN, MON, TUE, WED, THU, FRI, SAT	23	0	Edit

3.4.1.2 Configuration – Periodic Reboot

Figure 89. Service > Auto Reboot > Edit



Periodic Reboot

Periodic Reboot

Enable □ Enable periodic reboot feature

Days ☑ Sunday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday

Periodic reboot will be performed on selected days

Hours 23

Periodic reboot will be performed at this hour. Range [0 - 23]

Minutes 0

Periodic reboot will be performed at this minute. Range [0 - 59]

Table 74. Service > Auto Reboot > Edit

Field	Value	Description
Enable	default: **disable**	This check box will enable or disable Periodic reboot feature.
Days	SUN/MON/TUE/WED/THU/FRI/SAT; default: **SUN/MON/TUE/WED/THU/FRI/SAT**	Uploading will be done on that specific time of the day.
Hours	integer [0 – 23] hours; default: **23**	Uploading will be done on that specific time of the hours.
Minutes	integer [0 – 59] minitues; default: **0**	Uploading will be done on that specific time of the minutes.

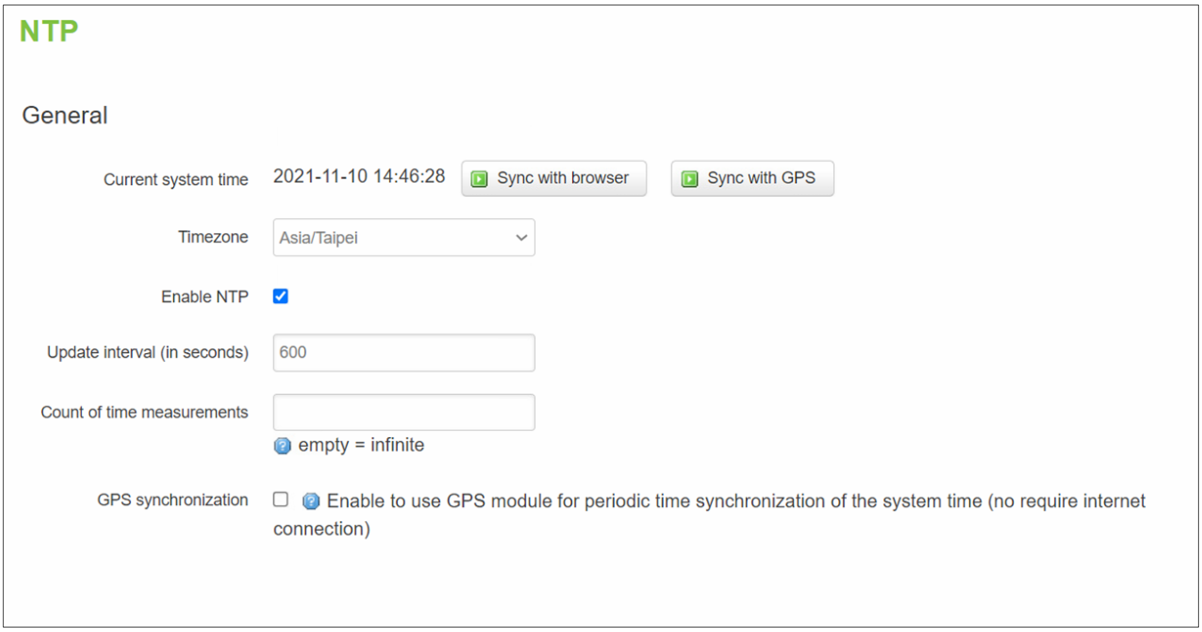
3.4.2 NTP

3.4.2.1 General Section

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

You synchronize the time values of CWR5805 device in the **General** section within NTP sub-menu. These time settings include an update interval (in seconds) and count of time measurements.

Figure 90. Services > NTP > General



NTP

General

Current system time 2021-11-10 14:46:28

Timezone Asia/Taipei

Enable NTP ☑

Update interval (in seconds) 600

Count of time measurements

empty = infinite

GPS synchronization □ Enable to use GPS module for periodic time synchronization of the system time (no require internet connection)

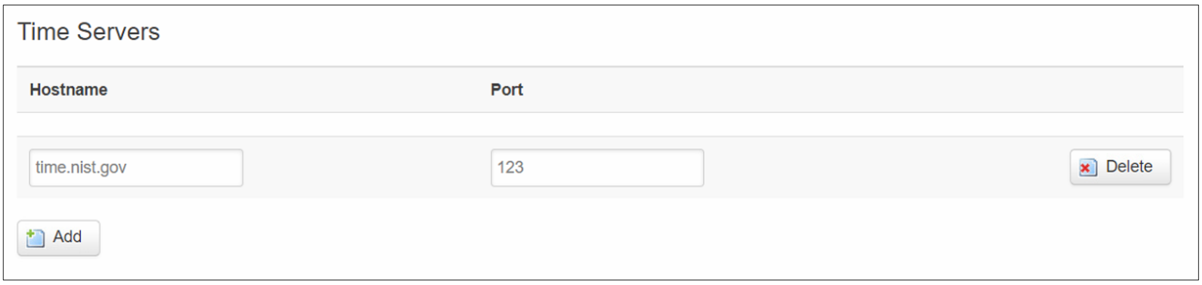
Table 75. Services > NTP > General

Field	Value	Description
Sync with browser	(none)	Sync with browser.
Sync with GPS	(none)	Sync with GPS.
Time zone	default: **UTC**	Time zone of your country.
Enable NTP	default: **enable**	Enable system's time synchronization with time server using NTP (Network Time Protocol).
Update Interval (in seconds)	default: **600**	Frequency that the NTP client service on CWR5805 device will update the time.
Count of Time Measurements	default: **none**	The amount of times that NTP client service on CWR5805 device will perform time synchronizations. Leave it empty if set to infinite.
GPS synchronization	default: **disable**	Enable to use GPS module for periodic time synchronization of the sys time.

3.4.2.2 Time Servers

The NTP servers used by the CWR5805 device is displayed in the **Time Servers** section within **Time Synchronisation** sub-menu.

Figure 91. Services > NTP > Time Servers



Time Servers

Hostname	Port
time.nist.gov	123

Table 76. Services > NTP > Time Servers

Field	Value	Description
Hostname	string [1 - 253] default: **time.nist.gov**	Hostname of NTP server
Port	integer [1 - 65535] default: **123**	Port number that the NTP server is listening on

3.4.3 VPN

Virtual Private Network (VPN) is a method to connect multiple private networks across the Internet. VPNs can be used to achieve many different goals, but its main purpose are for: device accessibility among the remote private networks, data encryption and anonymity when browsing the Internet.

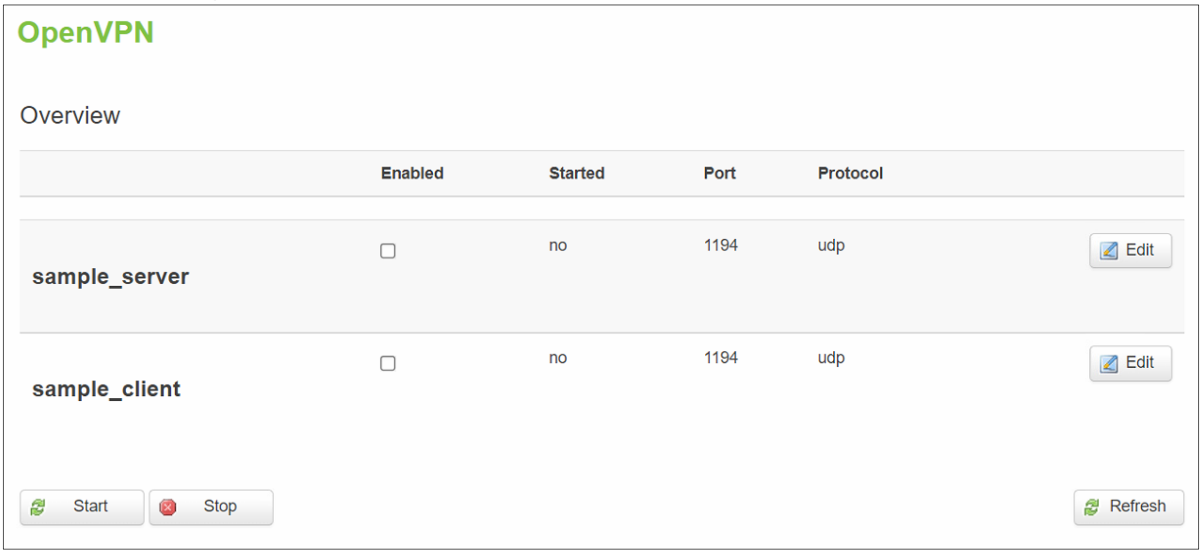
3.4.3.1 OpenVPN

OpenVPN that implements VPN techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It is often regarded as being the most universal VPN protocol because of its flexibility, support of SSL/TLS security, multiple encryption methods, many networking features.

3.4.3.1.1 Overview

In the **OpenVPN** sub-menu within the **Service** menu, two OpenVPN instances are already created by default, as shown in the figure below. It is referred to as “sample_server”and “sample_client”, respectively. These two instances are editable as it is not yet operational by default.

Figure 92. Services > VPN > OpenVPN > Overview



OpenVPN

Overview

	Enabled	Started	Port	Protocol	
sample_server	□	no	1194	udp	Edit
sample_client	□	no	1194	udp	Edit

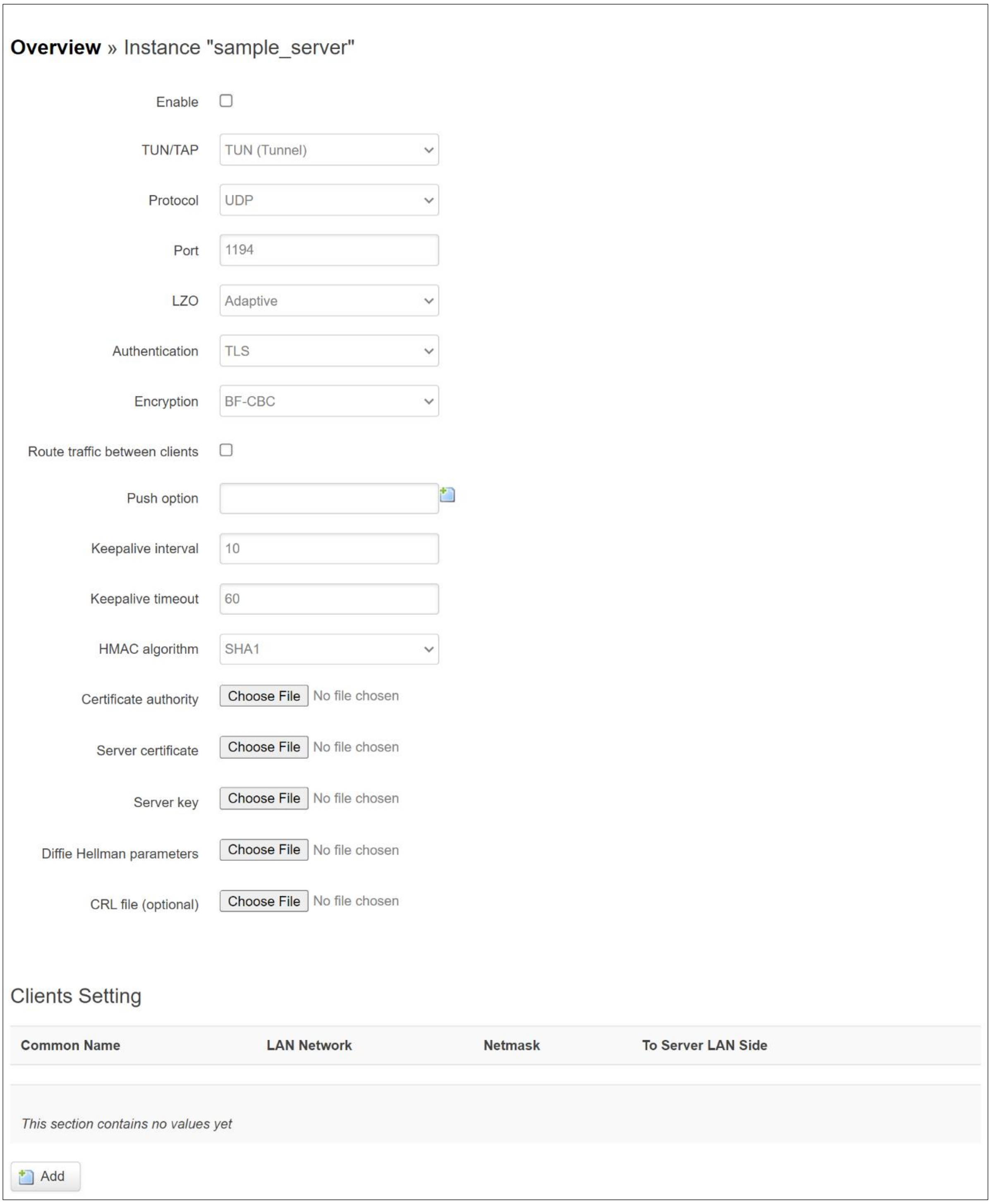
Table 77. Services > VPN > OpenVPN > Overview

Field	Description
Enabled	To enable/disable selected OpenVPN service instance.
Started	Display current OpenVPN service is started or not.
Port	Display port number the OpenVPN service listening on.
Protocol	Display TCP/UDP protocol the OpenVPN service used.
Edit	To configure selected OpenVPN service instance.
Start/Stop	To start/stop selected OpenVPN service.

3.4.3.1.2 OpenVPN Server

If you click “**Edit**” button to edit OpenVPN instance, the editing webpage which contains the OpenVPN instance’s configuration is intitialized. The Figure below shows the edit webpage of the default OpenVPN server instance called "sample_server". Note that the edit webpage here is for basic setting.

Figure 93. Services > VPN > OpenVPN > sample_server > Edit



Overview » Instance "sample_server"

Enable	□
TUN/TAP	TUN (Tunnel)
Protocol	UDP
Port	1194
LZO	Adaptive
Authentication	TLS
Encryption	BF-CBC
Route traffic between clients	□
Push option	
Keepalive interval	10
Keepalive timeout	60
HMAC algorithm	SHA1
Certificate authority	Choose File No file chosen
Server certificate	Choose File No file chosen
Server key	Choose File No file chosen
Diffie Hellman parameters	Choose File No file chosen
CRL file (optional)	Choose File No file chosen

Clients Setting

Common Name	LAN Network	Netmask	To Server LAN Side
This section contains no values yet			

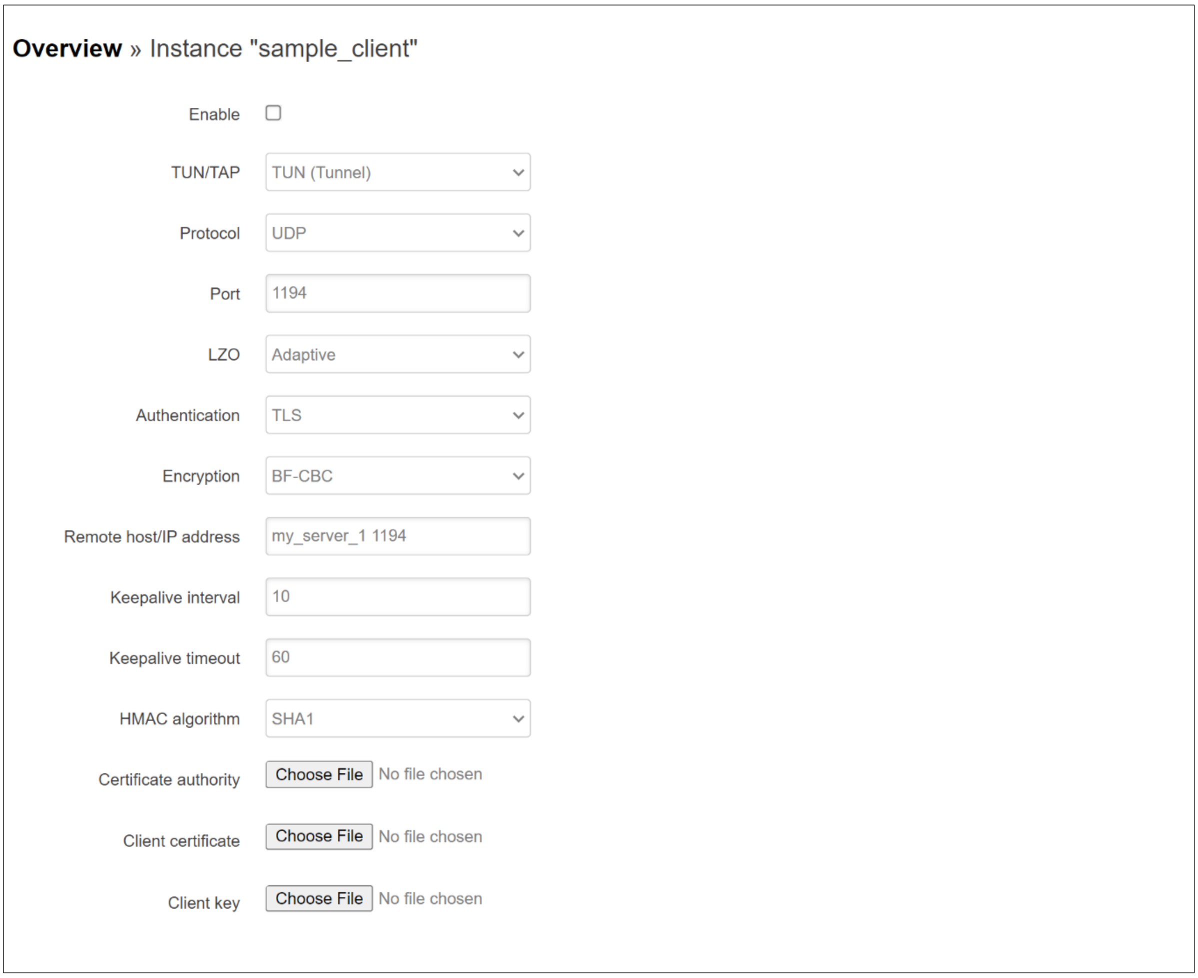
Table 78. Services > VPN > OpenVPN > sample_server > Edit

Field	Value	Description
Instance "sample_server"		
Enable	Enable/Disable; default: **Disable**	Switches configuration enable or disable. This must be selected to make configuration active.
TUN/TAP	TUN (Tunnel) | TAP (Bridged); default: **TUN (Tunnel)**	Virtual network device type. • **TUN -** a virtual point-to-point IP link which operates at the network layer (OSI layer 3), used when routing is required. • **TAP -** a virtual Ethernet adapter (switch), operates at the data link layer (OSI layer 2), used when bridging is required.
Protocol	UDP/TCP; default: **UDP**	Transfer protocol used by the OpenVPN connection. • **User Datagram Protocol (UDP)** - packets are sent to the recipient without error-checking or back-and-forth quality control, meaning that when packets are lost, they are gone forever. This makes it less reliable but faster than TCP; therefore, it should be used when transfer speed is crucial (for example, in video streaming, live calls). • **Transmission Control Protocol (TCP)** - most commonly used protocol in the Internet Protocol (IP) suite. It ensures the recipient will receive packets in the order they were sent by numbering, analysing response messages, checking for errors and resending them if an issue occurs. It should be used when reliability is crucial (for example, in file transfer).
Port	integer [1-65535] default: **1194**	TCP/UDP port number used for the connection. Make sure it matches the port number specified on the server side. **NOTE**: traffic on the selected port will be automatically allowed in the device firewall rules.
LZO	Adaptive/Yes/No; default: **Adaptive**	LZO data compression mode.
Authentication	TLS/Static Key; default: **TLS**	Authentication mode, used to secure data sessions. • **TLS** authentication mode uses X.509 type certificates: • Certificate Authority (CA) • Server certificate • Server key • Diffie Hellman parameters • CRL file (optional) All mentioned certificates can be generated using OpenVPN or Open SSL utilities on any type of host machine. One of the most popular utilities used for this purpose is called Easy-RSA. • **Static key** is a secret key used for server–client authentication.

Encryption	BF-CBC/AES-128-CBC/AES-192-CBC/AES-256-CBC/ AES-128-GCM/AES-192- GCM /AES-256-GCM /none; default: **BF-CBC**	Algorithm used for packet encryption.
Route traffic between clients	enable/disable; default: **disable**	Allows OpenVPN clients to communicate with each other on the VPN network.
Push option	default: **none**	Push options are a way to "push" routes and other additional OpenVPN options to connecting clients.
Keepalive interval	integer [1 to 60]; default: **10**	Frequency (in seconds) at which "keep alive" packets are sent to the remote instance. If no response is received, the device will attempt to re-establish the tunnel.
Keepalive timeout	integer [10 to 180]; default: **60**	Time in seconds. If no packets pass through the tunnel between this server and a client, the server will terminate the connection to that client after the amount of time specified in this field passes.
Virtual Network and Netmask	default: **none**	This field specifies the tunnel’s virtual IP and netmask.
HMAC algorithm	SHA1 | SHA512 | SHA384 | SHA256 | SHA224 | MD5 | None; default: **SHA1**	HMAC authentication algorithm type.
Certifcate authority	.ca file; default: **none**	Certificate authority is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.
Server certificate	.crt file; default: **none**	A type of digital certificate that is used to identify the OpenVPN server.
Serve key	.key file; default: **none**	Authenticates clients to the server.
Diffie Helman parameters	.pem file; default: **none**	DH parameters define how OpenSSL performs the Diffie-Hellman (DH) key-exchange.
CRL file (optional)	. pem file | .crl file; default: **none**	A certificate revocation list (CRL) file is a list of certificates that have been revoked by the certificate authority (CA). It indicates which certificates are no longer acccepted by the CA and therefore cannot be authenticated to the server.
Clients Setting		
Common Name	string; default: **none**	Client’s Common Name (CN) found in the client certificate file.
LAN Network	ip; default: **none**	Client’s private network (LAN) IP address.
Netmask	netmask; default: **none**	Client’s private network (LAN) IP netmask.
To Server LAN Side	default: **disable**	Enable LAN to LAN function

3.4.3.1.3 OpenVPN Client

Figure 94. Services > VPN > OpenVPN > sample_client > Edit



Overview » Instance "sample_client"

Enable	□
TUN/TAP	TUN (Tunnel)
Protocol	UDP
Port	1194
LZO	Adaptive
Authentication	TLS
Encryption	BF-CBC
Remote host/IP address	my_server_1 1194
Keepalive interval	10
Keepalive timeout	60
HMAC algorithm	SHA1
Certificate authority	Choose File No file chosen
Client certificate	Choose File No file chosen
Client key	Choose File No file chosen

Table 79. Services > VPN > OpenVPN > sample_client > Edit

Field	Value	Description
Enable	enable/disable; default: **disable**	Switches configuration enable or disable. This must be selected to make configuration active.
TUN/TAP	TUN (Tunnel) | TAP (Bridged); default: **TUN (Tunnel)**	Virtual network device type. • **TUN -** a virtual point-to-point IP link which operates at the network layer (OSI layer 3), used when routing is required. • **TAP** - a virtual Ethernet adapter (switch), operates at the data link layer (OSI layer 2), used when bridging is required.
Protocol	UDP/TCP; default: **UDP**	Transfer protocol used by the OpenVPN connection. • **User Datagram Protocol (UDP)** - packets are sent to the recipient without error-checking or back-and-forth quality control, meaning that when packets are lost, they are gone forever. This makes it less reliable but faster than TCP; therefore, it should be used when transfer speed is crucial (for example, in video streaming, live calls). • **Transmission Control Protocol (TCP)** - most commonly used protocol in the Internet Protocol (IP) suite. It ensures the recipient will receive packets in the order they were sent by numbering, analysing response messages, checking for errors and resending them if an issue occurs. It should be used when reliability is crucial (for example, in file transfer).
Port	integer [1-65535] default: **1194**	TCP/UDP port the local OpenVPN server listening on. TCP/UDP port number used for the connection. Make sure it matches the port number specified on the server side. **NOTE**: traffic on the selected port will be automatically allowed in the device firewall rules.
LZO	Adaptive/Yes/No; default: **Adaptive**	LZO data compression mode.
Authentication	TLS/Static Key; default: **TLS**	Authentication mode, used to secure data sessions. • **TLS** authentication mode uses X.509 type certificates: • Certificate Authority (CA) • Client certificate • Client key All mentioned certificates can be generated using OpenVPN or Open SSL utilities on any type of host machine. One of the most popular utilities used for this purpose is called Easy-RSA. • **Static key** is a secret key used for server–client authentication.

