Atop Technologies, Inc.

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

User Manual

V1.0

8th December 2021

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's 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 yous 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 You 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 yous. 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:	Saowanee Saewong
Revision:	1.0
Revision History:	Creation
Creation Date:	3 January 2022
Last Revision Date:	3 January 2022
Document Status:	draft

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 yous manage their devices, as well as some 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 Who Should Use This You Manual

This manual should be used by qualified network personnel or support technicians who are familiar with network operations. It can be useful for system programmers and network planners. This manual will also come handy for new yous. If there are any issues, please reach us at **www.atoponline.com**.

1.3 Supported Platform

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

1.4 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's 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.

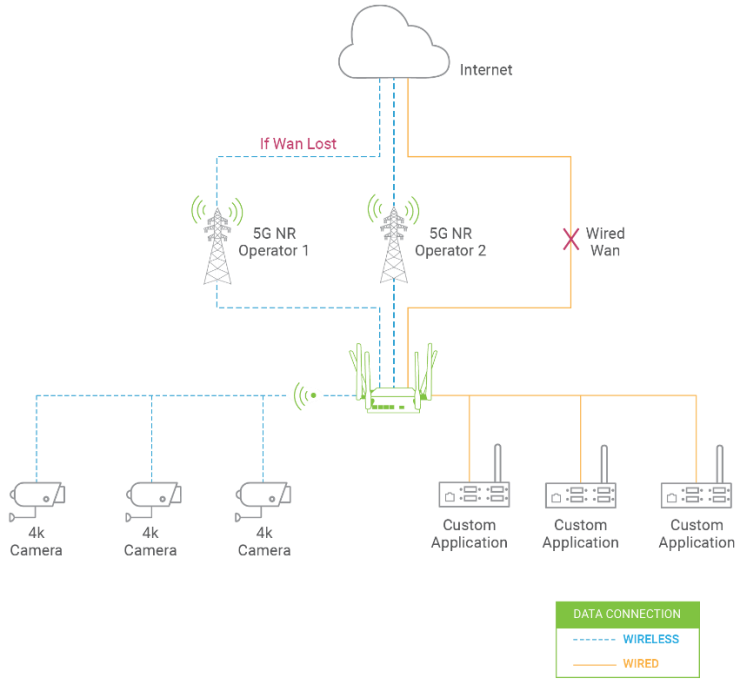
The CWR5805 support 5G NR and LTE network for device through wireless connection. And it has dual-SIM card backup to ensure stable wireless network connection. The CWR5805 devices radiate signal in the dual-band (2.4GHz, 5GHz), while users' Wi-Fi devices can conveniently connect to them via any chosen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

The device has also built-in full-duplex 10/100/1000 Mbps ports (WAN, LANs) to connect with user's wired Ethernet devices for the speed up to 1 Gbps. The Ethernet WAN and mobile module on CWR5805 device provides 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.

Nowdays, 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 are 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 cellular 5G/LTE router between existing wired WAN. This way, it is possible to use wired Internet option and share connection to IoT system via Ethernet and to 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/ITE as a source of Internet to provide continuous Internet service to conected 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 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 unit to cool for 5 minutes before touching.

2.3 Installion

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.

After you unpack the box, follow the steps documented below, in order to properly connect the device. For better Wi-Fi performance, put the device in clearly visible spot, as obstacles such as walls and door hinder the signal.

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 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
LTE Antenna*	2	LTE antenna (SMA male)
5G NR Antenna **	4	5G NR 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 only
**5G model only

2.3.2 Front Pannel and Back Panel

Figure 2. Front Pannel

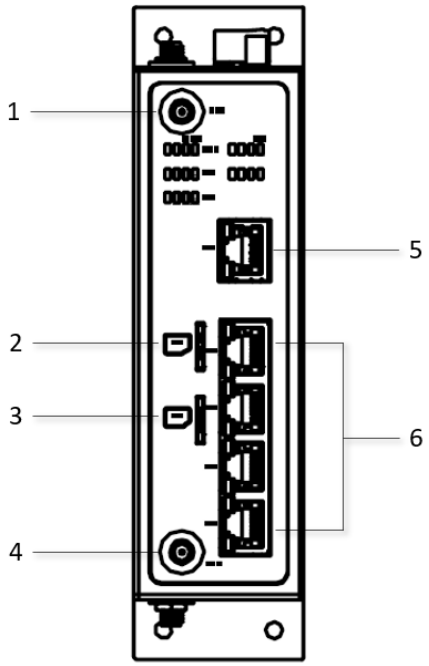


Table 2. Front Pannel

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

Figure 3. Top View

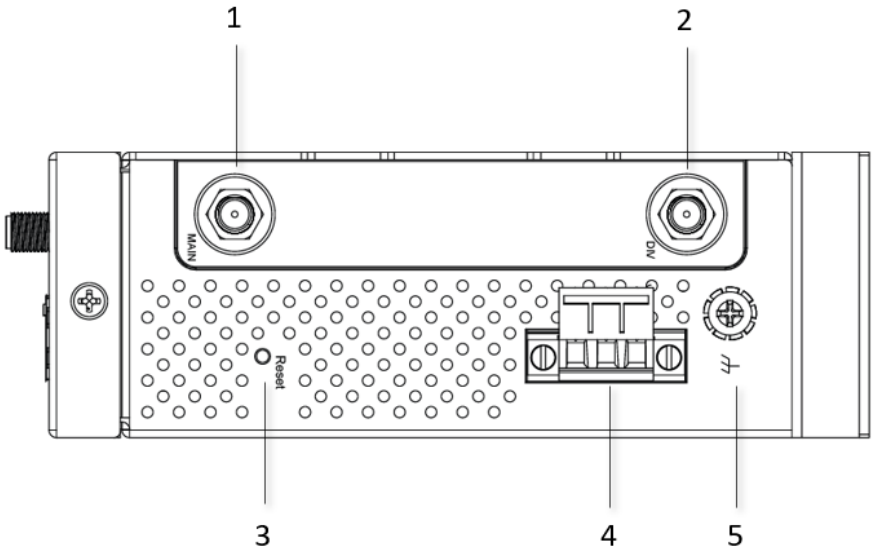


Table 3. Top View

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. Buttom view

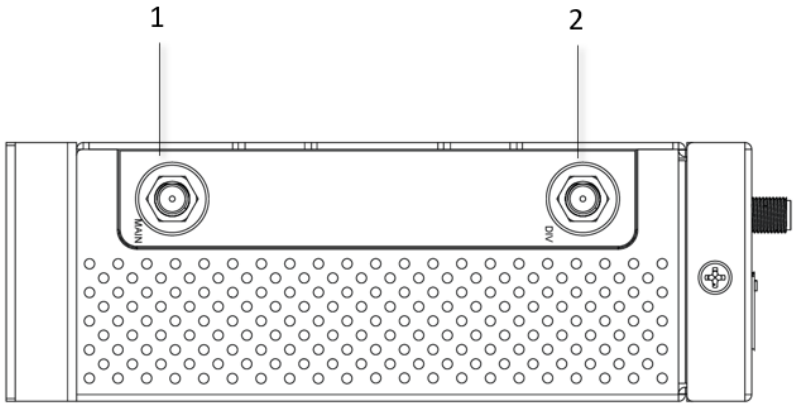


Table 4. Buttom view

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

2.3.3 Power Connector

Figure 5. Power Connector on the Top Panel

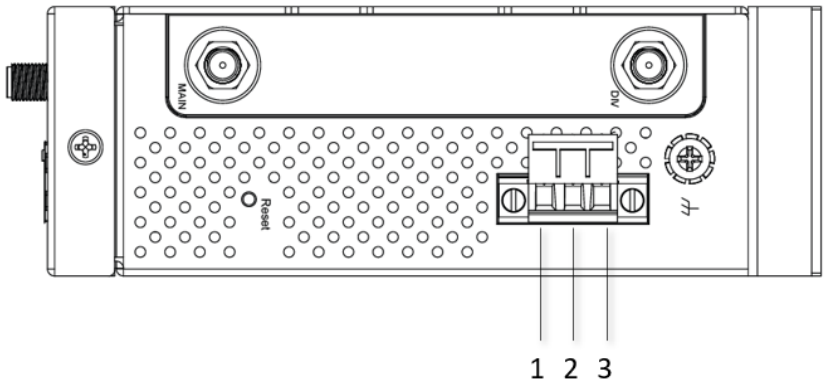


Table 5. Power Connector on the Top Panel

No.	Description
1	pwr -
2	pwr +
3	NC.

2.3.4 Connection Status LED

Table 6. Color Interpretation of LED Indicators on 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 chasis to close it.

Figure 6. SIM Card Installation

TBD

2.3.6 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.

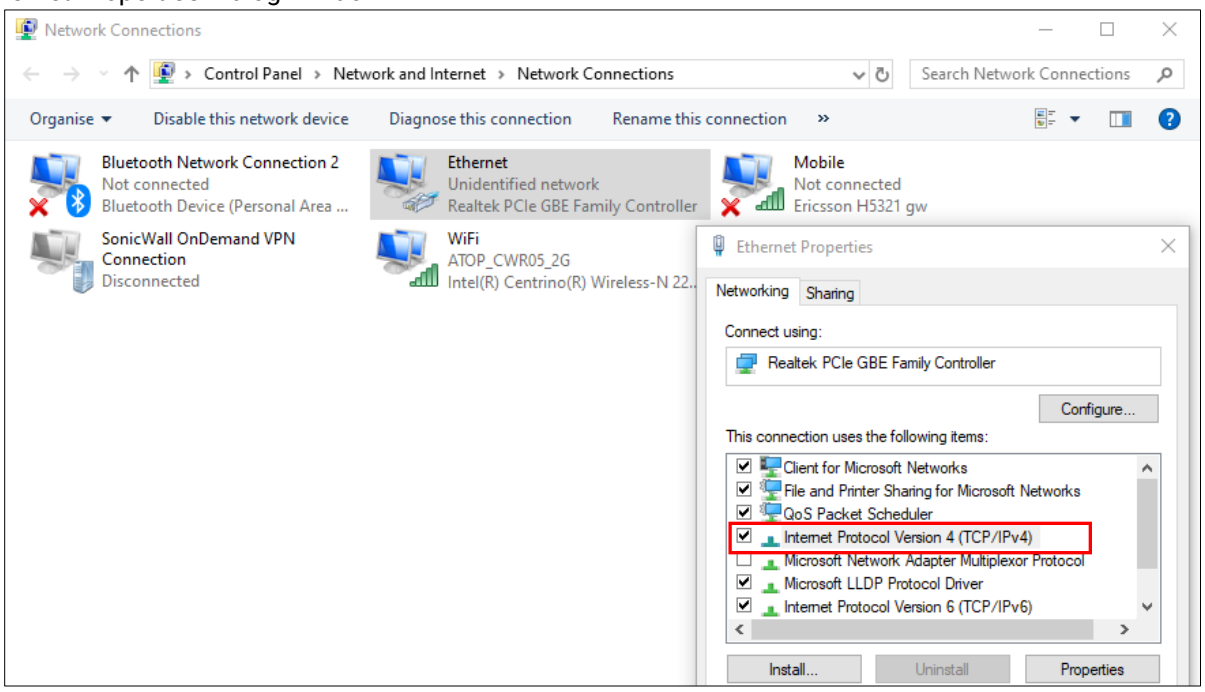
Power on CWR5805 Device

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

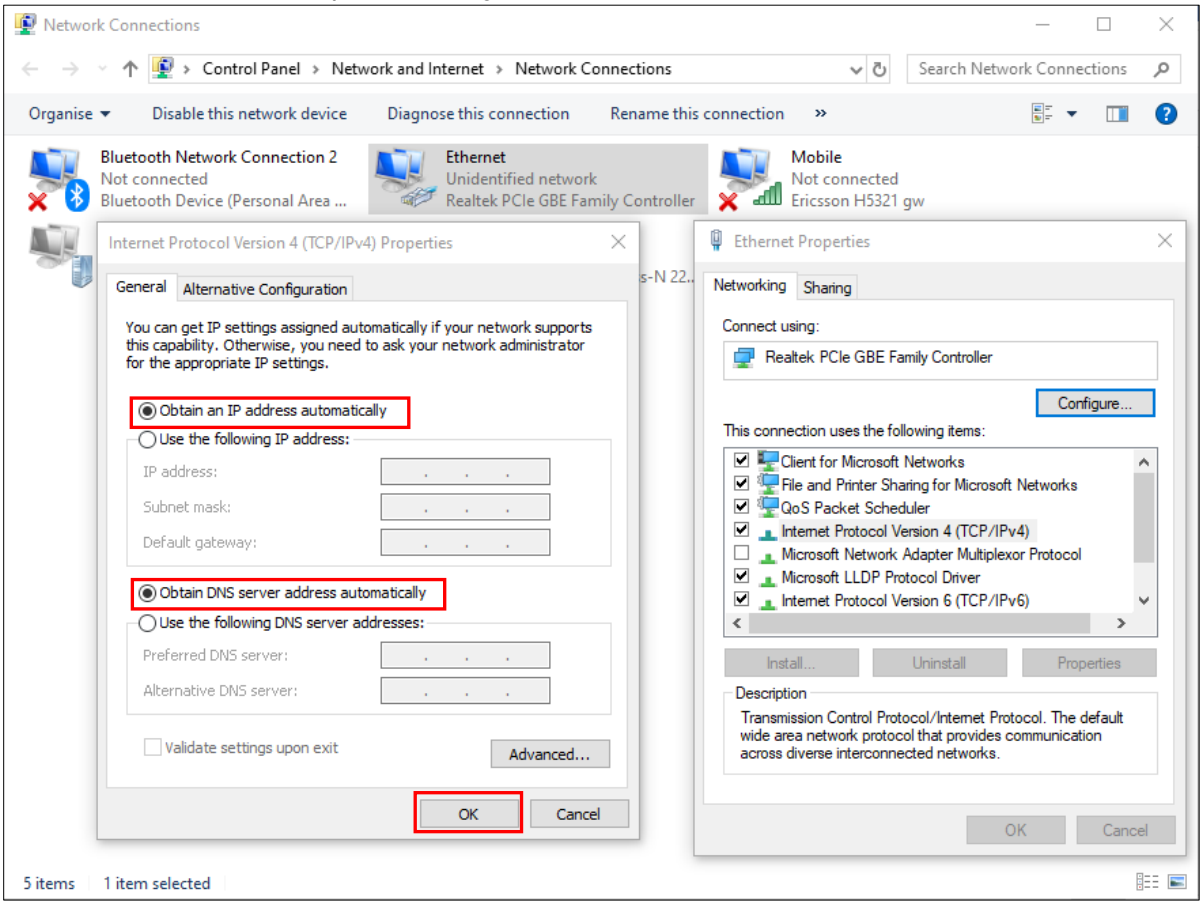
On the PC, open the Network Connections window. Then, select the physical network interface icon and right click to open properties and enter the EthernetProperties dialog window. As shown in Figure 7, check the **Internet Protocol Version 4 (TCP/IPv4)** item and push the properties button to enter the Internet Protocol Version 4 Properties dialog window.

Figure 7. Ethernet Properties Dialog Window



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 8. Internet Protocol Version 4 Properties Dialog Window



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 9. Status Dalog Window

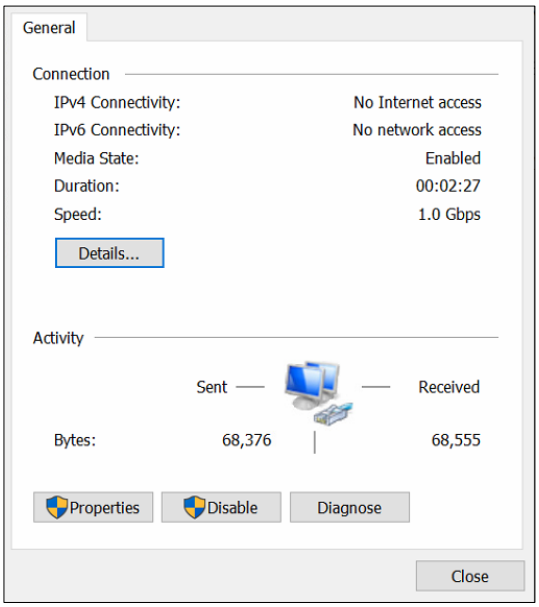
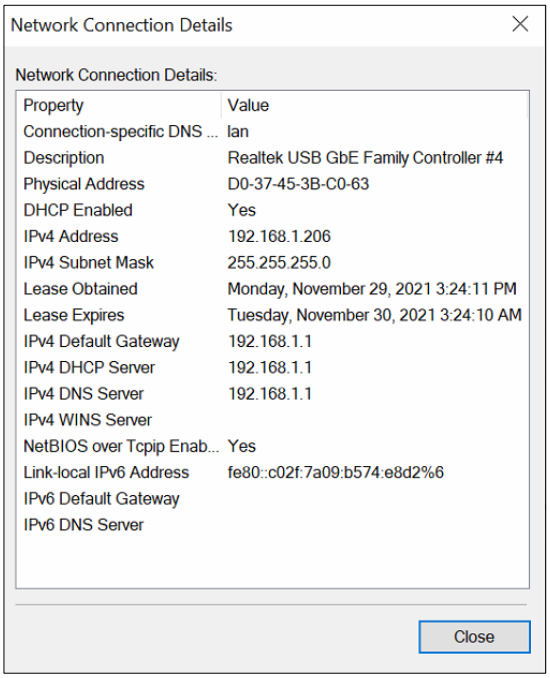


Figure 10. Network Connection Details on the Connection Details



2.4 Factory Default Settings

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 7. 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 8. Login Default Settings

Login Parameters	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 loss 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 that 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.

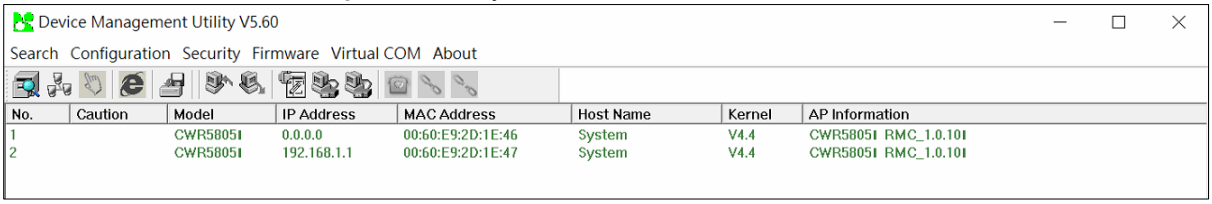
3.1 Configuration Interface

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 comes in the Product CD or 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 Figure 11.

Figure 11. List of Device in Device Management Utility



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

Sometime 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 Figure 12 or click on the second icon called **Network** on the menu icon bar, and a pop-up window will appear as shown in the Figure 13.

Figure 12. Pull-down Menu of Configuration and Network

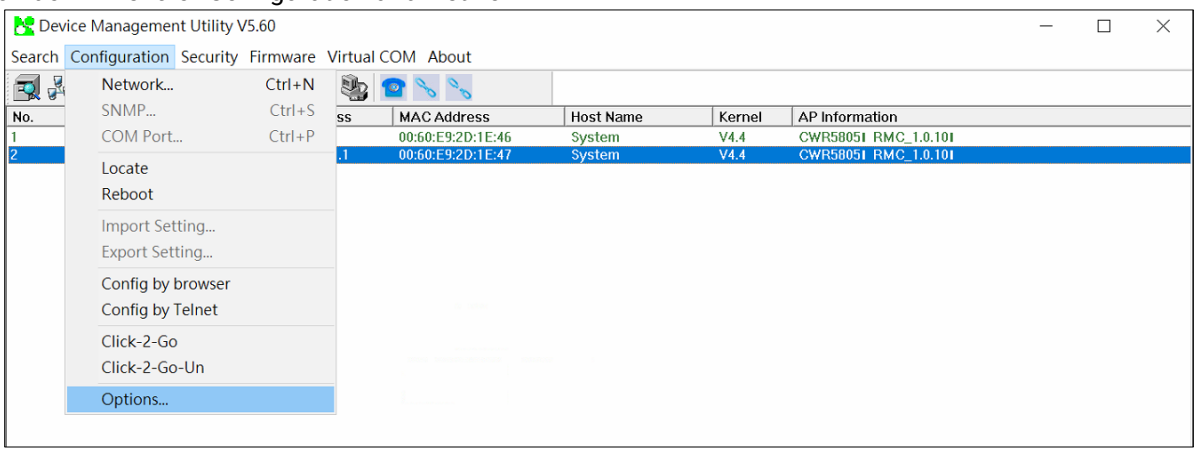
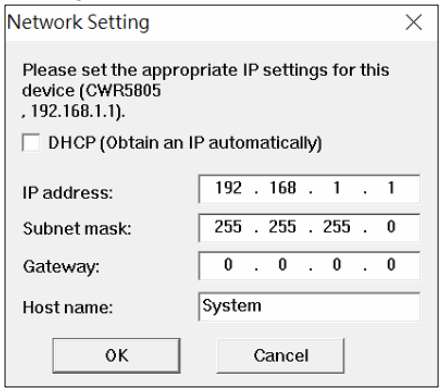


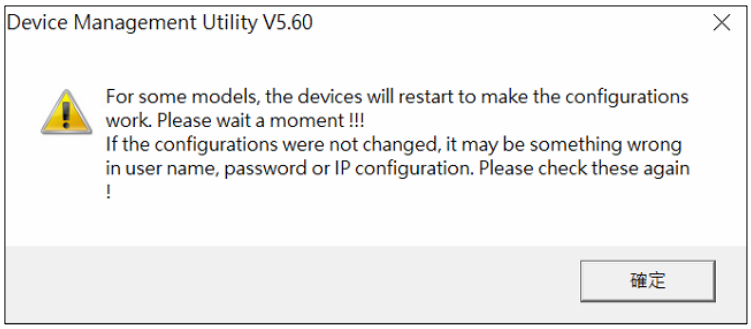
Figure 13. Pop-up Window of Network Setting



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 LAN as shown in the Figure 13. 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 Figure 14. 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 Figure 15 and some device may be restarted. After the device is restarted (for some model), 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 other parameter, you may encounter another notification window as shown in Figure 16.

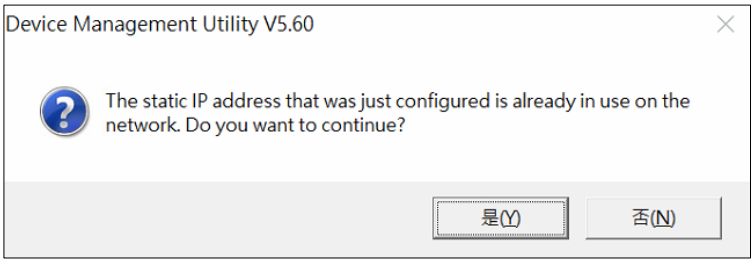
Figure 14. Authorization for Change of Network Settings

Figure 15. Pop-up Notification Window after Authorization



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

Figure 16. Pop-up Notification Window when there is the same IP address in the network

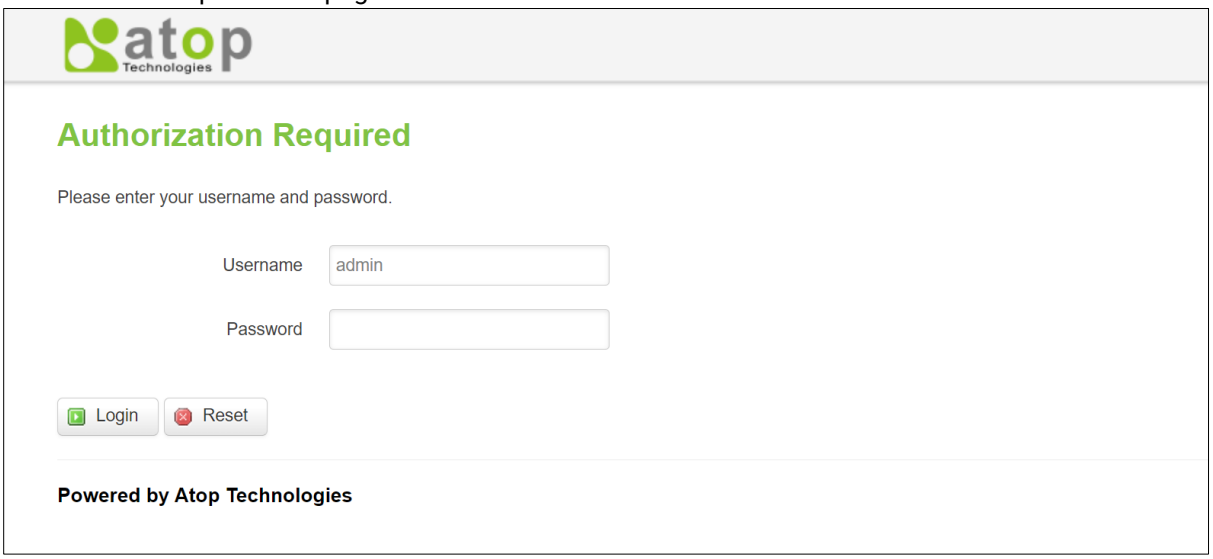


3.1.2 Configuring through Web

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 needs 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 **default**.

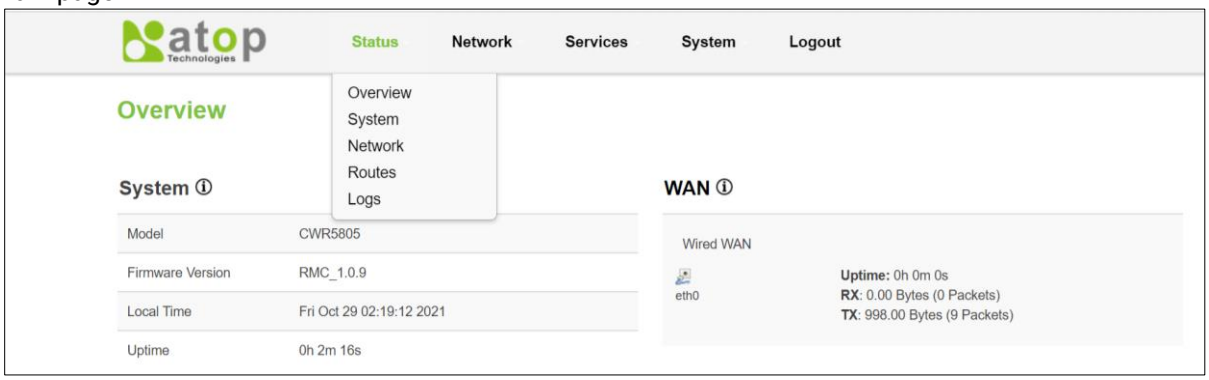
Figure 17. Authorization Required Webpage



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 18. Main page



3.2.1 Overview

The **Overview** sub-menu under 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 19. Status > Overview

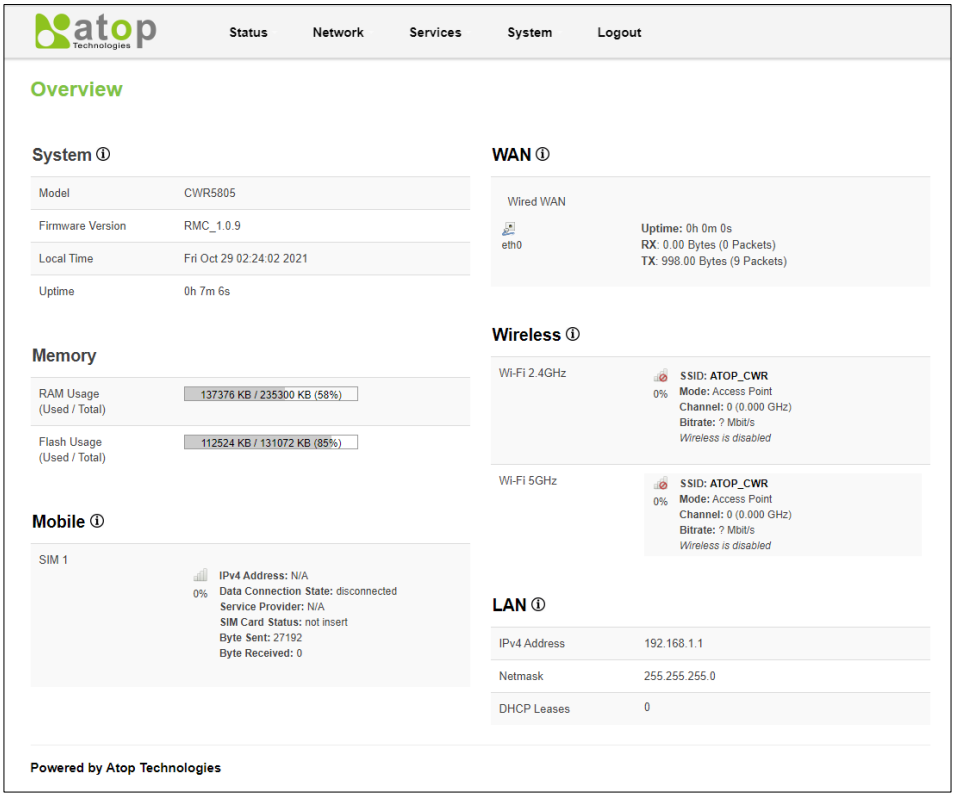


Table 9. Status > Overview

Field	Description
System	
Model	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 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 currect Primary SIM card state.
WAN	
Wired WAN	The currect WAN state.
Wireless	
Wi-Fi 2.4GHz	The currect Wi-Fi 2.4GHz state.
Wi-Fi 5GHz	The currect 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 Client connected.

3.2.2 System

This section shows the system status information of your router.

Figure 20. Status > System

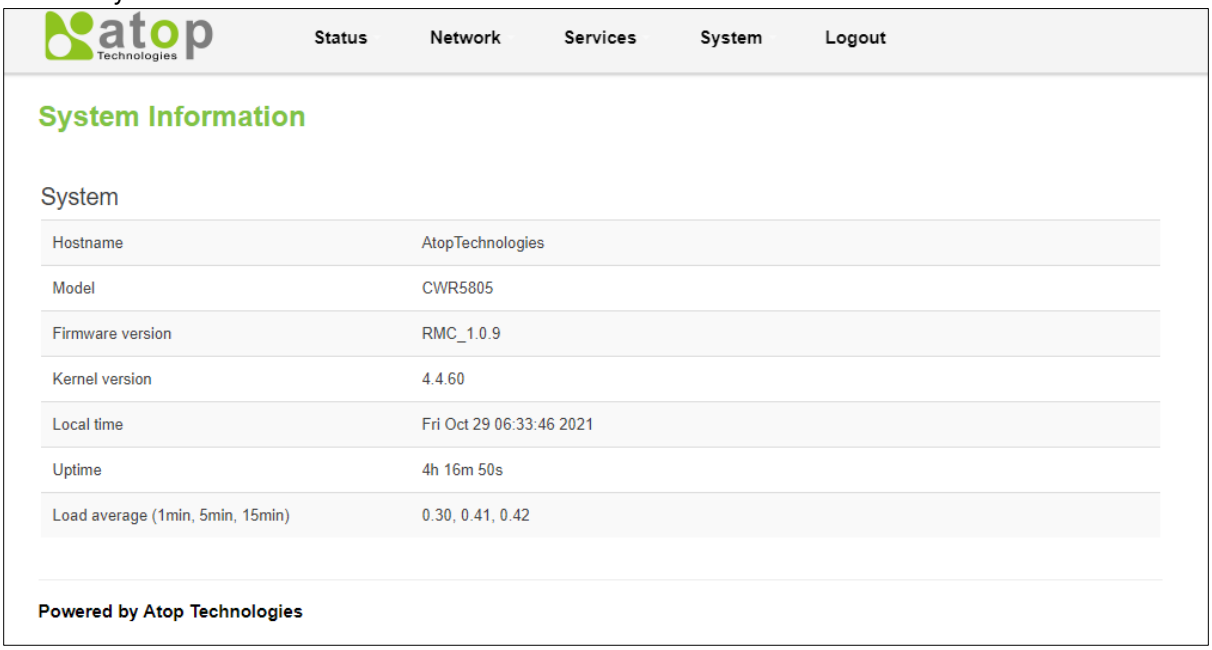


Table 10. Status > System

Field	Description
Hostname	This value can be modified on Hostname field of the System webpage.
Model	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 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 contains information of the primary SIM card number, the data connection state, the service provider, the network type, the signal strength, the number of byte sent, the number of byte received, IMEI, IMSI, and ICCID.