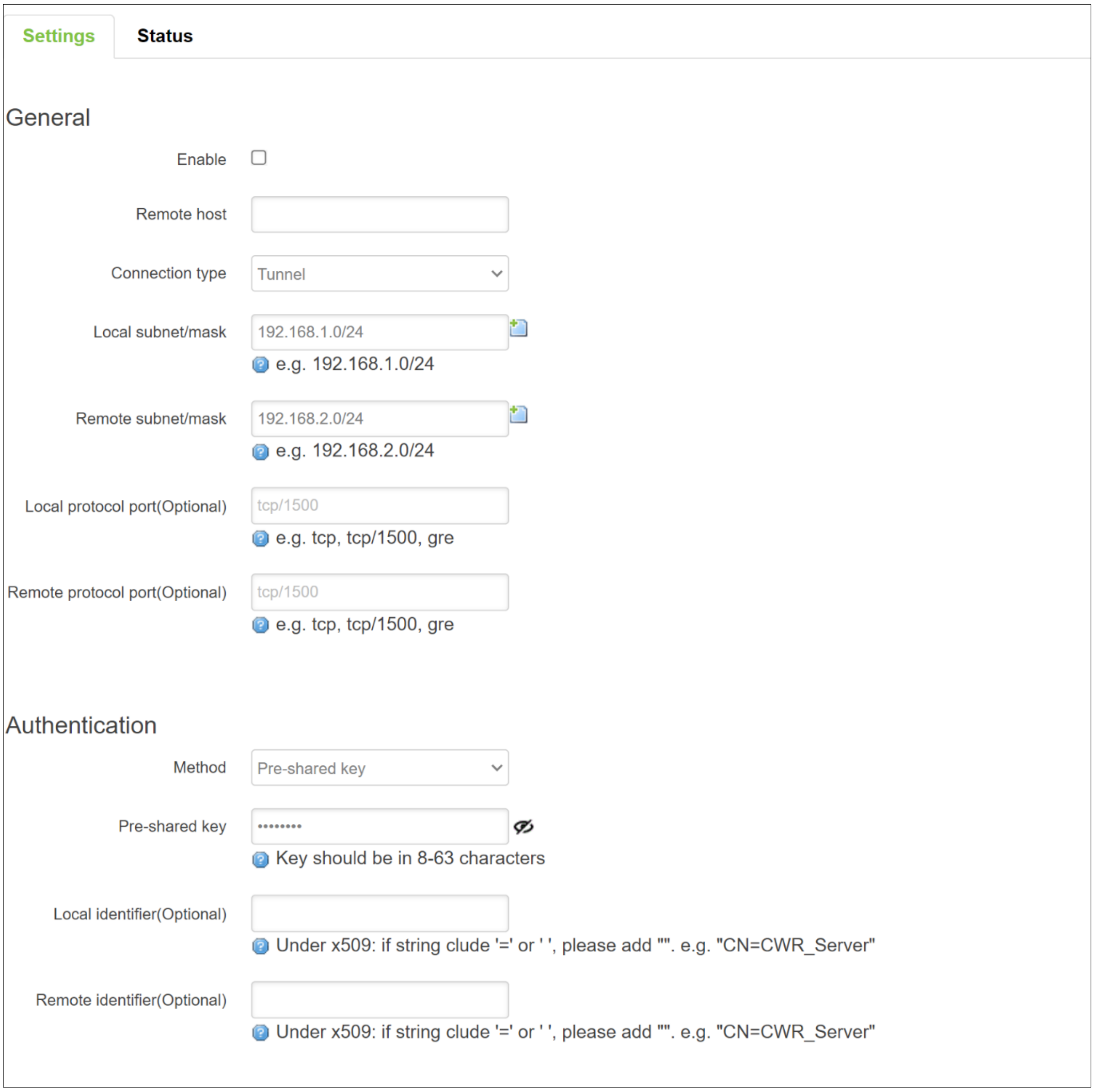
Encryption	BF-CBC/AES-128-CBC/AES-192-CBC/AES-256-CBC/ AES-128-GCM/AES-192-GCM /AES-256-GCM /none; default: **BF-CBC**	Algorithm used for packet encryption.
Rremote host/IP address	ip, netmask; default: **my_server_1 1194**	LAN IP address and LAN IP subnet of the remote network (server).
Keepalive interval	integer [1 to 60]; default: **10**	Frequency (in seconds) at which "keep alive" packets are sent to the remote instance.
Keepalive timeout	integer [10 to 180]; default: **60**	Time in seconds. If no packets pass through the tunnel between this server and a client, the server will terminate the connection to that client after the amount of time specified in this field passes.
Authentication algorithm	SHA1/SHA512SHA384/SHA256/SHA224/MD5/None; default: **SHA1**	The authentication algorithm must match with another incoming connection.
Certificate authority	.ca file; default: **none**	Certificate authority is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.
Client certificate	.crt file; default: **none**	Client certificate is a type of digital certificate that is used by client systems to make authenticated requests to a remote server. Client certificates play a key role in many mutual authentication designs, providing strong assurances of a requester's identity.
Client key	.key file; default: **none**	Authenticates the client to the server and establishes precisely who they are.

3.4.3.2 IPSec

Internet Protocol Security (IPsec) is a secure network protocol suite of IPv4 that authenticates and encrypts the packets of data sent over an IP Protocol network. It is used in virtual private networks (VPNs). IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks.

3.4.3.2.1 IPSec – Settings

Figure 95 Services > VPN > IPSec > Settings



General

Enable □

Remote host

Connection type: Tunnel

Local subnet/mask: 192.168.1.0/24
e.g. 192.168.1.0/24

Remote subnet/mask: 192.168.2.0/24
e.g. 192.168.2.0/24

Local protocol port(Optional): tcp/1500
e.g. tcp, tcp/1500, gre

Remote protocol port(Optional): tcp/1500
e.g. tcp, tcp/1500, gre

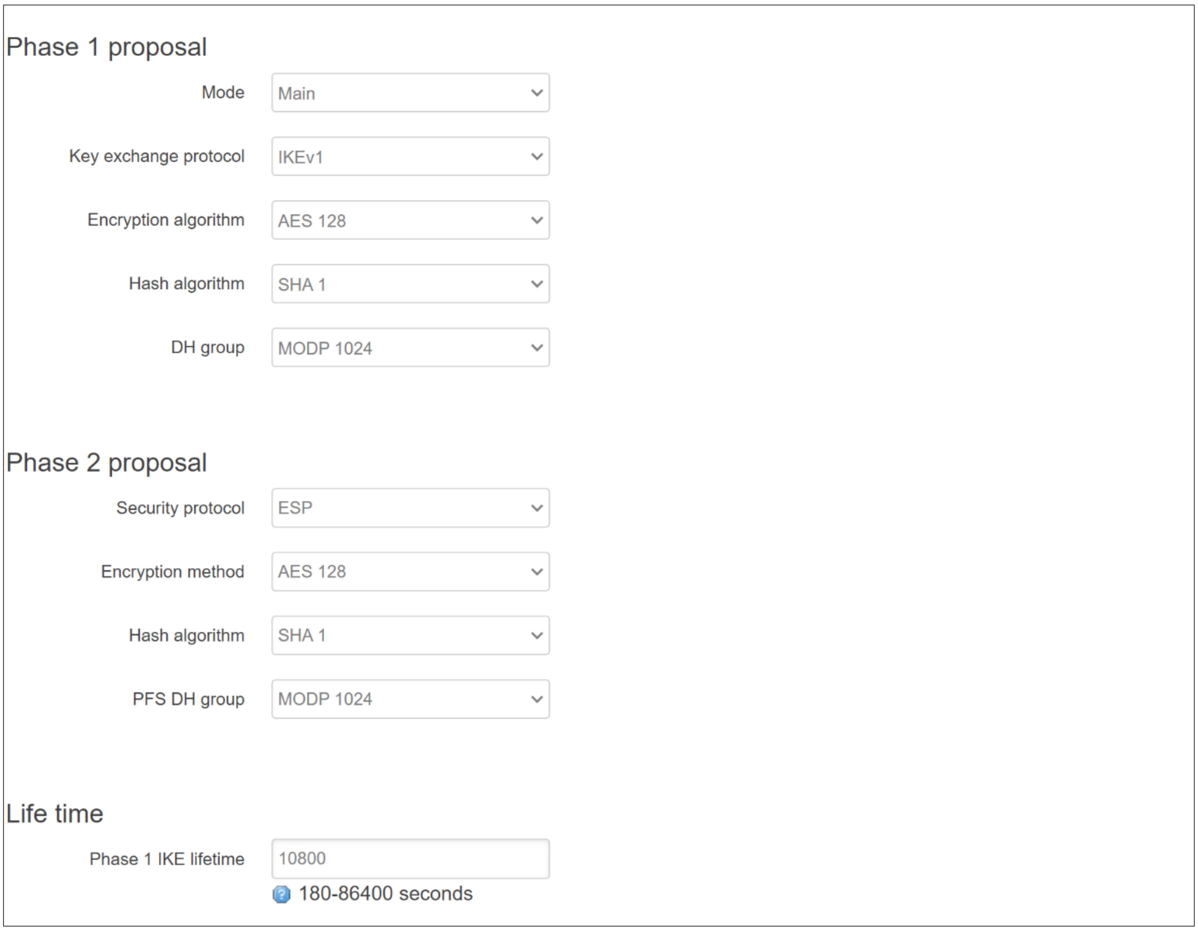
Authentication

Method: Pre-shared key

Pre-shared key: ••••••••
Key should be in 8-63 characters

Local identifier(Optional)
Under x509: if string clude '=' or ' ', please add "". e.g. "CN=CWR_Server"

Remote identifier(Optional)
Under x509: if string clude '=' or ' ', please add "". e.g. "CN=CWR_Server"



Phase 1 proposal

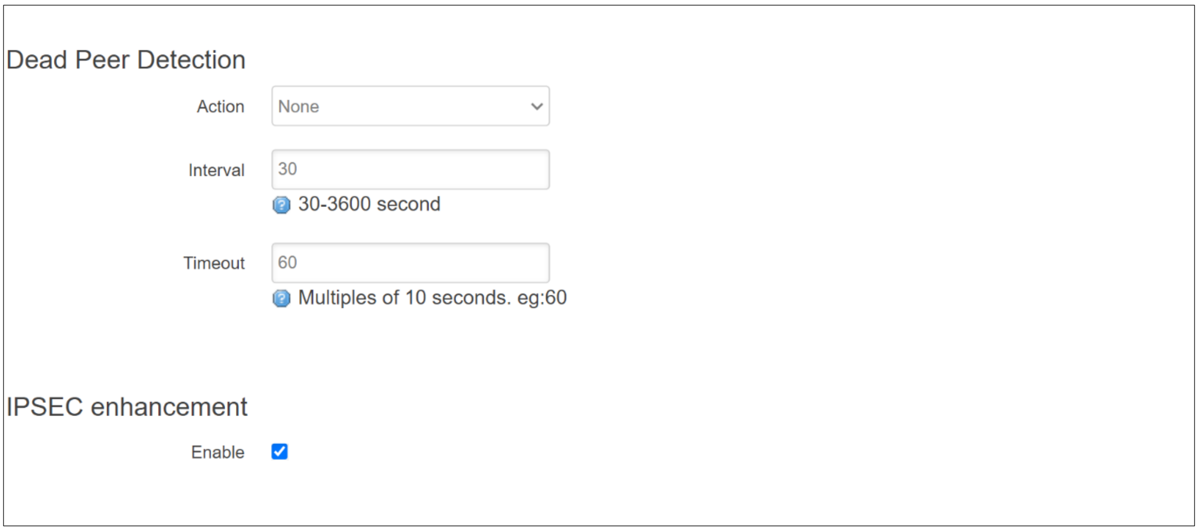
Mode	Main
Key exchange protocol	IKEv1
Encryption algorithm	AES 128
Hash algorithm	SHA 1
DH group	MODP 1024

Phase 2 proposal

Security protocol	ESP
Encryption method	AES 128
Hash algorithm	SHA 1
PFS DH group	MODP 1024

Life time

Phase 1 IKE lifetime	10800 180-86400 seconds



Dead Peer Detection

Action	None
Interval	30 30-3600 second
Timeout	60 Multiples of 10 seconds. eg:60

IPSEC enhancement

Enable	☑

Table 80 Services > VPN > IPSec > Settings

Field	Value	Description
General		
Enable	default: **disable**	Check the box to enable the IPSec function.
Remote host	default: **none**	WAN IP address of the Server | blank
Connection type	Tunnel | Transport; Default: **Tunnel**	Two distinct modes of IPsec operation
Local subnet/mask	default: **192.168.1.0/24**	(only for tunnel mode) LAN IP address/Subnet mask of the router on which the IPsec instance is configured
Remote subnet/mask (only for tunnel mode)	default: **192.168.2.0/24**	(only for tunnel mode) LAN IP address/Subnet mask of the opposite router
Protocol over IPSEC	None | GRE | L2TP; default: **None**	(only for transport mode) Only the selected protocol can be encrypted in IPSec tunnel.
Local protocol port(Optional)	default: **tcp/1500**	Only the selected protocol or port can be encrypted it.
Remote protocol port(Optional)	default: **tcp/1500**	Only the selected protocol or port can be encrypted it.
Authentication		
Method	Pre-shared key | X.509; default: **Pre-shared key**	Specify authentication method. Choose between Pre-shared key and X.509 certificates. • **Pre-shared key -** A shared password used for authentication between the peers. The value of this field must match on both instances • **X.509 -** An X.509 certificate binds an identity to a public key using a digital signature. When a certificate is signed by a trusted certificate authority, or validated by other means, the other device holding that certificate can use the public key it contains to establish secure communications.
Local identifier (Optional)	default: **none**	Defines which protocol and port can be encrypted in IPSec on local side.
Remote identifier (Optional)	default: **none**	Defines which protocol and port can be encrypted in IPSec on remote side.

Field	Value	Description
Phase 1 proposal		
Mode	Main | Aggreesive; default: **Main**	Choose the mode for outgoing connections. • **Main mode** - (a total of 6 messages) by storing most data into the first exchange. • **Aggressive mode -** performs fewer exchanges (a total of 4 messages) than
Key exchange protocol	IKEv1 | IKEv2; default: **IKEv1**	Internet Key Exchange (IKE) version used for key exchange. • **IKEv1** - more commonly used but contains known issues, for example, dealing with NAT. • **IKEv2** - updated version with increased and improved capabilities, such as integrated NAT support, supported multihosting, deprecated exchange modes (does not use main or aggressive mode; only 4 messages required to establish a connection).
Encryption algorithm	3DES | AES 128 | AES 192 | AES 256 | AES128 GCM8 | AES192 GCM8 | AES256 GCM8 | AES128 GCM12 | AES192 GCM12 | AES256 GCM12 | AES128 GCM16 | AES192 GCM16 | AES256 GCM16; default: **AES 128**	Algorithm used for data encryption.
Hash algorithm	D5 | SHA1 | SHA256 | SHA384 | SHA512; default: **SHA1**	Algorithm used for exchanging authentication and hash information.
DH group	MODP768 | MODP1024 | MODP1536 | MODP2048 | MODP3072 | MODP4096 | MODP6144 | MODP8192 | ECP192 | ECP224 | ECP256 | ECP384 | ECP521 | No PFS; default: **MODP1024**	Diffie-Hellman (DH) group used in the key exchange process. Higher group numbers provide more security, but take longer and use more resources to compute the key. Must match with another incoming connection to establish IPSec.

Field	Value	Description
Phase 2 proposal		
Security protocol	ESP | AH; default: **ESP**	• **ESP protocol -** provides data confidentiality (encryption) and authentication (data integrity, data origin authentication, and replay protection). • **AH - provides a mechanism for authentication only.**
Encryption method	3DES | AES 128 | AES 192 | AES 256 | AES128 GCM8 | AES192 GCM8 | AES256 GCM8 | AES128 GCM12 | AES192 GCM12 | AES256 GCM12 | AES128 GCM16 | AES192 GCM16 | AES256 GCM16; default: **AES 128**	Algorithm used for data encryption.
Hash algorithm	MD5 | SHA1 | SHA256 | SHA384 | SHA512; default: **SHA1**	Algorithm used for exchanging authentication and hash information.
PFS DH group	None | MODP768 | MODP1024 | MODP1536 | MODP2048 | MODP3072 | MODP4096 | MODP6144 | MODP8192 | ECP192 | ECP224 | ECP256 | ECP384 | ECP521; default: **MODP1024**	The PFS (Perfect Forward Secrecy). Must match with another incoming connection to establish IPSec.
Life time		
Phase 1 IKE lifetime	180-86400 seconds; default: **10800**	How long the keying channel of a connection (ISAKMP or IKE SA) should last before being renegotiated. The time is specified in seconds.
Phase 2 SA lifetime	180-86400 seconds; default: **3600**	How long the keying channel of a connection (ISAKMP or IKE SA) should last before being renegotiated. The time is specified in seconds.
Dead Peer Detection		
Action	None | Clear | Hold | Restart |; default: **None**	Controls the use of the Dead Peer Detection protocol where notification messages are periodically sent in order to check the liveliness of the IPsec peer.
Interval	30-3600 seconds; default: **30**	The frequency of sending messages or INFORMATIONAL exchanges to peer.
Timeout	default: **60**	Defines the timeout interval, after which all connections to a peer are deleted in case of inactivity.
IPSEC enhancement		
Enable	default: **disable**	Check the box to enhance the IPSec function.

3.4.3.2.2 IPSec – Status

Figure 96 Services > VPN > IPSec > Status

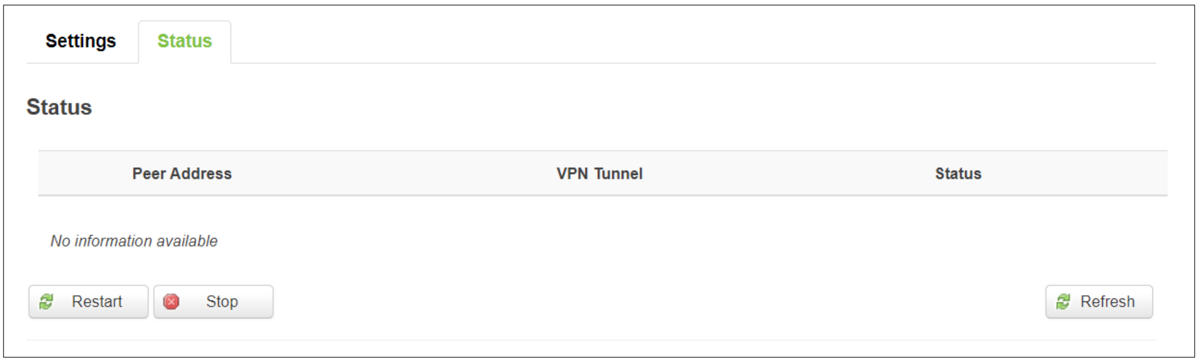


Table 81 Services > VPN > IPSec > Status

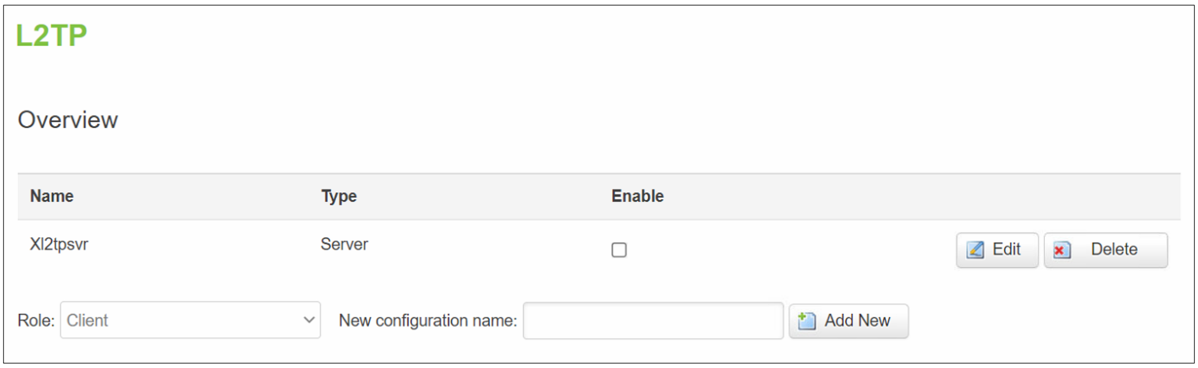
Field	Description
Peer address	The IP address of the device from which the VPN terminate.
VPN Tunnel	The local subnet/mask and the remote subnet/mask.
Status	Established time.
Restart	Restart the tunnel.
Stop	Stop the tunnel.
Refresh	Refresh the status.

3.4.3.3 L2TP

Layer 2 Tunneling Protocol (**L2TP**) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

3.4.3.3.1 L2TP Overview

Figure 97. Services > VPN > L2TP > Overview

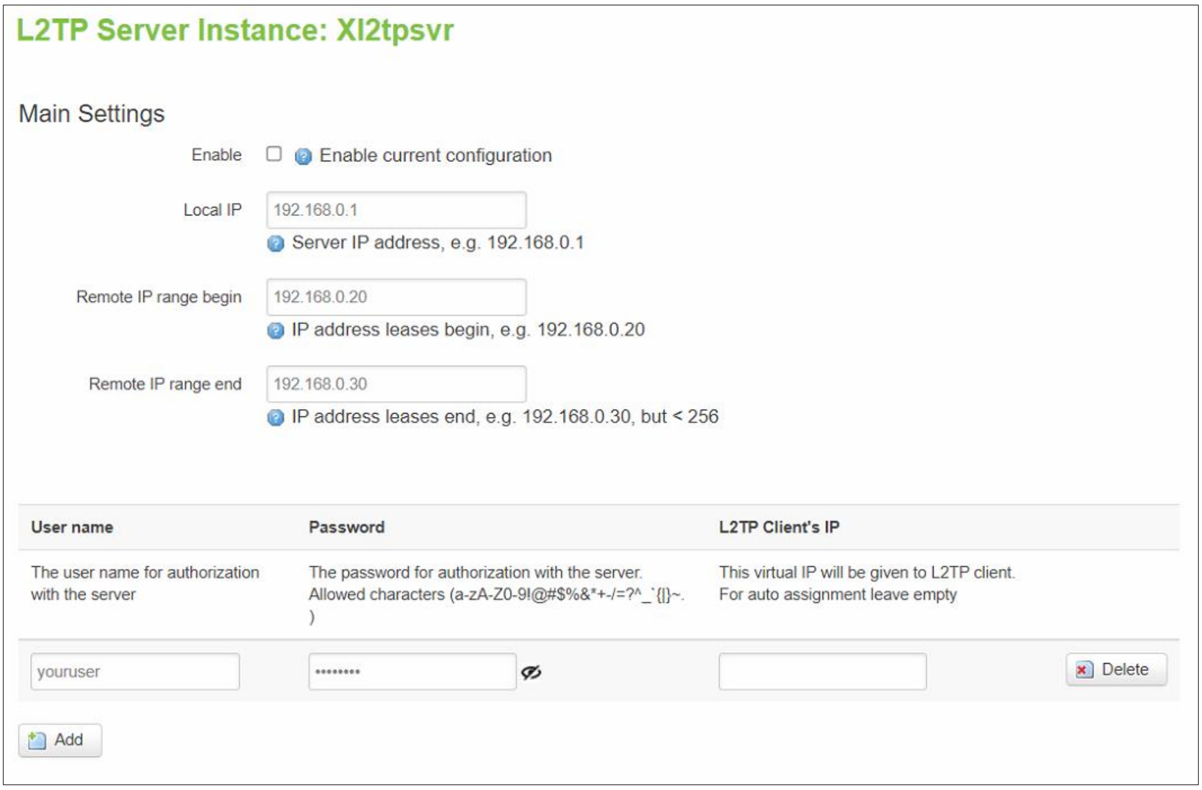


3.4.3.3.2 L2TP Server

Allows setting up a L2TP server or client. Below is L2TP server configuration example.

As mentioned in the prerequisites section, the router that acts as the **server** must have a Public Static or Public Dynamic IP address.

Figure 98. Services > VPN > L2TP > Xl2tpsvr > Edit



L2TP Server Instance: Xl2tpsvr

Main Settings

Enable ☐ Enable current configuration

Local IP: 192.168.0.1
Server IP address, e.g. 192.168.0.1

Remote IP range begin: 192.168.0.20
IP address leases begin, e.g. 192.168.0.20

Remote IP range end: 192.168.0.30
IP address leases end, e.g. 192.168.0.30, but < 256

User name	Password	L2TP Client's IP	
The user name for authorization with the server	The password for authorization with the server. Allowed characters (a-zA-Z0-9!@#$%&*+-/=?^_`{|}~.)	This virtual IP will be given to L2TP client. For auto assignment leave empty	
youruser	••••••••		Delete

The description of each field is shown in the table below.

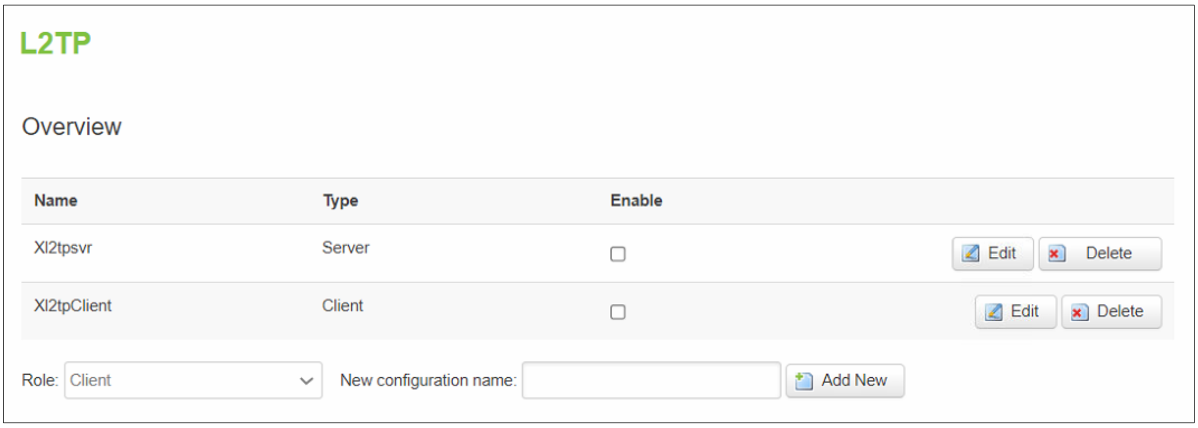
Table 82. Services > VPN > L2TP > Xl2tpsvr > Edit

Field	Value	Description
Enable	default: **disable**	Check the box to enable the L2TP Tunnel function.
Local IP	default: **192.168.0.1**	IP Address of this device.
Remote IP range begin	default: **192.168.0.20**	IP address leases beginning.
Remote IP range end	default: **192.168.0.30**	IP address leases end.
Username	default: **youruser**	Username to connect to L2TP (this) server.
Password	default: **yourpass**	Password to connect to L2TP server.
L2TP Client's IP	default: **none**	This virtual IP will be given to L2TP client. For auto assignment leave empty.

3.4.3.3.3 L2TP Client

The description of each field is shown in the table below.

Figure 99. Services > VPN > L2TP > Overview



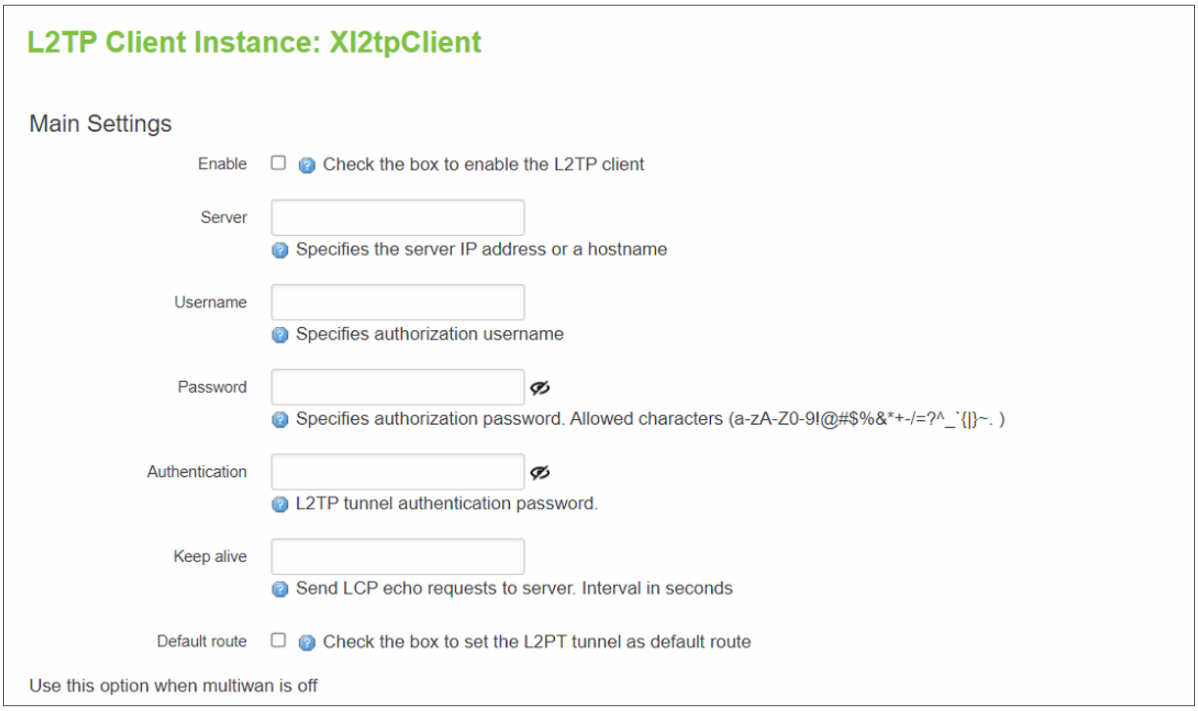
L2TP

Overview

Name	Type	Enable	
Xl2tpsvr	Server	□	Edit Delete
Xl2tpClient	Client	□	Edit Delete

Role: Client New configuration name: Add New

Figure 100. Services > VPN > L2TP > Xl2tpClient > Edit



L2TP Client Instance: Xl2tpClient

Main Settings

Enable □ Check the box to enable the L2TP client

Server: Specifies the server IP address or a hostname

Username: Specifies authorization username

Password: Specifies authorization password. Allowed characters (a-zA-Z0-9!@#$%&*+-/=?^_`{|}~.)

Authentication: L2TP tunnel authentication password.

Keep alive: Send LCP echo requests to server. Interval in seconds

Default route □ Check the box to set the L2PT tunnel as default route

Use this option when multiwan is off

Table 83. Services > VPN > L2TP > Xl2tpClient > Edit

Field	Value	Description
Enable	default: **disable**	Check the box to enable the L2TP Tunnel function.
Server	IP/hostname; default: **none**	Specifies the server IP address or a hostname.
Username	Username; default: **none**	Username to connect to L2TP server.
Password	default: **none**	Password to connect to L2TP server.
Authentication	default: **none**	L2TP tunnel authentication password.
Keep alive	default: **none**	Send LCP echo requests to server in seconds.
Default route	default: **none**	Check the box to set the L2PT tunnel as default route.

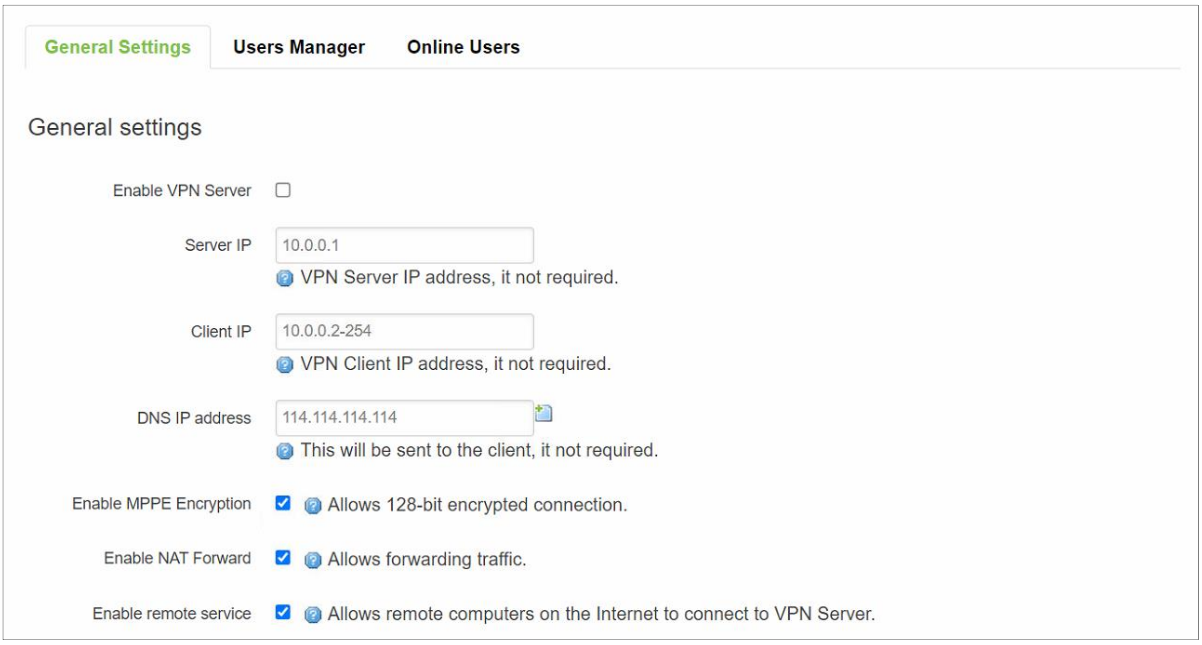
3.4.3.4 PPTP

Point-to-Point Tunneling Protocol (PPTP) is a protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network. A company no longer needs to lease its own lines for wide-area communication but can securely use the public networks. This kind of interconnection is known as a virtual private network (VPN).

3.4.3.4.1 PPTP Server – General Settings

A **PPTP server** is an entity that waits for incoming connections from PPTP clients.

Figure 101. Services > VPN > PPTP Server > General Settings



General settings

Enable VPN Server ☐

Server IP: 10.0.0.1
VPN Server IP address, it not required.

Client IP: 10.0.0.2-254
VPN Client IP address, it not required.

DNS IP address: 114.114.114.114
This will be sent to the client, it not required.

Enable MPPE Encryption ☑ Allows 128-bit encrypted connection.

Enable NAT Forward ☑ Allows forwarding traffic.

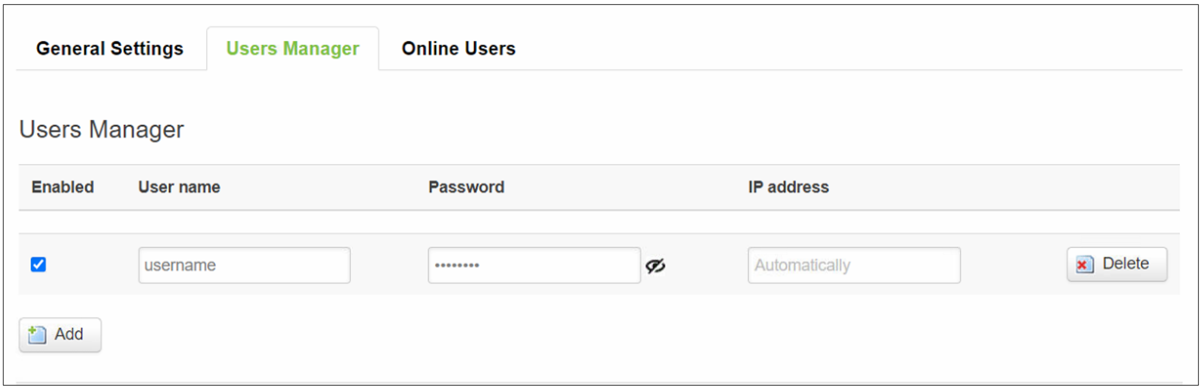
Enable remote service ☑ Allows remote computers on the Internet to connect to VPN Server.

Table 84. Services > VPN > PPTP Server > General Settings

Field	Value	Description
Enable VPN Server	default: **disable**	Check the box to enable the PPTP function.
Server IP	default: **10.0.0.1**	IP address of this CWR5805 PPTP network interface.
Client IP	default: **10.0.0.2-254**	PPTP IP address leases will begin to end from the address specified in this field.
DNS IP address	default: **114.114.114.114**	IP address of the DNS server which will be sent to the client.
Enable MPPE Encrption	default: **enable**	Allows 128-bit encrypted connection.
Enable NAT Forward	default: **enable**	Allows forwarding traffic.
Enable remote service	default: **enable**	Allows remote computers on the internet to connect to VPN server.

3.4.3.4.2 PPTP Server – Users Manager

Figure 102. Services > VPN > PPTP Server > Users Manager



Enabled	User name	Password	IP address	
☑	username	••••••••	Automatically	Delete

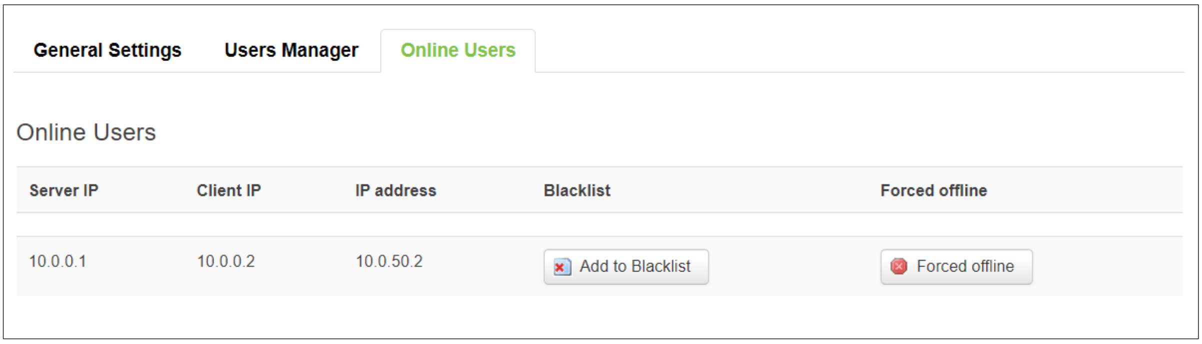
Table 85. Services > VPN > PPTP Server > Users Manager

Field	Value	Description
Enabled	default: **enable**	Check the box to enable the PPTP function.
You name	default: **username**	Username to connect to PPTP (CWR5805) server.
Password	default: **password**	Password to connect to PPTP (CWR5805) server.
IP address	default: **Automatically**	Accepted PPTP Client source IP.

3.4.3.4.3 PPTP Server – Online Users

The **Online User** section is used to user authentication settings required to successfully connect to this server. The list is empty by default.

Figure 103. Services > VPN > PPTP Server > Online Users



Server IP	Client IP	IP address	Blacklist	Forced offline
10.0.0.1	10.0.0.2	10.0.50.2	Add to Blacklist	Forced offline

Table 86. Services > VPN > PPTP Server > Online Users

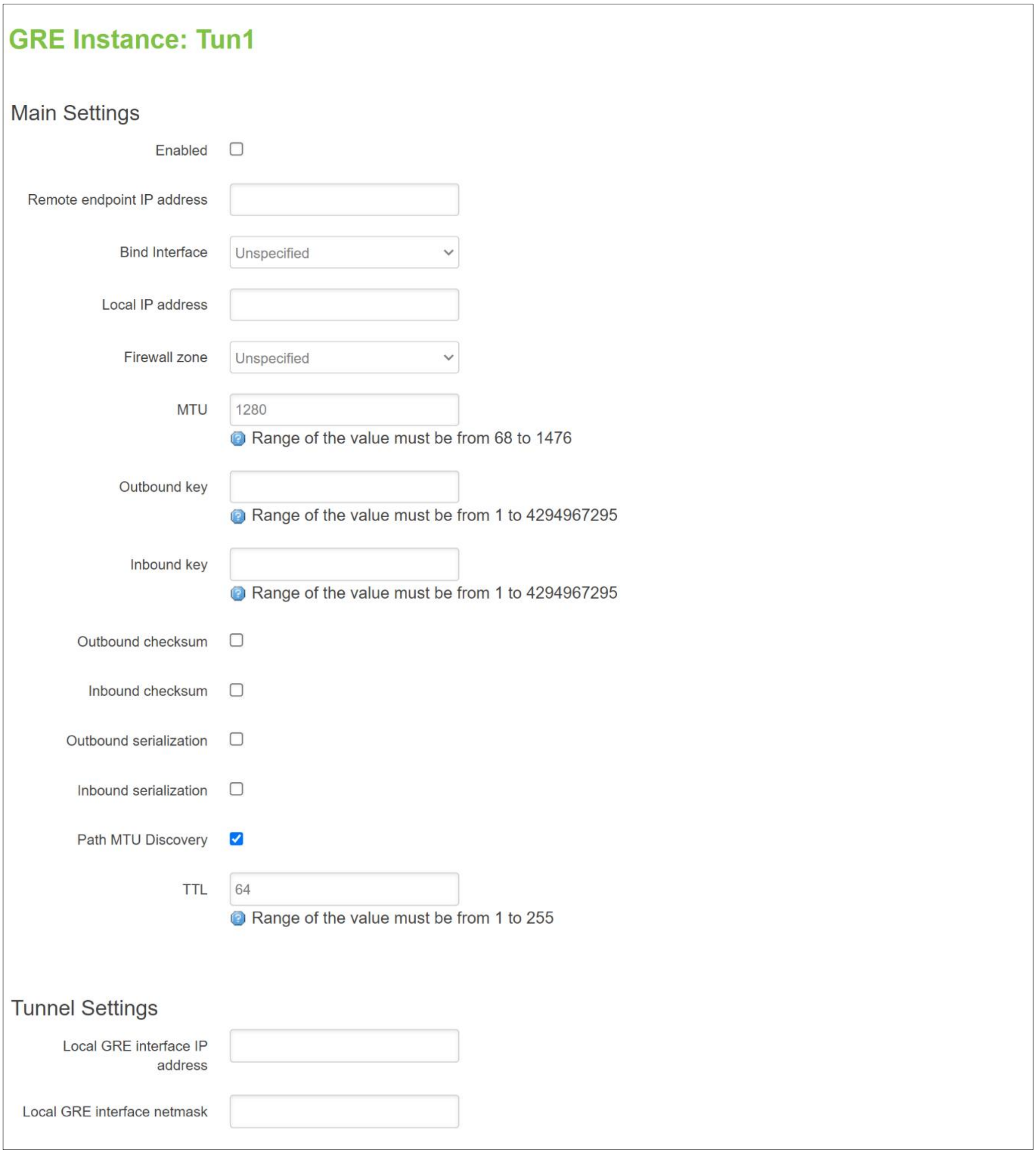
Field	Description
Server IP	The PPTP IP of the device.
Client IP	PPTP Client's PPTP IP.
IP address	PPTP Client's real IP.
Blacklist	Block PPTP Client on the list and allow everything else. Button type: Add to Blacklist/Remove from Blacklist.
Forced offine	Disconnect PPTP Client.

3.4.3.5 GRE

GRE (Generic Routing Encapsulation RFC2784) is a solution for tunneling RFC1812 private address-space traffic over an intermediate TCP/IP network such as the Internet. GRE tunneling does not use encryption it simply encapsulates data and sends it over the WAN.