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

Figure 21. Status > Network > Mobile

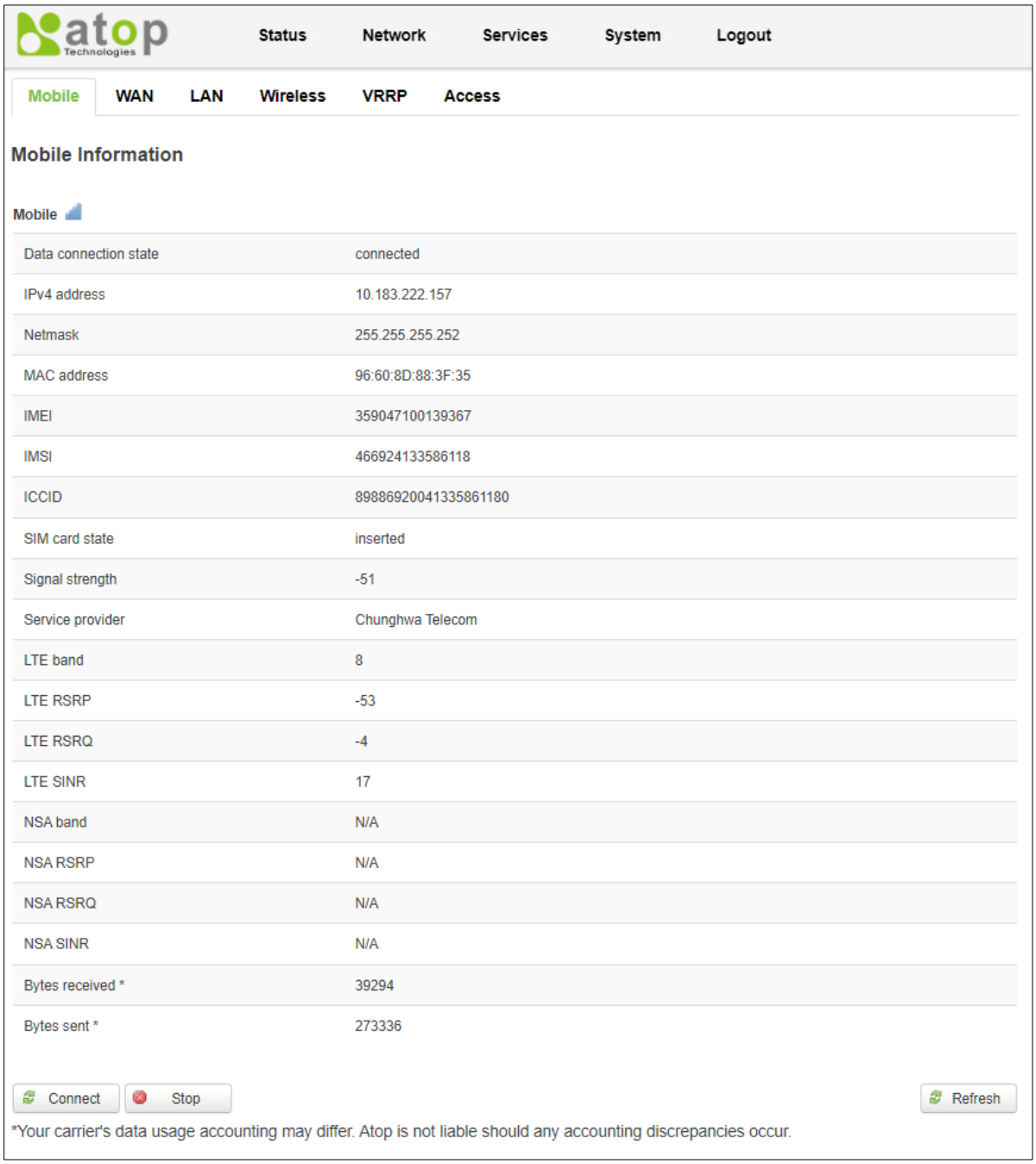


Table 11. Status > Network > Mobile

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 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 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 mobile data connection.
Bytes sent	The number of bytes were sent via mobile data connection.

3.2.3.2 WAN

This section shows the WAN status information of the router.

Figure 22. Status > Network > WAN

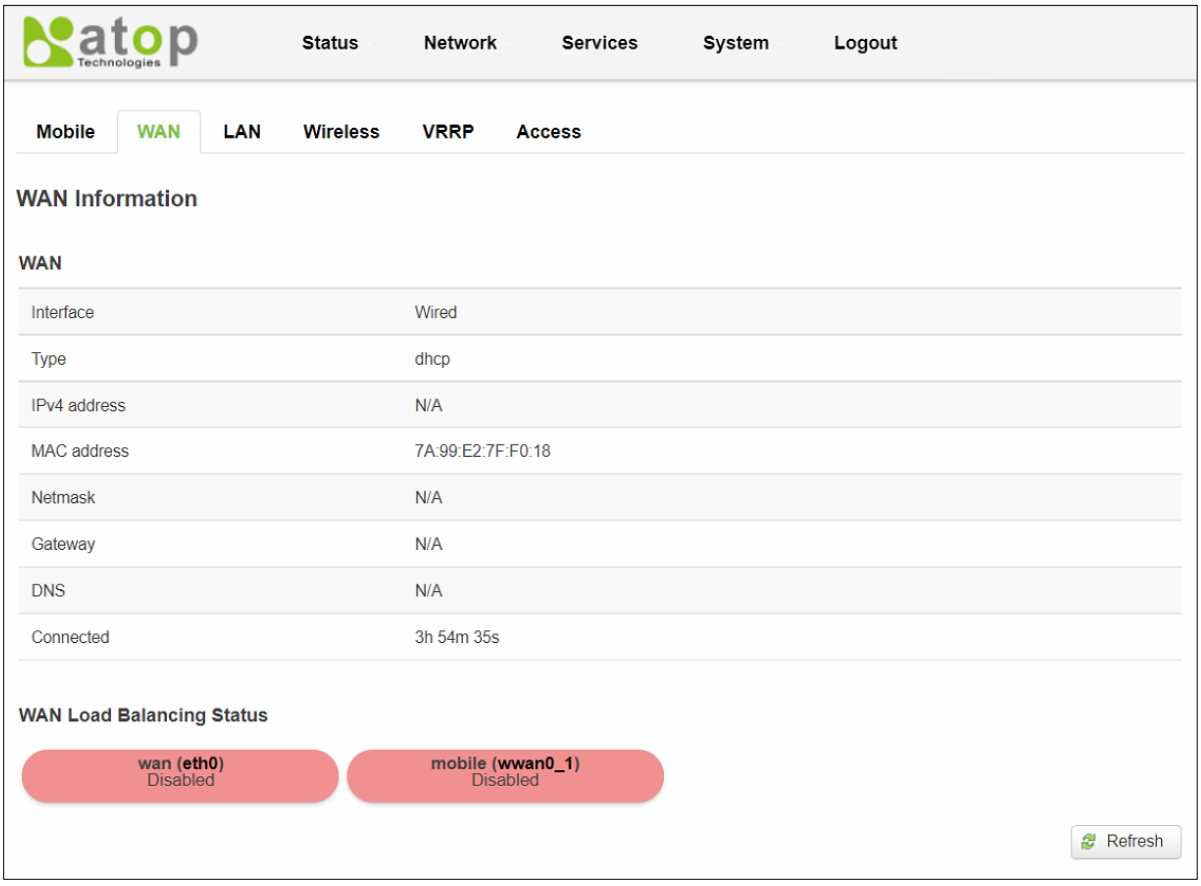


Table 12. Status > Network > WAN

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 23. Status > Network > LAN

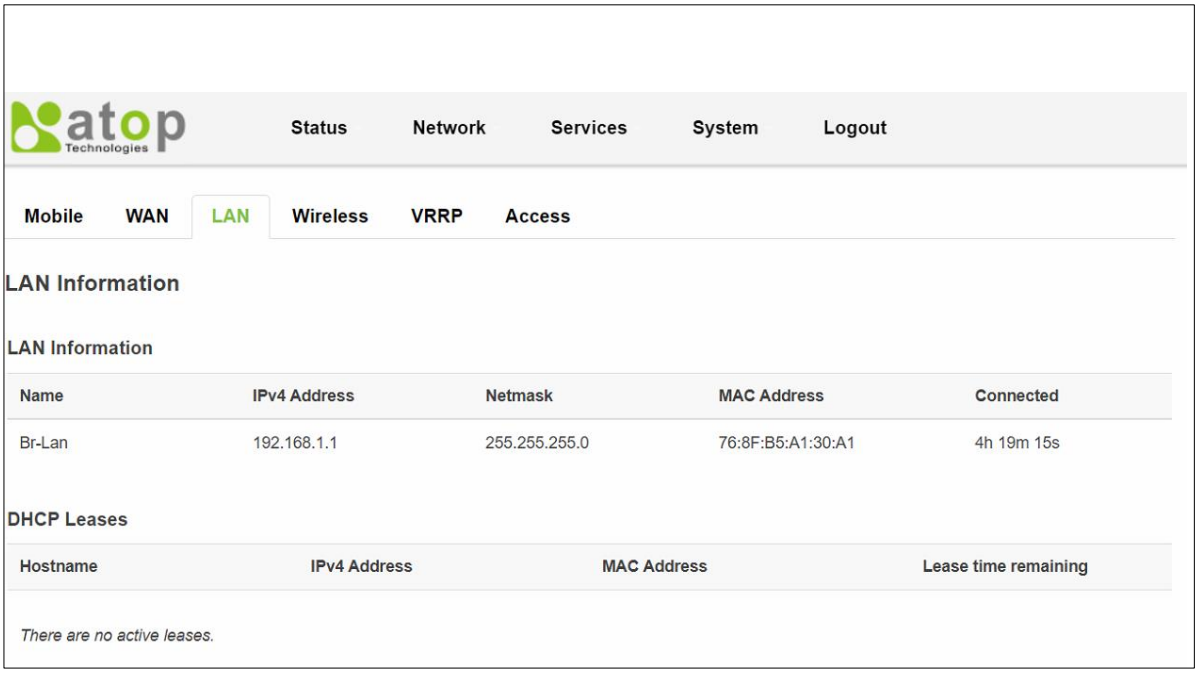


Table 13. Status > Network > LAN

Field	Description
Hostname	DHCP client's hostname.
IPv4-Address	DHCP client's IP address.
MAC-Address	DHCP client's MAC address.
Leasetime remaining	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 24 Status > Network > Wireless

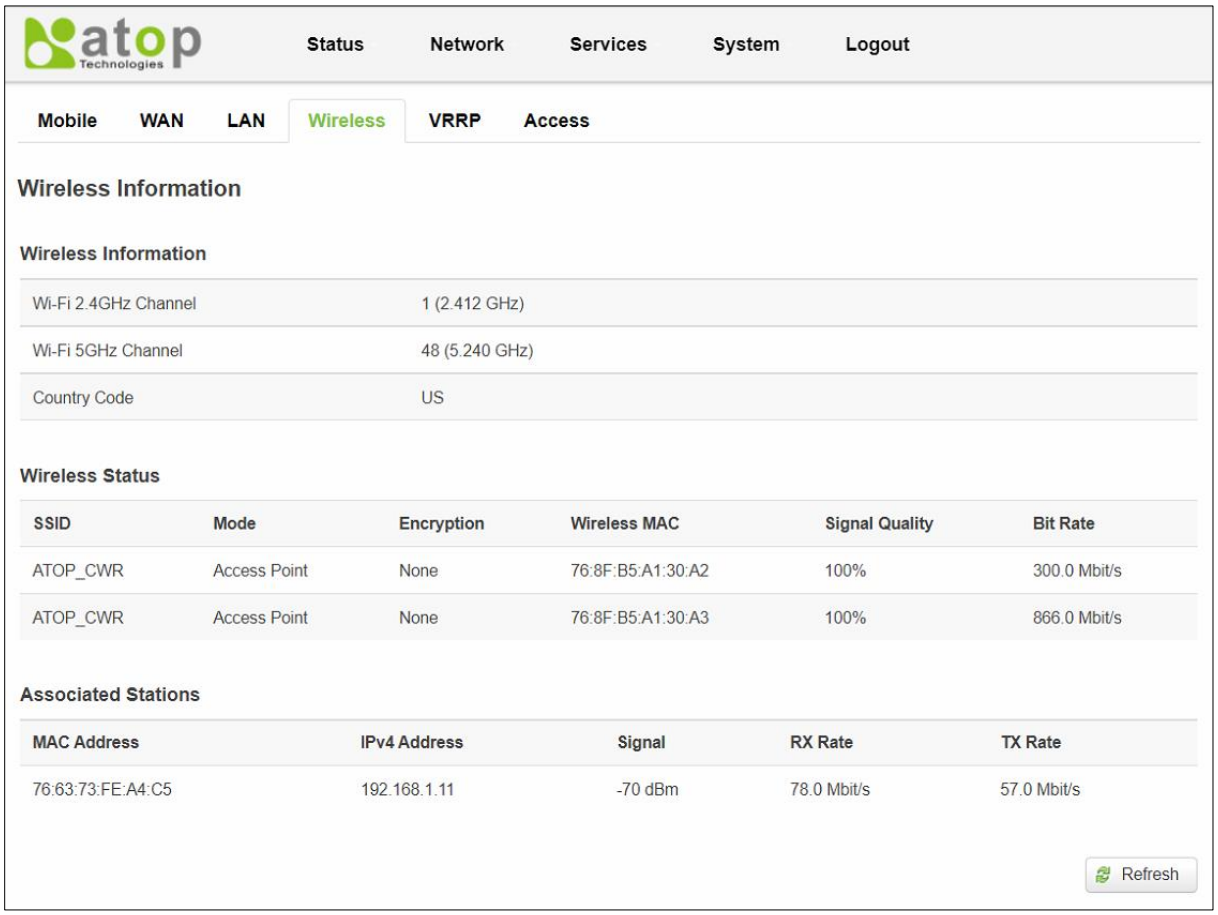


Table 14 Status > Network > Wireless

Field	Description
Wi-Fi 2.4GHz Channel	The display name of Wi-Fi 2.4GHz interface on CWR5805 device.
Wi-Fi 5GHz Channel	The display name of Wi-Fi 5GHz interface on 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 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 CWR5805 and associated station.
Rx Rate	The rate of the received packets from associated station.
Tx Rate	The rate of the sent packets to 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 25. Status > Network > VRRP (Master)

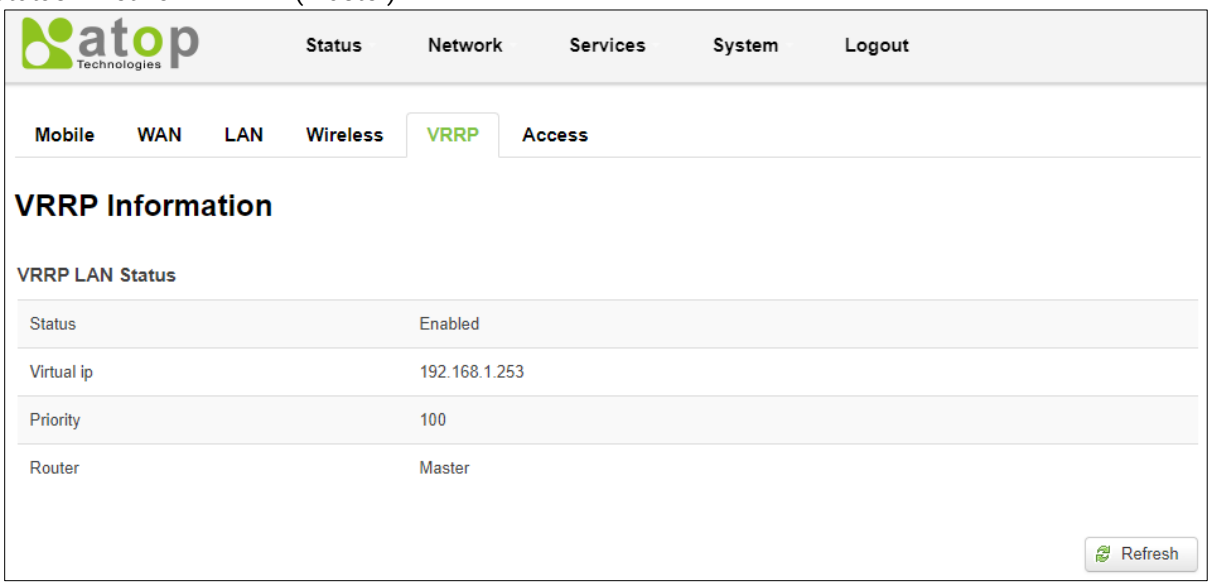


Figure 26. Status > Network > VRRP (Backup)

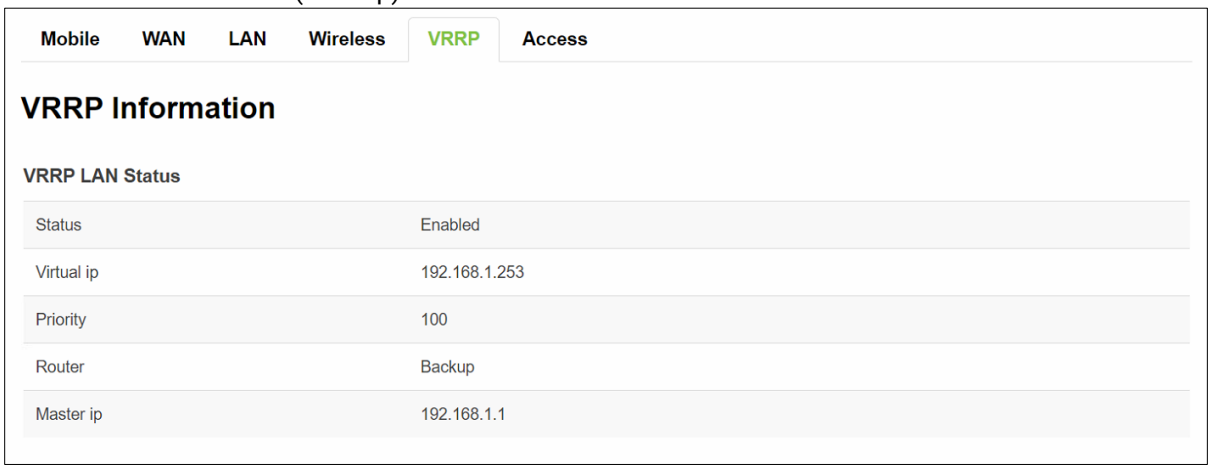


Table 15. Status > Network > VRRP

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**	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 27. Status > Network > Access

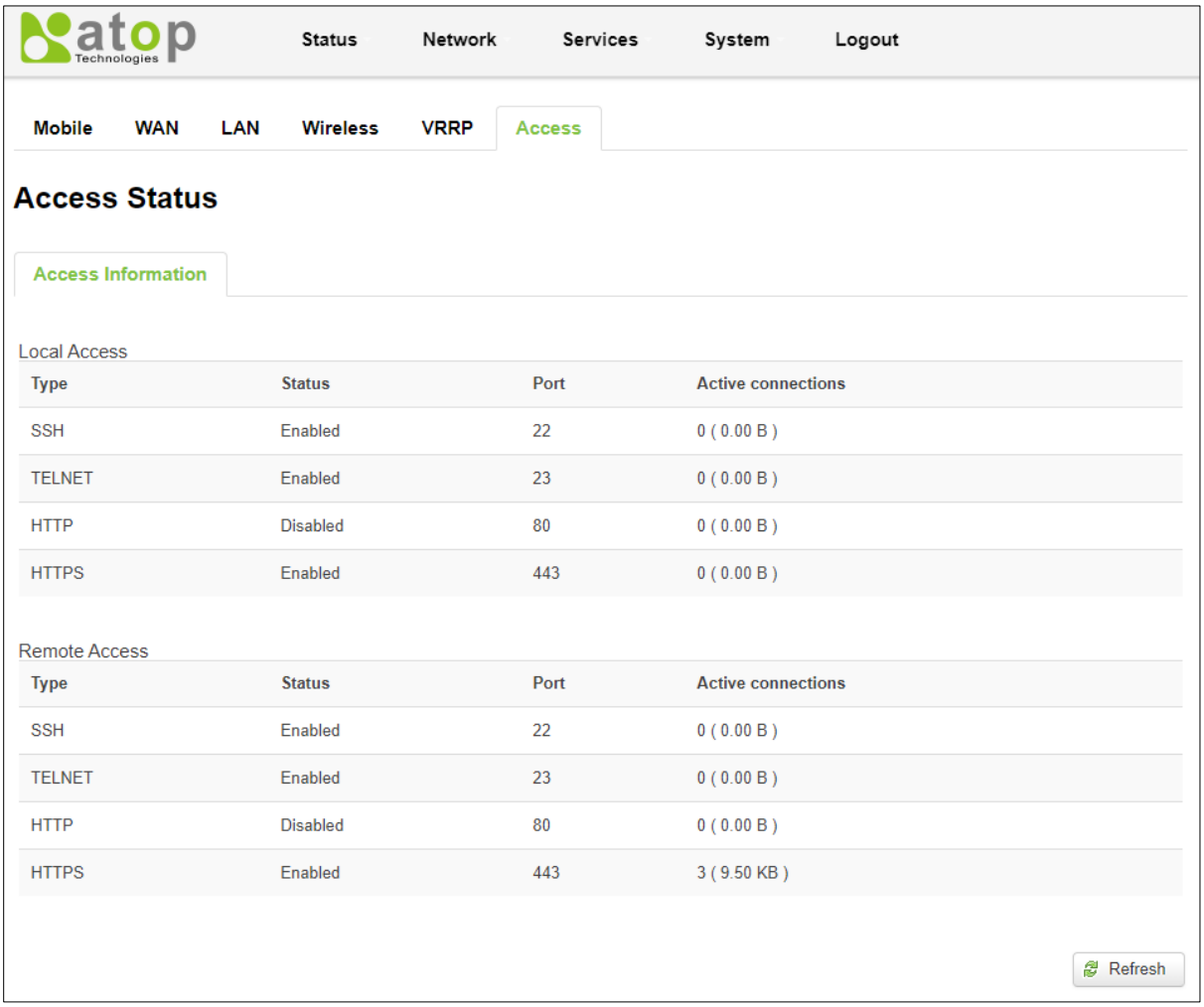


Table 16. Status > Network > Access

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 Status menu provides information such as 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 28. Status > Routes - ARP

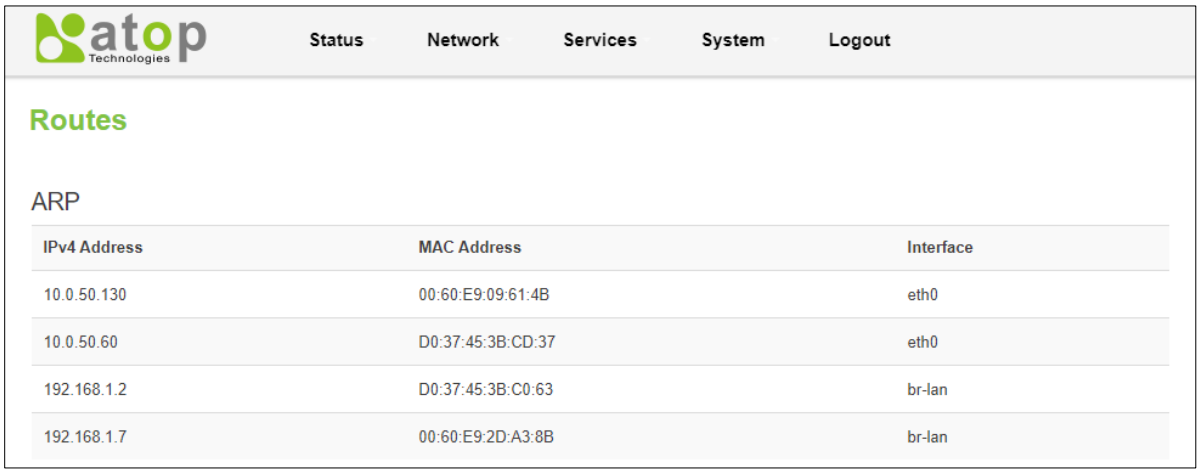


Table 17. Status > Routes - ARP

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 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 29. Status > Routes – Active IPv4 Routes

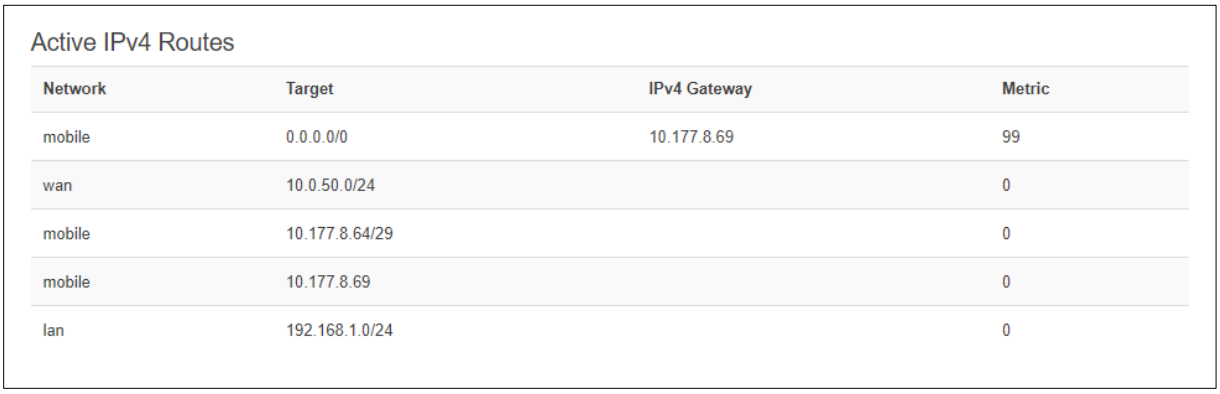


Table 18. Status > Routes – Active IPv4 Routes

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 actual IP addresses that the routing rule is applied. This fied 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	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 mertric is applied.

3.2.5 Logs

3.2.5.1 System Log

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

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

Figure 30. Status > System > System Log

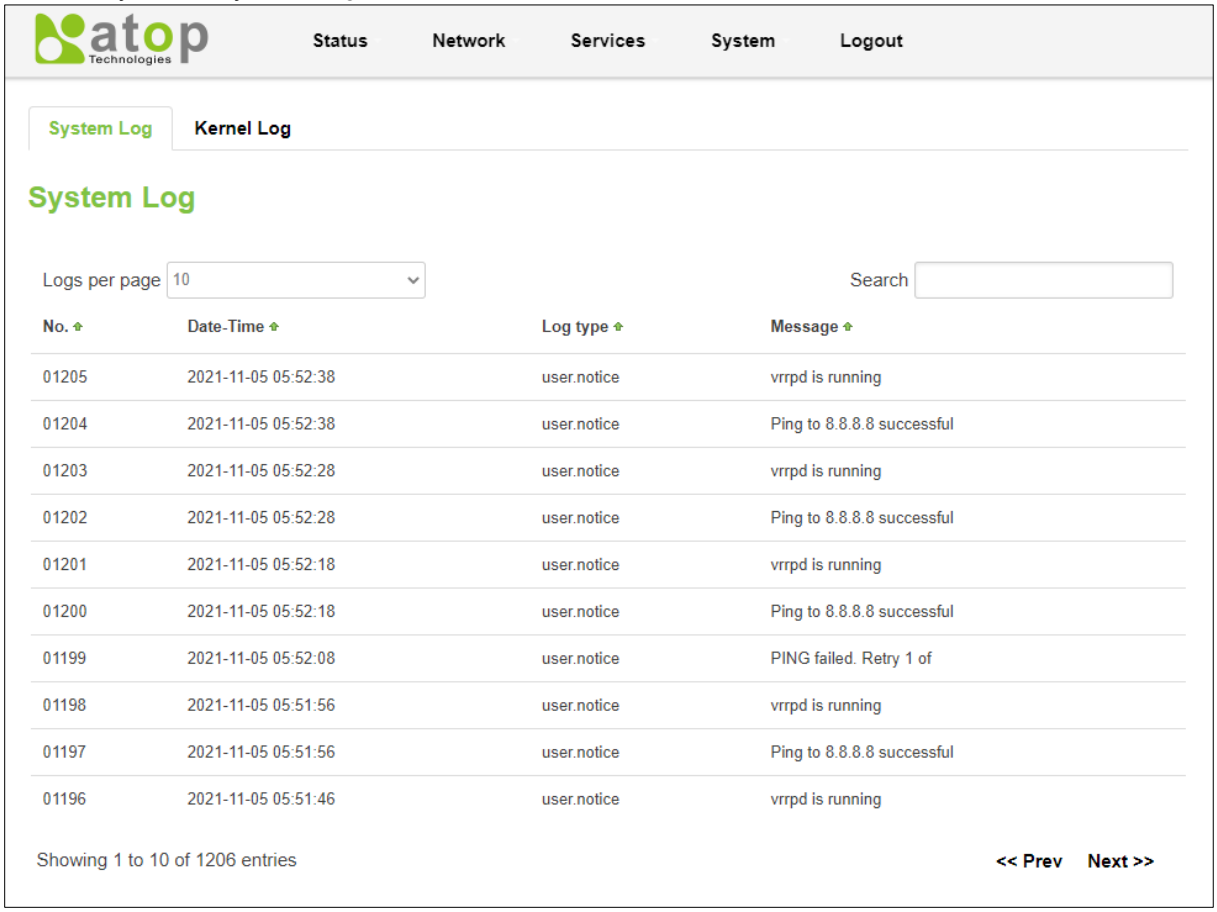


Table 19. Status > System > System Log

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 31. Status > System > Kernel Log