3.4.3.5.1 GRE Overview

Figure 104 Services > VPN > GRE > GRE Instance: Tun1



GRE Instance: Tun1

Main Settings

Enabled	□
Remote endpoint IP address	
Bind Interface	Unspecified
Local IP address	
Firewall zone	Unspecified
MTU	1280 Range of the value must be from 68 to 1476
Outbound key	Range of the value must be from 1 to 4294967295
Inbound key	Range of the value must be from 1 to 4294967295
Outbound checksum	□
Inbound checksum	□
Outbound serialization	□
Inbound serialization	□
Path MTU Discovery	☑
TTL	64 Range of the value must be from 1 to 255

Tunnel Settings

Local GRE interface IP address	
Local GRE interface netmask	

Table 87 Services > VPN > GRE > GRE Instance: Tun1

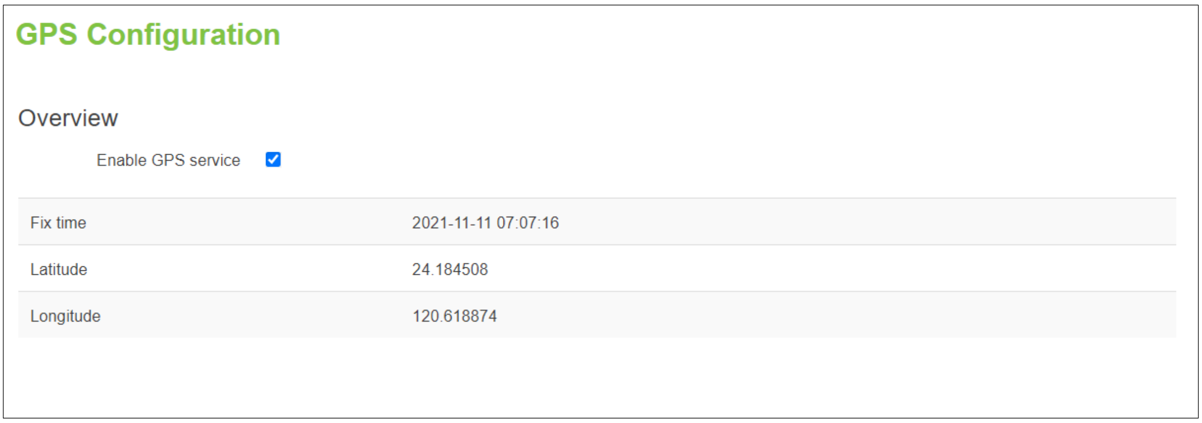
Field	Value	Description
Main Settings		
Enabled	default: **disable**	Check the box to enable the GRE function.

Remote endpoint IP address	default: **none**	The Public IP address of the opposite device.
Bind Interface	Unspecified | lan | wan; default: **Unspecified**	Network interface used to establish the GRE Tunnel.
Local IP address	default: **none**	IP Address of this device.
Firewall zone	Unspecified | lan | wan; default: **Unspecified**	Specify GRE work on which interface.
MTU	Value from 68 to 1476; default: **1280**	Sets the maximum transmission unit (MTU) size. It is the largest size of a protocol data unit (PDU) that can be transmitted in a single network layer transaction.
Outbound key	Value from 1 to 4294967295; default: **none**	A key used to identify outgoing packets. This value should match the "Inbound key" value set on the opposite GRE instance or both key values should be omitted on both sides.
Inbound key	Value from 1 to 4294967295; default: **none**	A key used to identify incoming packets. This value should match the "Outbound key" value set on the opposite GRE instance or both key values should be omitted on both sides.
Outbound checksum	default: **disable**	Check to verify outbound checksum for the GRE header and payload.
Inbound checksum	default: **disable**	Check to verify inbound checksum for the GRE header and payload.
Outbound serialization	default: **disable**	Check to verify outbound serialization for the GRE header and payload.
Inbound serialization	default: **disable**	Check to verify inbound serialization for the GRE header and payload.
Path MTU Discovery	Value from 1 to 255; default: **check | TTL: 64**	Sets a custom TTL (Time to Live) value for encapsulated packets. TTL is a field in the IP packet header which is initially set by the sender and decreased by 1 on each hop. When it reaches 0 it is dropped and the last host to receive the packet sends an ICMP "Time Exceeded" message back to the source.
Tunnel Settings		
Local GRE interface IP address	default: **none**	IP address of the local GRE Tunnel network interface.
Local GRE interface netmask	default: **none**	Subnet mask of the local GRE Tunnel network interface.

3.4.4 GPS

The Global Positioning System (GPS) is a space-based radio navigation system.

Figure 105. Services > GPS



GPS Configuration

Overview

Enable GPS service ☑

Fix time	2021-11-11 07:07:16
Latitude	24.184508
Longitude	120.618874

Table 88. Services > GPS

Field	Value	Description
Fix time	YYYY-MM-DD HH:MM:SS; default: **none**	The last GNSS fix time.
Latitude	xxx.xxxxxx; default: **none**	It it shows the angle between the straight line in the certain point and the equatorial plane.
Longitude	xxx.xxxxxx; default: **none**	It is defined as an angle pointing west or east from the Greenwich Meridian, which is taken as the Prime Meridian.

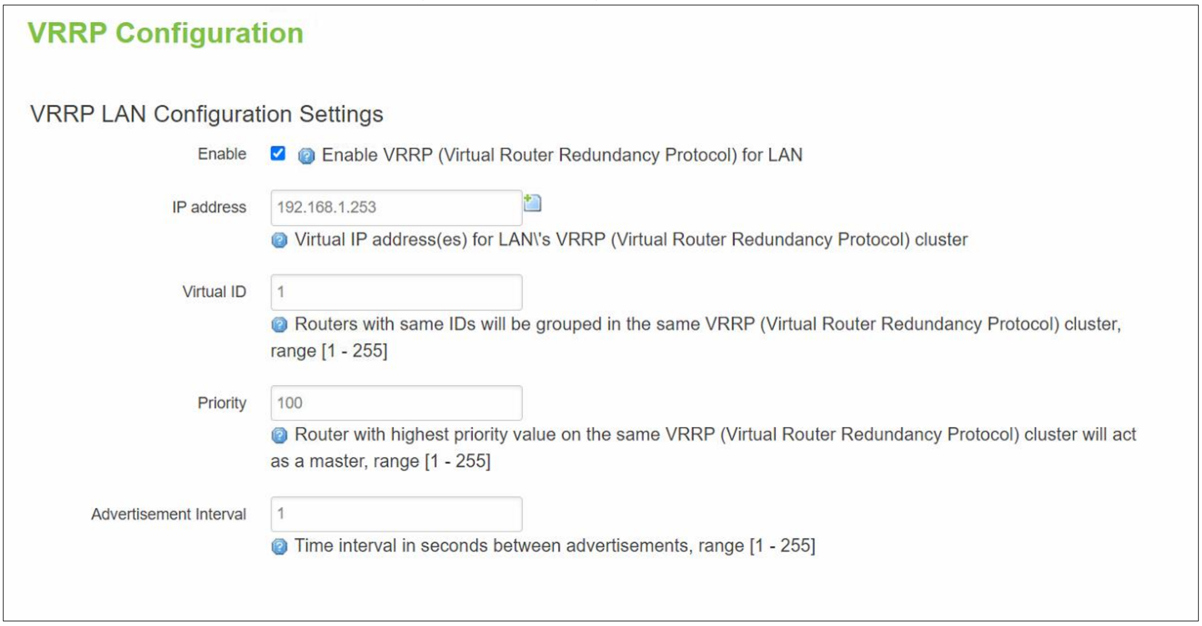
3.4.5 VRRP

The **Virtual Router Redundancy Protocol** (**VRRP**) is a computer networking protocol used for automatic default gateway selection for clients on a LAN network when the main router (Master) becomes unavailable. Another VRRP router (Backup) then assumes the role of Master and thus backing up the connection.

3.4.5.1 *VRRP LAN configuration settings*

The **VRRP LAN configuration settings** section is used to set the main settings of VRRP. Refer to the figure and table below for information on the fields contained in that section.

Figure 106. Services > VRRP > VRRP LAN Configuration Settings



VRRP Configuration

VRRP LAN Configuration Settings

Enable ☑ Enable VRRP (Virtual Router Redundancy Protocol) for LAN

IP address 192.168.1.253
Virtual IP address(es) for LAN\'s VRRP (Virtual Router Redundancy Protocol) cluster

Virtual ID 1
Routers with same IDs will be grouped in the same VRRP (Virtual Router Redundancy Protocol) cluster, range [1 - 255]

Priority 100
Router with highest priority value on the same VRRP (Virtual Router Redundancy Protocol) cluster will act as a master, range [1 - 255]

Advertisement Interval 1
Time interval in seconds between advertisements, range [1 - 255]

Table 89. Services > VRRP > VRRP LAN Configuration Settings

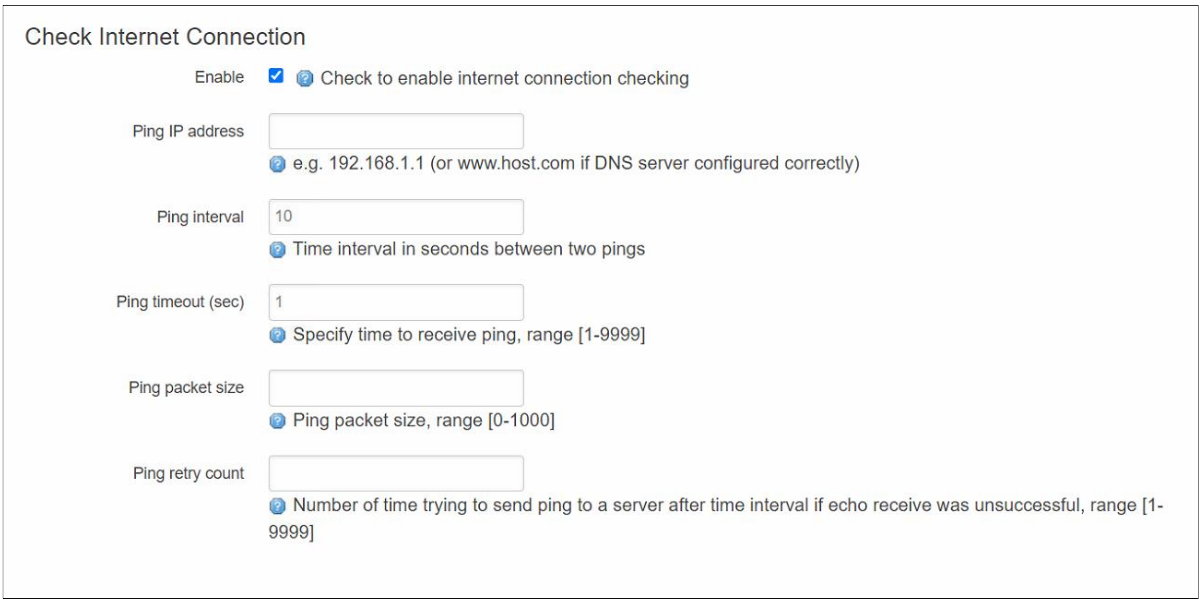
Field	Value	Description
Enable	default: **disable**	Turns VRRP on or off.
IP address	default: **192.168.1.253**	Virtual IP address for the router's LAN VRRP cluster.
Virtual ID	integer [1 - 255]; default: **1**	The Virtual Router Identifier (VRID) is a field in the VRRP packet IP header used to identify the virtual router in the VRRP cluster. Routers with identical IDs will be grouped in the same VRRP cluster.
Priority	integer [1 - 255]; default: **100**	VRRP priority of the virtual router. Smaller values equal higher priority. The router with the highest priority is considered to be the *Master router* while other routers are *Backup routers*. • **Master router** - the first hop router in the VRRP cluster (i.e., the router that provides connectivity to LAN devices by default). • **Backup router** - assumes the role of Master router in case it becomes unavailable. If there are multiple Backup routers in the VRRP cluster, the one with the highest priority will assume the role of Master.
Advertisement Interval	integer [1 - 255]; default: **1**	Time interval in seconds between advertisements.

3.4.5.2 *Check Internet connection*

The **Check Internet connection** section is used to set the parameters that define how the router will determine whether the Internet connection is still available or not. This is done by periodically sending ICMP packets to a defined host and awaiting responses. If no response is received after a defined period of time, the connection is determined to be down, and thus the role of Master is assumed by another router in the network.

Refer to the figure and table below for information on the fields contained in the Check Internet connection section.

Figure 107. Services > VRRP > Check Internet Connection



Check Internet Connection

Enable ☑ Check to enable internet connection checking

Ping IP address
e.g. 192.168.1.1 (or www.host.com if DNS server configured correctly)

Ping interval 10
Time interval in seconds between two pings

Ping timeout (sec) 1
Specify time to receive ping, range [1-9999]

Ping packet size
Ping packet size, range [0-1000]

Ping retry count
Number of time trying to send ping to a server after time interval if echo receive was unsuccessful, range [1-9999]

Table 90. Services > VRRP > Check Internet Connection

Field	Value	Description
Enable	default: **none**	Turns Internet connection checking on or off.
Ping IP address	default: **none**	IP address or hostname to which the router will send ICMP packets. This is used to determine whether the Internet connection is still available or not. Therefore, it is recommended that you enter the address of remote host that is usually available (for example, *8.8.8.8*).
Ping interval	default: **10**	Time interval (in seconds) between two Pings.
Ping timeout (sec)	integer [1 to 9999]; default: **1**	The maximum amount of time the router will wait for a response to a ping request. If it does not receive a response for the amount of time defined in this field, the ping request will be considered to have failed.
Ping packet size	integer [1 to 1000]; default: **none**	The size (in bytes) of sent ICMP packets.
Ping retry count	integer [1 to 9999]; default: **none**	How many times the router will retry sending ping requests before determining that the Internet connection has failed.

3.4.6 MQTT

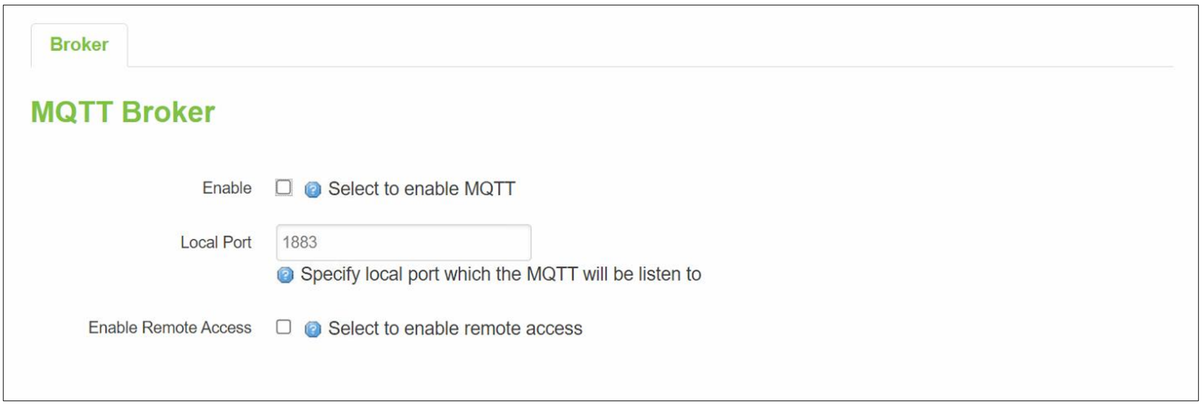
MQTT (MQ Telemetry Transport or Message Queue Telemetry Transport) is an ISO standard (ISO/IEC PRF 20922) publish-subscribe-based "lightweight" messaging protocol for use on top of the TCP/IP protocol. It is designed to send short messages from one client (*publisher*) to another (*subscriber*) through *brokers*, which are responsible for message delivery to the end point.

3.4.6.1 MQTT Broker

CWR5805 devices support this functionality via an open source Mosquitto broker. The messages are sent this way: a client (subscriber) subscribes to a topic(s); a publisher posts a message to that specific topic(s). The broker then checks who is subscribed to that topic(s) and transmits data from the publisher to the subscriber.

The **MQTT Broker** is an entity that listens for connections on the specified port and relays received messages to MQTT client. To begin using this device as an MQTT Broker, enable it in this page. In order to make the device accept MQTT connections from WAN (remote networks), you also need to check the 'Enable Remote Access' button on.

Figure 108. Services > MQTT > Broker



MQTT Broker

Enable □ Select to enable MQTT

Local Port 1883
Specify local port which the MQTT will be listen to

Enable Remote Access □ Select to enable remote access

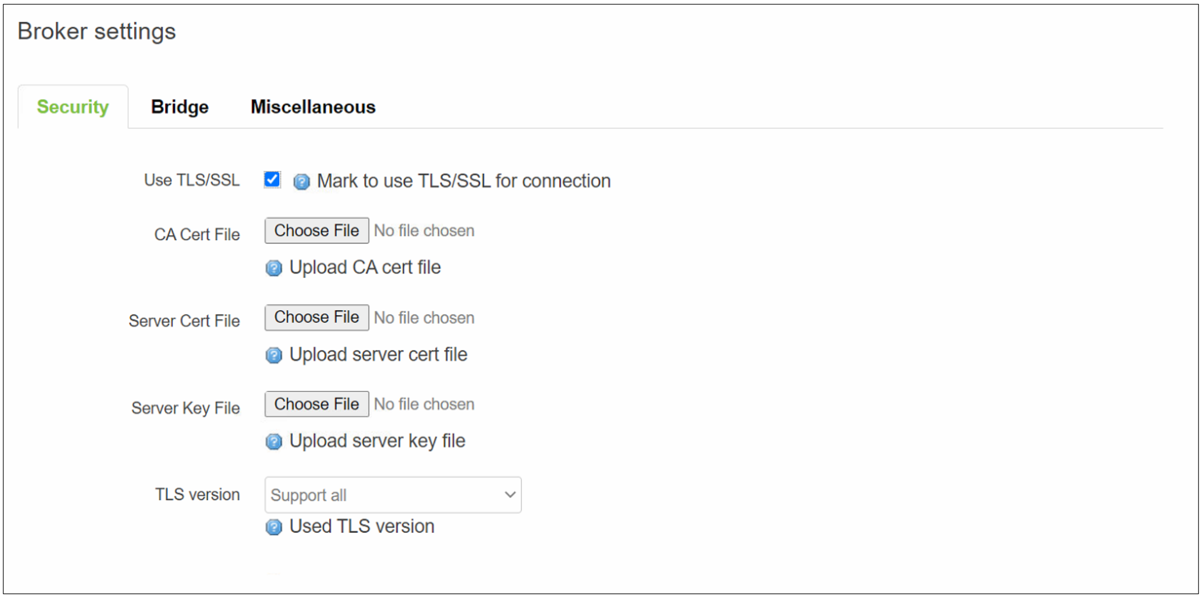
Table 91. Services > MQTT > Broker

Field	Value	Description
Enable	default: **disable**	Enable/Disable MQTT Broker.
Local Port	Integer [0 - 65535]; default: **1883**	The TCP port on which the MQTT broker will listen for connections.
Enable Remote Access	default: **disable**	Enable/Disable remote access to this MQTT broker function.

3.4.6.2 Broker Settings

3.4.6.2.1 Broker - Security

Figure 109. Services > MQTT > Security



Broker settings

Use TLS/SSL ☑ Mark to use TLS/SSL for connection

CA Cert File Choose File No file chosen
Upload CA cert file

Server Cert File Choose File No file chosen
Upload server cert file

Server Key File Choose File No file chosen
Upload server key file

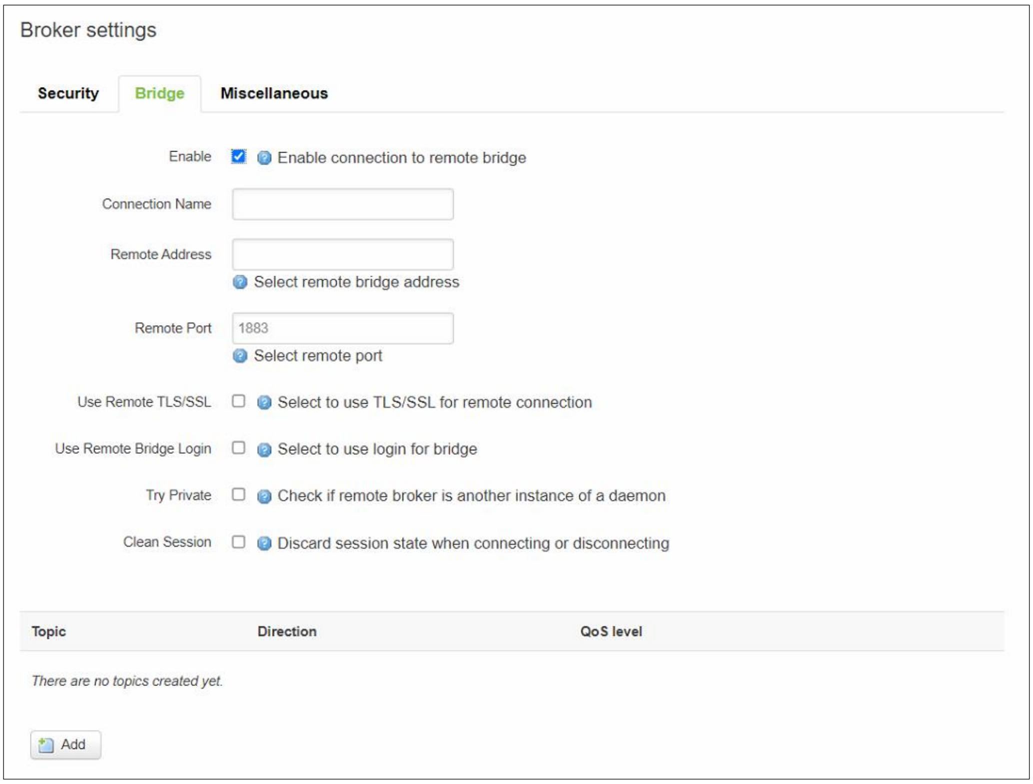
TLS version Support all
Used TLS version

Table 92. Services > MQTT > Security

Field	Value	Description
Use TLS/SSL	default: **disable**	Turns the use of TLS/SSL for this MQTT connection on or off.
CA Cert File	File type: .ca file default: **none**	Uploads a Certificate Authority (CA) file. A Certificate Authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.
Server Cert File	File type: .crt file default: **none**	Uploads a server (broker) certificate file. A certificate file is a type of digital certificate that is used by client systems to make authenticated requests to a remote server.
Server Key File	File type: .key file default: **none**	Uploads a server (broker) key file.
TLS version	tlsv1.1/tlsv1.2/Support all; default: Support all	Specifies which TLS version(s) is will be supported by this broker.

3.4.6.2.2 Borker - Bridge

Figure 110. Services > MQTT > Bridge



Broker settings

Enable ☑ Enable connection to remote bridge

Connection Name

Remote Address
Select remote bridge address

Remote Port 1883
Select remote port

Use Remote TLS/SSL ☐ Select to use TLS/SSL for remote connection

Use Remote Bridge Login ☐ Select to use login for bridge

Try Private ☐ Check if remote broker is another instance of a daemon

Clean Session ☐ Discard session state when connecting or disconnecting

Topic	Direction	QoS level

There are no topics created yet.

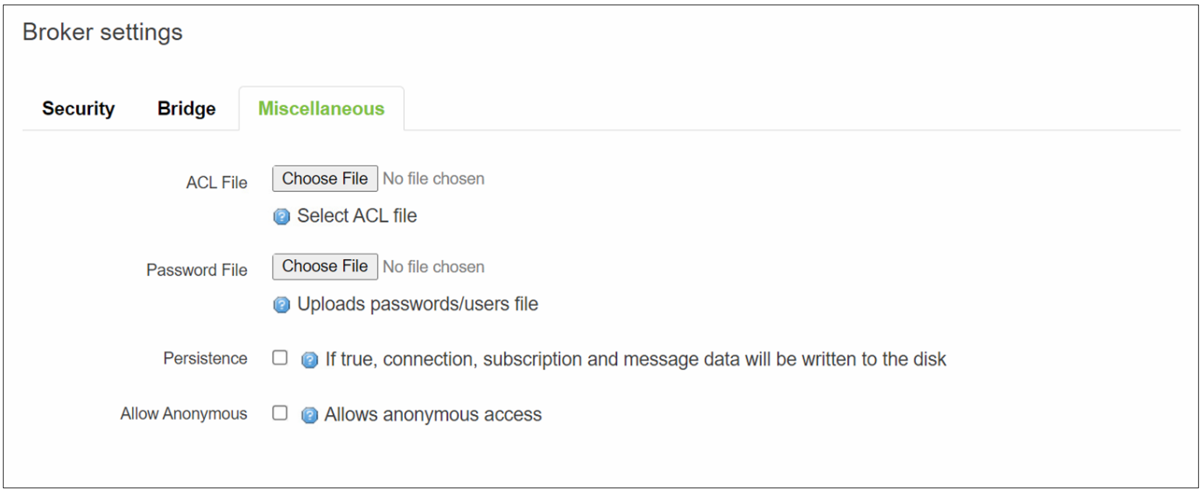
Table 93. Services > MQTT > Bridge

Field	Value	Description
Enable	default: **disable**	Enable/Disable MQTT Bridge.
Connection Name	default: **none**	Name of the Bridge connection. This is used for easier management purposes.
Remote Address	default: **none**	Remote Broker's address.
Remote Port	integer [0-65535]; default: **1883**	Specifies which port the remote broker uses to listen for connections.
Use Remote TLS/SSL	default: **disable**	Enables the use of TSL/SSL certificates of the remote broker. If this is checked, you will be prompted to upload TLS/SSL certificates. More information can be found in the Security section of this chapter.
Use Remote Bridge Login	default: **disable**	Indicates whether the remote side of the connection requires login information. If this is turned on, you will be required to enter a remote client ID, Username and password.
Try Private	default: **disable**	Check if the remote Broker is another instance of a daemon.
Clean Session	default: **disable**	When turned on, discards session state after connecting or disconnecting.
Topic Name	default: **none**	The name of the topics that the broker will subscribe to.
Direction	Out/In/Both; default: **none**	The direction that the messages will be shared.
QoS Level	At most once (0) | At least once (1) | Exactly once (2) default: **none**	Sets the publish/subscribe QoS level used for this topic

3.4.6.2.3 Borker – Miscellaneous

The **Miscellaneous** section is used to configure MQTT broker parameters that are related to neither Security nor Bridge.

Figure 111. Services > MQTT > Miscellaneous



Broker settings

ACL File: Choose File No file chosen
Select ACL file

Password File: Choose File No file chosen
Uploads passwords/users file

Persistence ☐ If true, connection, subscription and message data will be written to the disk

Allow Anonymous ☐ Allows anonymous access

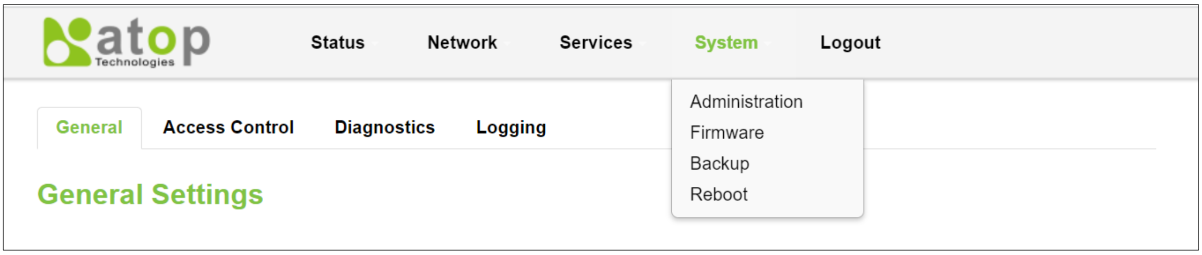
Table 94. Services > MQTT > Miscellaneous

Field	**Value**	**Description**
ACL File	ACL file default: **none**	Uploads an ACL file. The contents of this file are used to control client access to topics of the broker.
Password File	Password file default: **none**	Uploads a password. A password file stores Usernames and corresponding passwords, used for authentication.
Persistence	default: **disable**	When turned on, connection, subscription and message data will be written to the disk. Otherwise, the data is stored in the device memory only.
Allow Anoymous	default: **disable**	Turns anonymous access to this broker on or off.

3.5 System

As shown in the Figure below, the system menu consists of the following sub-menus: Administration, Firmware, Backup and Reboot which are related to system-level setup on the CWR5805 device.

Figure 112. System



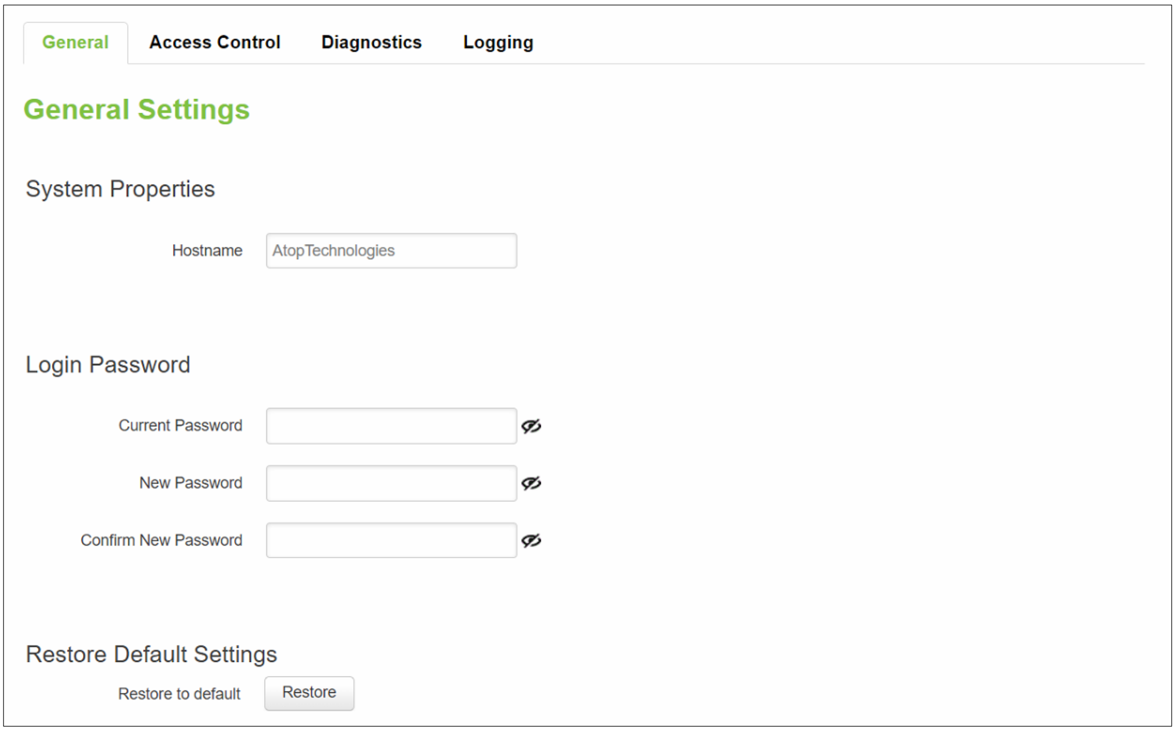
3.5.1 Administration

In **Hostnames** section, it provides a static mapping of an IP address to a hostname, which will be served by the DNS on the CWR5805 device. The hostname will also display on the Hostname field of DHCP Release section of the Overview menu when a DHCP client device is assigned a mapped IP address.

In the **Login Password** section, you can improve the system security by changing the password from the default value to ensure that only the authorized access to the router is allowed.

Click the "**Restore**" button to reset the configuration files to factory default settings of the CWR5805 device.

Figure 113. System > Administration > General Settings



Hostname: AtopTechnologies

Table 95. System > Administration > General Settings

Field	Description
Hostname	Hostname which is mapped to a specified IP address.
Current Password	Input current password for admin account.
New Password	Input new password for admin account.
Confirm New Password	Re-enter the new password for admin account. Both values on Password field and Comfirmation field must be the same, so that the new password can be saved and takes effect.

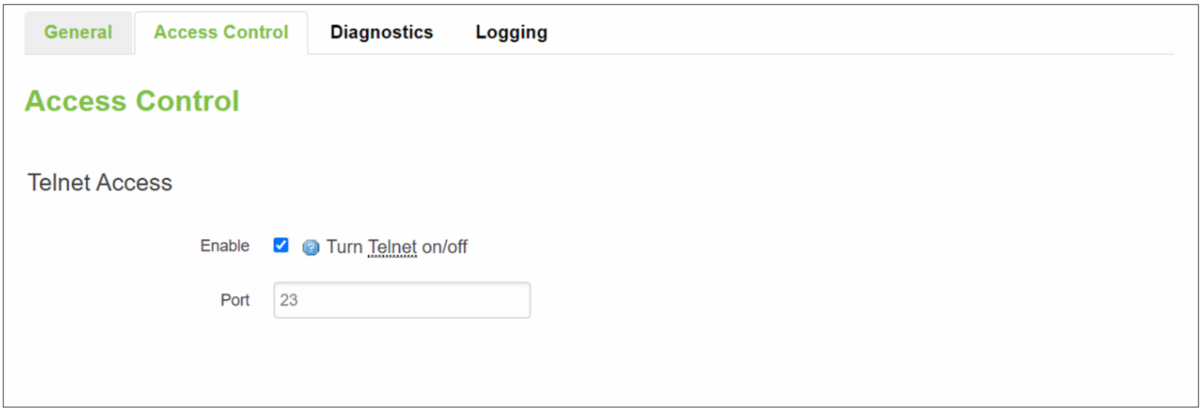
3.5.1.1 Access Control

The **Access Control** page is used to manage remote and local access to device.

***Important**: turning on remote access leaves your device vulnerable to external attackers. Make sure you use a strong password.*

3.5.1.1.1 Telnet Access

Figure 114. System > Administrator > Access Control > Telnet Access



Access Control

Telnet Access

Enable ☑ Turn Telnet on/off

Port 23

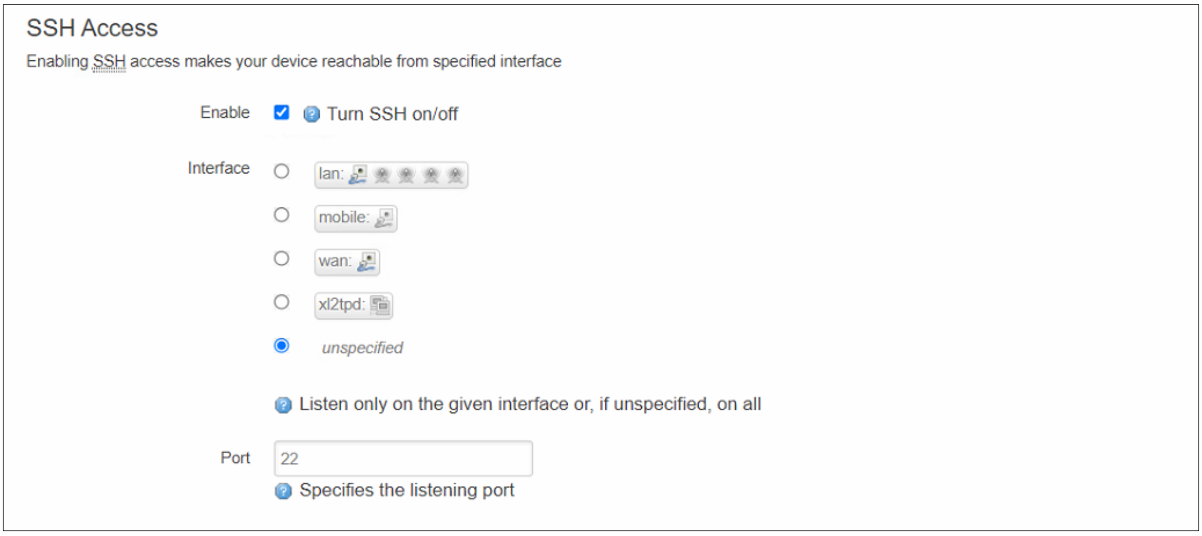
Table 96. System > Administrator > Access Control > Telnet Access

Field	Value	Description
Enable	defaut: **enable**	Check box to enable Telnet access.
Port	default: **23**	Port to be used for Telnet connection.

3.5.1.1.2 SSH Access

In the **SSH Access** Section within the **Administration** sub-menu, you can enable the SSH service (dropbear). The service will allow the remote SSH hosts to access CWR5805 device from the specified network interface.

Figure 115. System > Administrator > Access Control > SSH Access



SSH Access

Enabling SSH access makes your device reachable from specified interface

Enable ☑ Turn SSH on/off

Interface ○ lan: ○ mobile: ○ wan: ○ xl2tpd: ● *unspecified*

Listen only on the given interface or, if unspecified, on all

Port 22

Specifies the listening port

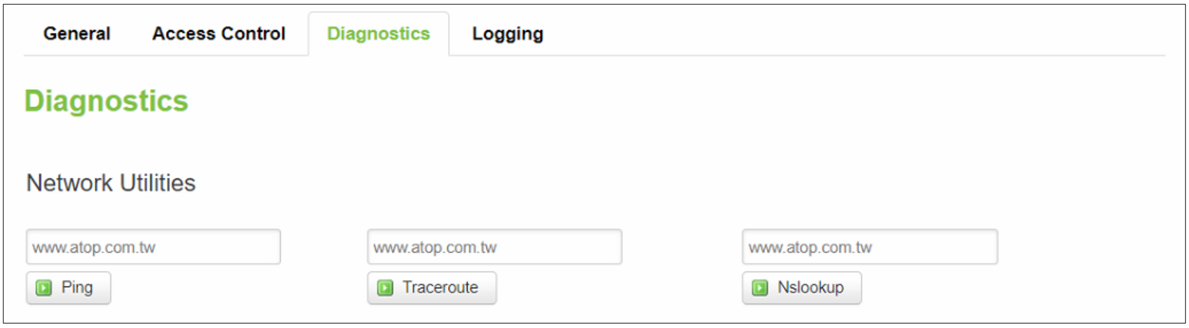
Table 97. System > Administrator > Access Control > SSH Access

Field	Value	Description
Enable	default: **enable**	Turn SSH service on/off.
Interface	default: **unspecified**	Network interface that the SSH service will be listening to.
Port	default: **22**	Port number that the SSH service will be listening to.

3.5.1.2 Diagnostics

There are three network diagnostic utilities available in **Diagnostics** webpage under Network menu. As shown in the Figure below, these utilities are called **ping**, **traceroute**, and **nslookup**. Each utility can be used to test network functionality, and to diagnose network quality and network connection state.

Figure 116. System > Administrator > Access Control > Diagnostics



Diagnostics

Network Utilities

www.atop.com.tw

www.atop.com.tw

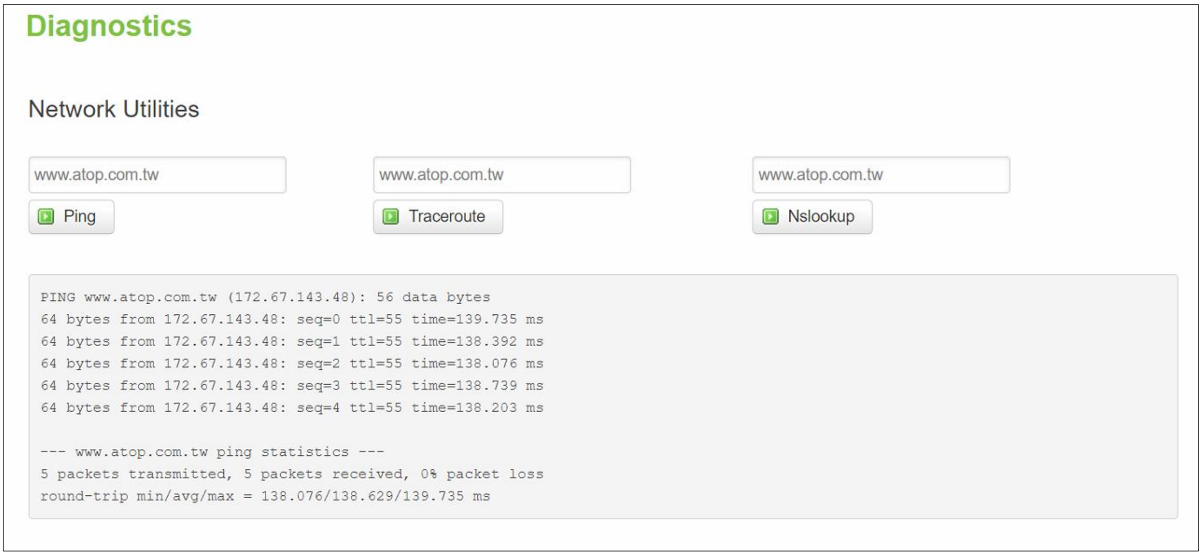
www.atop.com.tw

3.5.1.2.1 Ping

The ping network diagnostic utility is used to test network reachability. You can use the **Ping** function to determine whether CWR5805 device can reach the gateway or other devices in the network.

To use the Ping, enter a destination IP address or FQDN (Fully Qualified Domain Name) in the text box above the **Ping** button and click Ping button to start a ping process as shown in the Figure below. This process takes a few second, also represents successful ping process without packet loss from CWR5805 device to http://www.atop.com.tw and back.

Figure 117. System > Administrator > Access Control > Diagnostics > Ping



www.atop.com.tw www.atop.com.tw www.atop.com.tw

```
PING www.atop.com.tw (172.67.143.48): 56 data bytes
64 bytes from 172.67.143.48: seq=0 ttl=55 time=139.735 ms
64 bytes from 172.67.143.48: seq=1 ttl=55 time=138.392 ms
64 bytes from 172.67.143.48: seq=2 ttl=55 time=138.076 ms
64 bytes from 172.67.143.48: seq=3 ttl=55 time=138.739 ms
64 bytes from 172.67.143.48: seq=4 ttl=55 time=138.203 ms

--- www.atop.com.tw ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 138.076/138.629/139.735 ms
```

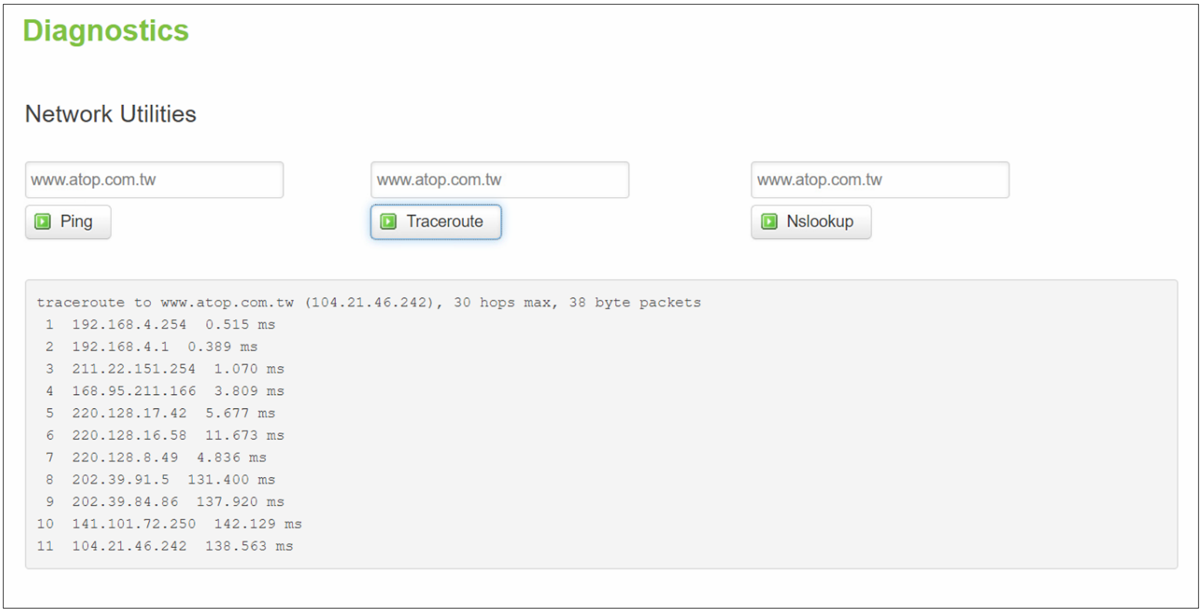
3.5.1.2.2 Traceroute

The traceroute network diagnostic utility is used to trace routing path of packets.

You can use the **Traceroute** function to trace the routes of packets to destination IP address or FQDN from CWR5805 device in the network. To use Traceroute function, enter a destination IP address or FQDN in the text box above the **Traceroute** button and click the button to start a traceroute process as shown in the Figure below.

This process usually takes a few seconds, also represents a successful traceroute process from CWR5805 device to Atop's website http://www.atop.com.tw.

Figure 118. System > Administrator > Access Control > Diagnostics > Traceroute



www.atop.com.tw www.atop.com.tw www.atop.com.tw

```
traceroute to www.atop.com.tw (104.21.46.242), 30 hops max, 38 byte packets
 1  192.168.4.254  0.515 ms
 2  192.168.4.1  0.389 ms
 3  211.22.151.254  1.070 ms
 4  168.95.211.166  3.809 ms
 5  220.128.17.42  5.677 ms
 6  220.128.16.58  11.673 ms
 7  220.128.8.49  4.836 ms
 8  202.39.91.5  131.400 ms
 9  202.39.84.86  137.920 ms
10  141.101.72.250  142.129 ms
11  104.21.46.242  138.563 ms
```

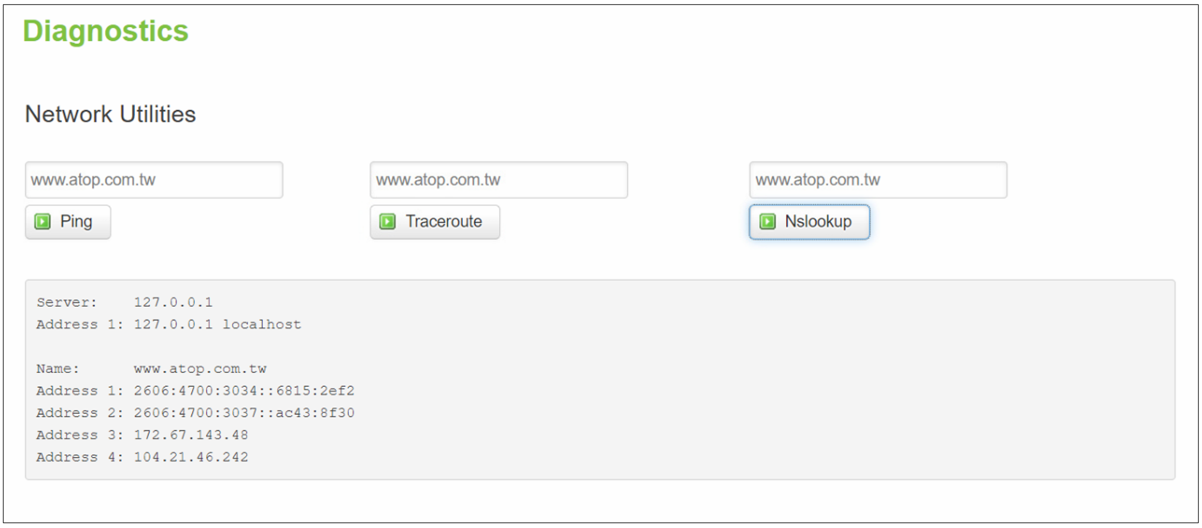
3.5.1.2.3 Nslookup

The nslookup network diagnostic utility is used to send a query to the DNS (Domain Name System) to obtain domain or IP address mapping, or other DNS records.