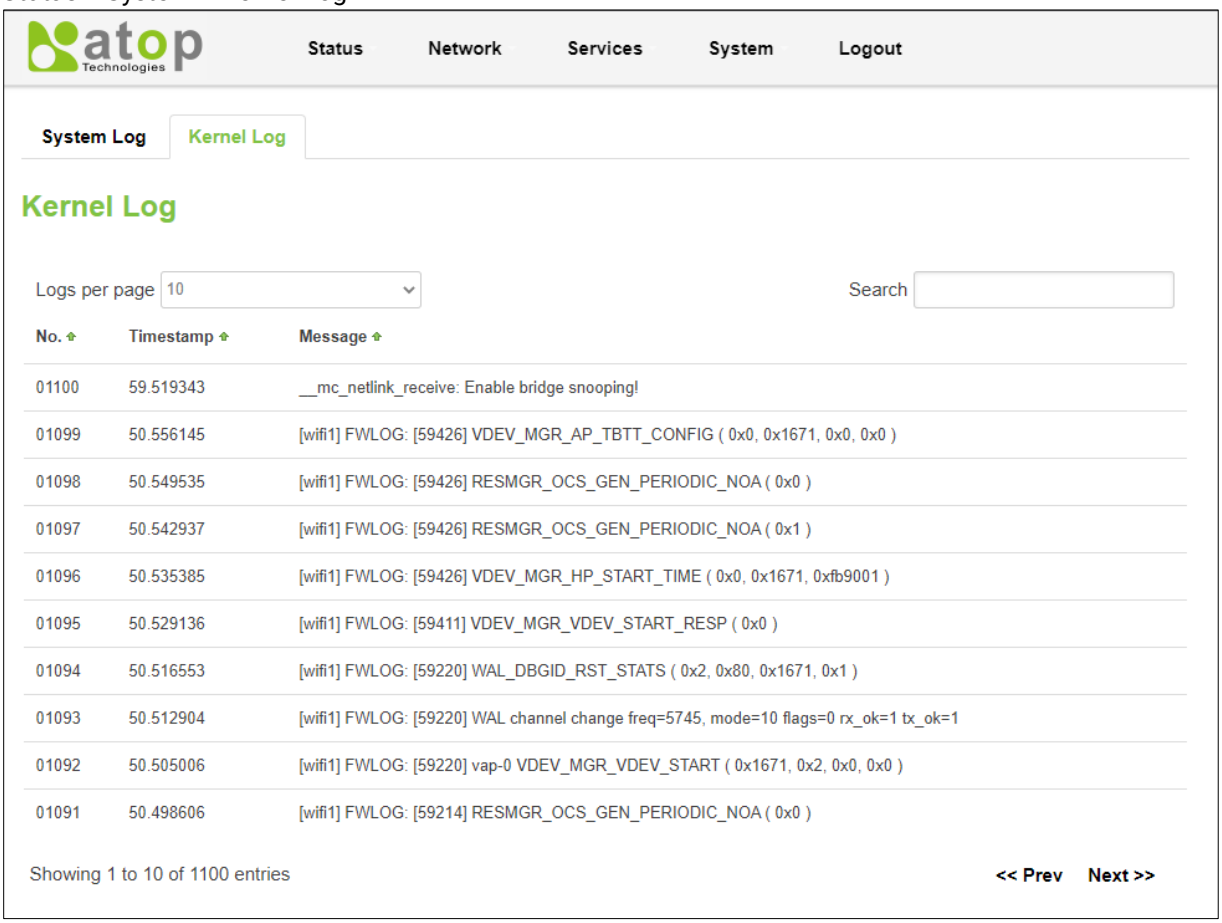


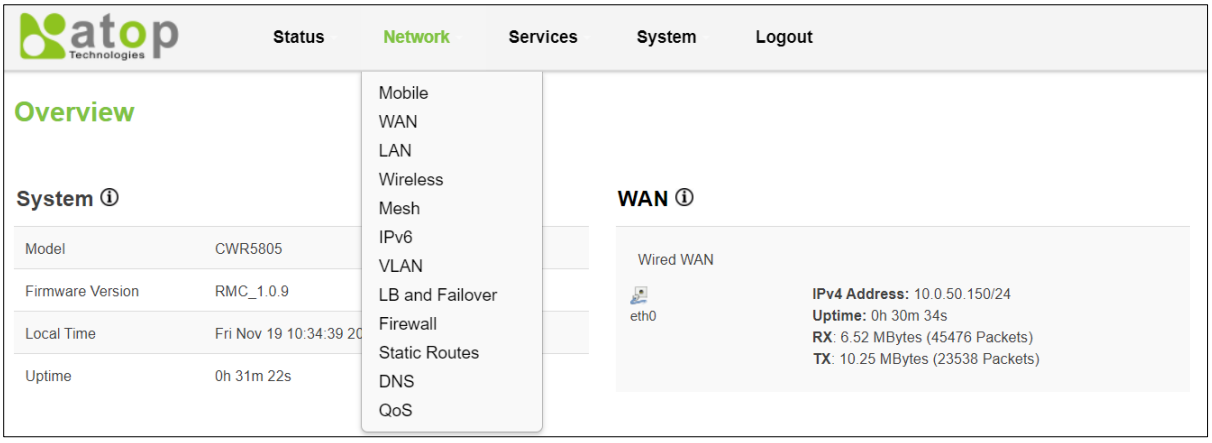
Table 20. Status > System > Kernel Log

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 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 32. Network



3.3.1 Mobile

CWR5805 is also equipped with 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 Moble 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 General Setup tab except IP, which depend 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 APN field can 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 Internet, the default value of 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 33. Network > Mobile > General Setup

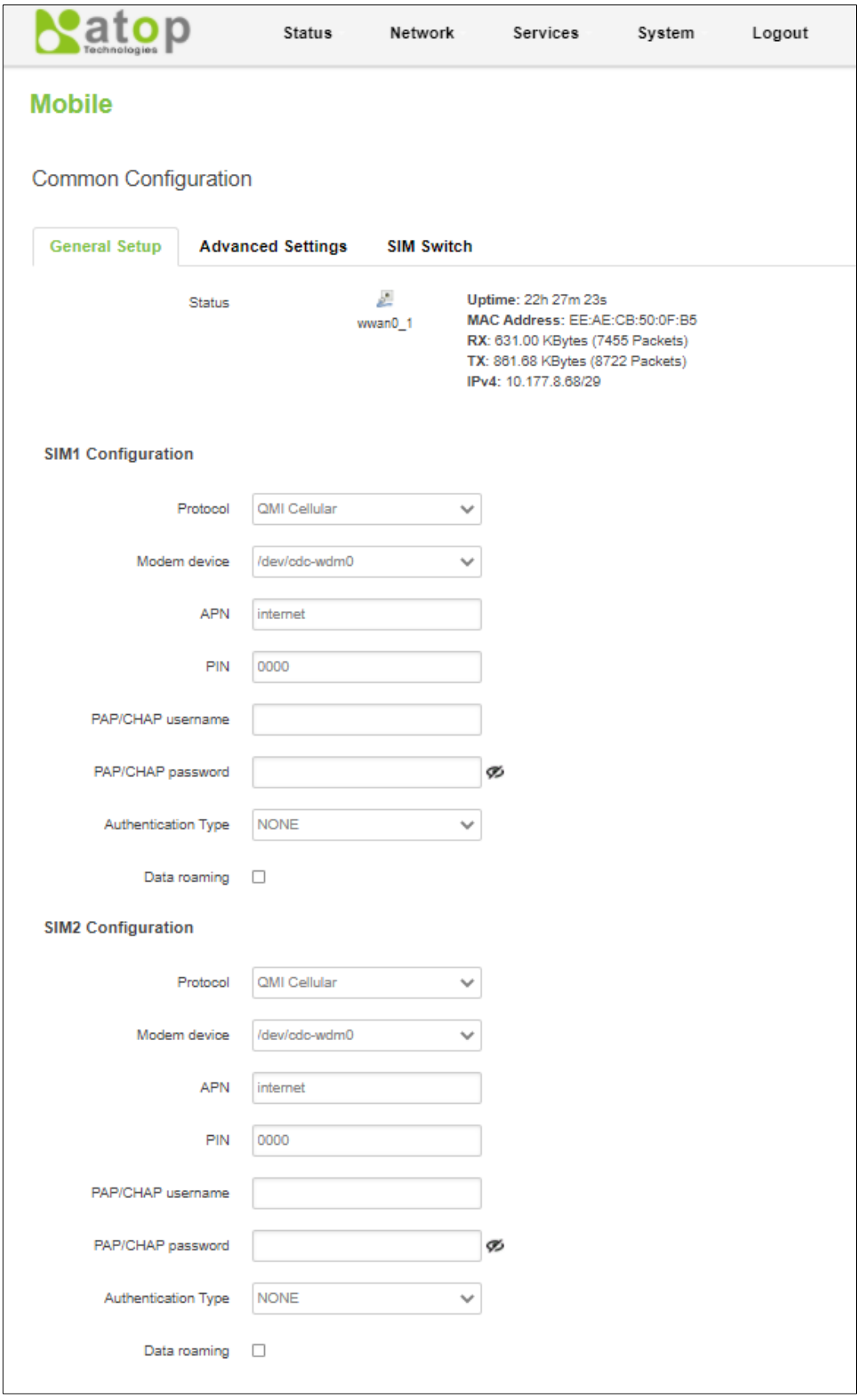


Table 21. Network > Mobile > General Setup

Field	Value	Description
Protocol	default: **QMI Cellular**	The protocol 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 suitable type of network connection for that mobile device, depending on the contract with the operator.
PIN	default: **0000**	A password 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 Network-Interfaces-MOBILE tab, you can configure network functionalities in more details based on your requirements of the mobile interface.

Figure 34. Network > Mobile > Advanced Settings

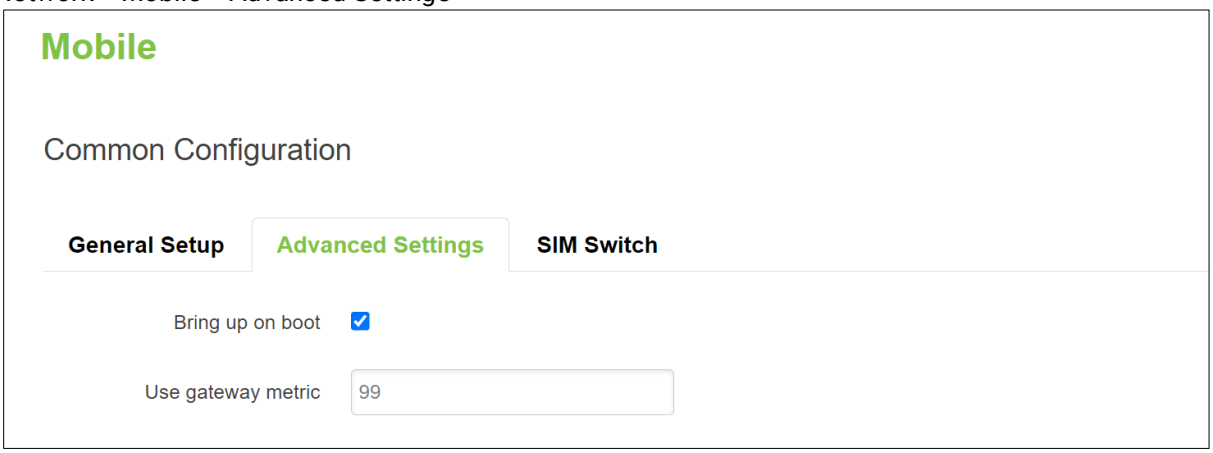


Table 22. Network > Mobile > Advanced Settings

Field	Value	Description
Bring Up on Boot	default: **enable**	Specify whether or not to bring up WAN interface on 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 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 35. Network > Mobile > SIM Switch

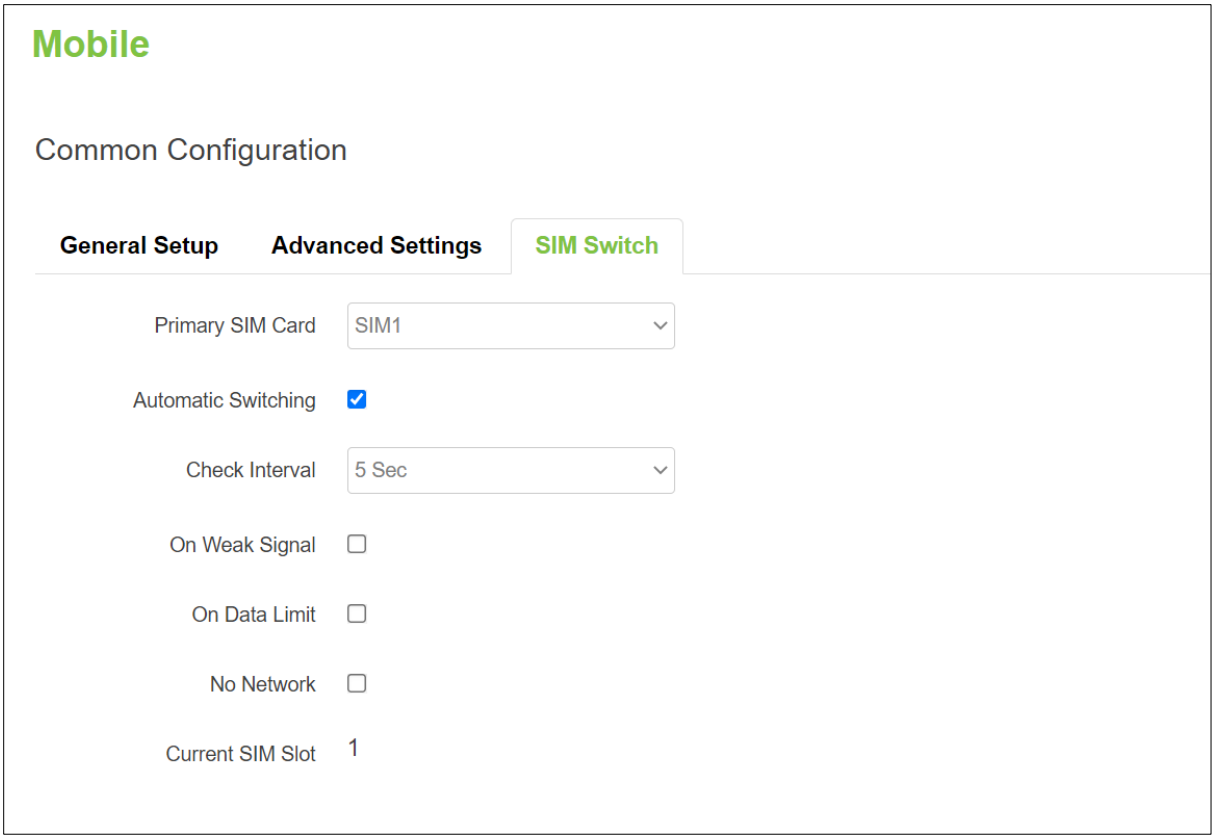


Table 23. Network > Mobile > SIM Switch

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 mechansism 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 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, CWR5805 device will no longer use the mobile connection to establish a data connection until the limit period is over or the limit is reset by you.

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

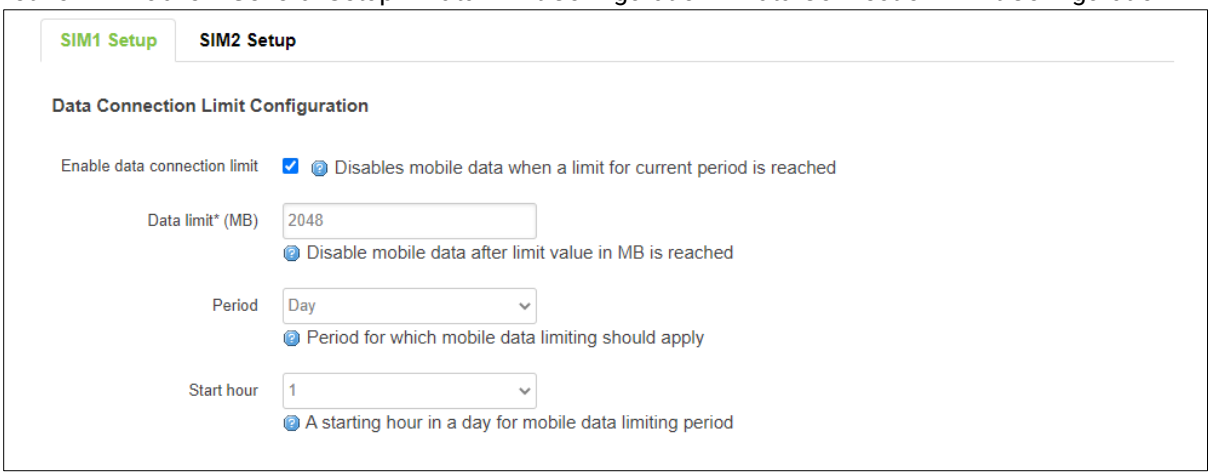


Table 24. Network > Mobile > General Setup > Data Limit Configuration > Data Connection Limit Configuration

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 time. 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 CWR5805 device's SIM card reached the specified limit.

Figure 37. Network > Mobile > General Setup > Data Limit Configuration > SMS Warning Configuration

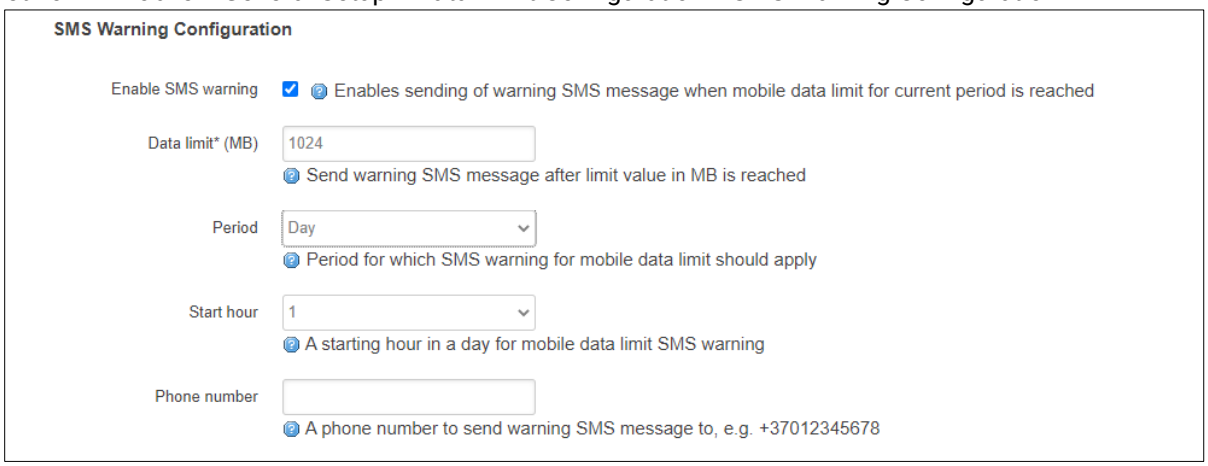


Table 25. Network > Mobile > General Setup > Data Limit Configuration > SMS Warning Configuration

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 of 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 to.

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 38. Network > Mobile > General Setup > Data Limit Configuration > Clear Data Limit

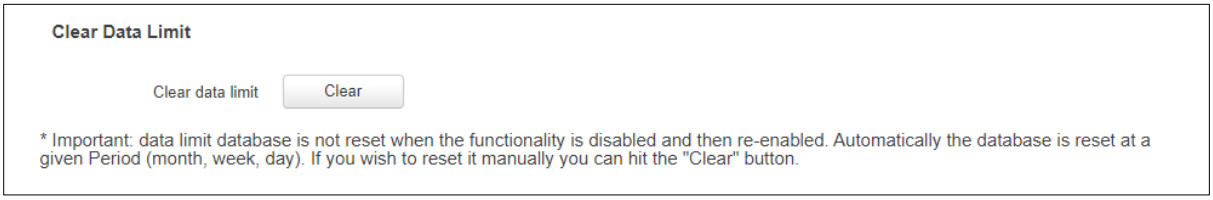


Figure 39. Network > Mobile > General Setup > Data Limit Configuration > Clear Data Limit

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

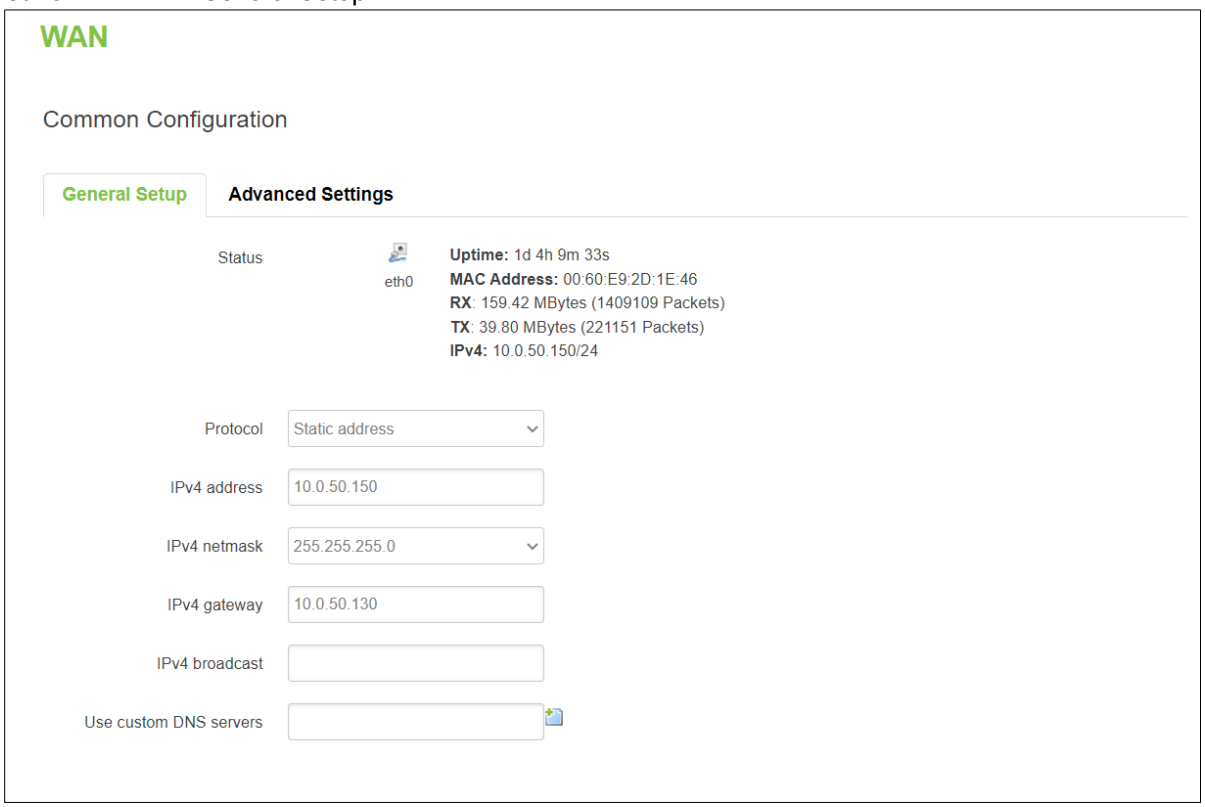
3.3.2 WAN

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 are network.

3.3.2.1 General Setup

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

Figure 40. Network > WAN > General Setup



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

In **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 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 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 41. Network > WAN > General Setup – DHCP Client

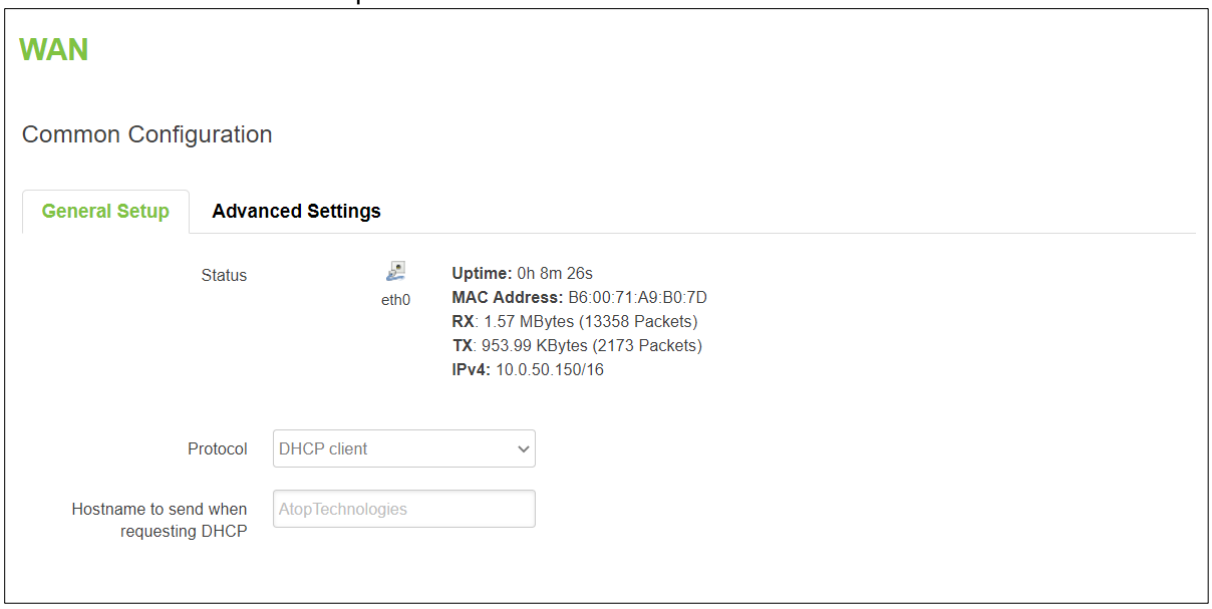


Table 26. Network > WAN > General Setup – DHCP Client

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

3.3.2.2.2 Advanced Settings

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

Figure 42. Network > WAN > Advanced Settings – DHCP Client

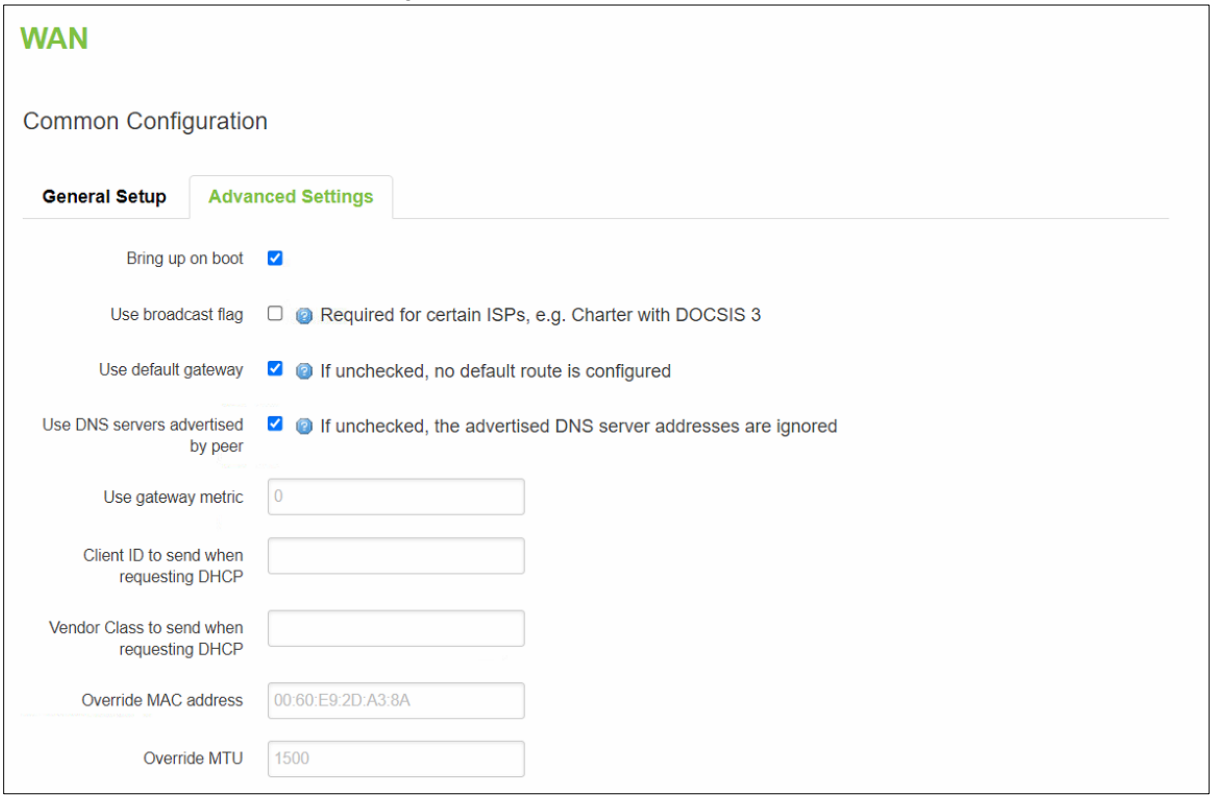


Table 27. Network > WAN > Advanced Settings – DHCP Client

Field	Value	Description
Bring Up on Boot	default: **enable**	Specify whether to bring up WAN interface on boot.
Use Broadcast Flag	default: **disable**	Neccessary for some ISPs (Internet Service Providers).
Use Default Gateway	default: **enable**	Use the default gateway obtained from DHCP. If left unchecked, no default route is configured.
Use DNS Servers Advertised by Peer	default: **enable**	Uses DNS servers obtained from DHCP. If left unchecked, the advertised DNS server addresses are ignored.
Use Gateway Metric	default: **0**	By default, the WAN configuration generates a routing table entry. You can change the metric of that entry here.
Client ID to Send When Reguesting DHCP	default: **none**	Sending client ID when requesting a DHCP lease.
Vendor Class to Send When Reguesting DHCP	default: **none**	Sending vendor class which requesting a DHCP lease.
Override MAC address	default: **CWR's MAC**	To override 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.