You can use the **Nslookup** function to query an IP address mapping of destination FQDN from CWR5805 device in the network. To use the Nslookup function, enter a FQDN in the text box above the **Nslookup** button and click it to start a nslookup process as shown in the Figure below.

This process usually takes a few seconds, also represents a successful nslookup process from CWR5805 device to the Atop's website http://www.atop.com.tw.

Figure 119. System > Administrator > Access Control > Diagnostics > Nslookup



Diagnostics

Network Utilities

www.atop.com.tw www.atop.com.tw www.atop.com.tw

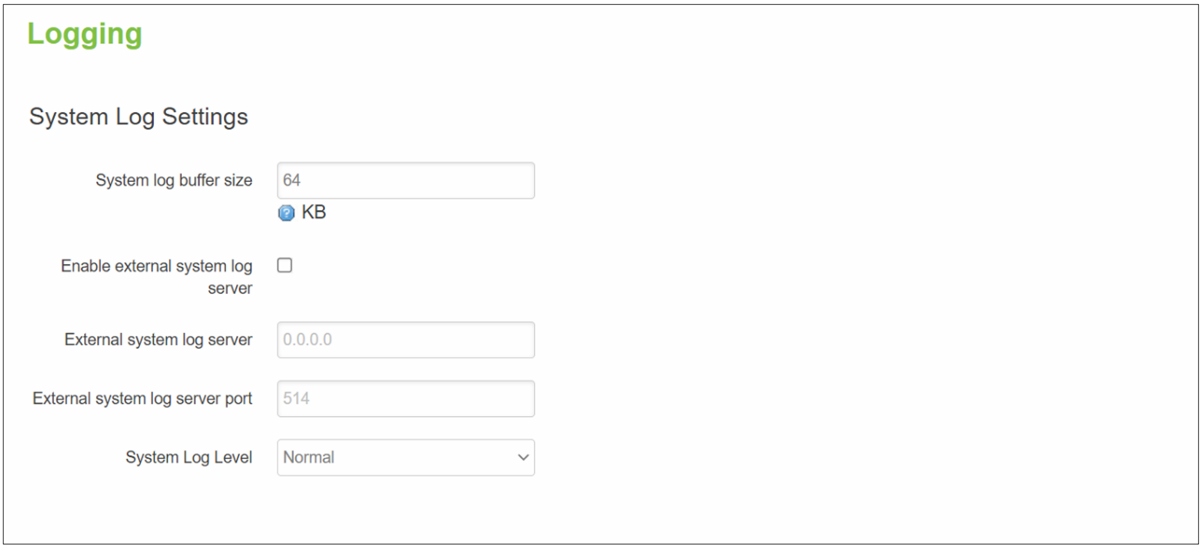
```
Server:    127.0.0.1
Address 1: 127.0.0.1 localhost

Name:      www.atop.com.tw
Address 1: 2606:4700:3034::6815:2ef2
Address 2: 2606:4700:3037::ac43:8f30
Address 3: 172.67.143.48
Address 4: 104.21.46.242
```

3.5.1.3 Logging

Shows the **Logging** tab within the **System** sub-menu. You can monitor the system log for debugging purpose on the CWR5805 device. The configuration is also allowed you to send message log to the external server.

Figure 120. System > Administrator > Access Control > Logging



Logging

System Log Settings

System log buffer size: 64 KB

Enable external system log server: □

External system log server: 0.0.0.0

External system log server port: 514

System Log Level: Normal

Table 98. System > Administrator > Access Control > Logging

Field	Value	Description
System Log Buffer Size	default: **64**	Size of the system log message buffer.
External System Log Server	default: **disable**	IP address of a syslog server to which the system log messages should be sent in addition to the local destination.
External System Log Server Port	default: **none**	Port number of the remote syslog server
Log Output Level	default: **none**	The maximum log level for system messages to be logged to the console. Only messages with a level lower than this will be printed to the console. Messages with higher system level will have lower number of log level. For example, the highest system level message will be saved in log level 0. If you want more messages in console, put "log output level" to Debug. But if you want less messages in the console, put "log output level" to Error.
Cron Output Level	Debug/Normal/ Warning; default: N**ormal**	The minimum level for cron messages to be logged to syslog

3.5.2 Firmware

The mechanism to upgrade firmware of the CWR5805 device to optimize performance or fix bugs is provided in the **Flash new firmware image** Section within the **Backup/Flash Firmware** sub-menu. It is imperative that CWR5805 device must **NOT be turned off or powered off during the firmware upgrade**.

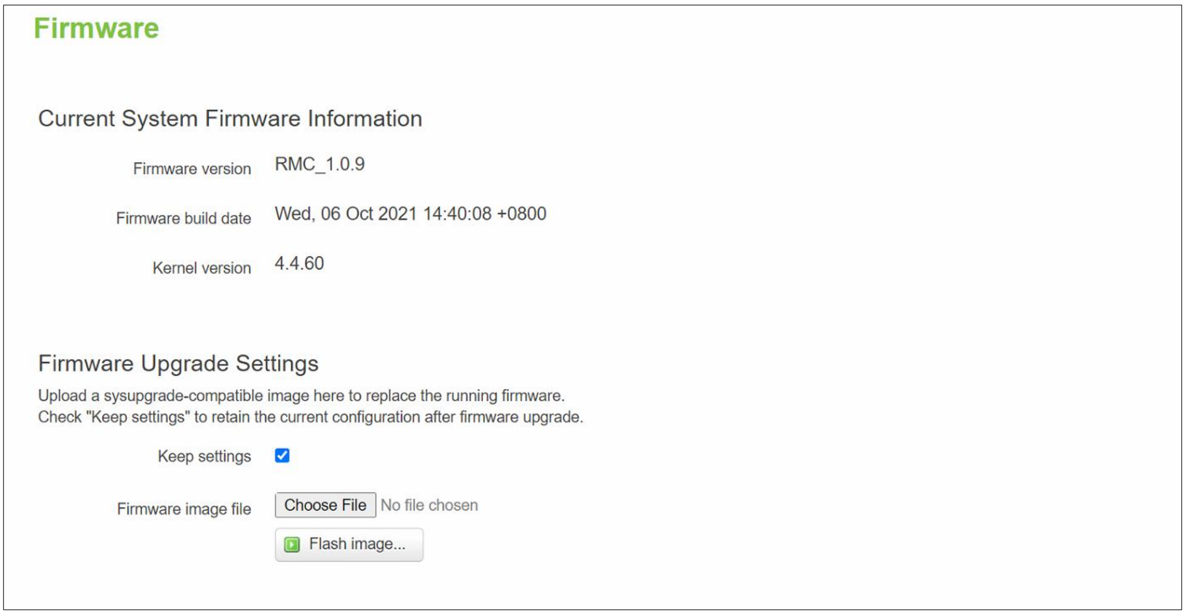
Here are the steps to follow for the firmware upgradation:

1. Before upgrading the firmware, please make sure that the device has a reliable power source and will not power off or restart during the firmware upgrading process.
2. Download the latest firmware for the correct model of the CWR5805 device from the Download page under the Support link on Atop's main webpage.
3. Copy the newly downloaded firmware file on to your local computer. Note that the firmware file is a binary file with ".img" extension.
4. Open the Web UI and select Backup/Flash Firmware sub-menu under the System > Firmware menu.
5. For a more advanced feature, you can click on "Generate archive" checkbox on the System > Backup to perform backup configuration files of the CWR5805 device before upgrading its firmware. This will allow you to restore the CWR5805 device's configuration after firmware upgrade has been done.
6. Click "Chose File" button to find and choose the new firmware file.

Note: You may need to re-configure your CWR5805 device if you had unchecked the "Keep settings" field in Flash new firmware image section after the firmware upgrade.

7. Then, click "Flash image" button to start the firmware upgrade process.

Figure 121. System > Firmware



Firmware

Current System Firmware Information

Firmware version: RMC_1.0.9

Firmware build date: Wed, 06 Oct 2021 14:40:08 +0800

Kernel version: 4.4.60

Firmware Upgrade Settings

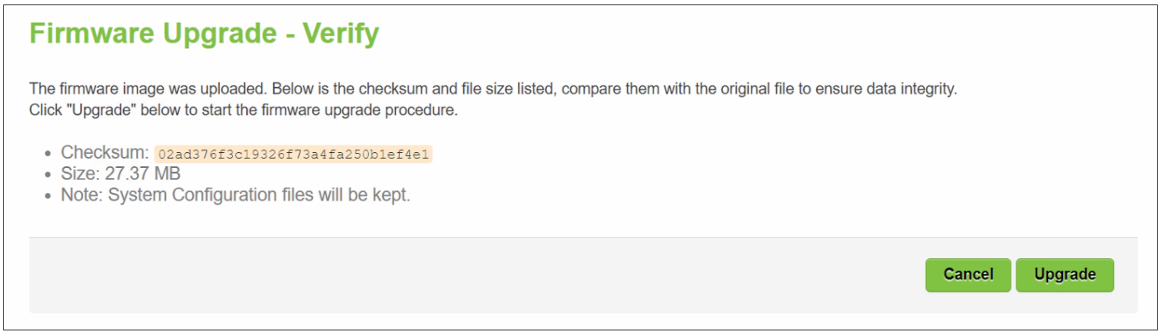
Upload a sysupgrade-compatible image here to replace the running firmware.
Check "Keep settings" to retain the current configuration after firmware upgrade.

Keep settings: ☑

Firmware image file: Choose File No file chosen

8. In the Figure below, the "Flash Upgrade – Verify" webpage will be displayed after the firmware file has been successfully verified by system successfully.

Figure 122. Confirm message of the Firmware Upgrade



Firmware Upgrade - Verify

The firmware image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity.
Click "Upgrade" below to start the firmware upgrade procedure.

- Checksum: `02ad376f3c19326f73a4fa250b1ef4e1`
- Size: 27.37 MB
- Note: System Configuration files will be kept.

9. Click the "Upgrade" button. Then, program will show "Waiting for changes to applied…" on the System – Flashing… webpage. Please wait until the uploading process is finished (the amount of time varies depending on the equipment used).
10. The CWR5805 device will be restarted and the web browser on the local computer will be redirected to Login webpage.

Attention: It is very important that the CWR5805 device is **not** turned off while the firmware upgrade is in progress.

3.5.3 Backup

In the **Backup** sub-menu within the **System** menu, you can perform system backup and restore CWR5805 device's configuration files.

Backup System Configuration

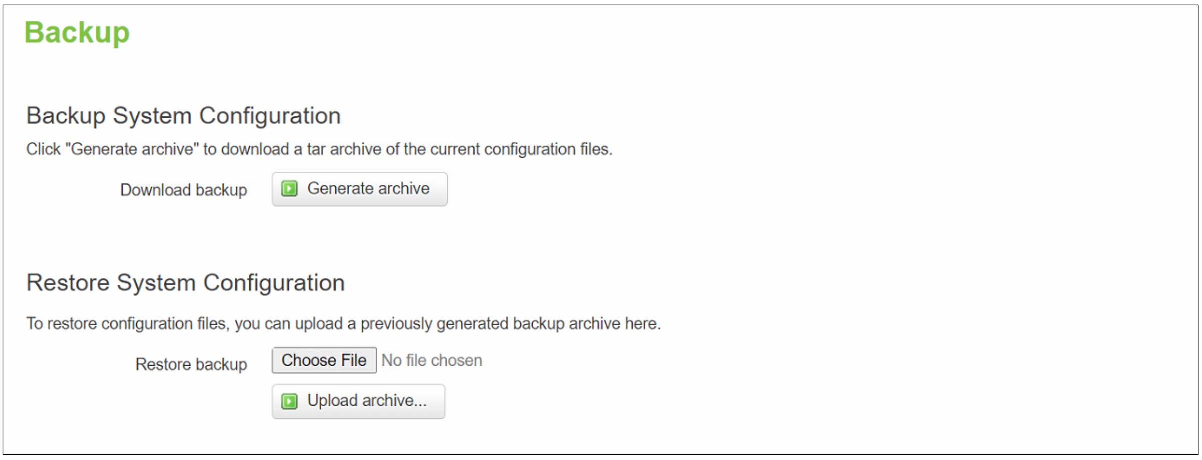
Click the **Generate archive** button to backup configuration files from CWR5805 device to your local host device. These backup configuration files are archived to a **backup-Hostname-yyyy-mm-dd.tar.gz** file.

Restore System Configuration

To restore previously saved configuration files from a local host device to the CWR5805 device, please perform the following steps:

1. Click **Choose File** button to select the archive file (backup-Hostname-yyyy-mm-dd.tar.gz).
2. Click **Upload archive b**utton to start restoring the archive file to the CWR5805 device.

Figure 123. System > Backup



Backup

Backup System Configuration

Click "Generate archive" to download a tar archive of the current configuration files.

Download backup: Generate archive

Restore System Configuration

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

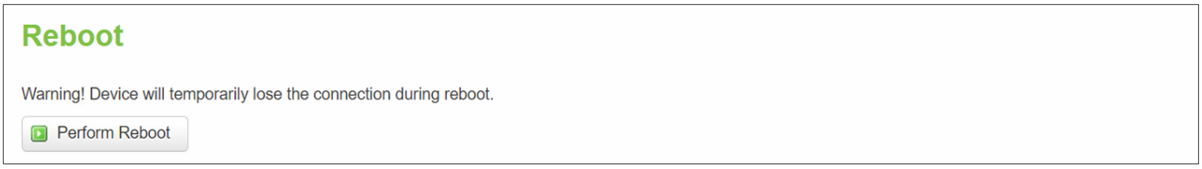
Restore backup: Choose File No file chosen

Upload archive...

3.5.4 Reboot

In the **Reboot** sub-menu within the **System** menu, you can reboot the CWR5805 device by clicking the **Perform Reboot** button. The webpage will then display “**Please wait: Device rebooting…**” and initiate a system restart. When the system rebooting process is finished, the web browser will be redirected to the **Login** webpage. Please enter the correct login password in the **Password** field for logging in.

Figure 124. System > Reboot



Reboot

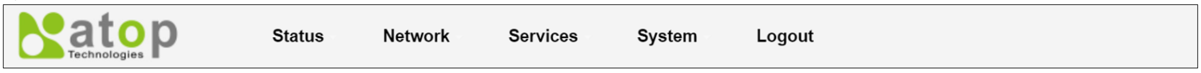
Warning! Device will temporarily lose the connection during reboot.

Perform Reboot

3.6 Logout

Click to log the current you out safely, after logging out, it will switch to login page.

Figure 125. System > Logout



4 Tutorials

This tutorial shows how to set up a CWR by configuring its wireless access point functions and testing its connectivities.

4.1 Setting up a CWR connection

There are essential communication devices and items which are needed to be prepared before setting up a testing environment. A personal computer (PC) or a laptop computer is used for testing network connection to LAN interfaces of CWR5805. A network cable such as unshield twisted pair (UTP) with RJ45 connectors is also required for the Ethernet LAN interface. A 5G/LTE Nano-SIM card is used to insert into the Nano-SIM card slot of the CWR5805 for testing the mobile interface connection.

A cable modem or an ADSL modem can be one of the external Internet connection sources for testing the WAN interface connection of CWR5805. A mobile phone or a tablet can be used for testing network connection to wireless AP interface of the device.

Follow the steps outlined below to setting up network connectiions for CWR5805 device.

LAN Connection

The first step is to configure a LAN connection between a PC and the CWR5805 device. Plug in one end of a network cable to one of the LAN port sockets of CWR5805 and the other end of the network cable to the PC's Ethernet port socket.

In the CWR5805 device, the IPv4 DHCP server is enabled by default for the LAN interfaces. Any device with IPv4 DHCP client enabled in its Ethernet interface will be assigned a dynamic IP address from CWR5805 device. The default IP address of CWR5805 is **192.168.1.1**, and the dynamic IP address range of LAN port is start from **192.168.1.100** to **192.168.1.250**.

WAN Connection

The second step is to configure a WAN connection between the CWR5805 device and a Cable/ADSL modem. The default mode of DHCP protocol of WAN interface on the CWR5805 is set to DHCP client. On the Cable/ADSL modem, make sure that there is an IPv4 DHCP server enabled for its Ehternet port interface which will be used to assign an IP address to the WAN interface of CWR5805 device. Plug in one end of a network cable to the WAN interface of CWR5805 device and the other end of the network cable to an Ethernet port interface of a Cable/ADSL modem.

Mobile Port Connection

The third step is to setup the 5G/LTE network for the mobile Internet connection. The SIM slots of CWR5805 only support Nano-SIM cards. Insert a 5G/LTE Nano-SIM card into the primary Nano-SIM slot of the device.

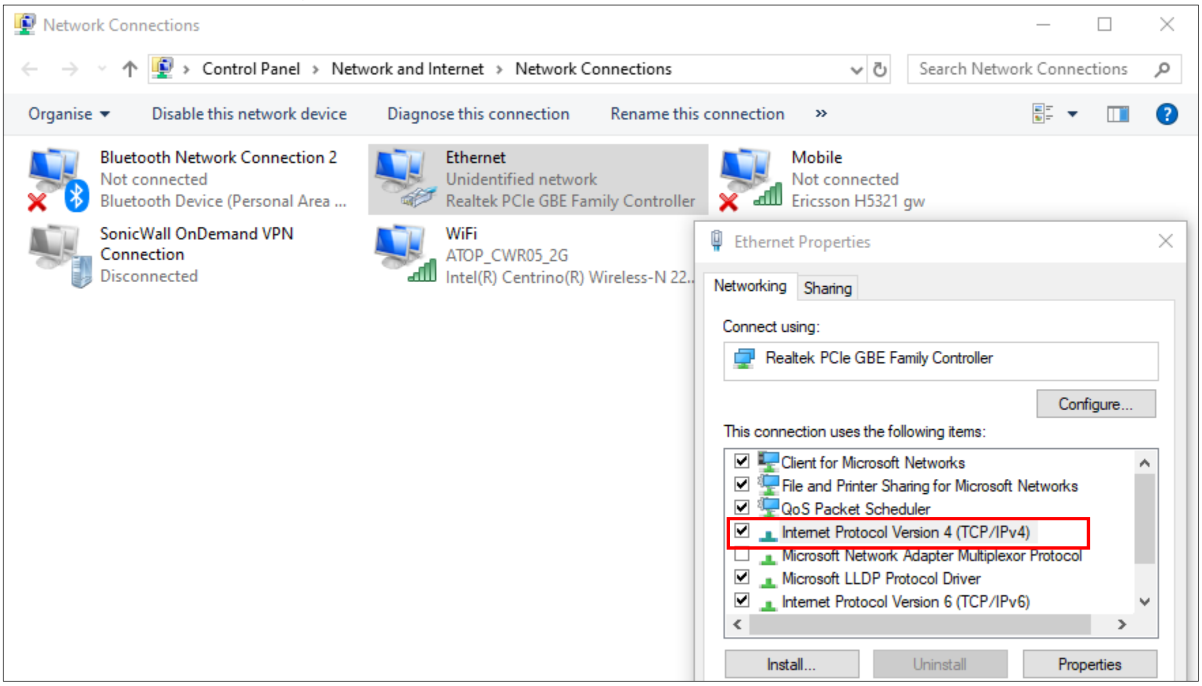
Power on CWR5805 Device

Before powering on the CWR5805 device, make sure that all of the 2.4GHz, 5GHz, and 5G/LTE SMA antennas are connected to the CWR5805 device firmly and correctly. Plug in the power line to CWR5805 device and turn on the power. The system takes approximately 50 seconds to boot into a stable state.

Setting up a DHCP IP address on a Windows 10 PC

On the PC, open the Network Connections window. Then, select the physical network interface icon and right click to open properties and enter the EthernetProperties dialog window. As shown in the Figure below, check the **Internet Protocol Version 4 (TCP/IPv4)** item and push the properties button to enter the Internet Protocol Version 4 Properties dialog window.

Figure 126. Ethernet Properties Dialog Window


Network Connections
Control Panel > Network and Internet > Network Connections
Search Network Connections
Organise
Disable this network device
Diagnose this connection
Rename this connection
Bluetooth Network Connection 2
Not connected
Bluetooth Device (Personal Area ...
Ethernet
Unidentified network
Realtek PCIe GBE Family Controller
Mobile
Not connected
Ericsson H5321 gw
SonicWall OnDemand VPN Connection
Disconnected
WiFi
ATOP_CWR05_2G
Intel(R) Centrino(R) Wireless-N 22..
Ethernet Properties
Networking
Sharing
Configure...
Install...
Uninstall
Properties

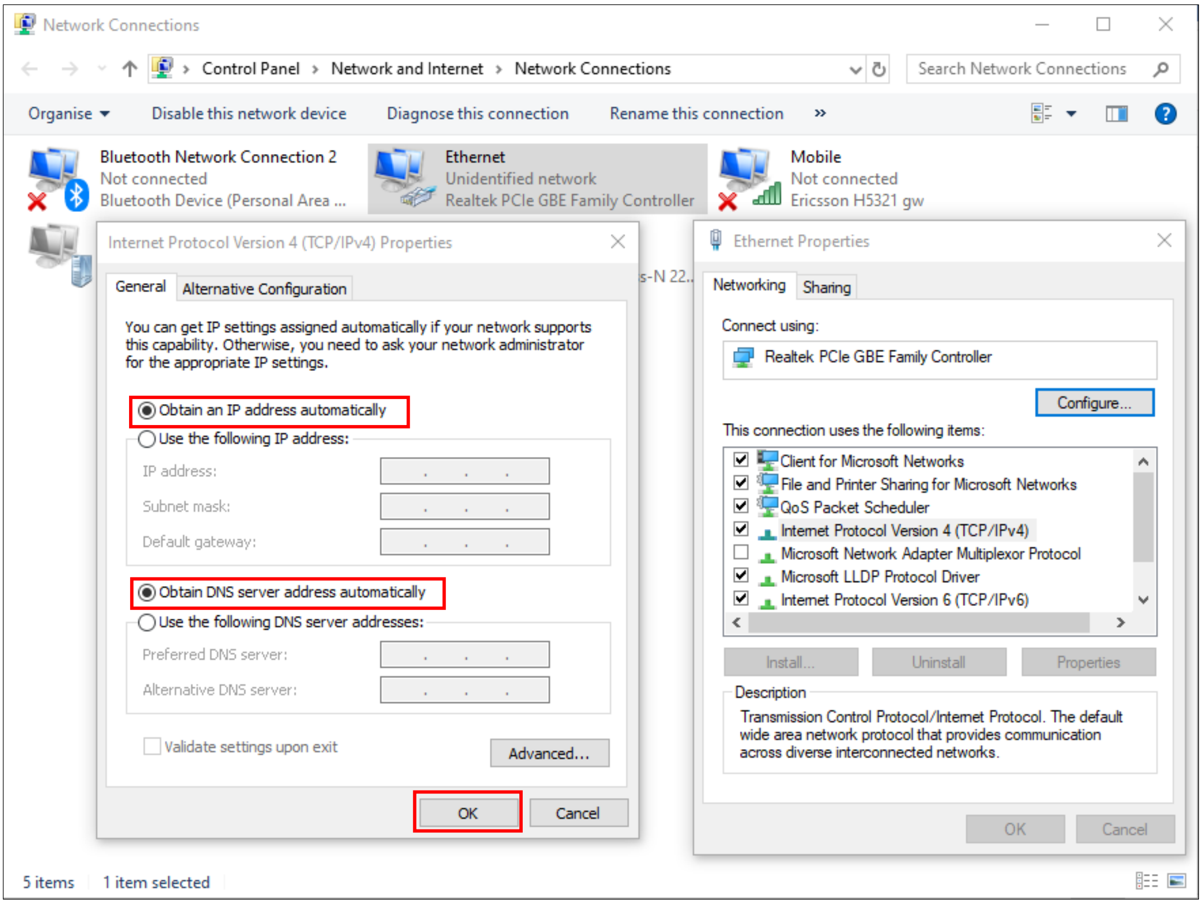
Connect using:
Realtek PCIe GBE Family Controller

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Then, as shown in the Figure below, select the **Obtain an IP address automatically** item and the **Obtain DNS server address automatically** item on General tab of the Internet Protocol Version 4 (TCP/IPv4) Properties dialog window. Click the OK button to obtain a dynamic IP address from CWR5805 device.