3.3.2.3 Static address

3.3.2.3.1 General Setup

Figure 43. Network > WAN > General Setup – Static Address

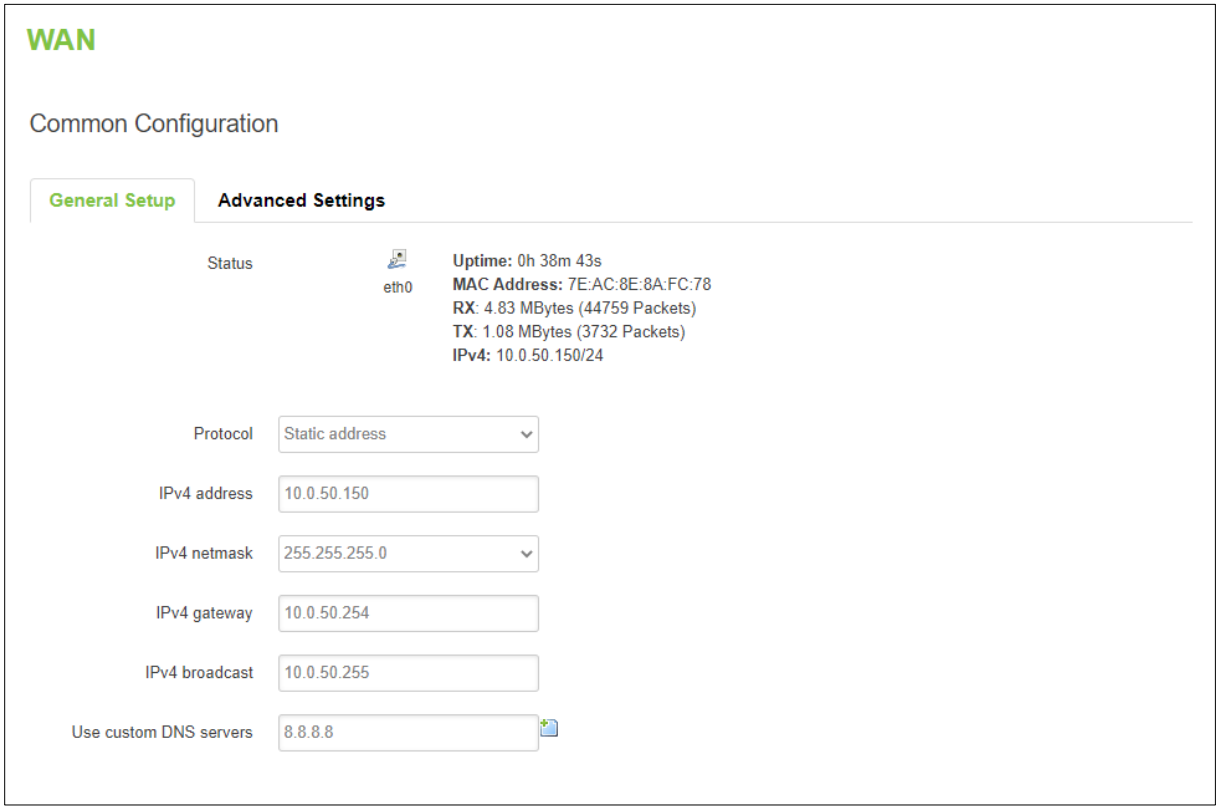


Table 28. Network > WAN > General Setup – Static Address

Field	Value	Description
Protocol	Static/DHCP/PPPoE; default: **DHCP**	The protocol used by the WAN interface. This field currently supports DHCP client, 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 host name 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 44. Network > WAN > Advanced Settings – Static Address

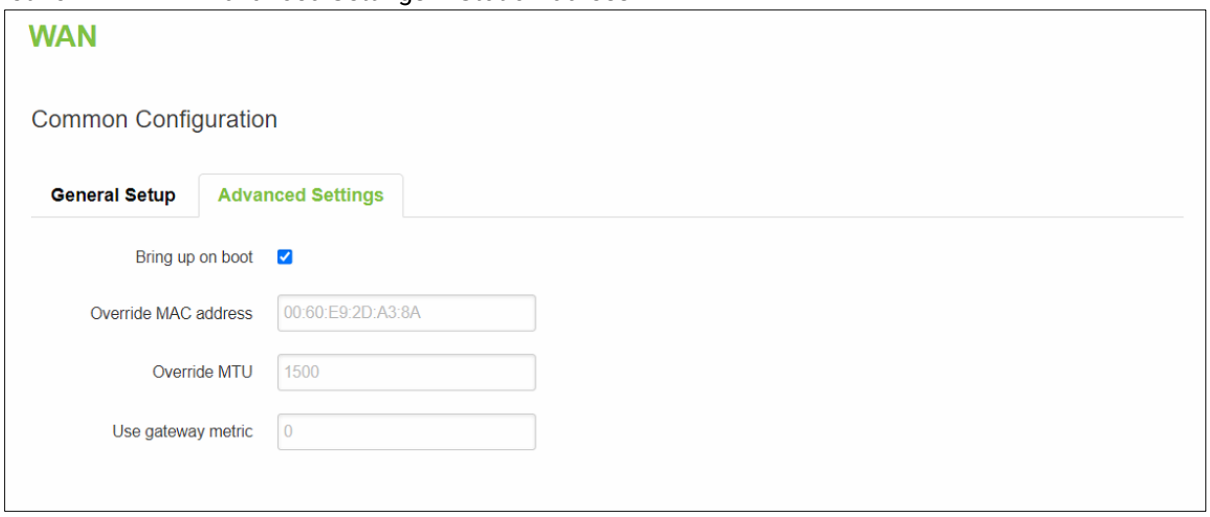


Table 29. Network > WAN > Advanced Settings – Static Address

Field	Value	Description
Bring up on boot	default: **enable**	Specify whether to bring up LAN interface on boot or not.
Override MAC address	default: **Device's MAC**	Override 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 45. Network > WAN > General Setup – PPPoE

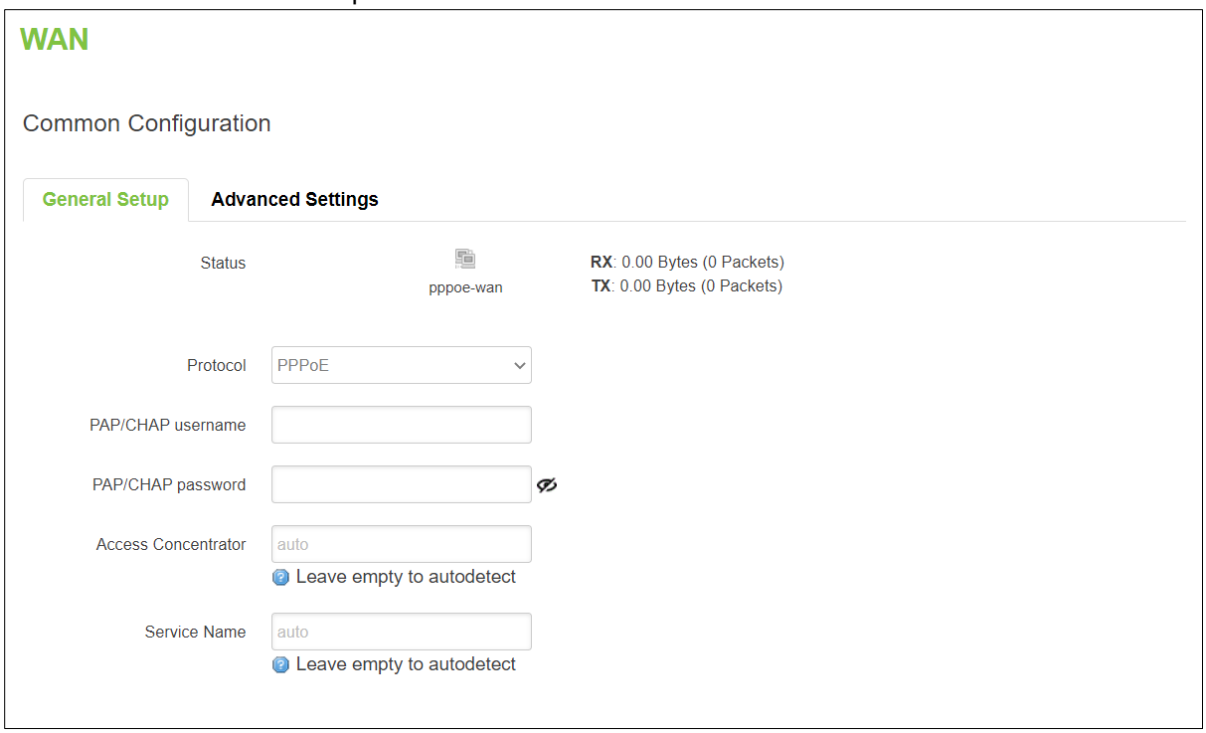


Table 30. Network > WAN > General Setup – PPPoE

Field	Value	Description
Protocol	Static /DHCP /PPPoE default: DHCP	The protocol used by the WAN interface. This field currently supports DHCP client, static address, and PPPoE.
PAP/CHAP Username	dfeault: **non**	Username used in PAP/CHAP authentication.
PAP/CHAP password	dfeault: **none**	Password used in PAP/CHAP authentication.
Access Concentrator	dfeault: **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	dfeault: **auto**	The Service Name to connect to. Leave this field empty to detect Service name automatically.

3.3.2.4.2 Advanced Settings

Figure 46. Network > WAN > Advanced Setting – PPPoE

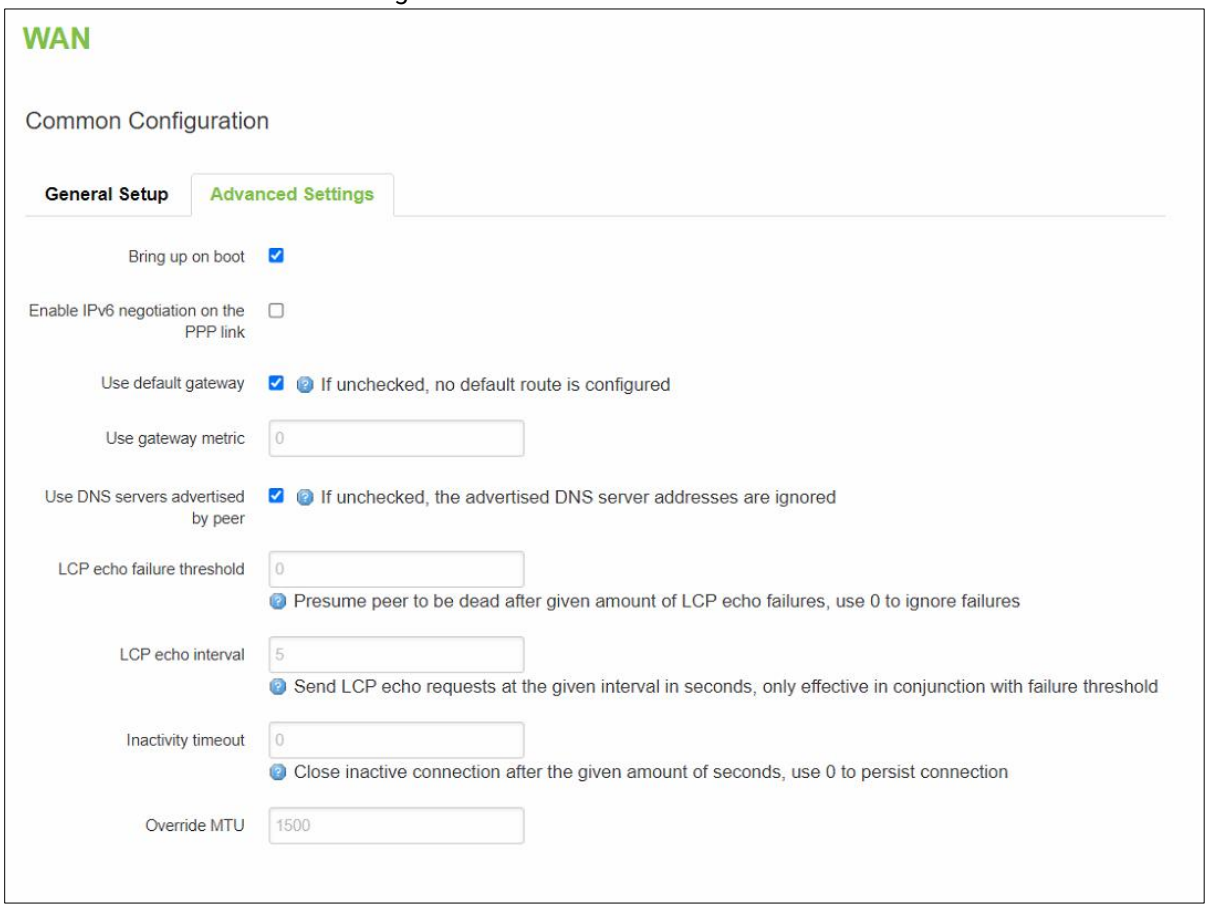


Table 31. Network > WAN > Advanced Setting – PPPoE

Field	Value	Description
Bring up on boot	default: **enable**	Specify whether to bring up 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 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 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 **Interface-LAN** webpage, the default protocol is set to **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 IPv4 DHCP server is 192.168.1.1, and the dynamic IP address range is start from 192.168.1.100 to 192.168.1.250.

3.3.3.1 General Setup

In the **General Setup** sub-tab of 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 Figure below, the Status field currently displays LAN port interface (br-lan) infomation 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 47. Network > LAN > Common Configuration – Static Address

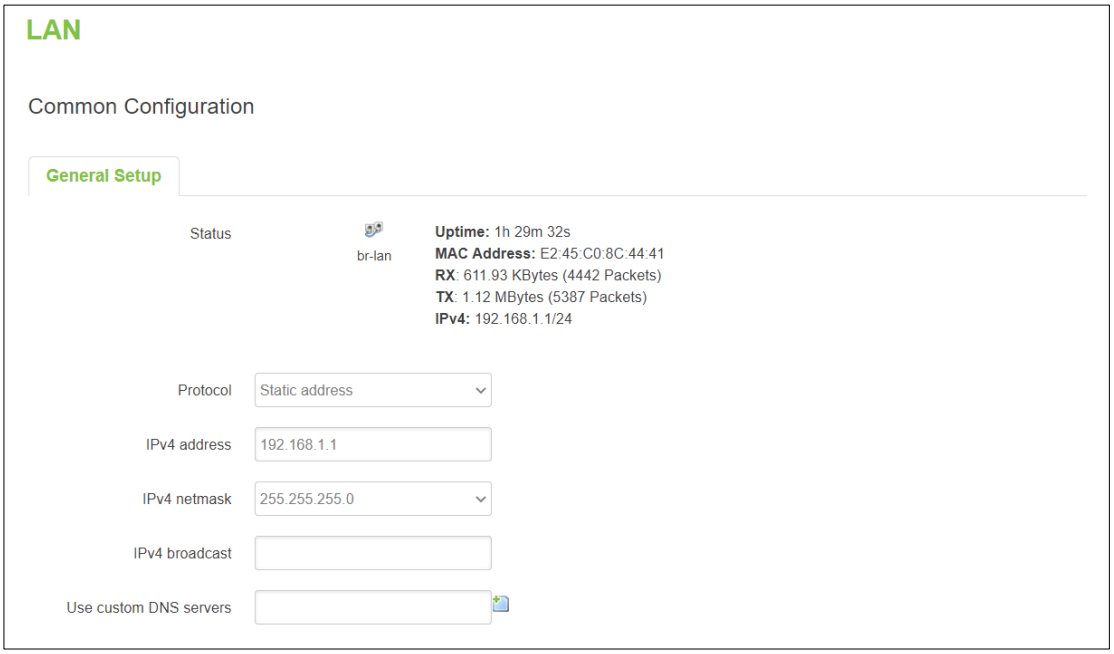


Table 32. Network > LAN > Common Configuration – Static Address

Field	Value	Description
Protocol	Static address	The protocol 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 words, any IPv4 DHCP client devices connected to 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 Network-Interface-LAN tab-All sub tabs, the basic setting of the DHCP server service is available.

Figure 48. Network > LAN > DHCP Server > General Setup

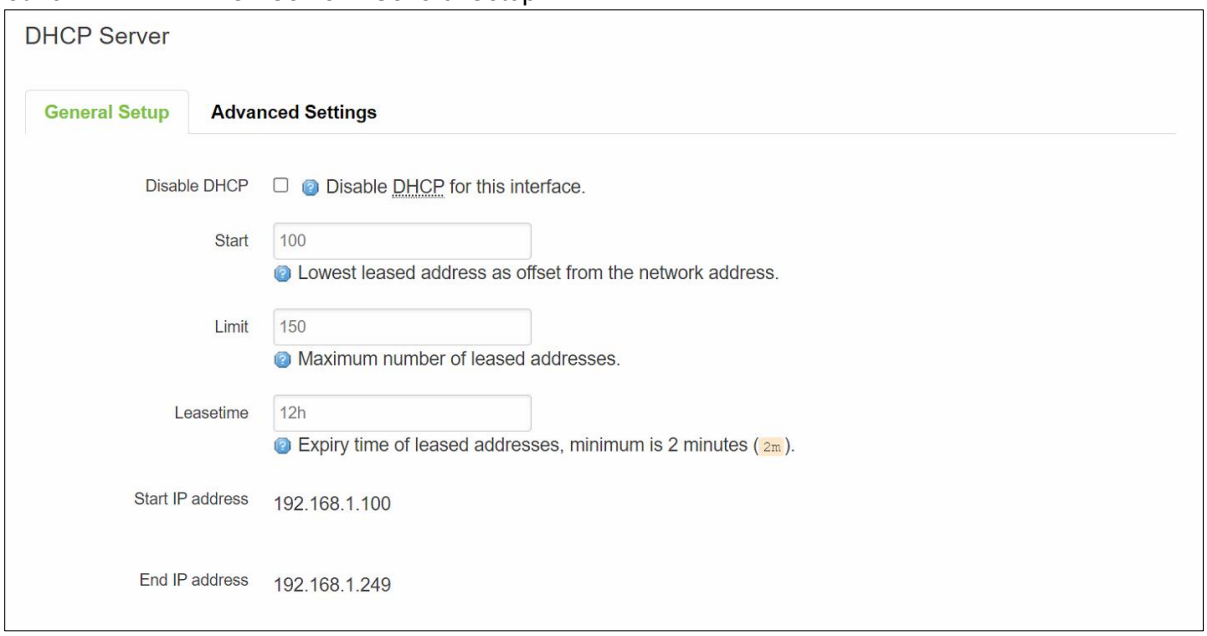


Table 33. Network > LAN > DHCP Server > General Setup

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 need to be reached frequently, e.g., printer, IP phone, etc.

Figure 49. Network > LAN > DHCP Server > Static Leases

Table 34. 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 that 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 tab-All sub tabs, you can configure more complicated setting of the DHCP server service.

Figure 50. Network > LAN > DHCP Server > Advanced Settings

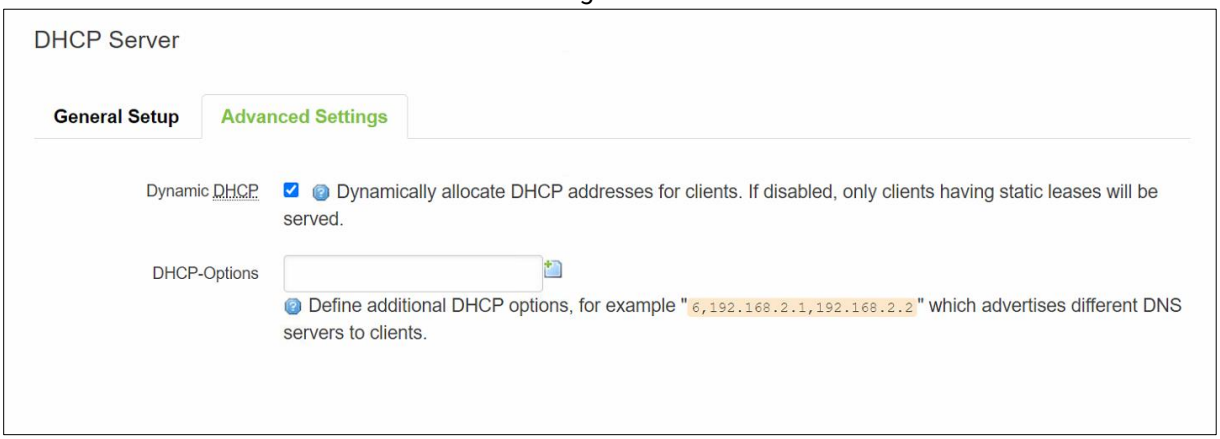


Table 35. Network > LAN > DHCP Server > Advanced Settings

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 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 Edit button. The configuration webpage of the selected WiFi interface will be initialized.

In the **Wifi** sub-menu within 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 51. Network > Wireless > Wireless Overview

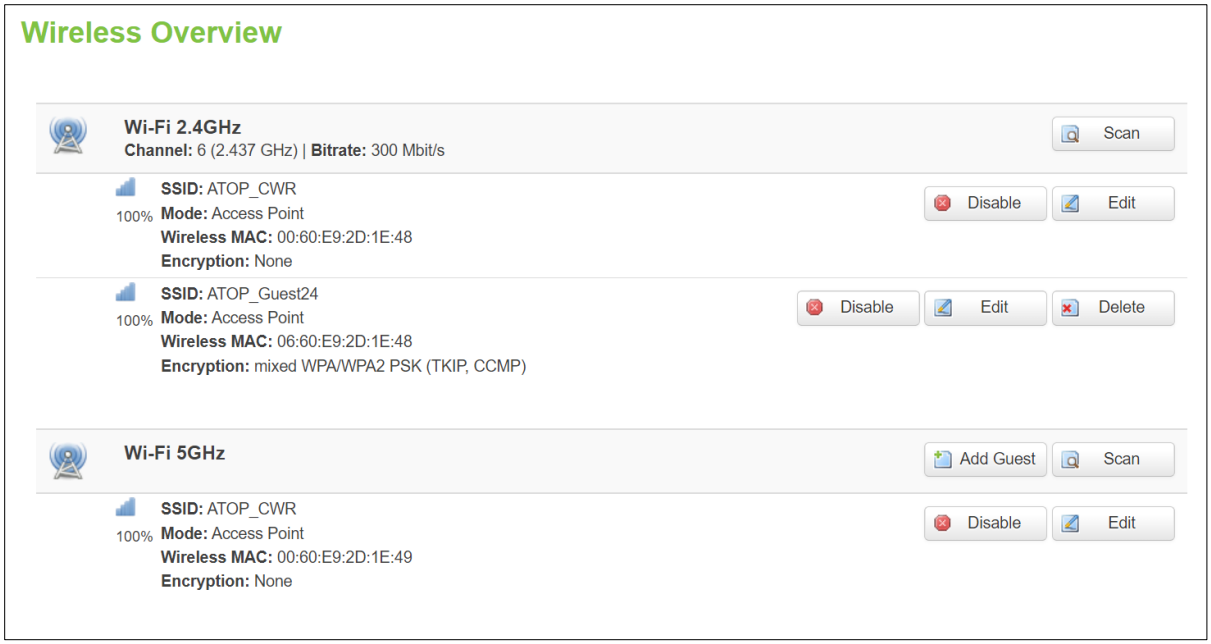


Table 36. Network > Wireless > Wireless Overview

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 details.

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 “Scan” button in the Wireless Overview section.

Figure 52. Network > Wireless > Wireless Scan

Table 37. Network > Wireless > Wireless Scan

Field	Description
Signal Level	Received Signal Strength Indicatior (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 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

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

Figure 53. Network > Wireless > Associated Stations

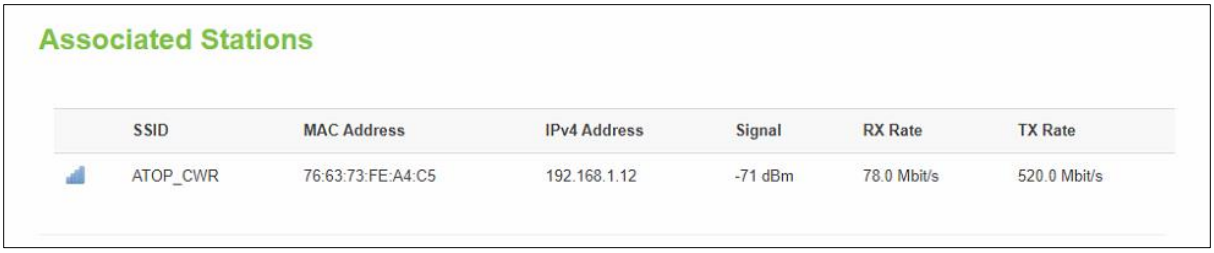


Table 38. Network > Wireless > Associated Stations

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 CWR5805 and associated station.
Rx Rate	The rate of the received packets from associated station.
Tx Rate	The rate of the sent packets to associated station.

3.3.4.3 Device Configuration

In the **Device Configuration** webpage of Wireless Overview section within the Network-Wifi sub-menu, you can configure 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 “Edit” button in the Wireless Overview section.

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

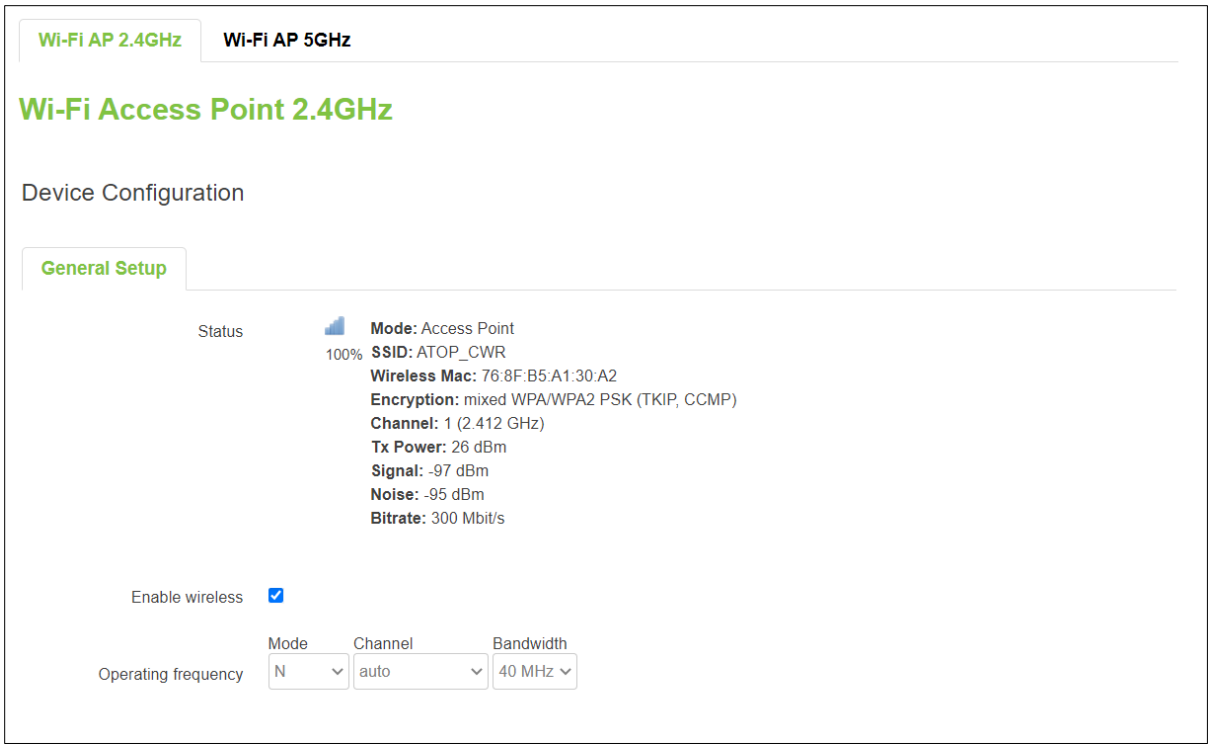


Figure 55. Network > Wireless > Edit Wi-Fi AP 5GHz

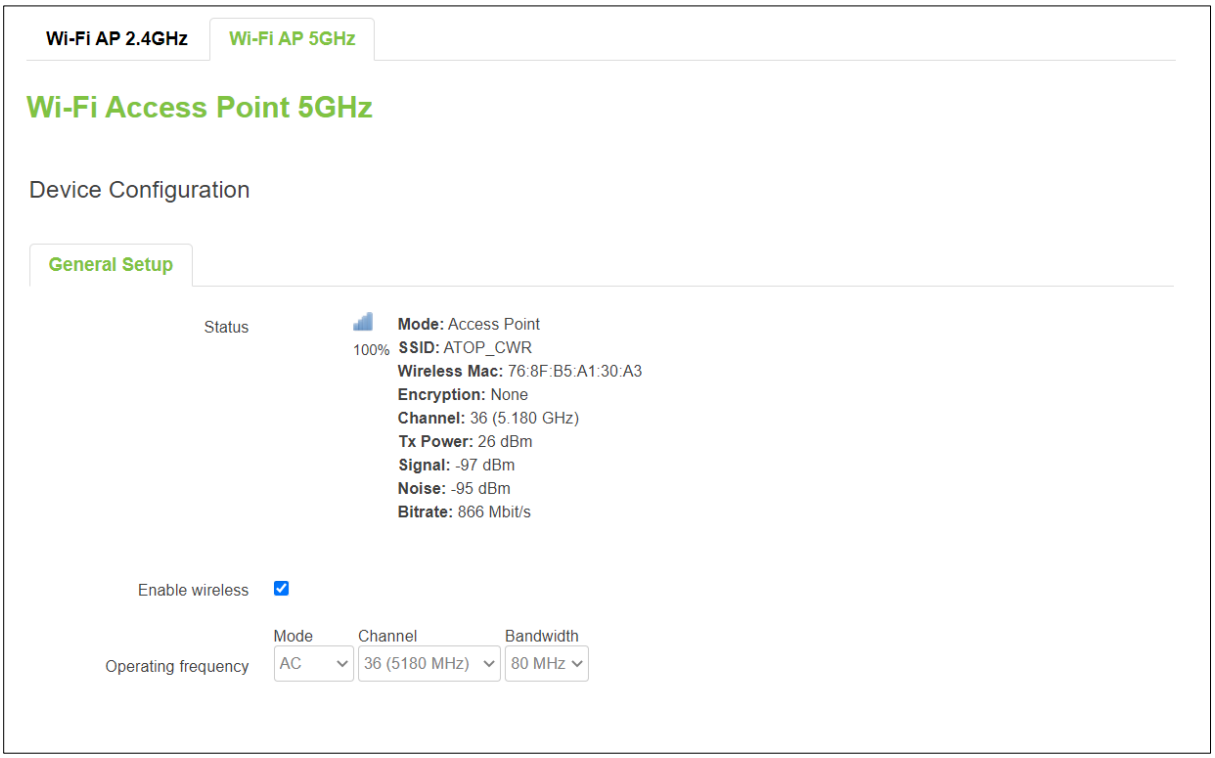


Table 39. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz

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, bit rate 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 used by 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 Wireless Overview section within the Network-Wifi sub-menu, you can configure software parameters of the Wi-Fi 2.4GHz/5GHz access point. This section will be initialized when you click on “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 SSID of Wi-Fi 2.4GHz/5GHz Access Points, as shown in the Figure below.

Figure 56. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > General Setup

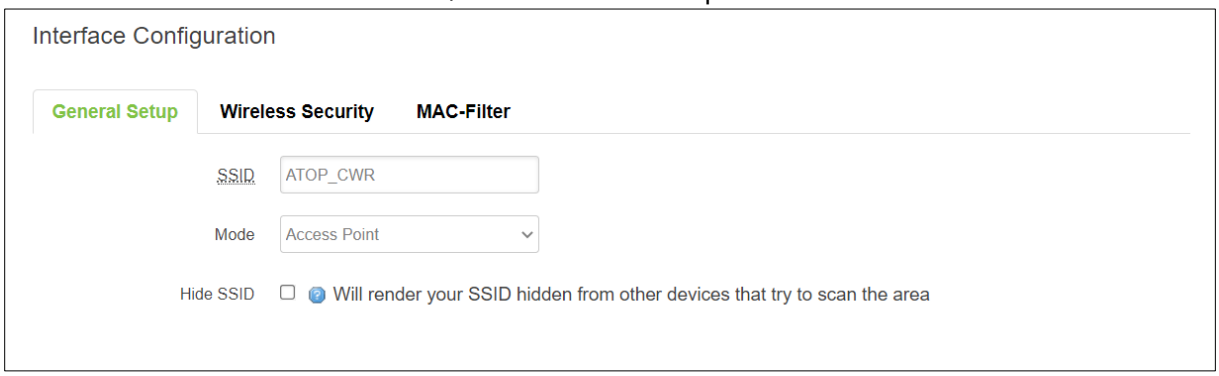


Table 40. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > General Setup

Field	Value	Description
SSID	default: **ATOP_CWR**	The broadcast SSID of the wireless network that clients will be connectd to.
Mode	default: **Access Point**	Aaccess Point mode only.
Hide ssid	default: **dissable**	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 encryption type that will be used in Wi-Fi Access Point 2.4GHz/5GHz, as shown in the Figure below.

Figure 57. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > Wireless Security

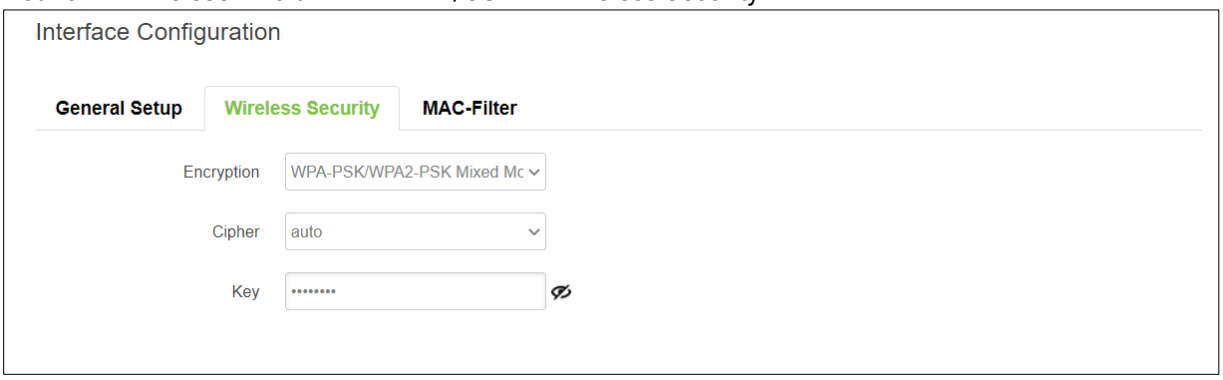


Table 41. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > General Setup

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

Table 42. 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

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

Figure 59. Network > Mesh > Basic Settings

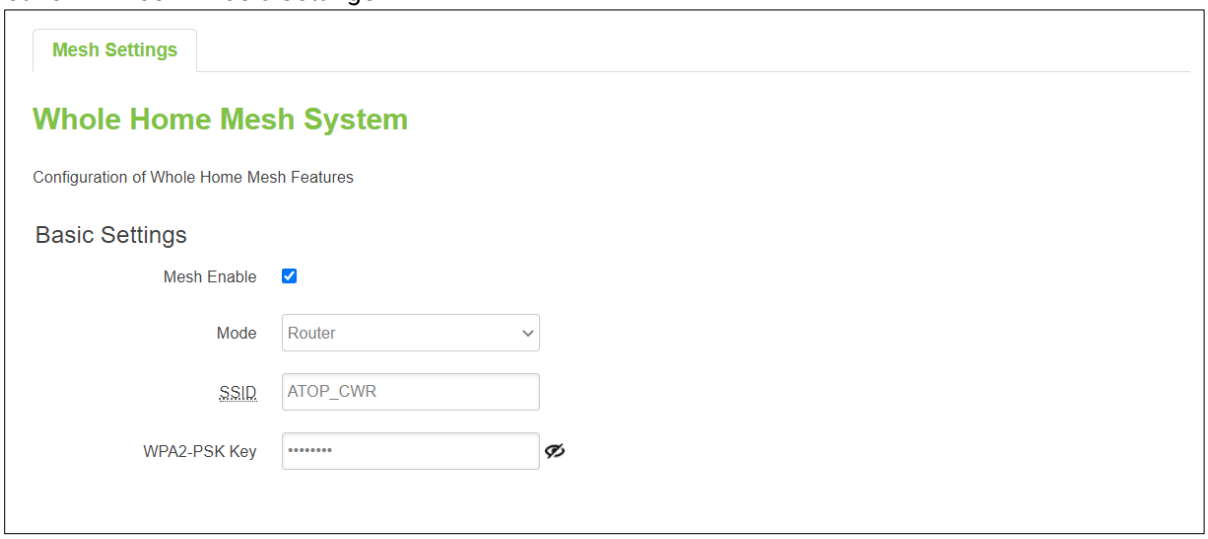


Table 43. Network > Mesh > Basic Settings

Field	Value	Description
Mesh Enable	Disable/Enable; default: **disable**	To enable/disable 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 **IPv6** webpage, you can management the IPv6 IP settings.

Figure 60. Network > IPv6

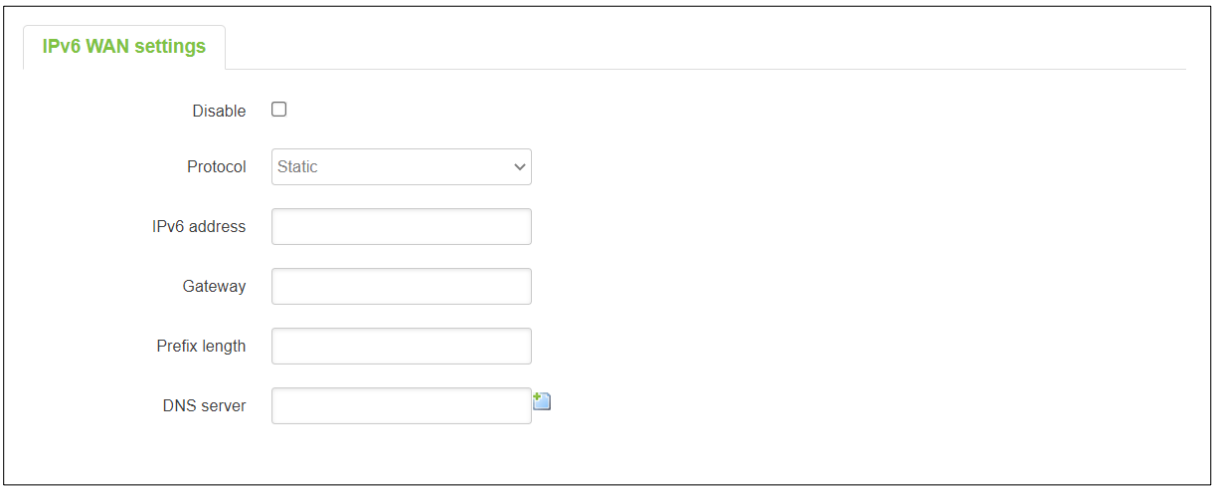


Table 44. Network > IPv6

Field	Value	Description
Disable	Disable/Enable; default: **Enable**	Check Disable box to disable IPv6.
Protocol	DHCPv6/Static; default: DHCPv6	The protocol 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 host name 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 61. Network > VLAN > Interface Based

Table 45. Network > VLAN > Interface Based

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

3.3.7.2 Port Based

The **Port Based** VLAN section allows you to create Port based and Tag based VLAN networks.

Figure 62. Network > VLAN > Port Based

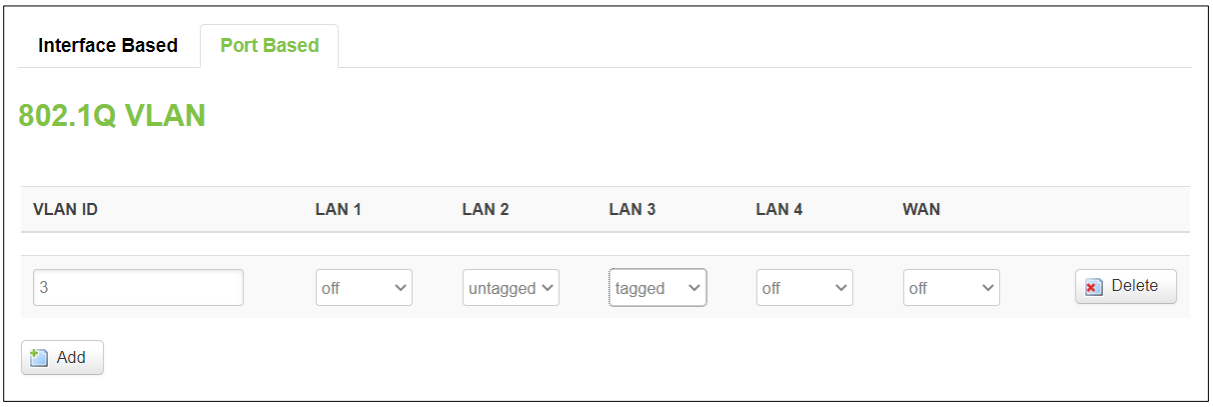


Table 46. Network > VLAN > Port Based

Field	Values	Description
VLAN ID	[1 to 4094]; default: **none**	VLAN Identification number.
LAN/WAN ports	Off | Untagged | Tagged; default: **untagged**	Select which Ethernet ports and how you want to use them with your VLAN. • **Tagged** - used for **tag-based** VLAN. • **Untagged** - used for **port-based** VLAN. • **Off** - disables the port.

3.3.8 LB (Load Balancing) and Failover

Load balancing (LB) lets yous create rules that divide 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 connection.

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 configuread Multi-WAN interfaces.

Figure 63. Network > LB and Failover > Overview

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 (Systemlog) section shows recent Multi-WAN interface log messages.

In Detailed Status sub-tab, the Multi-WAN interfaces status, configured policies, actived 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 64. Network > LB and Failover > Configuration > General

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 your network configuration.

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

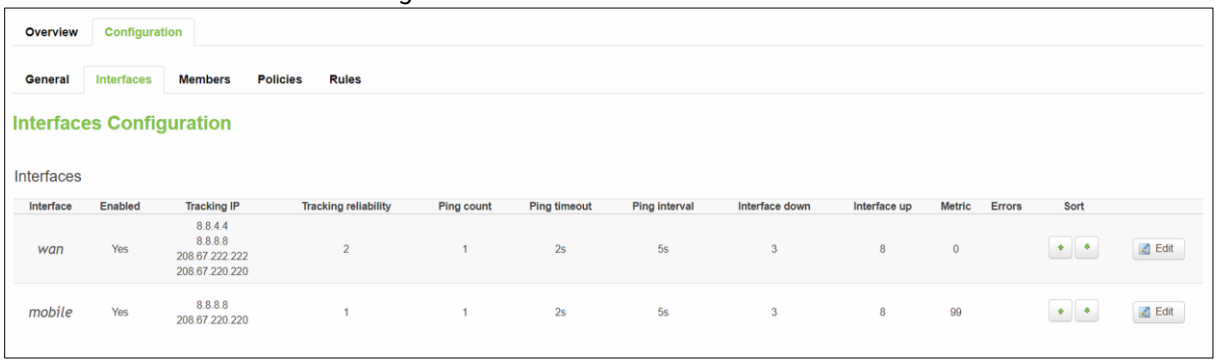


Table 49. Network > LB and Failover > Configuration > Interfaces

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 interface is still alive. If this value is missing the interface is always considered up.
Tracking Reliability	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	Number of checks to send to each host with each test.
Ping Timeout	Number of seconds to wait for an echo-reply after an echo-request.
Ping Interval	Number of seconds between each test.
Interface down	Number of failed tests to considered link as dead.
Interface Up	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 66. Network > LB and Failover > Configuration > Interfaces > Edit

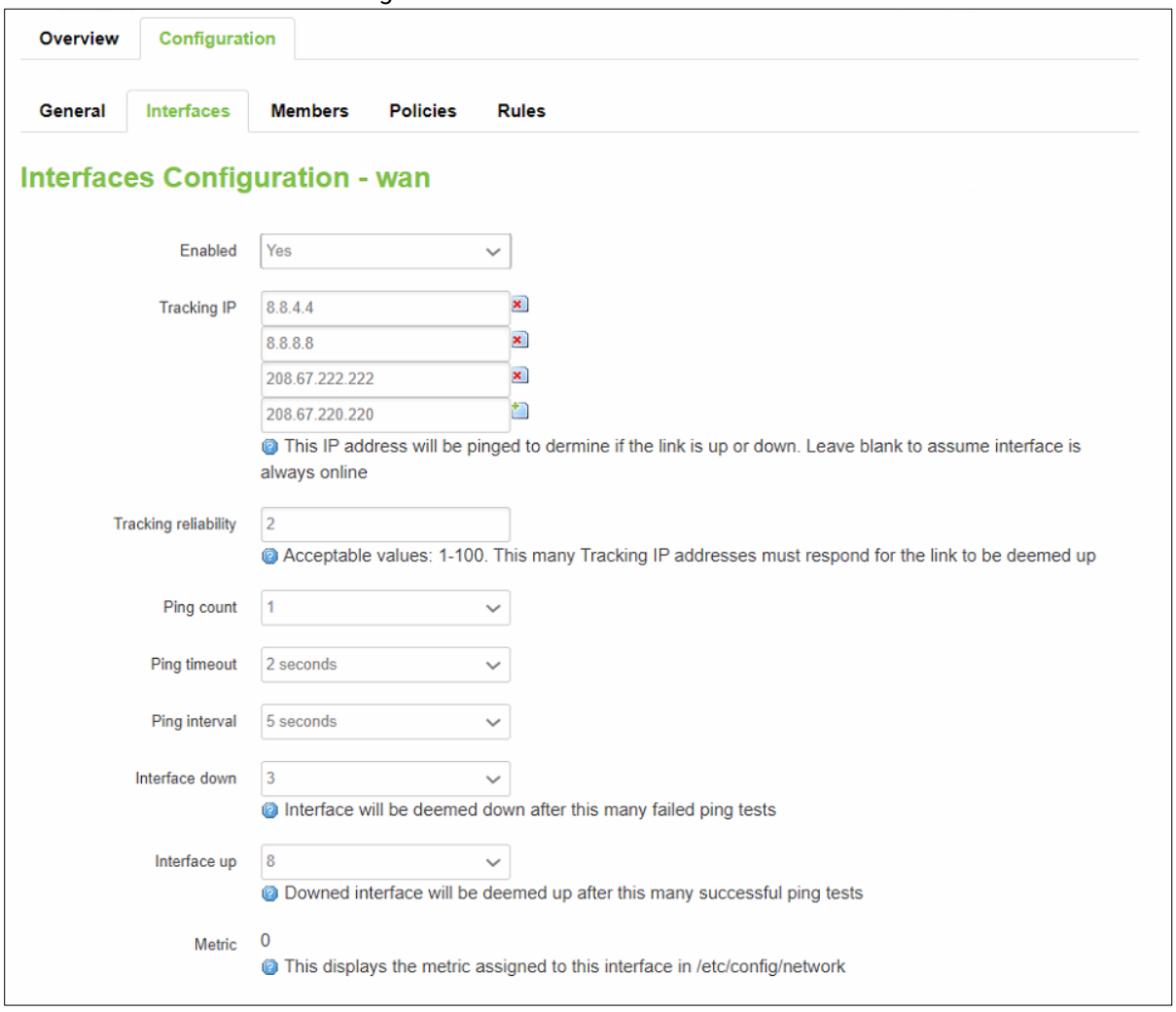


Table 50. Network > LB and Failover > Configuration > Interfaces > Edit

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 interface is still alive. If this value is missing the interface is always considered up.
Tracking Reliability	integer [1 – 100]; default: **1**	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**	Number of checks to send to each host with each test.
Ping Timeout	intger [1 – 10]; default: **1**	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**	Number of seconds between each test.
Interface down	integer [1 – 10]; default: **3**	Number of failed tests to considered link as dead.
Interface Up	integer [1 – 10]; default: **8**	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 cannot be used for rules directly.

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

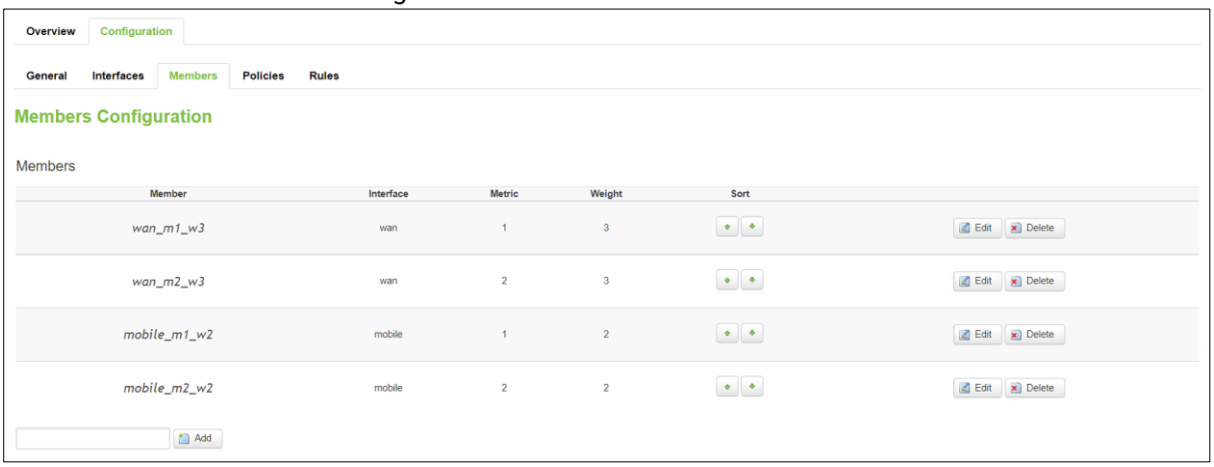


Table 51. Network > LB and Failover > Configuration > Members

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 load based on this weight value.

3.3.8.2.5 Member – Configuration

Figure 68. Network > LB and Failover > Configuration > Members > Edit

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. Larger number means higher priority. Used as a sorting measure. If a packet routed with two rules, the higher metric will be chosen first.
Weight	integer [1 – 1000]; default: 4	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 thorugh that member. If a policy has more than one member, it wills either load-balance among members or use 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 same metric) will distribute load based on assigned weights values.

Figure 69. Network > LB and Failover > Configuration > Policies

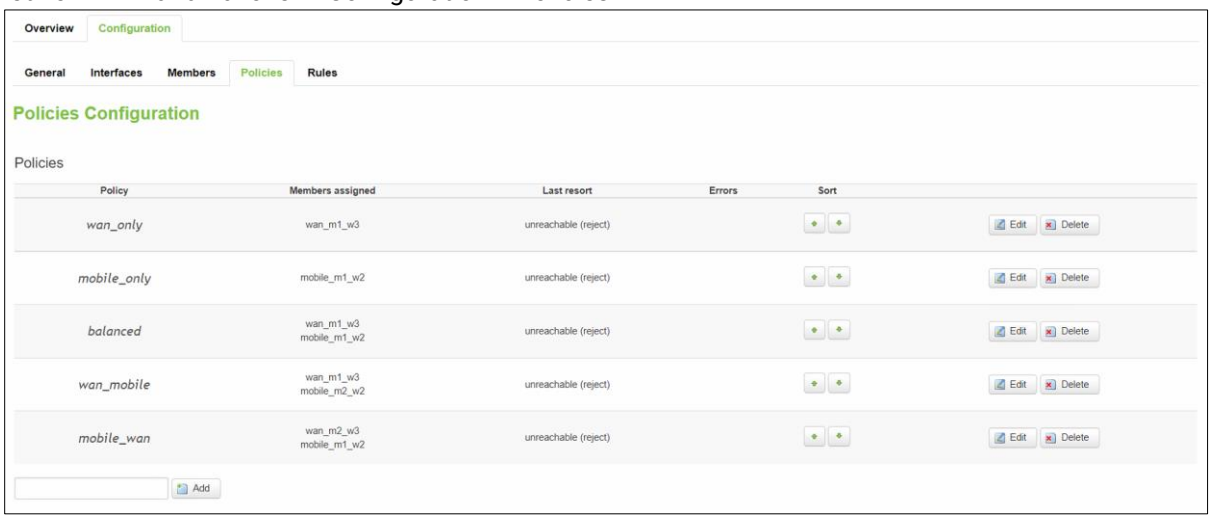


Table 53. Network > LB and Failover > Configuration > Policies

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

3.3.8.2.7 Policies – Configuration

Figure 70. Network > LB and Failover > Configuration > Policies > Edit/Add

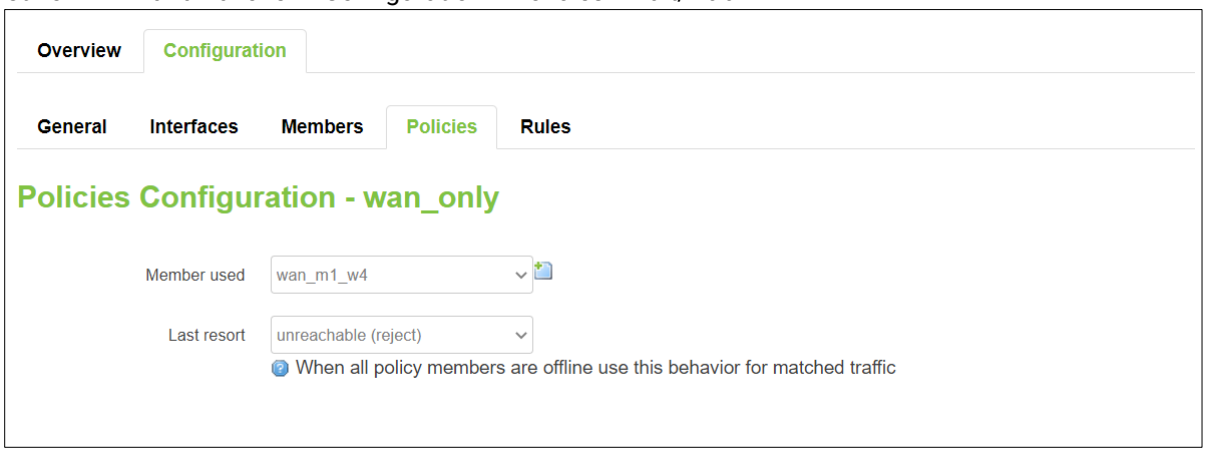


Table 54. Network > LB and Failover > Configuration > Policies > Edit/Add

Field	Description
Member used	The member assigned to this policy.
Last resort	Determine the fallback routing behaviour 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 71. Network > LB and Failover > Configuration > Rules

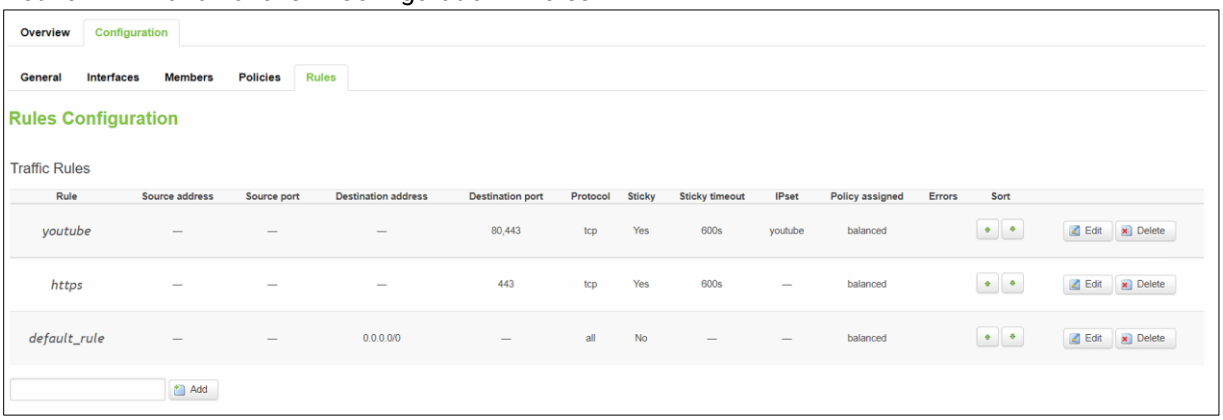


Table 55. Network > LB and Failover > Configuration > Rules

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 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 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 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 same WAN interface as prior session.
Sticky Timeout	Stickiness timeout value in seconds.

3.3.8.2.9 Rules – Configuration

Figure 72. Network > LB and Failover > Configuration > Rules > Edit/Add

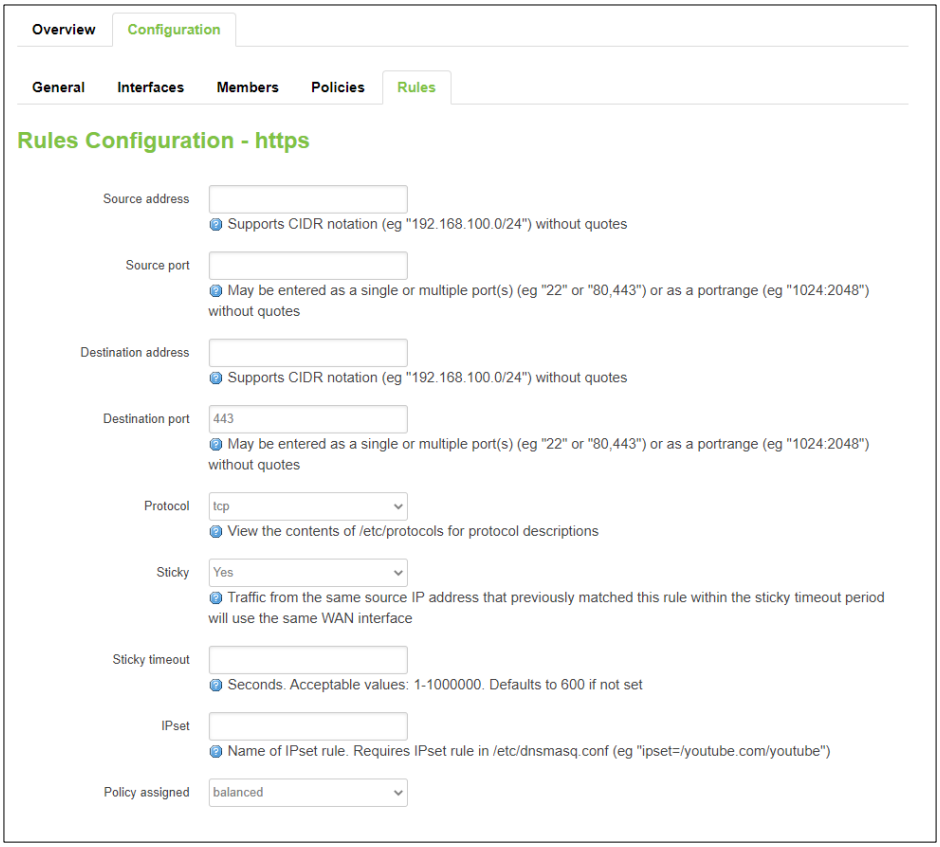


Table 56. Network > LB and Failover > Configuration > Rules > Edit/Add

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 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 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 same WAN interface as 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 set.
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 as below:

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

Figure 73. Network > Firewall > General Settings

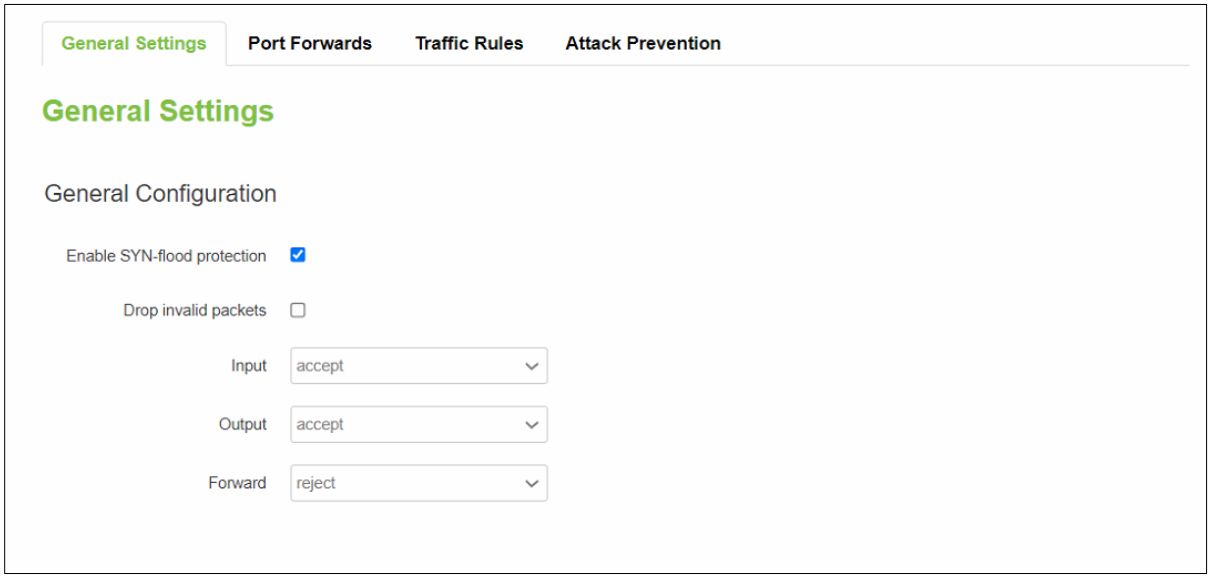


Table 57. Network > Firewall > General Settings

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 74. Network > Firewall > General Settings > Zone Configuration

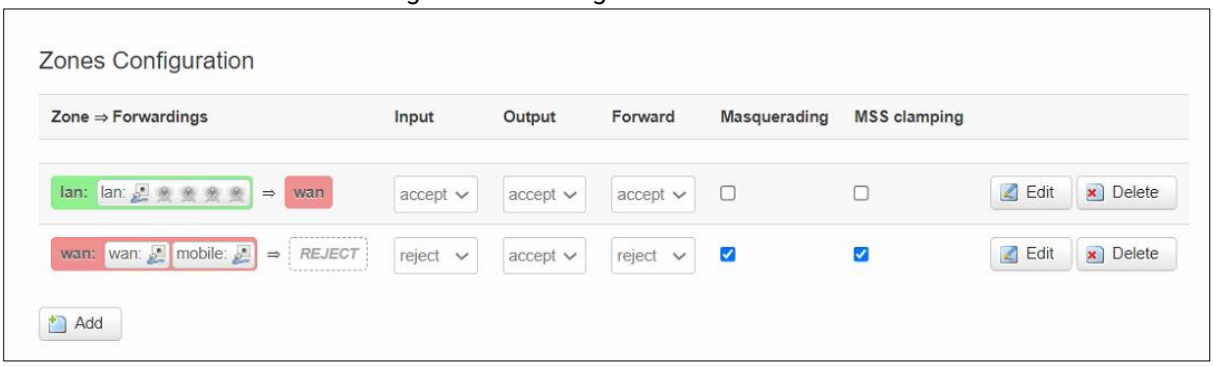


Table 58. Network > Firewall > General Settings > Zone Configuration

Field	Description
Zone➔Forwardings	The zone forwarding contains the source zone from which data packets will redirected from, and the destination zone to which data packets will be redirected to.
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 75. Network > Firewall > General Settings > Zone Configuration > Zone "Lan"

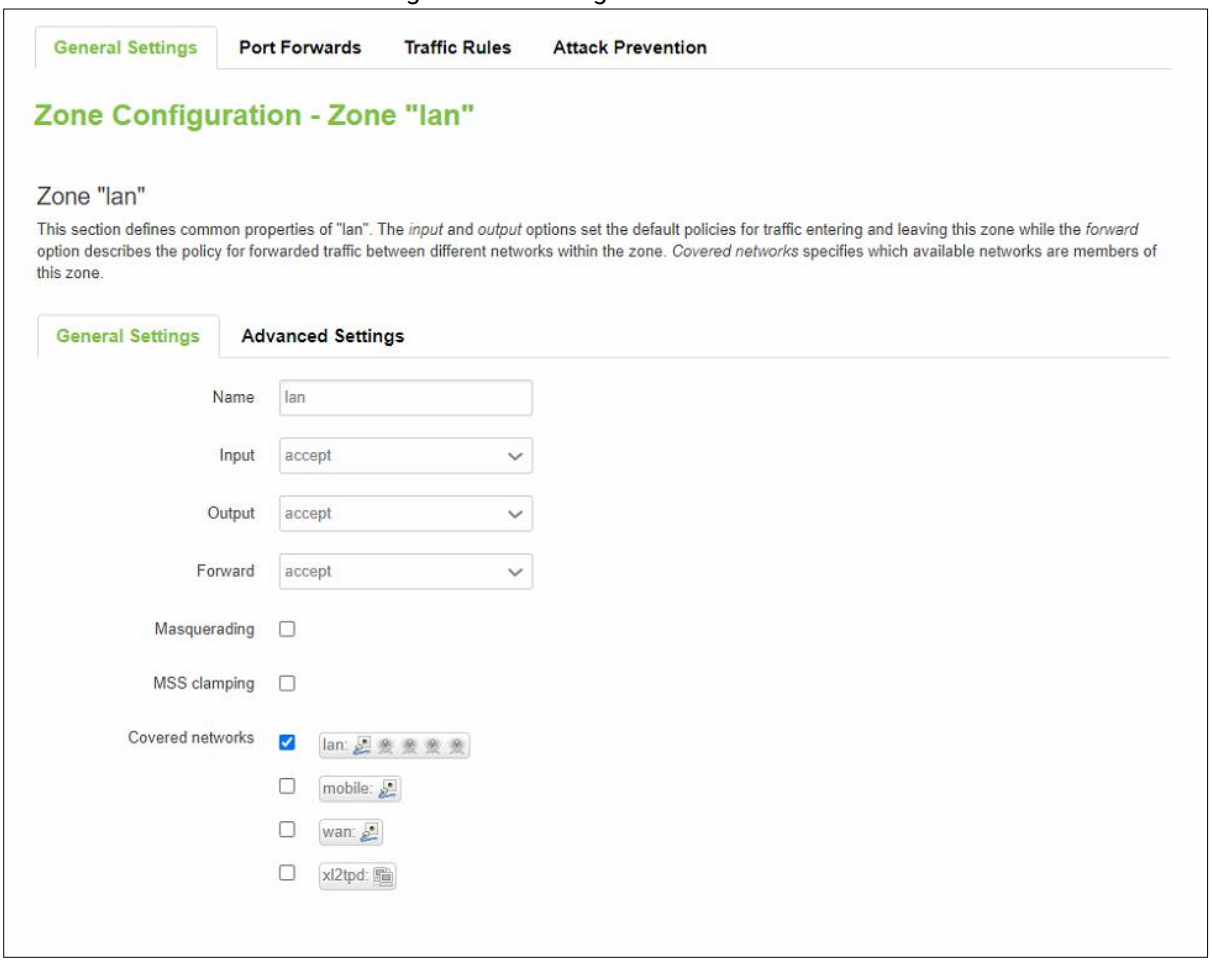
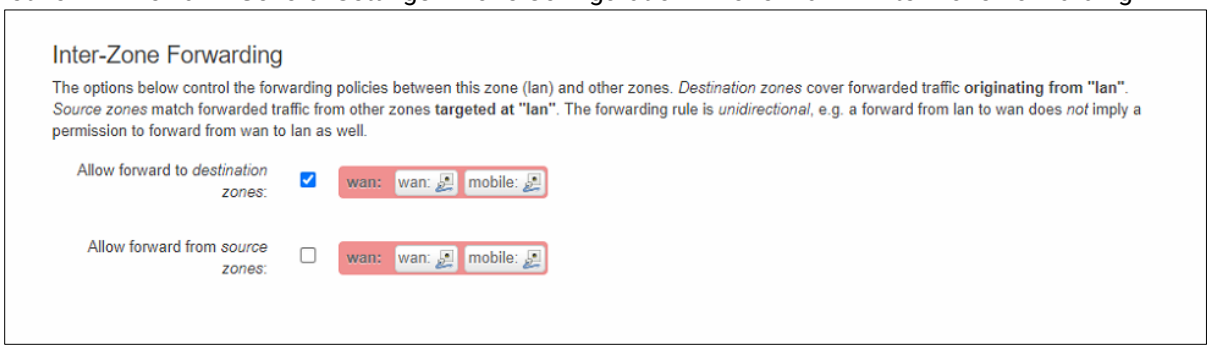