Figure 127. Internet Protocol Version 4 Properties Dialog Window



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server: . . .
Alternative DNS server: . . .

□ Validate settings upon exit

Connect using:
Realtek PCIe GBE Family Controller

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

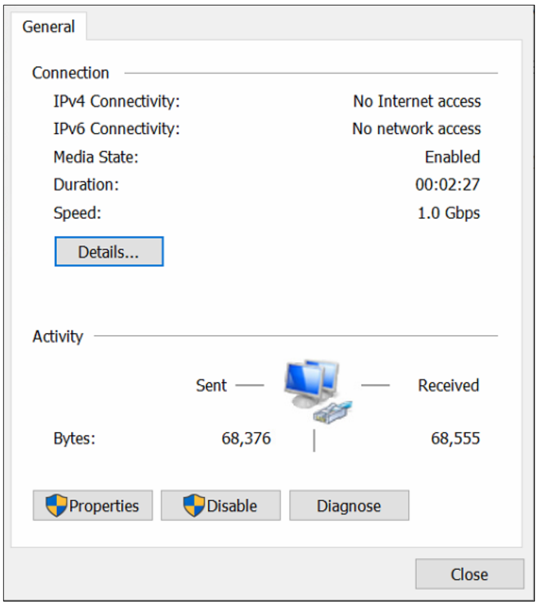
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Next, select the physical network interface icon again, then double-click mouse to enter the Ethernet Status dialog window as shown in the Figure below.

Push the **Details** button to view the assigned IPv4 address and others info. In Network Connection Details dialog window, the IPv4 address of IPv4 Default Gateway, IPv4 DHCP Server, and IPv4 DNS Sever are the same **192.168.1.1** address which is an IPv4 address of the LAN port interface on CWR5805 device.

In this example, the assigned IPv4 address of the PC is 192.168.1.227 which is within the dynamic IP address range of 192.168.1.100 to 192.168.1.250.

Figure 128. Status Dalog Window

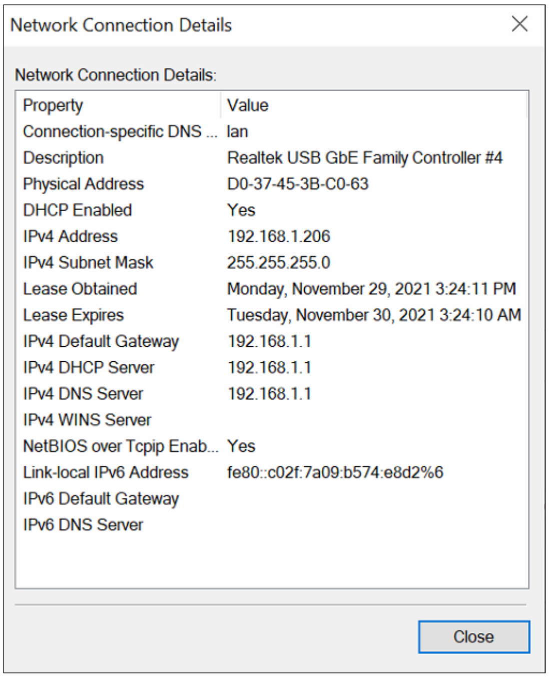


Connection

IPv4 Connectivity:	No Internet access
IPv6 Connectivity:	No network access
Media State:	Enabled
Duration:	00:02:27
Speed:	1.0 Gbps

	Sent	Received
Bytes:	68,376	68,555

Figure 129. Network Connection Details on the Connection Details



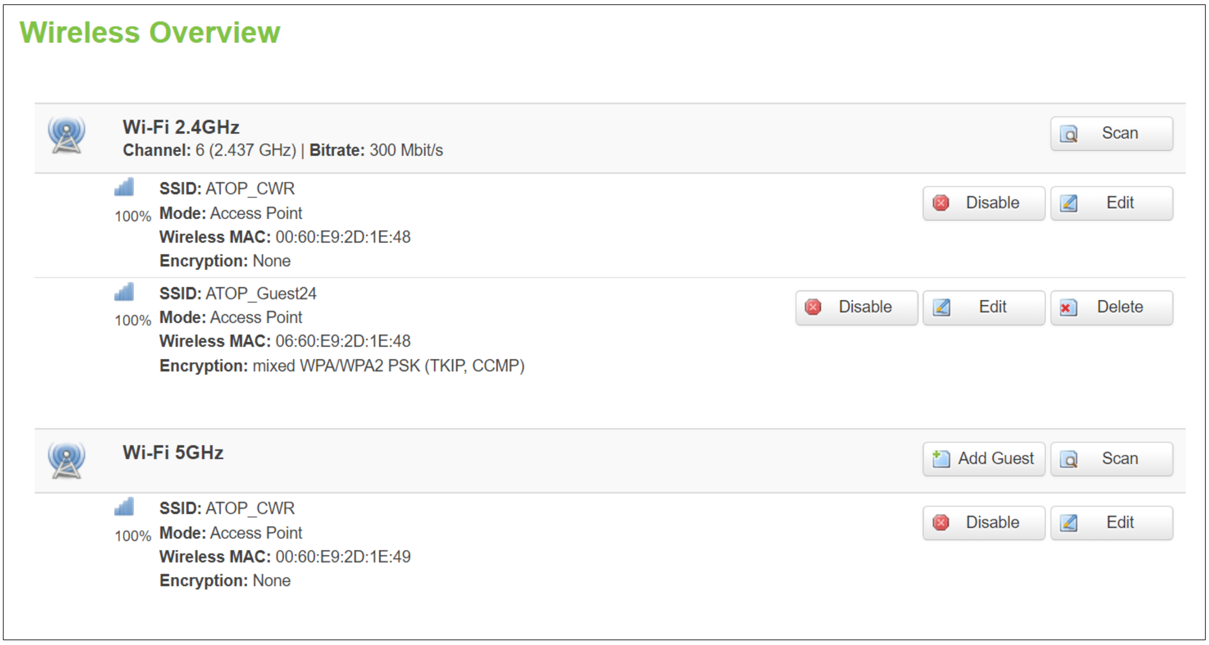
Network Connection Details:

Property	Value
Connection-specific DNS ...	lan
Description	Realtek USB GbE Family Controller #4
Physical Address	D0-37-45-3B-C0-63
DHCP Enabled	Yes
IPv4 Address	192.168.1.206
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Monday, November 29, 2021 3:24:11 PM
Lease Expires	Tuesday, November 30, 2021 3:24:10 AM
IPv4 Default Gateway	192.168.1.1
IPv4 DHCP Server	192.168.1.1
IPv4 DNS Server	192.168.1.1
IPv4 WINS Server	
NetBIOS over Tcpip Enab...	Yes
Link-local IPv6 Address	fe80::c02f:7a09:b574:e8d2%6
IPv6 Default Gateway	
IPv6 DNS Server	

4.2 Configuring Wireless Access Point

In Wireless Overview webpage, there are two wireless AP services available. By default, the Wi-Fi 2.4Ghz interface operated with 802.11N mode, and the Wi-Fi 5GHz interface operated with 802.11AC mode. The Associated Stations table lists connected client devices under the two wireless AP networks (SSID).

Figure 130. Wireless Overview Webpage under Wifi Menu



Wireless Overview

Wi-Fi 2.4GHz
Channel: 6 (2.437 GHz) | **Bitrate:** 300 Mbit/s

100% **SSID:** ATOP_CWR
Mode: Access Point
Wireless MAC: 00:60:E9:2D:1E:48
Encryption: None

100% **SSID:** ATOP_Guest24
Mode: Access Point
Wireless MAC: 06:60:E9:2D:1E:48
Encryption: mixed WPA/WPA2 PSK (TKIP, CCMP)

Wi-Fi 5GHz

100% **SSID:** ATOP_CWR
Mode: Access Point
Wireless MAC: 00:60:E9:2D:1E:49
Encryption: None

You can use any wireless devices such as mobile phone, tablet, and laptop to connect to wireless APs.

For the 2.4 GHz band wireless AP

1. ESSID is set to **ATOP_WiFi_24G** in General Setup tab.
2. Encryption is set to mixed **WPA-PSK/WPA2-PSK Mixed Mode** in Wireless Security tab.
3. Key is set ***atopatop*** in Wireless Security tab.

For the 5 GHz band wireless AP

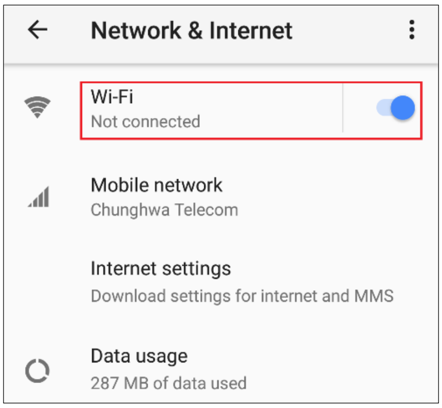
1. ESSID is set to ATOP_WiFi_5G in General Setup tab.
2. Encryption is set to mixed WPA-PSK/WPA2-PSK Mixed Mode in Wireless Security tab.
3. Key is set atopatop in Wireless Security tab.

The following steps show the method to connect an Android smartphone to the 2.4GHz band wireless AP on CWR5805 devic.

Step1: *Turning on Wi-Fi on Andriod Smartphone*

Select the **Settings** icon to enter Settings and then select **Network & Internet** to enter the Network & Internet screen. As shown in the Figure below, select the Wi-Fi item and turn Wi-Fi on.

Figure 131. Network & Internet Settings on the Android System



Network & Internet

Wi-Fi
Not connected

Mobile network
Chunghwa Telecom

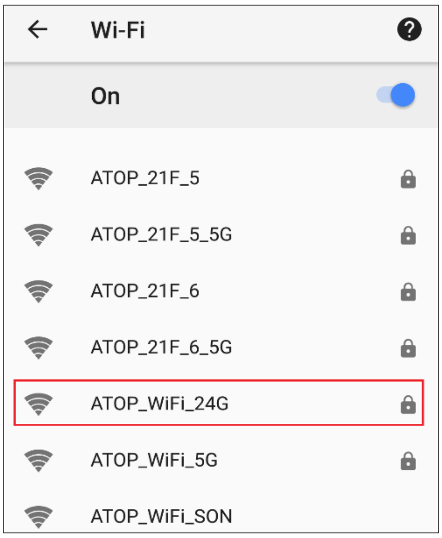
Internet settings
Download settings for internet and MMS

Data usage
287 MB of data used

Step 2: *Selecting the 2.4 GHz band wireless AP*

Tap on the **Wi-Fi** icon to enter the Wi-Fi scanning screen, select SSID named **ATOP_WiFi_24G** for connection.

Figure 132. Select ATOP_WiFi_24G AP under Network & Internet Menu



Wi-Fi

On

ATOP_21F_5

ATOP_21F_5_5G

ATOP_21F_6

ATOP_21F_6_5G

ATOP_WiFi_24G

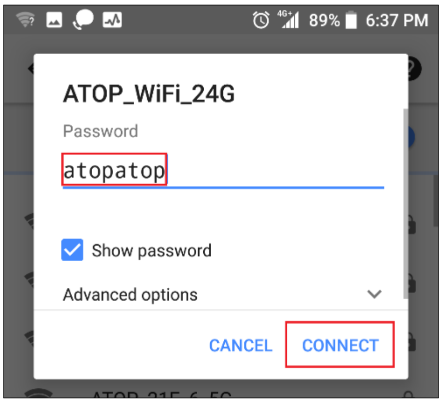
ATOP_WiFi_5G

ATOP_WiFi_SON

Step 3: *Input password (network key) for Wi-Fi connection*

As shown in the Figure below, input the password (network key) which is “atopatop” in the Password field, then push the CONNECT button thus starting a Wi-Fi connection.

Figure 133. Input Password (Network Key) for WiFi Connection



89% 6:37 PM

ATOP_WiFi_24G

Password

atopatop

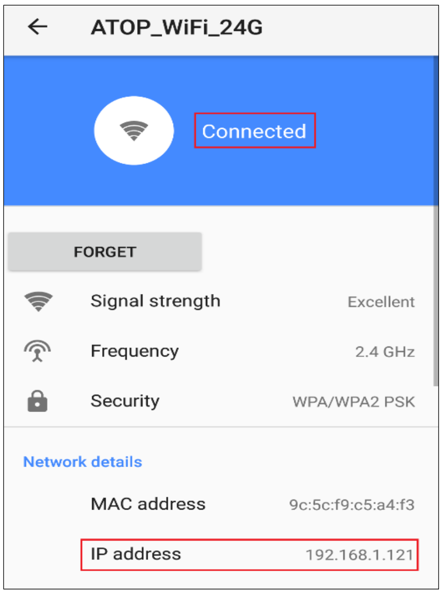
☑ Show password

Advanced options

Step 4: *Wi-Fi Connected Infomation*

After Wi-Fi connection is established successfully, push the **SSID** named **ATOP_WiFi_24G** again to enter the connection details screen. As shown in the Figure below, the assigned IPv4 address, subnet mask, gateway, and DNS come from bridged interface (br-lan) of CWR5805 device.

Figure 134. Wi-Fi Connected Information



ATOP_WiFi_24G

Connected

Signal strength Excellent

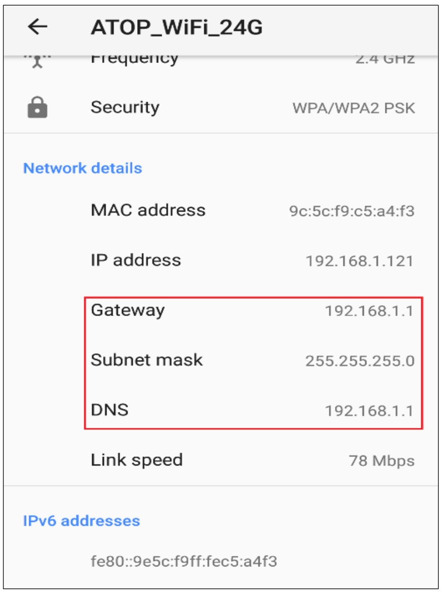
Frequency 2.4 GHz

Security WPA/WPA2 PSK

Network details

MAC address 9c:5c:f9:c5:a4:f3

IP address 192.168.1.121



ATOP_WiFi_24G

Frequency 2.4 GHz

Security WPA/WPA2 PSK

Network details

MAC address 9c:5c:f9:c5:a4:f3

IP address 192.168.1.121

Gateway 192.168.1.1

Subnet mask 255.255.255.0

DNS 192.168.1.1

Link speed 78 Mbps

IPv6 addresses

fe80::9e5c:f9ff:fec5:a4f3

For the 5 GHz wireless access point connection of an Android mobile phone, repeat Step 1 to Step 4 to establish the Wi-Fi connection but selecting the SSID name of **ATOP_WiFi_5G** for connection.

4.3 Testing Communication with multiple devices

Each DHCP client device can connect to CWR5805 device via either a LAN port or the wireless 2.4GHz/5GHz interface. For outbound Internet connection, each connected DHCP client device can access the Internet via either the WAN port or the Mobile interface.

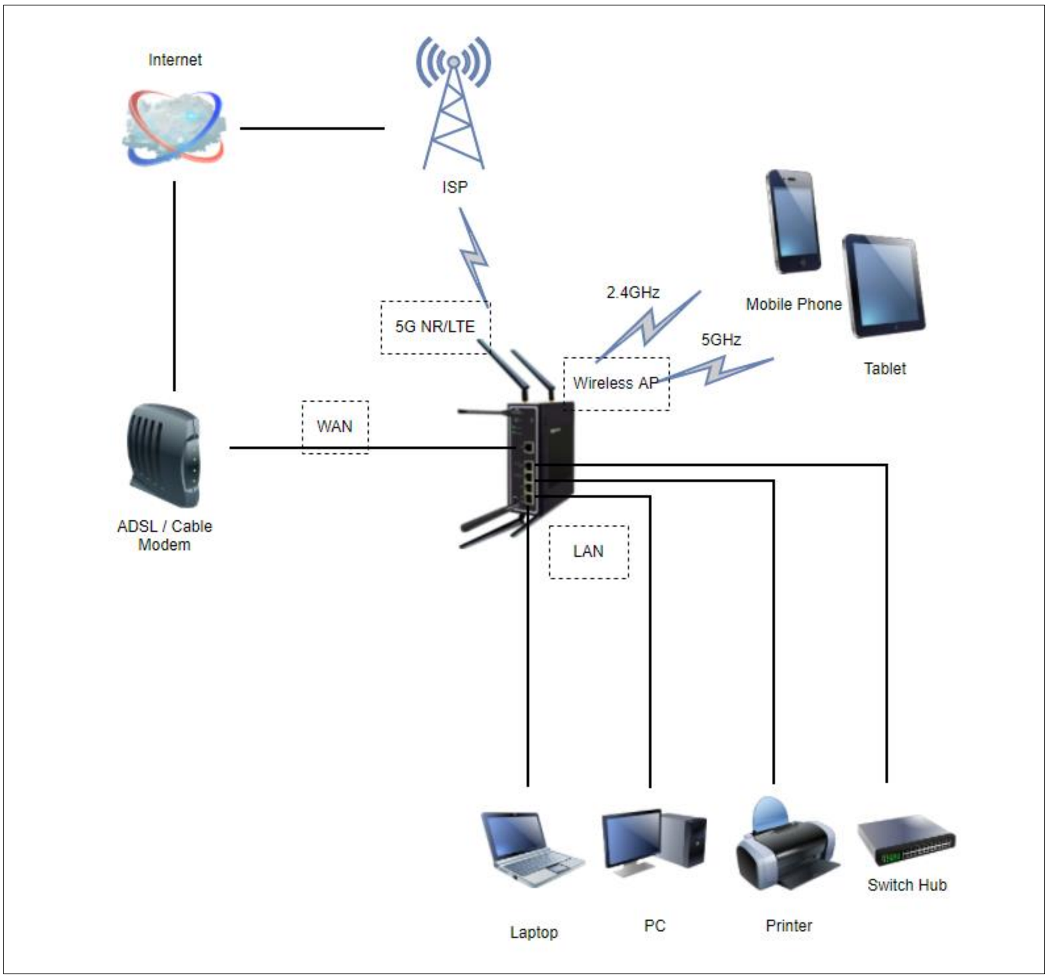
As shown in the Figure below, DHCP client devices connected to the LAN port or wireless 2.4GHz/5GHz interface are under the same network domain of **192.168.1.x**. This means that all DHCP clients can communicate with each other.

Section 6.1 illustrates how to test a communication by DHCP client with other devices using ping utility such as PingTools.

In section 6.2, according to the failover rules, outbound Internet traffic will be redirected to the Mobile port interface when the WAN port interface loses its connection. The failover also can be verified using traceroute utility in a DHCP client.

The Figure blow, illustrates multiple client devices connected to the CWR5805 device. A personal computer, a laptop, and a printer are connected to the LAN port interfaces of the CWR5805 device through a switch hub. Whereas a mobile phone and a tablet are connected through the wireless AP interface of the CWR5805 device. The WAN interface is connected to a cable/ADSL modem for the Internet access. The QMI Cellular interface provides a mobile Internet access that acts as Internet load balancing/failover role with WAN interface.

Figure 135. Multiple Devices are Assigned Dynamic IP Addresses by CWR5805 for Internet Connection



4.3.1 Ping Test of DHCP Client Devices

The following procedures provide examples of how to test network reachability of each DHCP client device.

***Step 1**: Assign a dynamic IPv4 address to a personal computer (PC)*

On the personal computer which get an assigned dynamic IPv4 address from CWR5805 device. Assuming that the assigned dynamic IPv4 address is **192.168.1.227**.

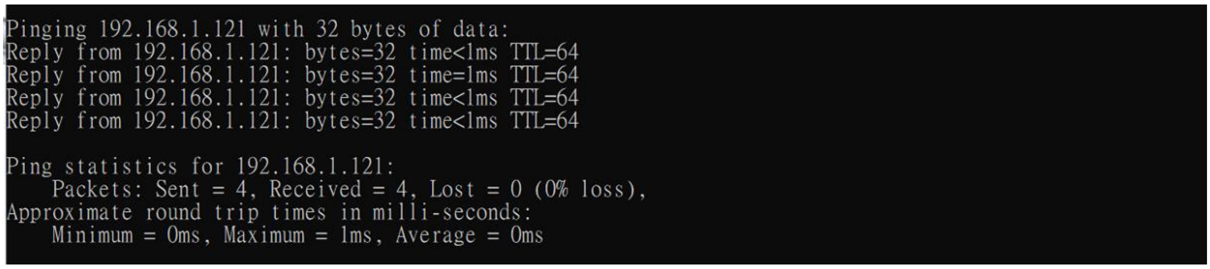
***Step 2**: Assign a dynamic IPv4 address to a mobile phone*

On the mobile phone which get an assigned dynamic IPv4 address from CWR5805. Assuming that the assigned dynamic IPv4 address is **192.168.1.121**.