Table 59. Network > Firewall > General Settings > Zone Configuration > Zone "Lan"

Field	Description
Zone➔Forwardings	The zone forwarding contains the source zone from which data packets will redirected from, and the destination zone to which data packets will be redirected to.
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 76. Network > Firewall > General Settings > Zone Configuration > Zone “Lan” > Inter-Zone Forwarding



3.3.9.1.4 Zone Configuration-WAN

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

Figure 77. Network > Firewall > General Settings > Zone “wan”

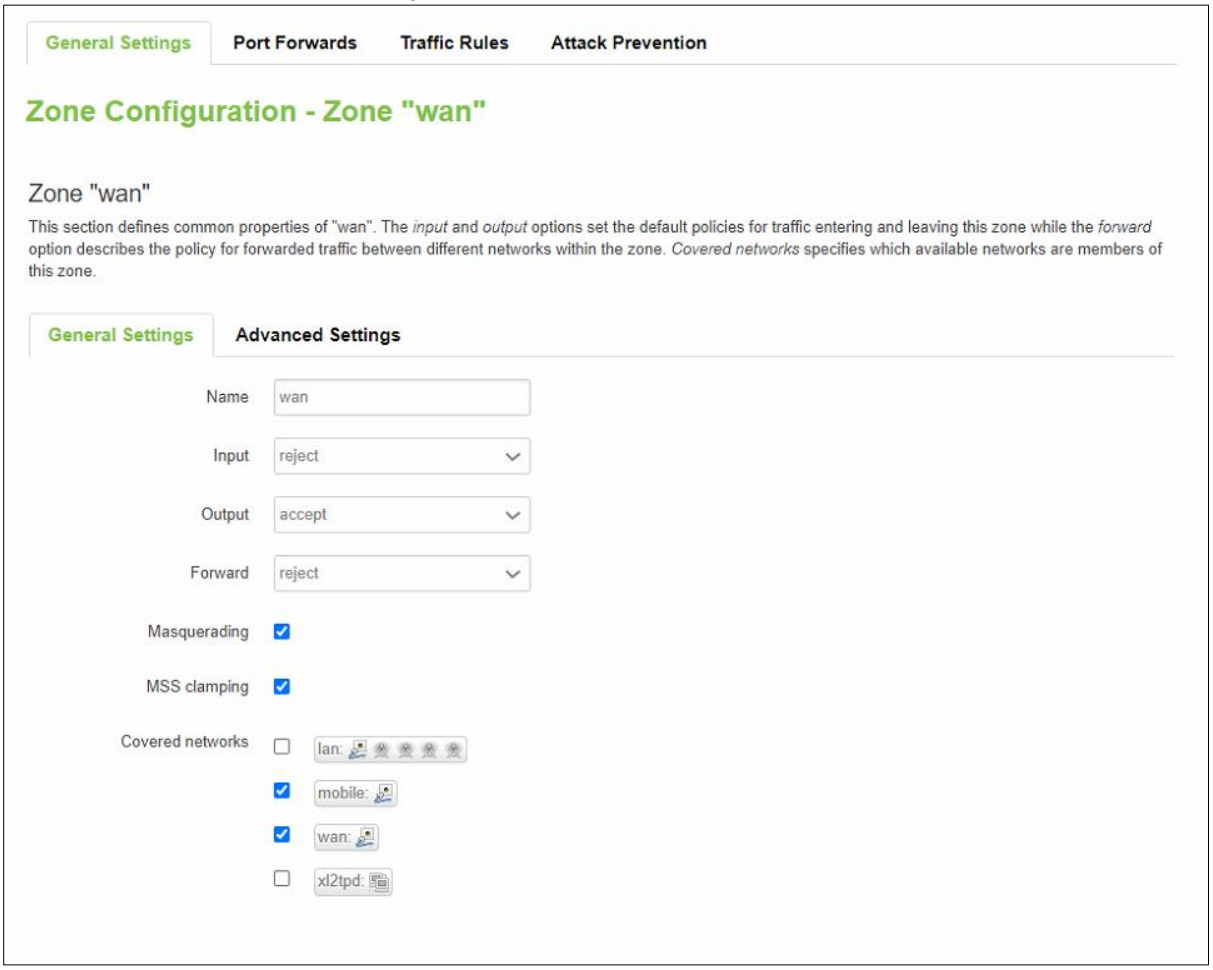
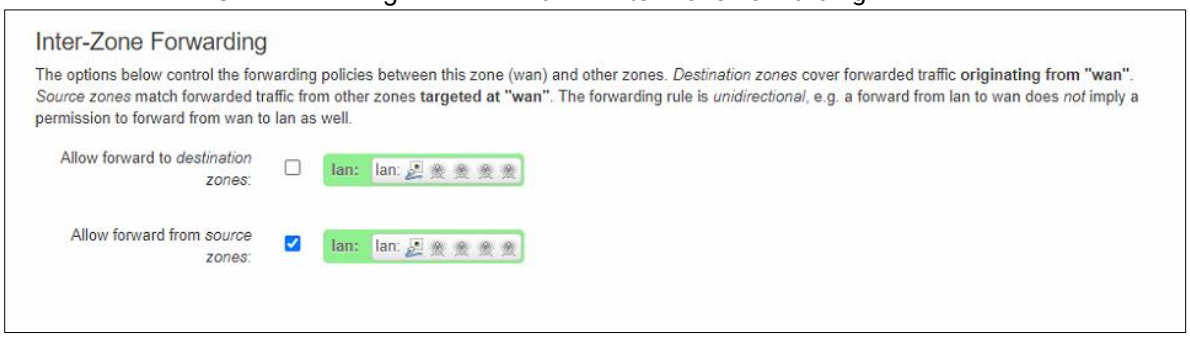


Table 60. Network > Firewall > General Settings > Zone “wan” > Inter-Zone Forwarding



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 the combination of both.

Figure 78. Network > Firewall > Port Forwards > Port Forwards Rules

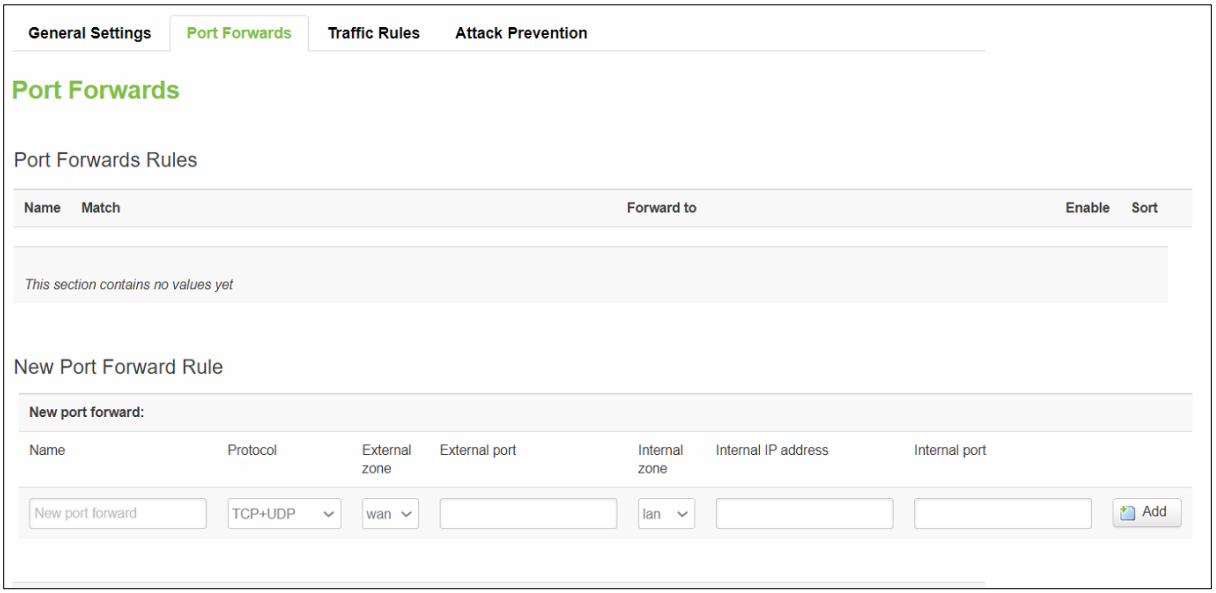


Table 61. Network > Firewall > Port Forwards > Port Forwards Rules

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 the conditions.

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

Field	Description
Name	Name of the port forward rule, used only for easier management purposes.
Protocol	Type of protocol of incoming packet.
External Zone	The WAN network that data traffic will be redirected from.
External Port	Traffic will be forwarded from this port on the WAN network.
Internal Zone	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	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 79. Network > Firewall > Traffic Rules > Traffic Rules

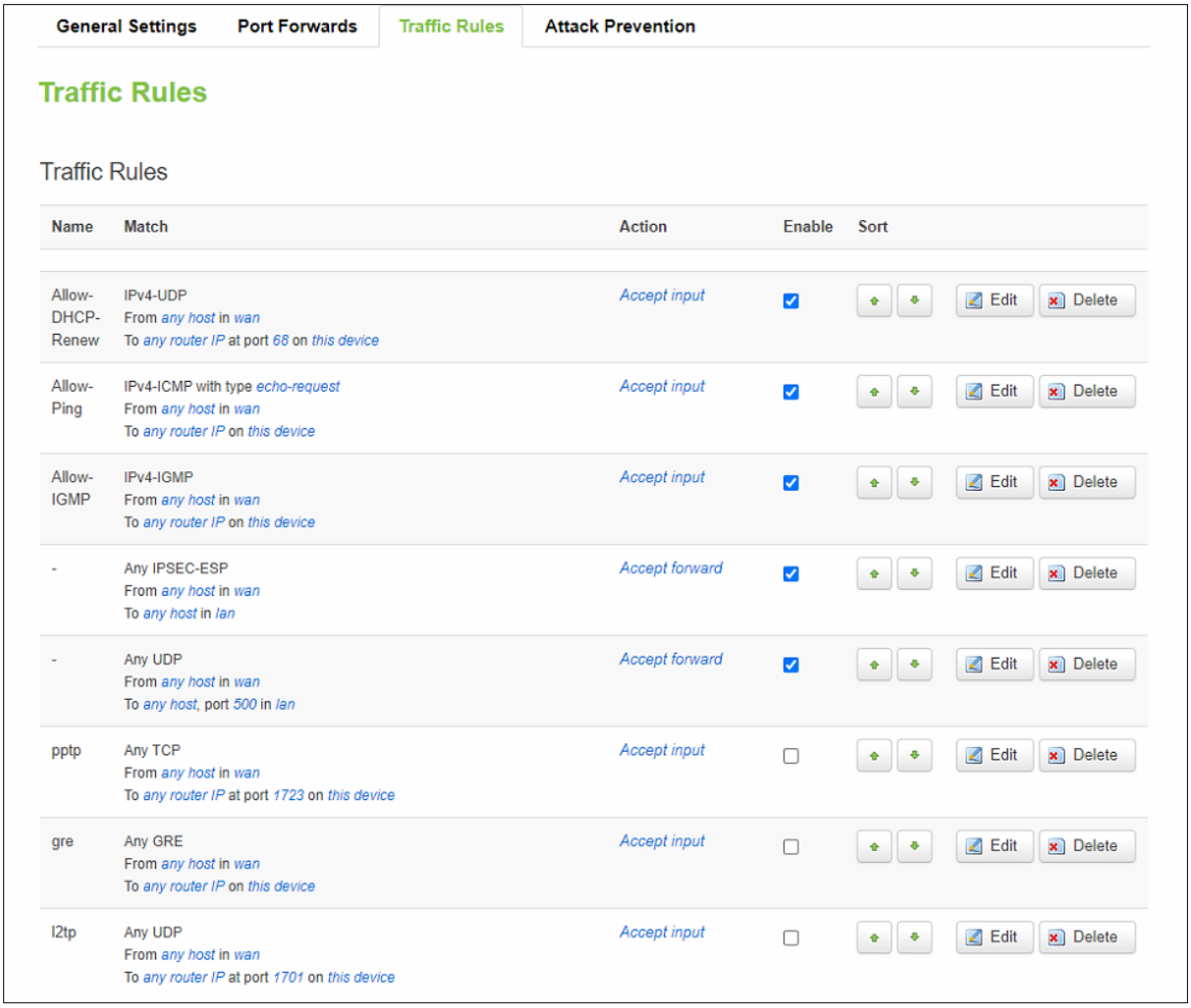


Table 63. Network > Firewall > Traffic Rules > Traffic Rules

Field	Description
Name	Name of the traffic rule, used only for easier 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 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 80. Network > Firewall > Traffic Rules > Open ports on router

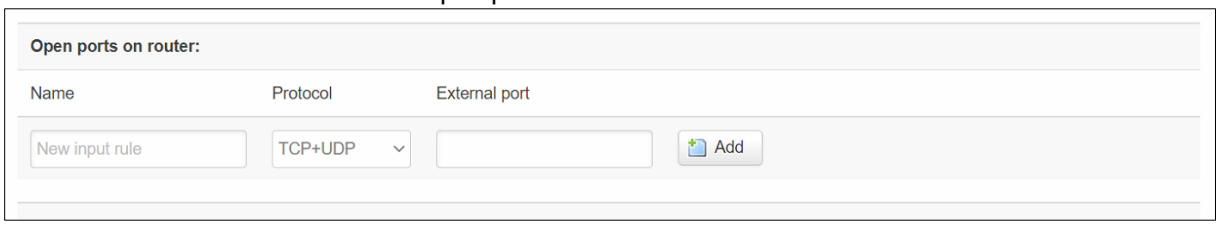


Table 64. Network > Firewall > Traffic Rules > Open ports on router

Field	Description
Name	Name of the traffic rule, used only for simplified 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 router rule.

3.3.9.3.2 New Forward Rule

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

Figure 81. Network > Firewall > Traffic Rules > New forward rule

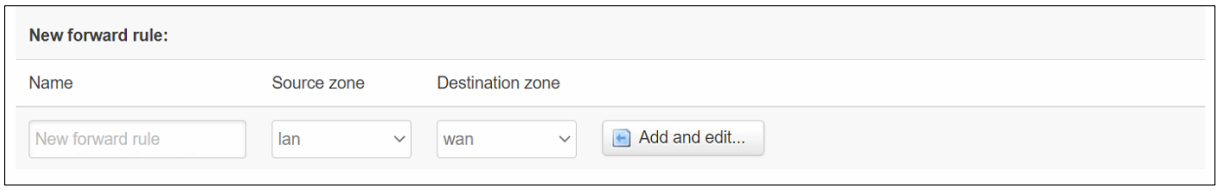


Table 65. Network > Firewall > Traffic Rules > New forward rule

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 82. Network > Firewall > Traffic Rules > Source NAT

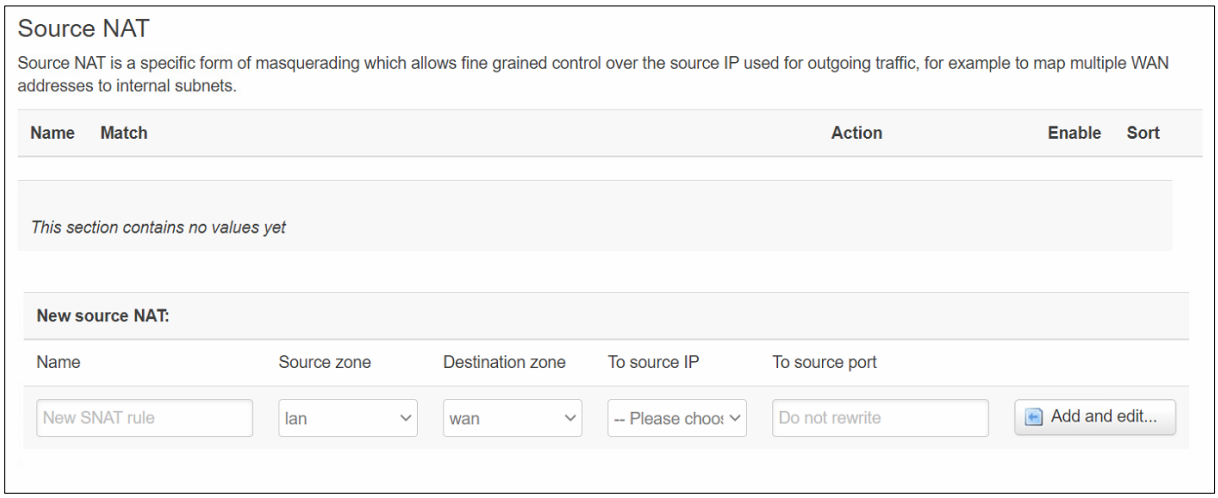


Table 66. Network > Firewall > Traffic Rules > Source NAT

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 83. Network > Firewall > Attack Prevention > SYN Flood Protection

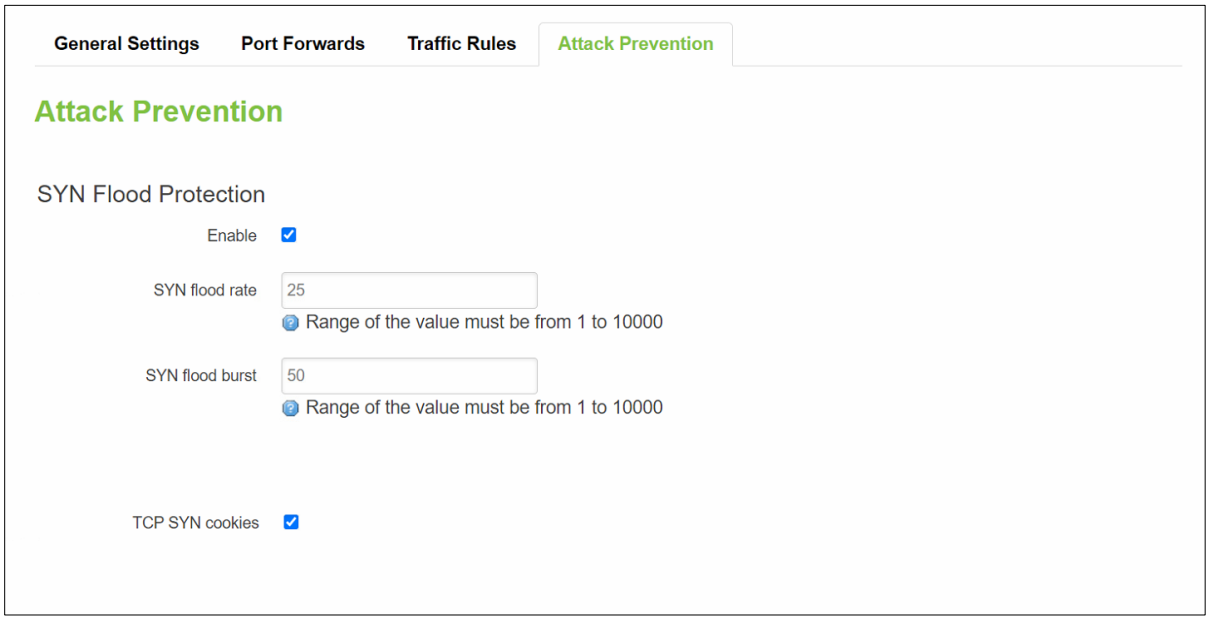


Table 67. Network > Firewall > Attack Prevention > SYN Flood Protection

Field	Value	Description
Enable	default: **enable**	Makes 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 flooded.
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 84. Network > Firewall > Attack Prevention > SSH Attack Protection

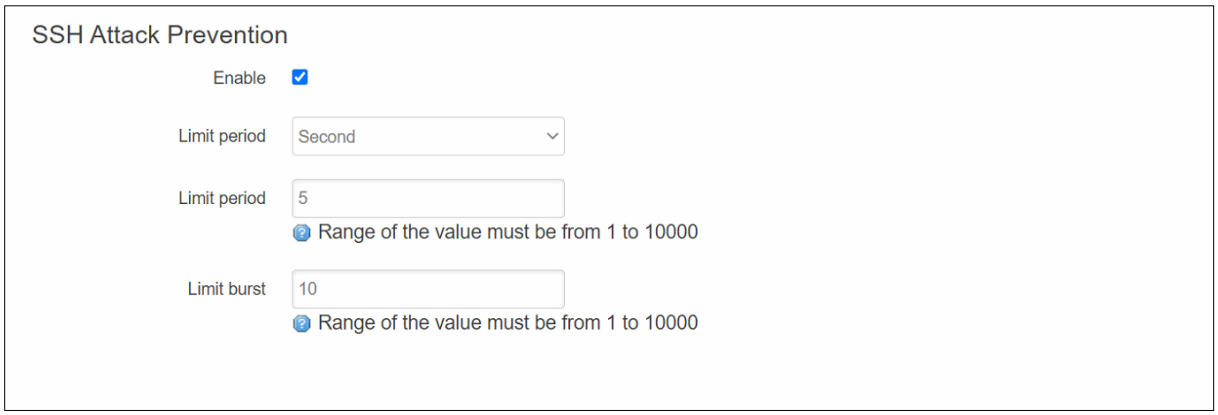


Table 68. Network > Firewall > Attack Prevention > SSH Attack Protection

Field	Value	Description
Enable	default: **enable**	Enable SSH connections limit in selected period.
Limit period	Second/Minitute/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 85. Network > Firewall > Attack Prevention > Http/Https Attack Protection

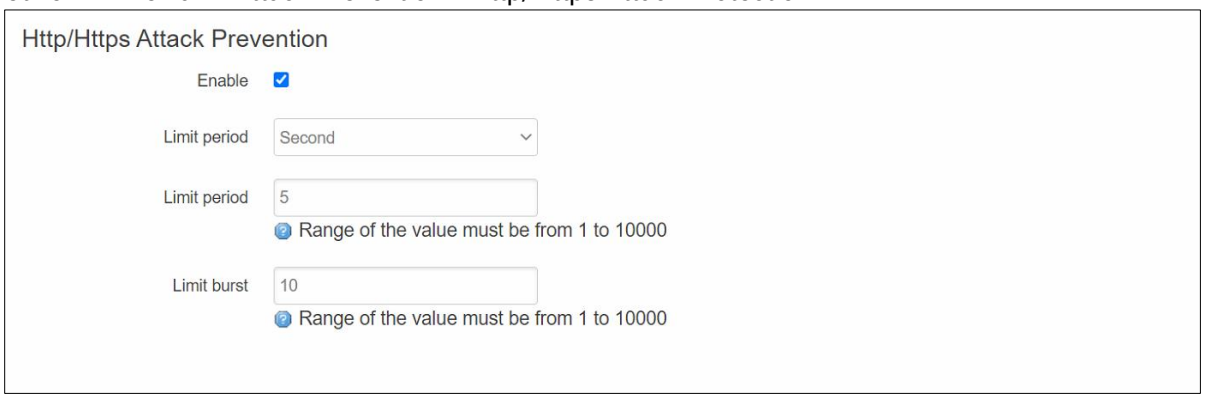


Table 69. Network > Firewall > Attack Prevention > Http/Https Attack Protection

Field	Value	Description
Enable	default: **enable**	Enable HTTP connections limit in selected period.
Limit period	Second/Minitute/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 is able to 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 86. Network > Firewall > Attack Prevention > Port Scan

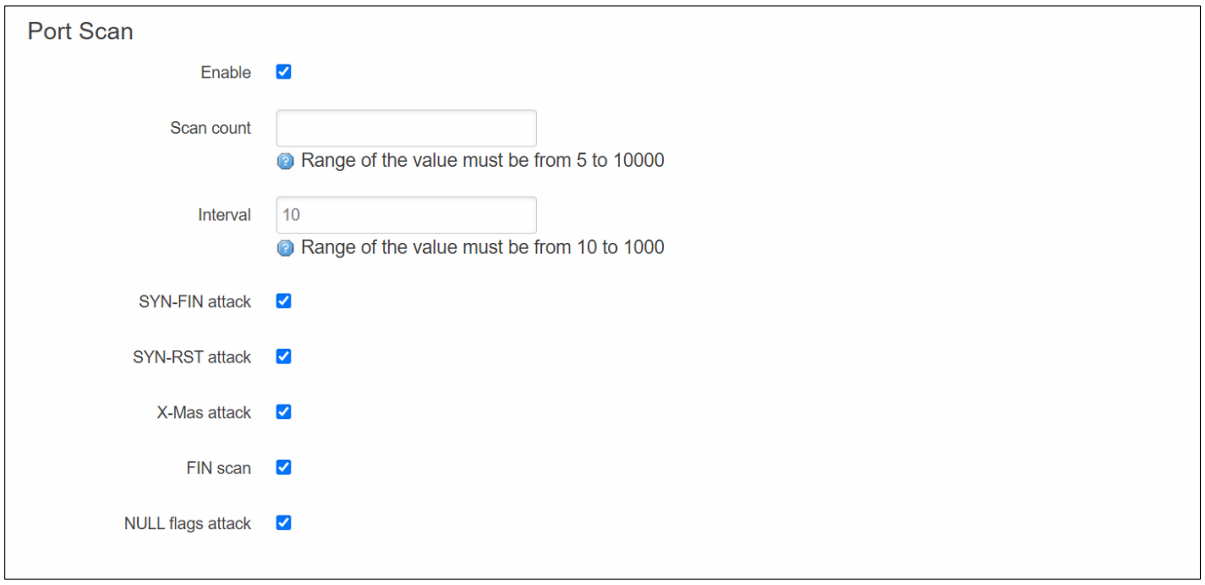


Table 70. Network > Firewall > Attack Prevention > Port Scan

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 87. Network > Static Routes

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 88. Network > DNS

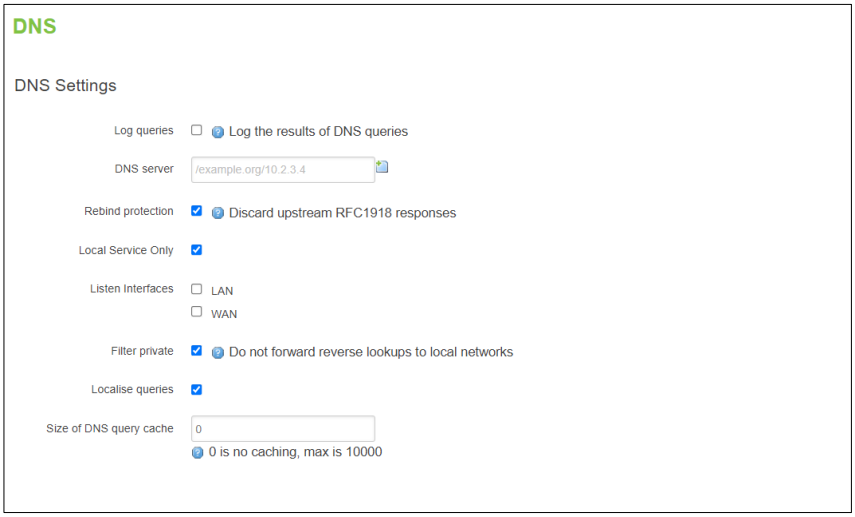


Table 72. Network > DNS

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 89. Network > QoS

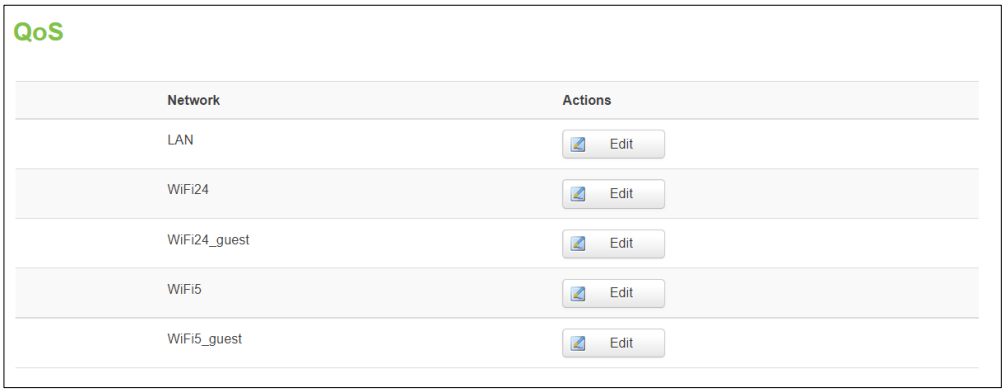


Figure 90. Network > QoS > QoS-LAN Settings

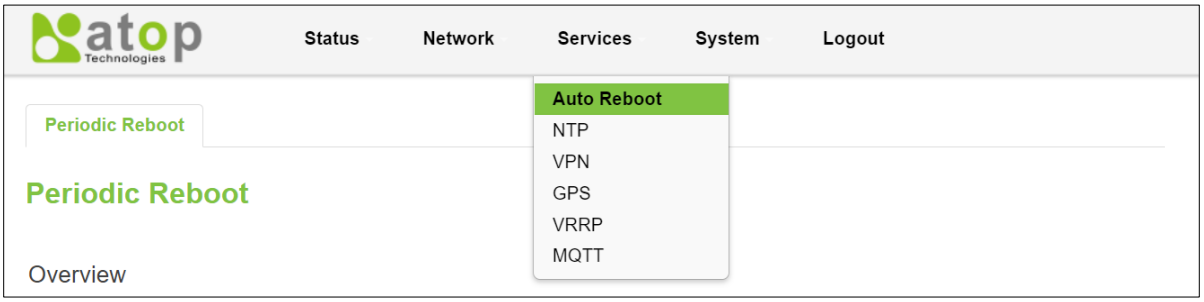
Table 73. Network > QoS > QoS-LAN Settings

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 91. Service



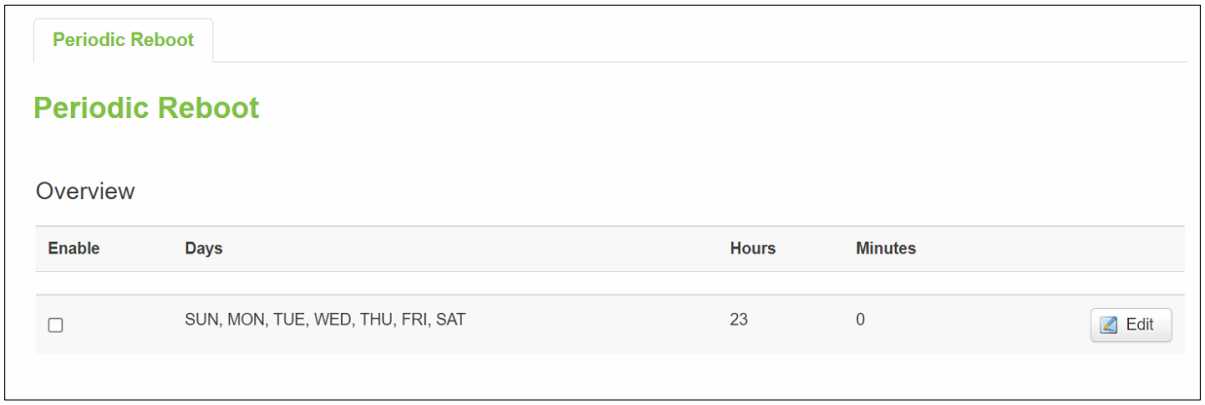
3.4.1 Auto Reboot

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 92. Service > Auto Reboot



3.4.1.2 Configuration – Periodic Reboot

Figure 93. Service > Auto Reboot > Edit

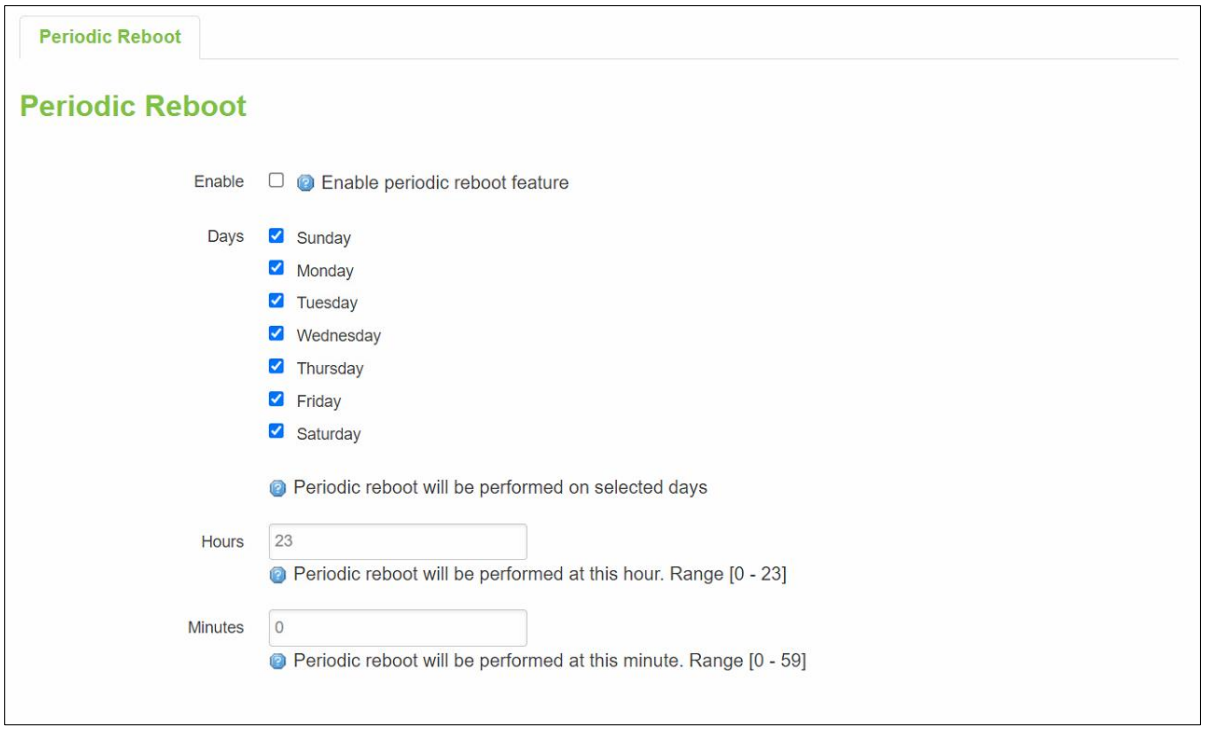


Table 74. Service > Auto Reboot > Edit

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 94. Services > NTP > General

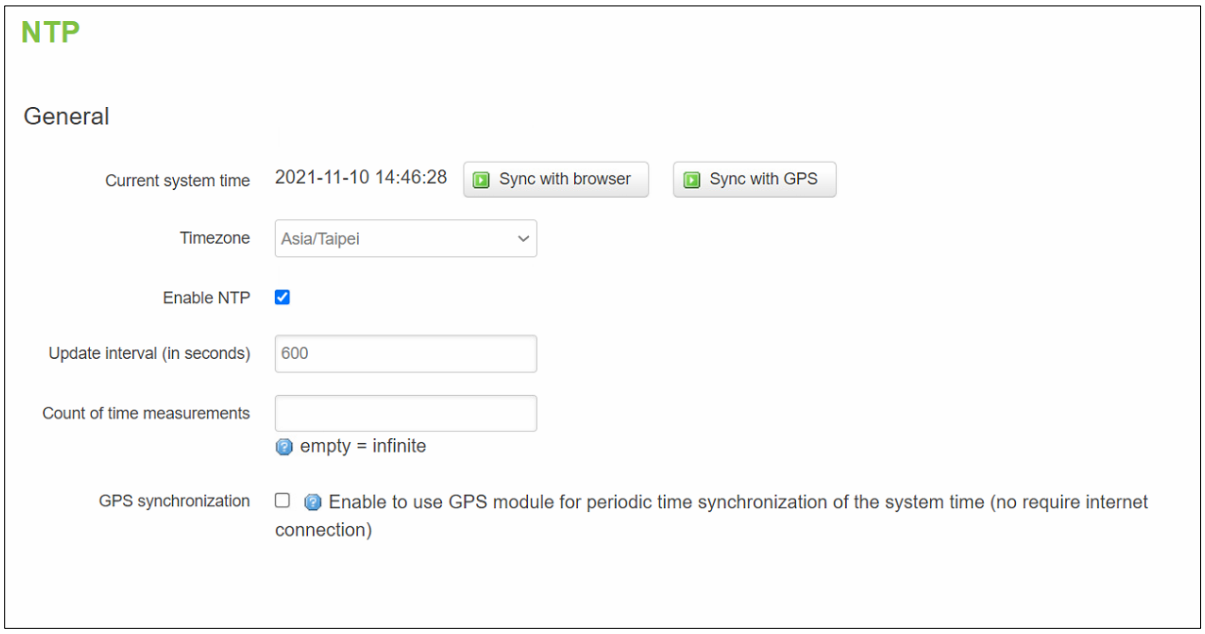


Table 75. Services > NTP > General

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 95. Services > NTP > Time Servers

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 and compatibility with most OS platforms.

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 96. Services > VPN > OpenVPN > Overview

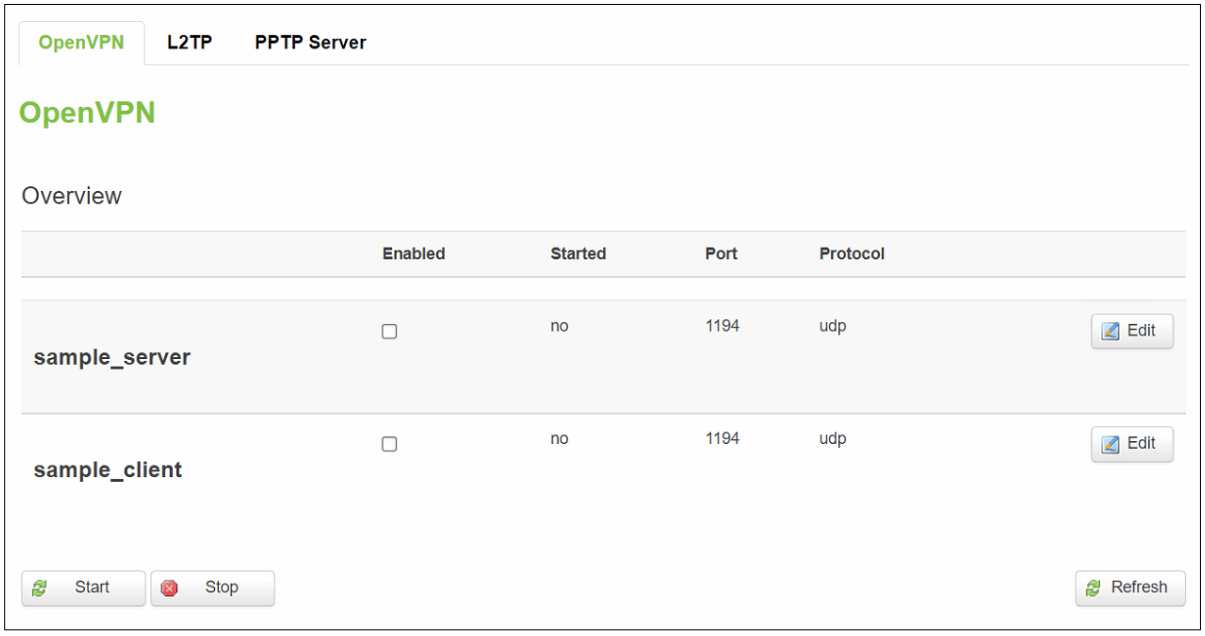


Table 77. Services > VPN > OpenVPN > Overview

Field	Description
Enabled	To enable/disable selected OpenVPN service instance.
Started	Display current OpenVPN service is started or not.
Start/Stop	To start/stop selected OpenVPN service.
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.

3.4.3.1.2 Configuration – OpenVPN

If you presses "**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 97. Services > VPN > OpenVPN > Edit

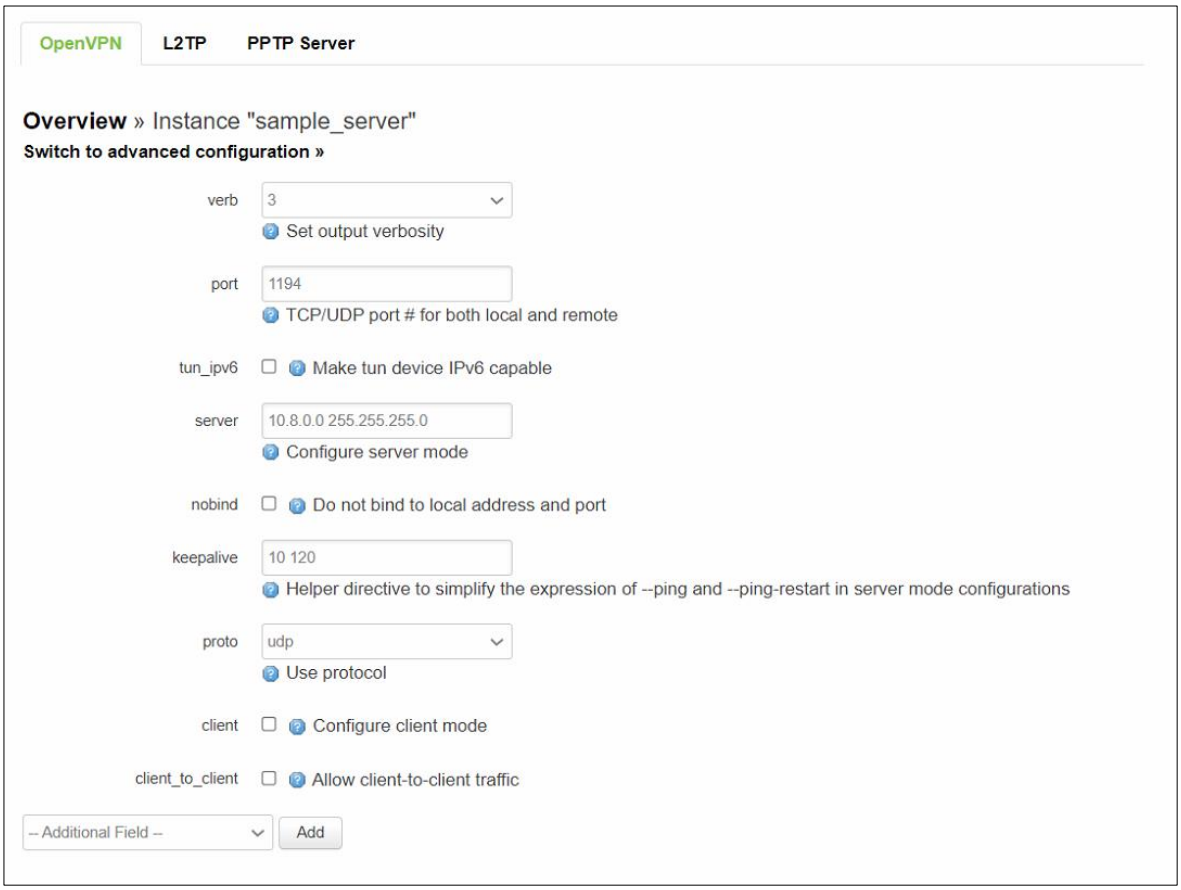


Table 78. Services > VPN > OpenVPN > Edit

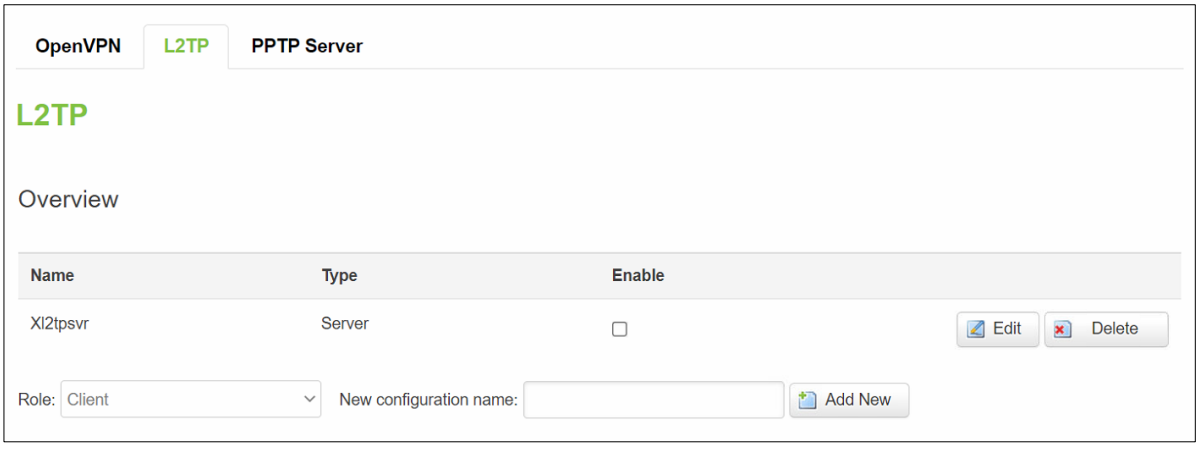
Field	Value	Description
Verb	0-11 default: **3**	Set output verbosity.
Port	integer [1-65535] default: **1194**	TCP/UDP port the local OpenVPN server listening on.
Tun_ipv6	disable/enable; default: **disable**	Make tunnel device IPv6 capable.
Server	IP/mask default: **10.8.0.0/255.255.255.0**	Configure OpenVPN server mode.
Nobind	disable/enable; default: **disable**	Do not bind to local IP address and port.
Keepalive	default:**10/120**	Helper directive to simplify the expression of ping and ping-restart in OpenVPN server mode configurations.
Proto	TCP/UDP; default: **udp**	To use TCP or UDP protocol on OpenVPN server.
Client	disable/enable; default: **disable**	Uncheck as server mode, check as client mode.
Client_to_client	disable/enable; default: **disable**	Allow client-to-client traffic.
Add	default: **none**	Add an extra field which is selected from Additional Field: nice/dev_type/ifconfig/server_bridge/comp_lzo/remote/secret/pkcs12/ca/dh/cert/key .

3.4.3.2 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.

3.4.3.2.1 L2TP Overview

Figure 98. Services > VPN > L2TP > Overview

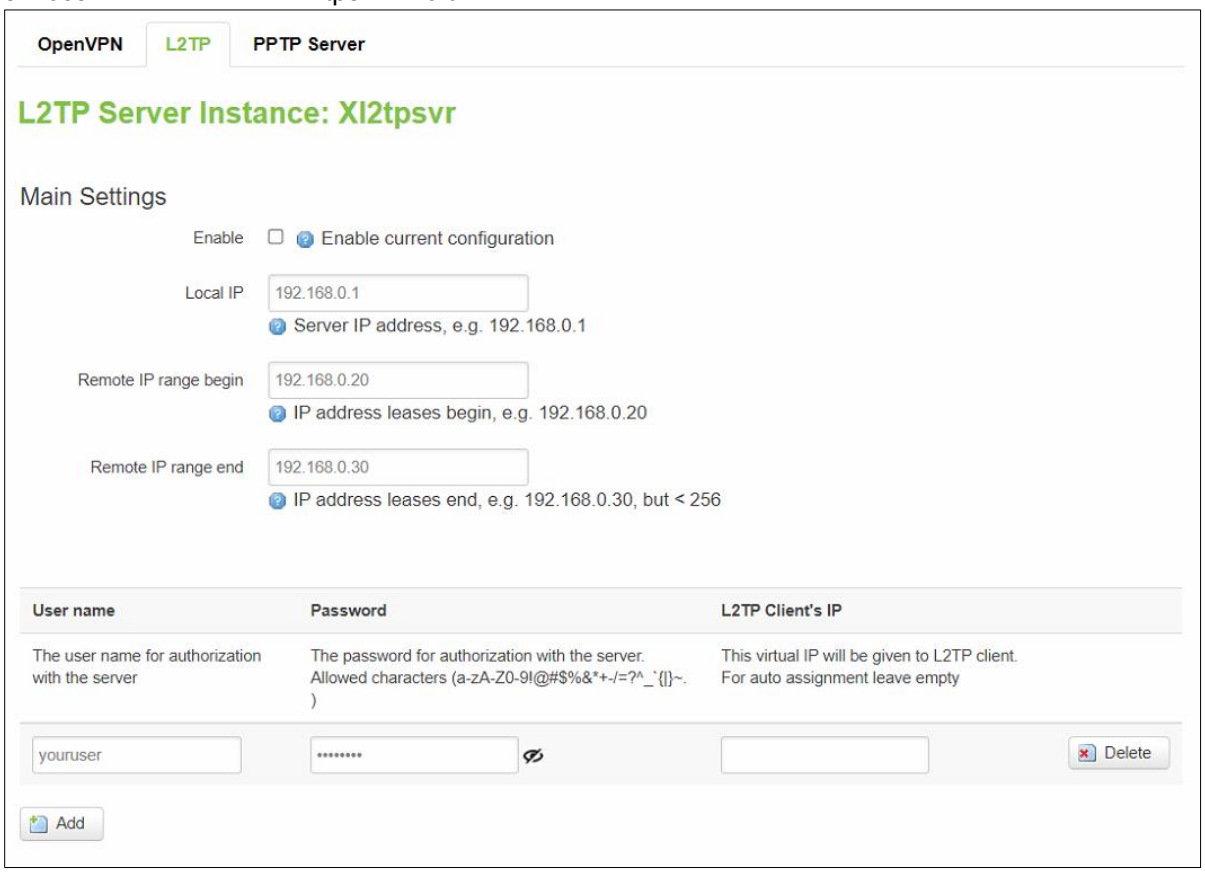


3.4.3.2.2 L2TP Server

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 99. Services > VPN > L2TP > Xl2tpsvr > Edit



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

Table 79. Services > VPN > L2TP > Xl2tpsvr > Edit

Field	Description
Enable	Check the box to enable the L2TP Tunnel function.
Local IP	IP Address of this device (RUT).
Remote IP range begin	IP address leases beginning.
Remote IP range end	IP address leases end.
Username	Username to connect to L2TP (this) server.
Password	Password to connect to L2TP server.
L2TP Client's IP	This virtual IP will be given to L2TP client. For auto assignment leave empty.

3.4.3.2.3 L2TP Client

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

Figure 100. Services > VPN > L2TP > Overview

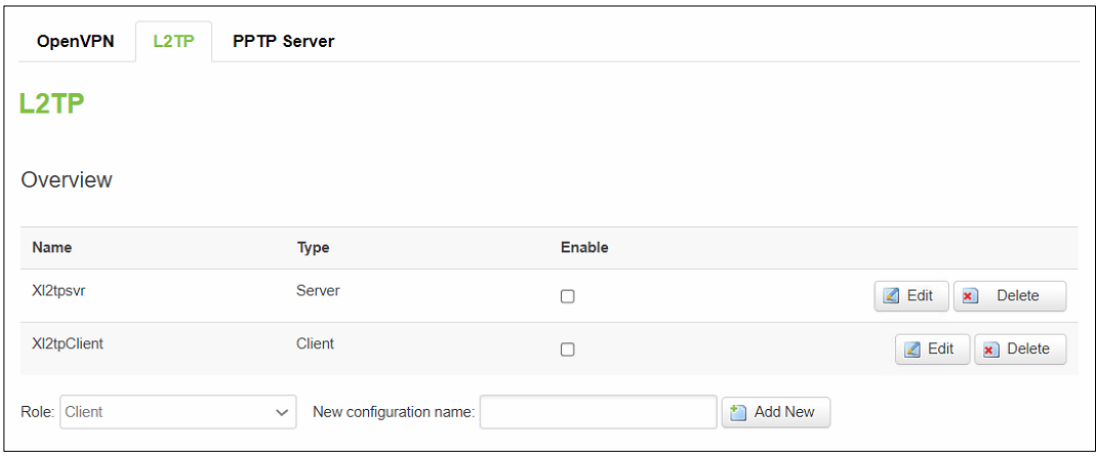


Figure 101. Services > VPN > L2TP > Xl2tpClient > Edit

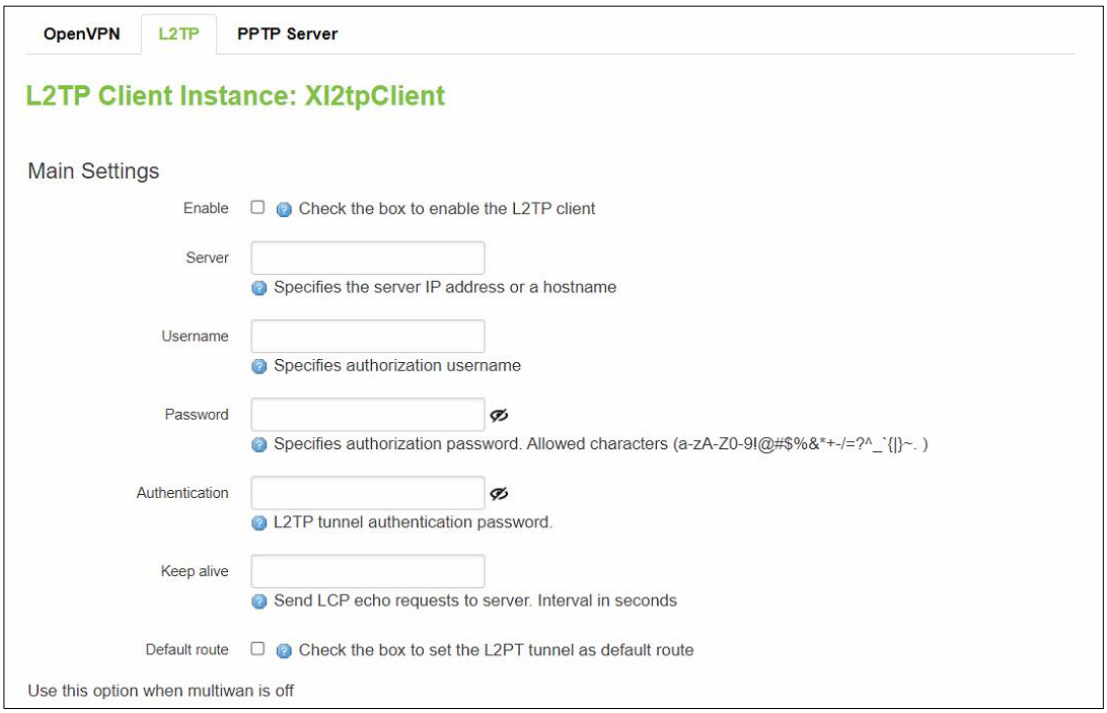


Table 80. Services > VPN > L2TP > Xl2tpClient > Edit

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.

3.4.3.3 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).

3.4.3.3.1 PPTP Server – General Settings

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

Figure 102. Services > VPN > PPTP Server > General Settings

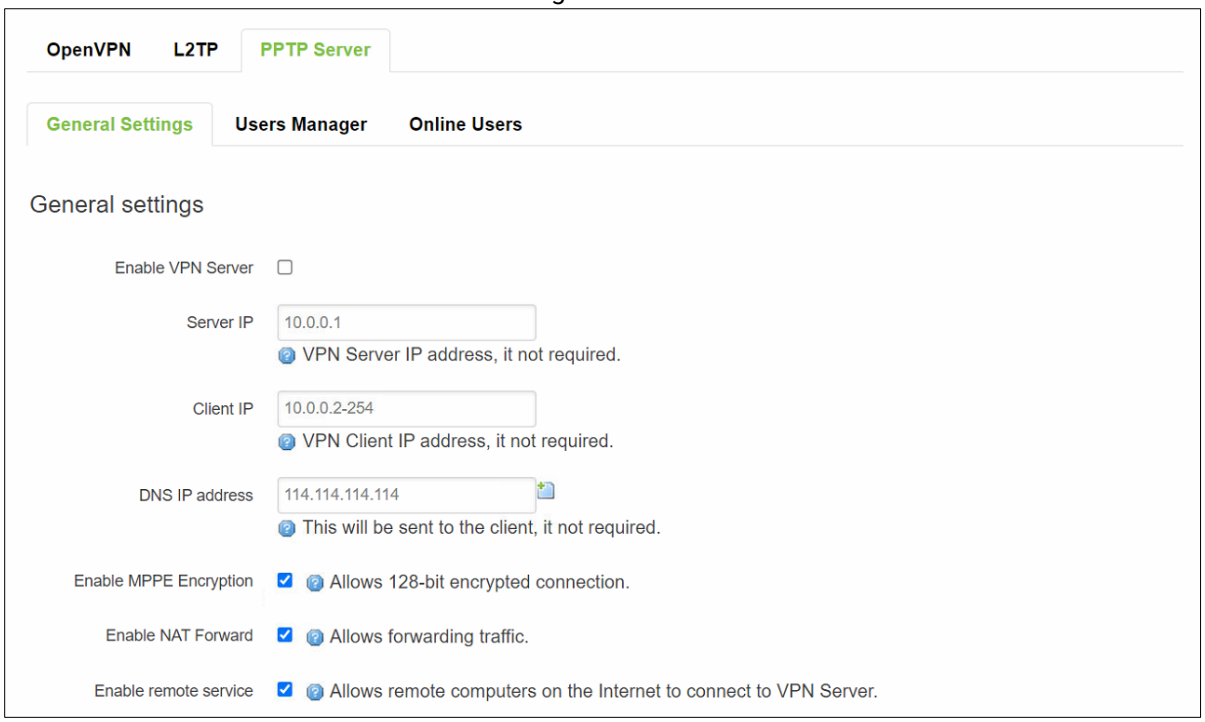


Table 81. Services > VPN > PPTP Server > General Settings

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 CWR 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.

3.4.3.3.2 PPTP Server – Users Manager

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

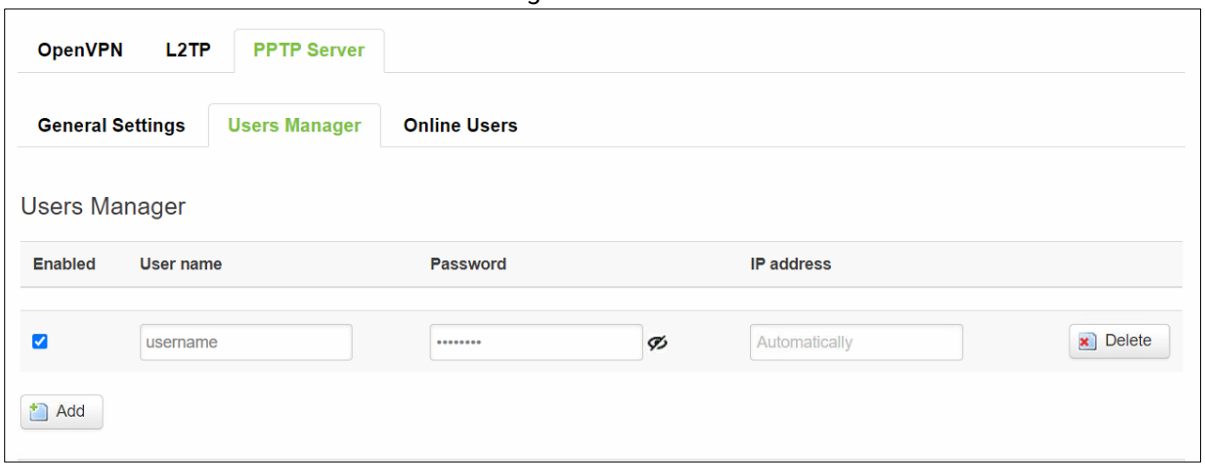


Table 82. Services > VPN > PPTP Server > Users Manager

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: **Allow any**	Accepted PPTP Client source IP.

3.4.3.3.3 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 104. Services > VPN > PPTP Server > Online Users

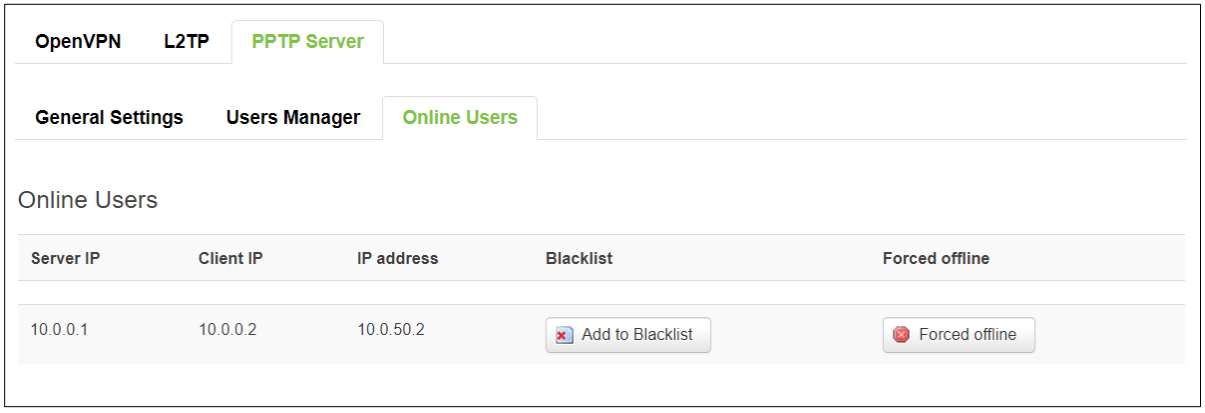


Table 83. Services > VPN > PPTP Server > Online Users

Field	Description
Server IP	The PPTP IP of CWR.
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.