***Step 3**: Ping the DHCP client to each other*

On the personal computer, open Windows' command prompt window, type in the "**ping 192.168.1.121** " command. As shown in the Figure below, the personal computer is receiving the response packets from the remote mobile phone side.

Figure 136. Local Personal Computer ping Android Mobile Phone

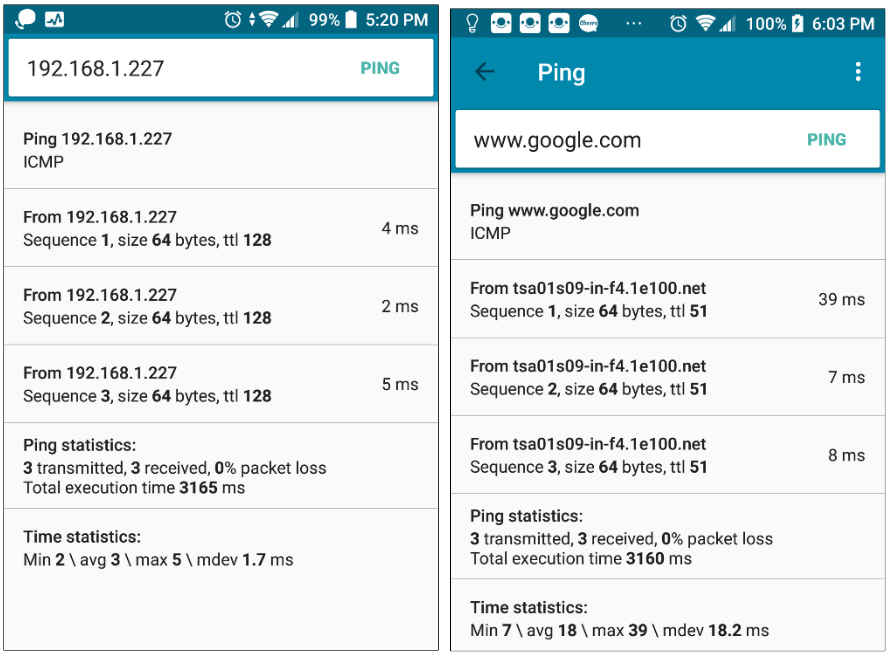


```
Pinging 192.168.1.121 with 32 bytes of data:
Reply from 192.168.1.121: bytes=32 time<1ms TTL=64
Reply from 192.168.1.121: bytes=32 time=1ms TTL=64
Reply from 192.168.1.121: bytes=32 time<1ms TTL=64
Reply from 192.168.1.121: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.121:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Similarly, any network diagnostic apps of Android mobile phone likes **PingTools Network Utilities** can be used to test the network communication. (If you do not have the PingTools app, installing it from the Google's Play Store first.) Run **PingTools** app and select the Ping item from menu. Input the remote IP address as **192.168.227**, and push **PING** button to start test. As shown in the Figure below, the Android mobile phone is receiving the response packets from the remote personal computer side.

Figure 137. Android Mobile Phone ping Local Personal Computer



192.168.1.227

Ping 192.168.1.227
ICMP

From 192.168.1.227
Sequence **1**, size **64** bytes, ttl **128** 4 ms

From 192.168.1.227
Sequence **2**, size **64** bytes, ttl **128** 2 ms

From 192.168.1.227
Sequence **3**, size **64** bytes, ttl **128** 5 ms

Ping statistics:
3 transmitted, **3** received, **0**% packet loss
Total execution time **3165** ms

Time statistics:
Min **2** \ avg **3** \ max **5** \ mdev **1.7** ms

www.google.com

Ping www.google.com
ICMP

From tsa01s09-in-f4.1e100.net
Sequence **1**, size **64** bytes, ttl **51** 39 ms

From tsa01s09-in-f4.1e100.net
Sequence **2**, size **64** bytes, ttl **51** 7 ms

From tsa01s09-in-f4.1e100.net
Sequence **3**, size **64** bytes, ttl **51** 8 ms

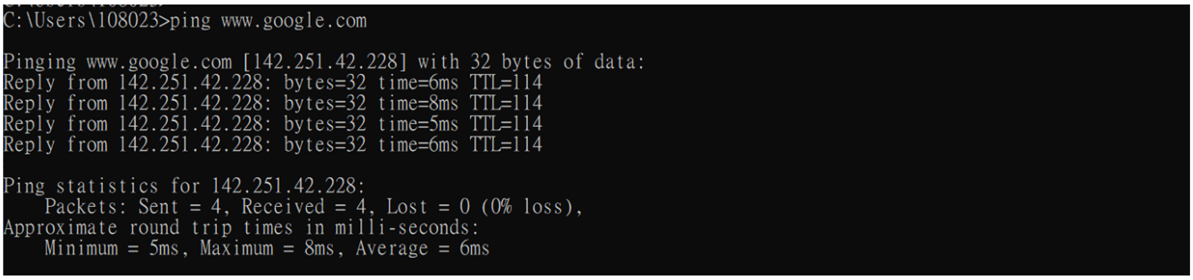
Ping statistics:
3 transmitted, **3** received, **0**% packet loss
Total execution time **3160** ms

Time statistics:
Min **7** \ avg **18** \ max **39** \ mdev **18.2** ms

Step 4: *Ping outbound host/FQDN (Fully Qualified Domain Name)*

On the personal computer, open Windows' command prompt window, type in the "ping www.google.com" command. The local personal computer thus receives the response packets from an IP address of Google.

Figure 138. Local Personal Computer ping www.google.com



```
C:\Users\108023>ping www.google.com

Pinging www.google.com [142.251.42.228] with 32 bytes of data:
Reply from 142.251.42.228: bytes=32 time=6ms TTL=114
Reply from 142.251.42.228: bytes=32 time=8ms TTL=114
Reply from 142.251.42.228: bytes=32 time=5ms TTL=114
Reply from 142.251.42.228: bytes=32 time=6ms TTL=114

Ping statistics for 142.251.42.228:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 8ms, Average = 6ms
```

Similarly, Run **PingTools** app on the Android phone, input the www.google.com and push **PING** button to start the test. The Android mobile phone can be seen receiving the response packets from a host IP address of Google.

Using the ping testing on DHCP client devices, it can verify that data packets can be transmitted and received between any two DHCP client devices on CWR5805 device. For outbound host/FQDN (Fully Qualified Domain Name), data packets also can be routed to WAN port interface of CWR5805 device.

4.3.2 Failover Test for Internet Connection

The following procedures provide examples of how to test the failover mechanism of CWR5805 for Internet connection.

Step 1: *Confirm connection status of both the WAN interface and the Mobile interface on CWR5805*

In CWR5805 device, follow the description of Section 5.2.1 to get an assigned dynamic IPv4 address on the WAN port interface from a cable/ADSL modem. Assuming that the address is assigned as **192.168.4.116**.

Follow the description of Section 3.3.2.2 to get an assigned dynamic IPv4 address on the Mobile port interface from ISP. Assuming that the assigned dynamic IPv4 address is **10.52.17.x**.

In the **LB and Failover** webpage of the **Network** menu as shown in Figure 4.18, confirm that both interfaces of the **WAN (eth0)** and the **Mobile (wwan0)** under the WAN Interface Live Status display as **Online (tracking active)** status.

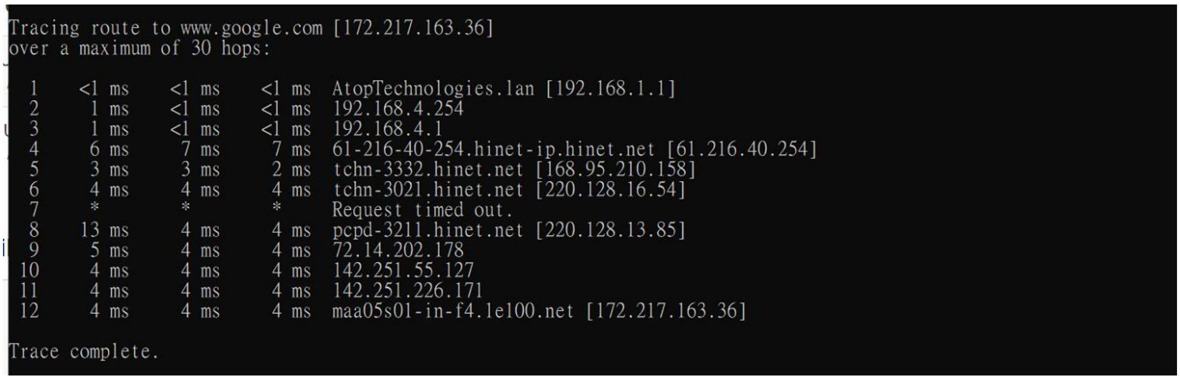
Step 2: *Trace outbound host/FQDN (Fully Qualified Domain Name) route*

On the local personal computer, open Windows' command prompt window, type in the "**tracert www.google.com**" command. As shown in Figure 139, the output packet of the first hop is on LAN port interface of **192.168.1.1**. The second hop is on WAN interface gateway of **192.168.4.254**. The system thus ultimately arrives at an IP address of Google host.

Similarly, run **PingTools** app on Android mobile phone, input the www.google.com and push **TRACE** to start test. As shown in Figure 140, the output packet of the first hop is on LAN port interface of **192.168.1.1**. The second hop is on the WAN port interface gateway of **192.168.4.254**. The hops continue until the system arrives at an IP address of Google.

These two traceroute tests have proven that the output packet is being routed from the main WAN port interface via its gateway to the destination host which is the Google site.

Figure 139. Traceroute Test on Command Prompt Window of Local Computer

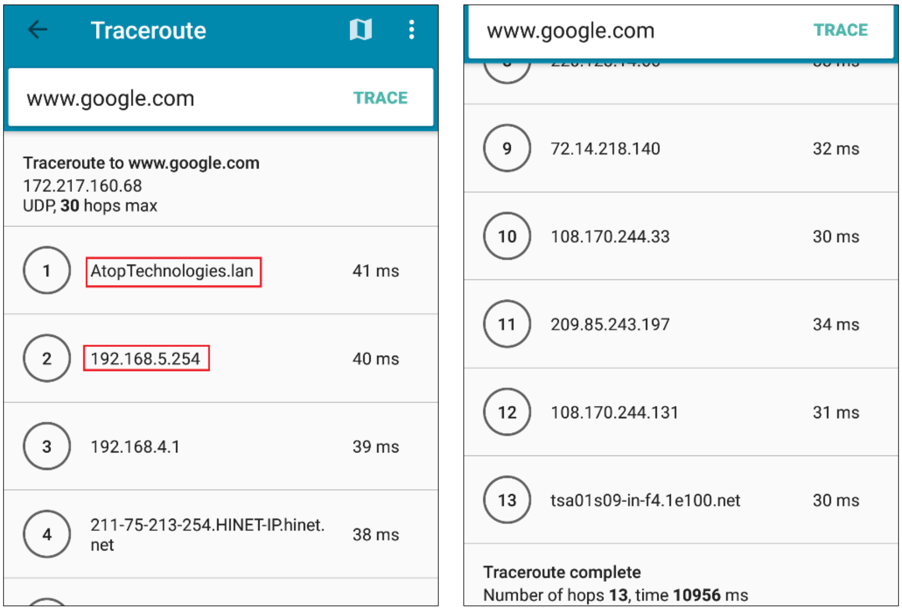


```
Tracing route to www.google.com [172.217.163.36]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  AtopTechnologies.lan [192.168.1.1]
  2     1 ms    <1 ms    <1 ms  192.168.4.254
  3     1 ms    <1 ms    <1 ms  192.168.4.1
  4     6 ms     7 ms     7 ms  61-216-40-254.hinet-ip.hinet.net [61.216.40.254]
  5     3 ms     3 ms     2 ms  tchn-3332.hinet.net [168.95.210.158]
  6     4 ms     4 ms     4 ms  tchn-3021.hinet.net [220.128.16.54]
  7     *        *        *     Request timed out.
  8    13 ms     4 ms     4 ms  pcpd-3211.hinet.net [220.128.13.85]
  9     5 ms     4 ms     4 ms  72.14.202.178
 10     4 ms     4 ms     4 ms  142.251.55.127
 11     4 ms     4 ms     4 ms  142.251.226.171
 12     4 ms     4 ms     4 ms  maa05s01-in-f4.1e100.net [172.217.163.36]

Trace complete.
```

Figure 140. Traceroute Test on PinTools App of Android Mobile Phone



Traceroute to www.google.com
172.217.160.68
UDP, **30** hops max

1 AtopTechnologies.lan 41 ms

2 192.168.5.254 40 ms

3 192.168.4.1 39 ms

4 211-75-213-254.HINET-IP.hinet.net 38 ms

9 72.14.218.140 32 ms

10 108.170.244.33 30 ms

11 209.85.243.197 34 ms

12 108.170.244.131 31 ms

13 tsa01s09-in-f4.1e100.net 30 ms

Traceroute complete
Number of hops **13**, time **10956** ms

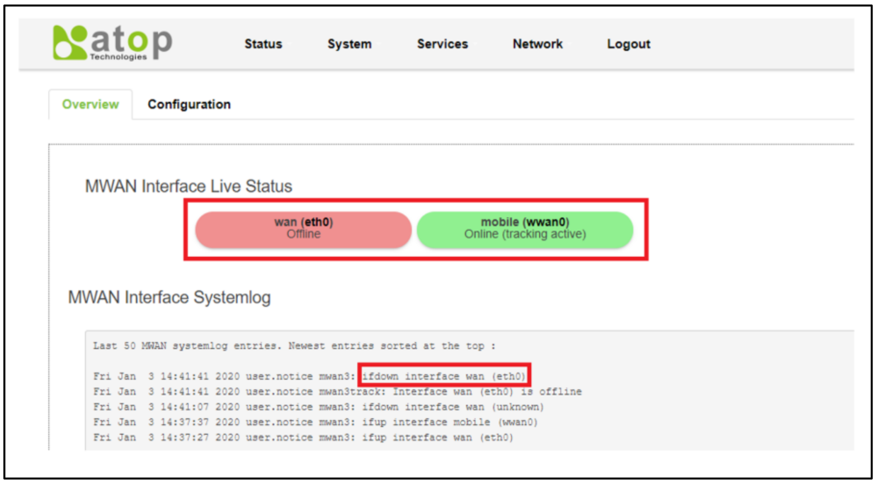
***Step 3:** Disconnect WAN Interface*

Unplug the network connection cable from WAN port socket of CWR5805 device. In the **Loading Balancing** webpage of the **Network** menu as shown in the Figure below, confirm tha the **WAN (eth0)** interface is in the **Offline** status and the **Mobile (wwan0)** interface is in the **Online (tracking active)** status.

In **WAN Interface Systemlog** field, the log text of "ifdown interface wan (eth0)" means that the WAN port Interfce has been closed.

Meanwhile as shown in the Figure below, the load balancing policy has changed to fully load on the Mobile port interface. This shows that 100% of output data traffic is redirected to the Mobile port interface.

Figure 141. Load Balancing - Interface Status webpage for WAN Port offline case



MWAN Interface Live Status

wan (eth0)
Offline

mobile (wwan0)
Online (tracking active)

MWAN Interface Systemlog

```
Last 50 MWAN systemlog entries. Newest entries sorted at the top :

Fri Jan  3 14:41:41 2020 user.notice mwan3: ifdown interface wan (eth0)
Fri Jan  3 14:41:41 2020 user.notice mwan3track: Interface wan (eth0) is offline
Fri Jan  3 14:41:07 2020 user.notice mwan3: ifdown interface wan (unknown)
Fri Jan  3 14:37:37 2020 user.notice mwan3: ifup interface mobile (wwan0)
Fri Jan  3 14:37:27 2020 user.notice mwan3: ifup interface wan (eth0)
```

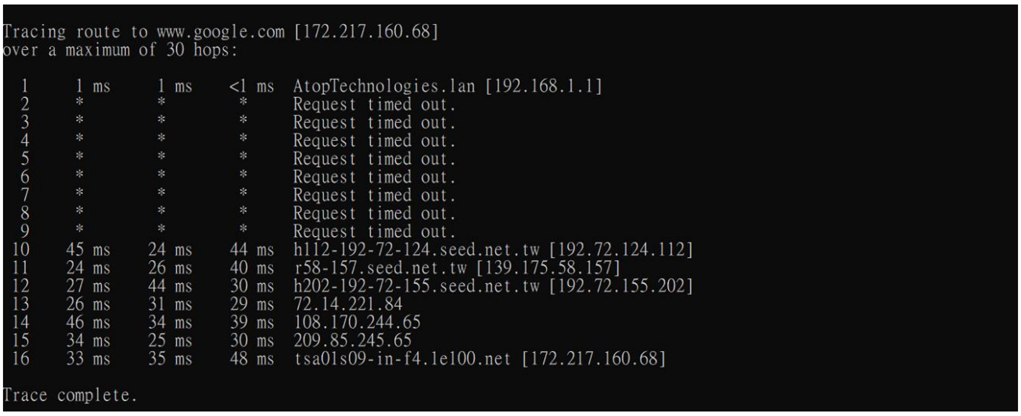
***Step 4:** Traceroute outbound host/FQDN again*

In local personal computer side, open Windows' command prompt window, type in the "**tracert www.google.com**" command. As shown in Figure 142, the output packet of the first hop is on the LAN port interface of **192.168.1.1**. It then routes to the third hop on the Mobile ISP gateway of **192.72.124.112**. The process goes on for serveral hops until it arrives at an IP address of Google host.

Similarly, run **PingTools** app on Android mobile phone, input www.google.com and push **TRACE** button to start the test. The output packet of the first hop is on the LAN port interface of **192.168.1.1**. It then continues to the second hop on the Mobile ISP gateway and then continues serveral hops until it arrives at an IP address of Google host.

These two traceroute tests prove that the output packet is routed from the Mobile port interface via its ISP gateway to the destination host while the WAN port interface is down.

Figure 142. Traceroute Test Again on Command Prompt Window of Local Computer



```
Tracing route to www.google.com [172.217.160.68]
over a maximum of 30 hops:

  1     1 ms     1 ms    <1 ms  AtopTechnologies.lan [192.168.1.1]
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10    45 ms    24 ms    44 ms  h112-192-72-124.seed.net.tw [192.72.124.112]
 11    24 ms    26 ms    40 ms  r58-157.seed.net.tw [139.175.58.157]
 12    27 ms    44 ms    30 ms  h202-192-72-155.seed.net.tw [192.72.155.202]
 13    26 ms    31 ms    29 ms  72.14.221.84
 14    46 ms    34 ms    39 ms  108.170.244.65
 15    34 ms    25 ms    30 ms  209.85.245.65
 16    33 ms    35 ms    48 ms  tsa01s09-in-f4.1e100.net [172.217.160.68]

Trace complete.
```

Step 5: *Reconnect the WAN Interface*

Plug the network connection cable into the WAN port socket of CWR5805 device. In the **Loading Balancing** webpage of the **Network** menu as shown in the Figure 134, confirm that both the **WAN (eth0)** interface and the **Mobile (wwan0)** interface are displaying as **Online (tracking active)** status.

Step 6: *Make the WAN interface as the main outbound interface*

Repeat traceroute testing described in Step 2 and confirm that all data packets are being correctly routed from WAN interface to the outbound network.

5 Specifications

5.1 Hardware Specification

Table 99. Hardware Specification

System	
CPU	*Qualcomm IPQ4029*
Flash Memory	*128MB*
RAM	*DDR3L 256MB*
Network	
Ethernet Interface	1x10/100/1000 WAN 4x10/100/1000 LAN Connector: RJ45
Wireless Interface	802.11ac, 802.11a, 802.11n, 802.11 b/g MU-MIMO access point
5G/LTE Interface	Up to 2x Nano-SIM card slots 5G model 5G-NR SA and NSA LTE Model LTE Cat.6
Wi-Fi Security	AES-CCMP, TKIP, WPA3-PSK, WPA2-PSK, WPA-PSK
LED Indicator	
LED indication	Power x1 Wi-Fi 2.4G x 1 Wi-Fi 5G x 1 WAN x 1 LAN x 4 Mobile SIM1 signal x 3 Mobile SIM2 signal x 3
Power Requirement	
Input	Single 12~48 VDC 3-pin terminal block connector
Mechanical	
Dimensions (W x H x D)	145 x 120 x 46 mm
Enclosure	IP30 protection, metal housing
Environmental	
Temperature	Operations -40°C ~ 75°C Storage -40°C ~ 85°C
Relative Humidity	5% ~ 95%, 55°C Non-condensing

5.2 CWR5805 Device Pin Assignments for WAN/LAN Port

RJ45 connectors for 10/100/1000Base-T(X) Ethernet

Figure 143. WAN/LAN Port on RJ45 with Pin Numbering of CWR5805 Device

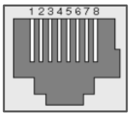


Table 100. Assignment for RJ-45 Connector of CWR5805 Device

10/100/1000Base-T(x)								
Pin#	1	2	3	4	5	6	7	8
Signal	Tx+	Tx-	Rx+	-	-	Rx-	-	-
1000Base-T								
Pin#	1	2	3	4	5	6	7	8
Signal	BI_DA+	BI_DA-	BI_DB+	BI_DC+	BI_DC+	BI_DB-	BI_DD+	BI_DD-

6 Glossary

- AP – Access Point
- APN – Access Point Name
- AS – Autonomous System
- BIRD – Bird Internet Routing Daemon
- BSSID – Basic Service Set Identifiers
- CAP – Central Acccess Point
- CIDR – Classless Inter-Domain Routing
- DHCP – Dynamic Host Configuration Protocol
- DDNS – Dynamic Domain Name Service
- DNS –Domain Name Service
- FQDN – Fully Qualified Domain Name
- IP – Internet Protocol
- IP Address – Internet Protocol Address
- IGP – Interior Gateway Protocol
- ISP – Internet Service Provider
- LAN – Local Area Network
- LSR – Link State Routing
- LTE – Long Term Evolution
- MTU - Maximum Transmission Unit
- MU-MIMO – Multi-You Multiple-Input Multiple-Output
- NAT – Network Address Translation
- NTP – Network Time Protocol
- OSPF – Open Shortest Path First
- PPPoE – Point-to-Point Protocol over Ethernet
- QMI – Qualcomm MSM Interface
- RSSI - Received Signal Strength Indicatior
- SIM – Subscriber Identity Module
- SMS – Short Message Service
- SNR – Signal to Noise Ratio
- SSID – Service Set Identifier
- SSL – Secure Sockets Layer
- STP – Spanning Tree Protocol
- TLS – Transport Layer Security
- VPN – Virtual Private Network
- WAN – Wide Area Network

Atop Technologies, Inc.

www.atoponline.com

TAIWAN HEADQUARTER and INTERNATIONAL SALES:

2F, No. 146, Sec. 1, Tung-Hsing Rd,
30261 Chupei City, Hsinchu County
Taiwan, R.O.C.
Tel: +886-3-550-8137
Fax: +886-3-550-8131
sales@atop.com.tw

ATOP CHINA BRANCH:

3F, 75th, No. 1066 Building,
Qingzhou North Road,
Shanghai, China
Tel: +86-21-64956231