3.4.4 GPS

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

Figure 105. Services > GPS

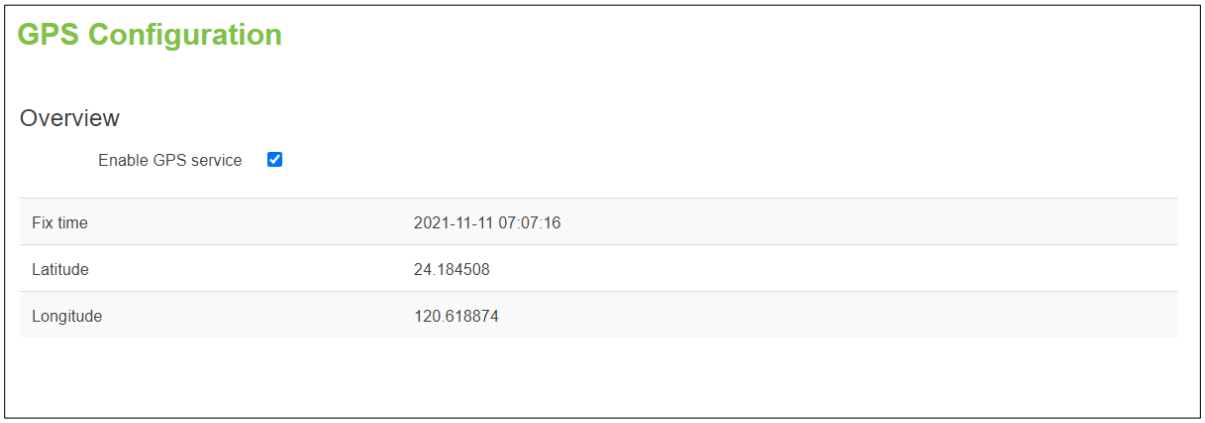


Table 84. Services > GPS

Field	Value	Description
Fix time	YYYY-MM-DD HH:MM:SS; default: **none**	The last GNSS fix time.
Latitude	xxx.xxxxxx; default: **none**	It 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

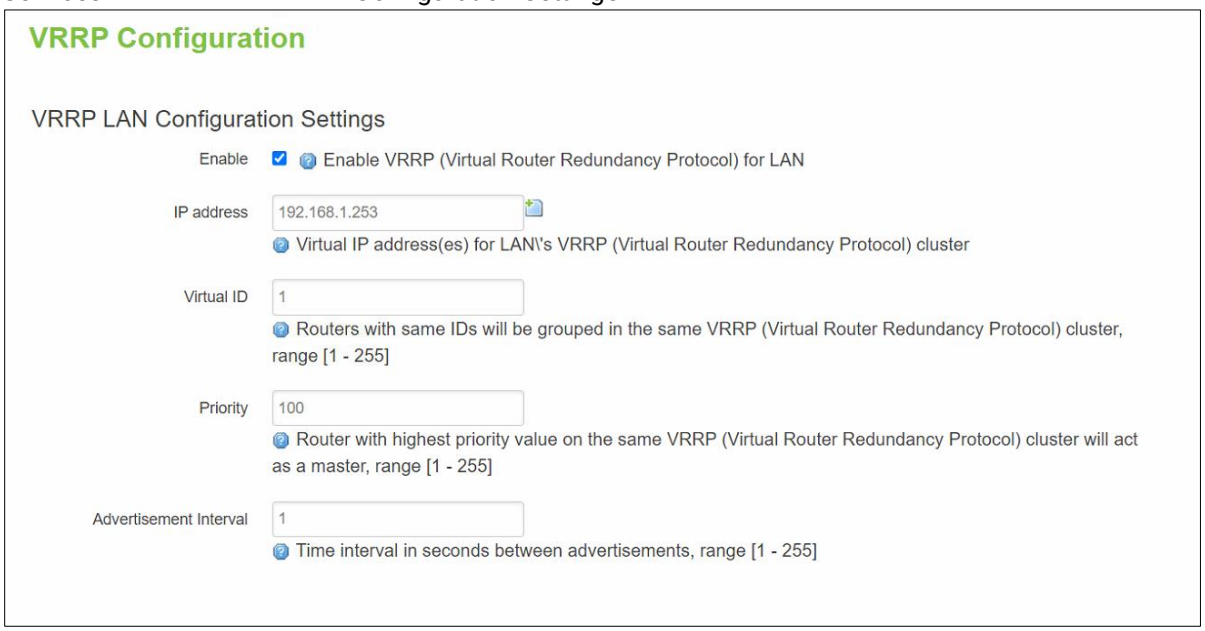


Table 85. Services > VRRP > VRRP LAN Configuration Settings

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. Higher values equal higher priority. The router with the highest priority is considered to be the *Master router* while other routers are *Backup routers*. sends periodic VRRP Advertisement messages • **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

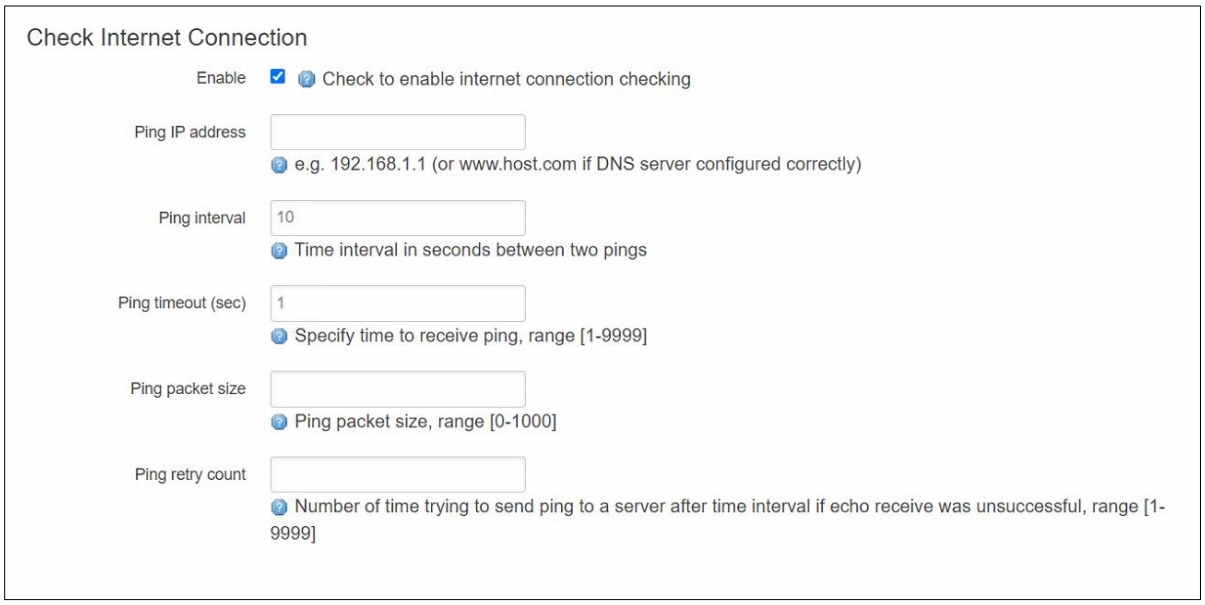


Table 86. Services > VRRP > Check Internet Connection

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

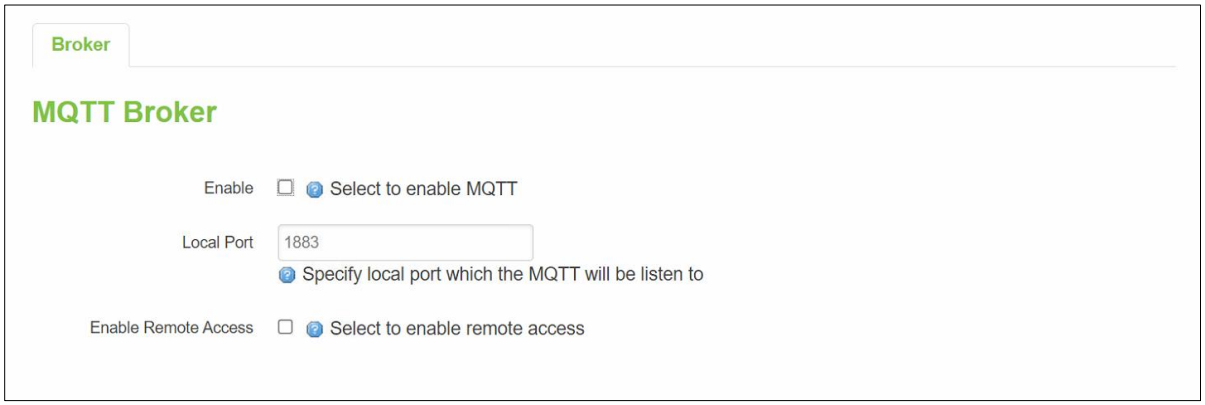


Table 87. Services > MQTT > Broker

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

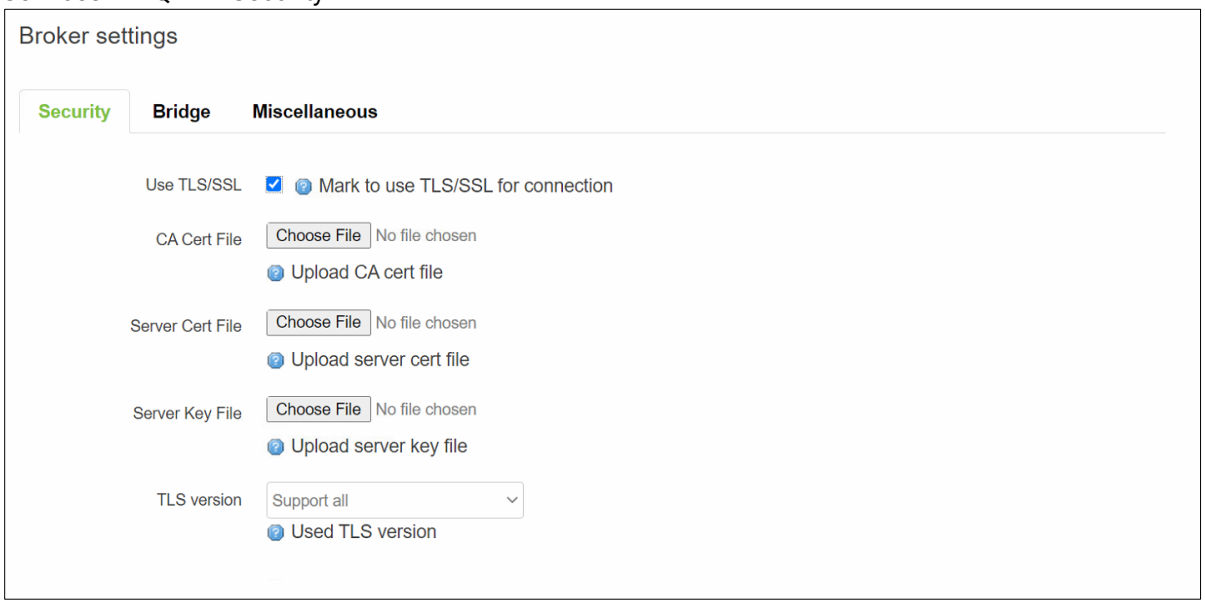


Table 88. Services > MQTT > Security

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

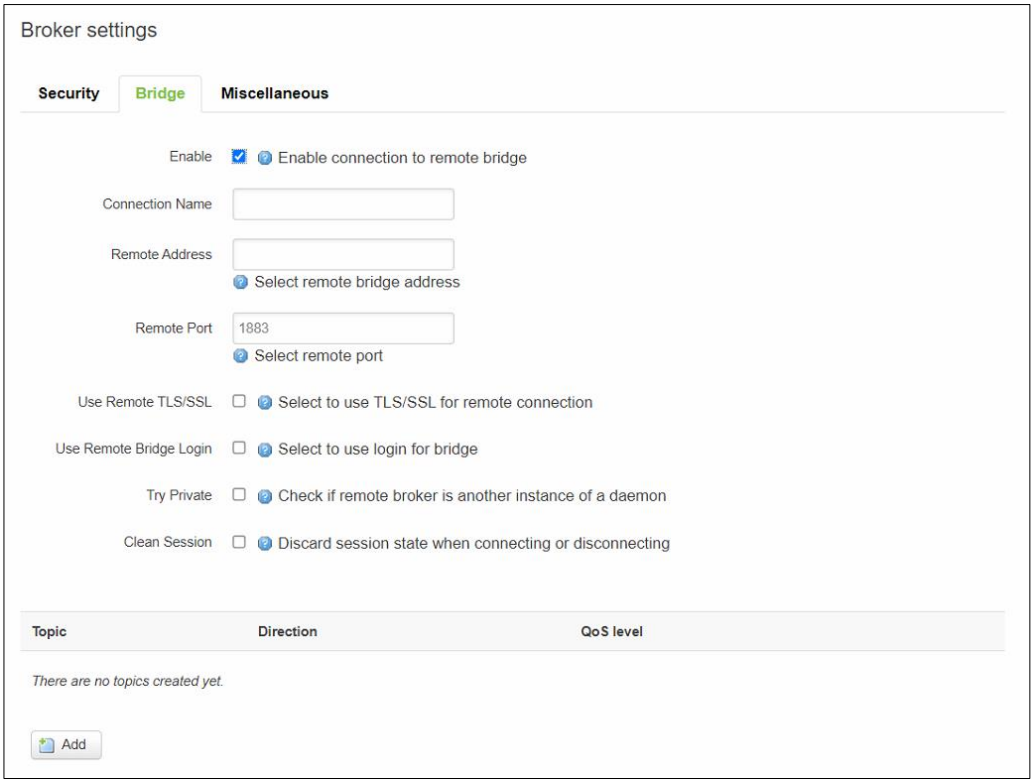


Table 89. Services > MQTT > Bridge

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

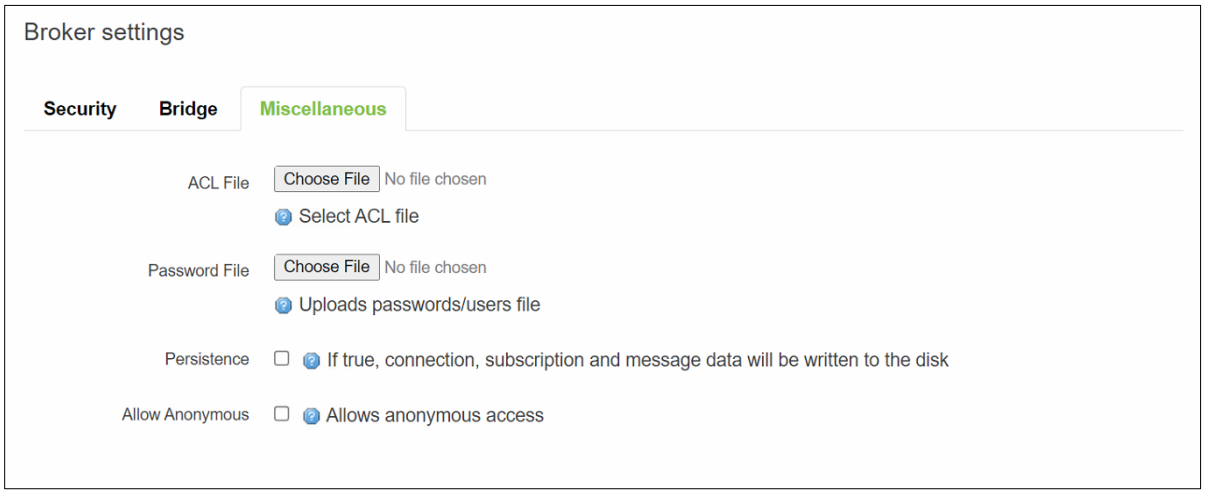


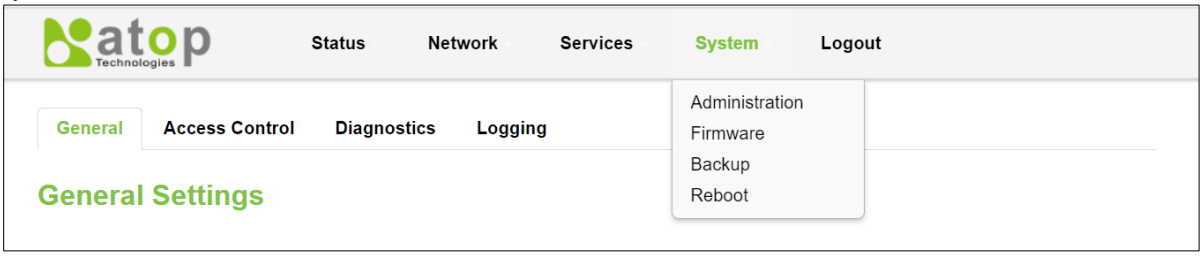
Table 90. Services > MQTT > Miscellaneous

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

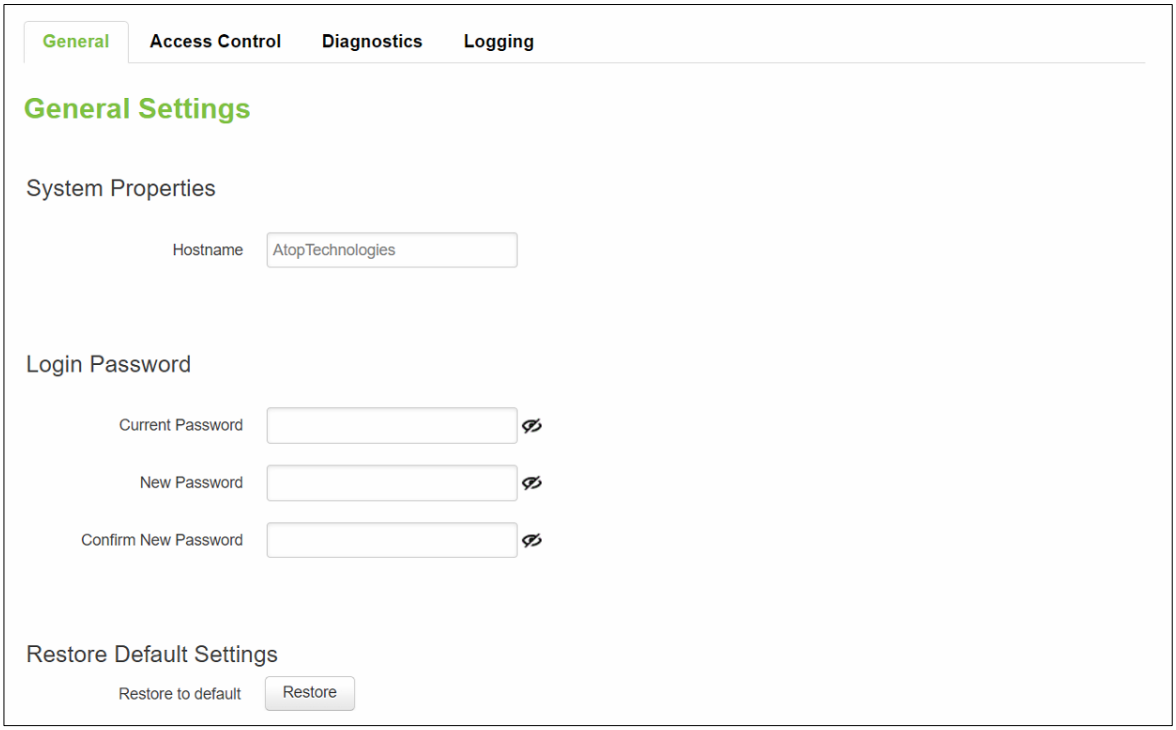


Table 91. System > Administration > General Settings

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

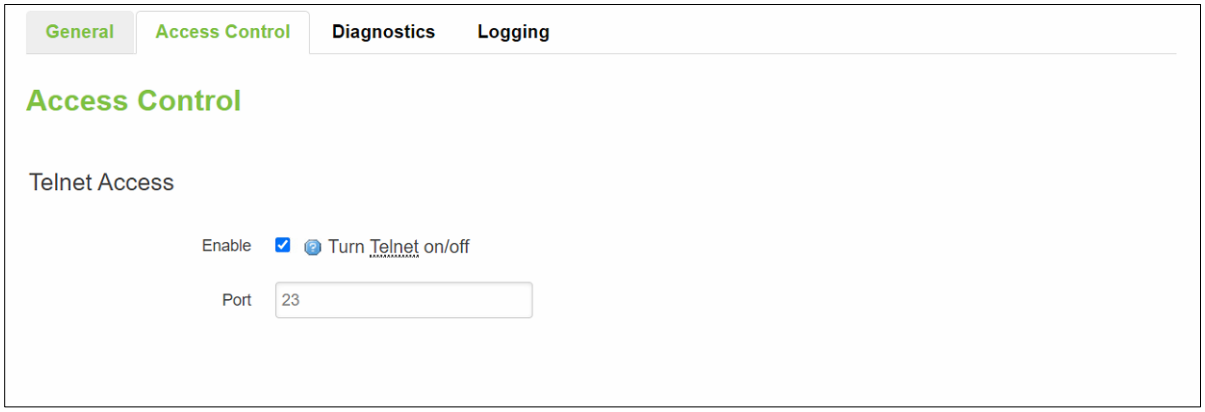


Table 92. System > Administrator > Access Control > Telnet Access

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

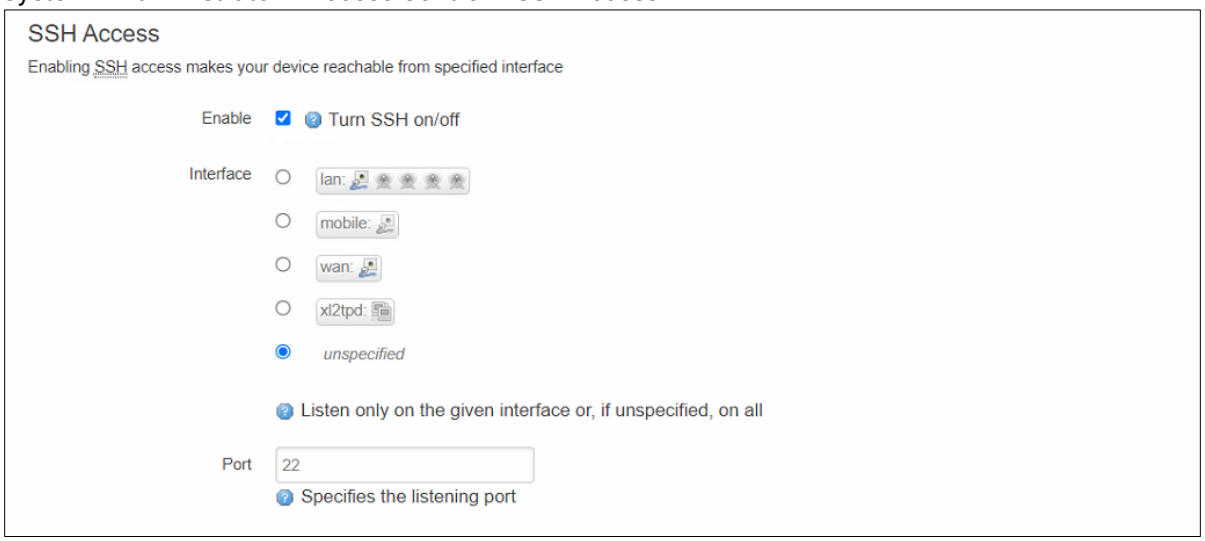


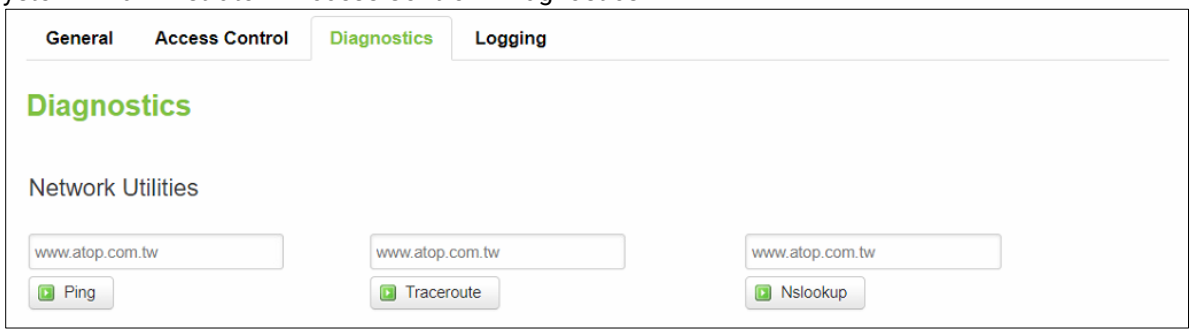
Table 93. System > Administrator > Access Control > SSH Access

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

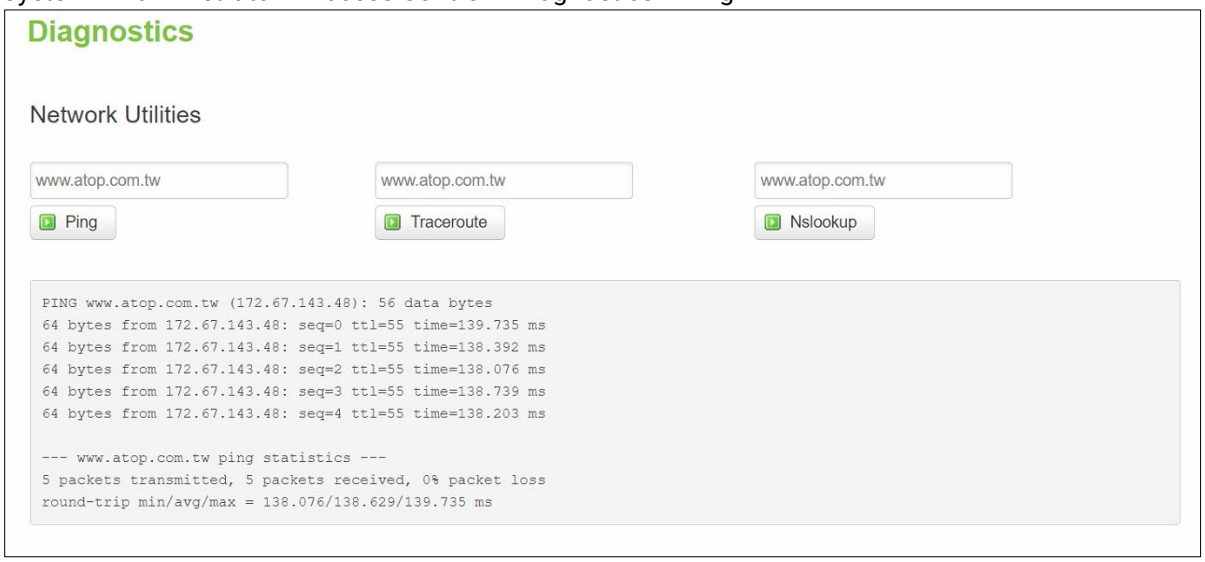


3.5.1.2.1 Ping

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



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

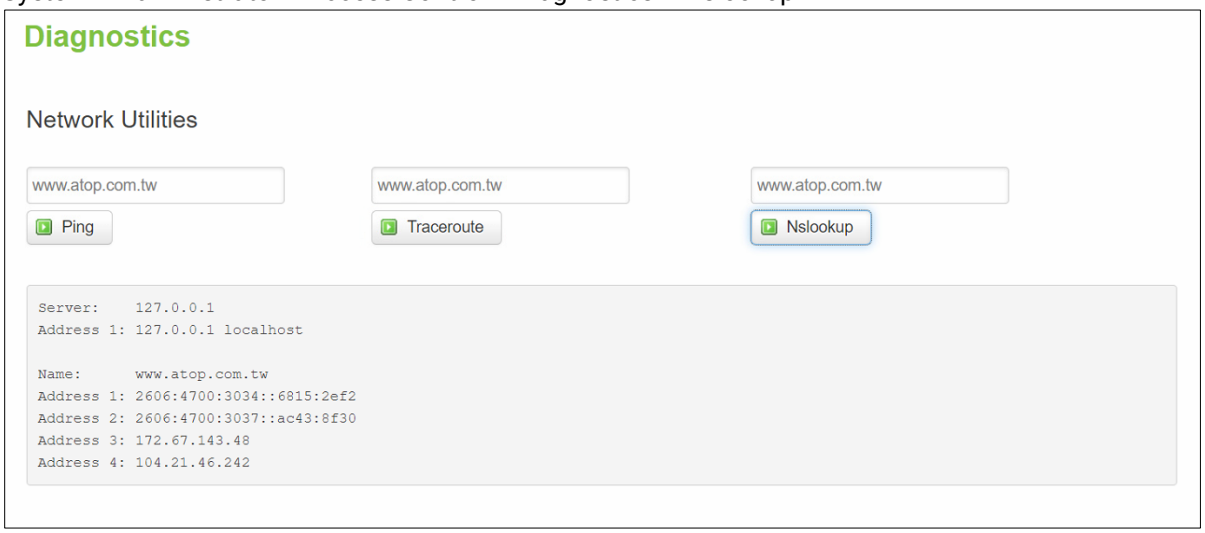
3.5.1.2.3 Nslookup

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



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

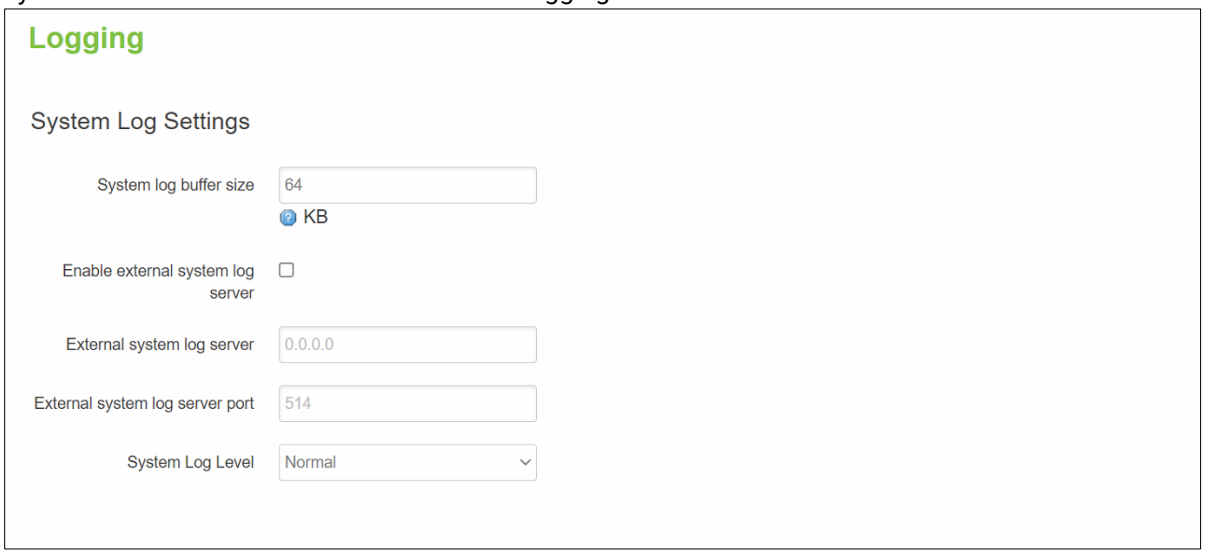


Table 94. System > Administrator > Access Control > Logging

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**.

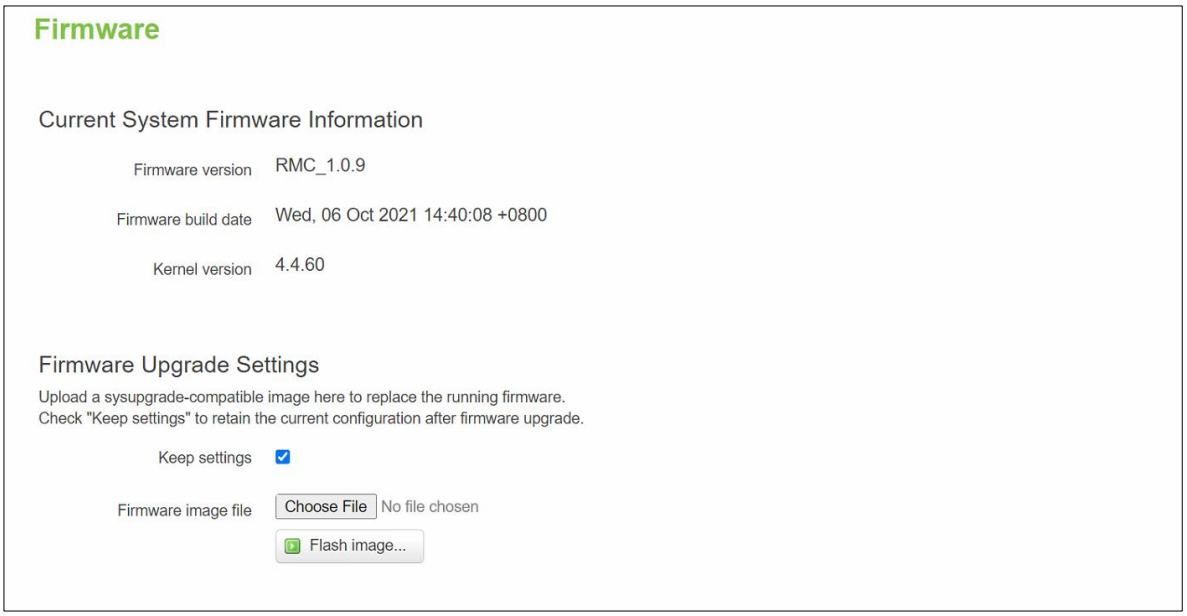
Here are the steps to follow for the firmware upgradation:

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.

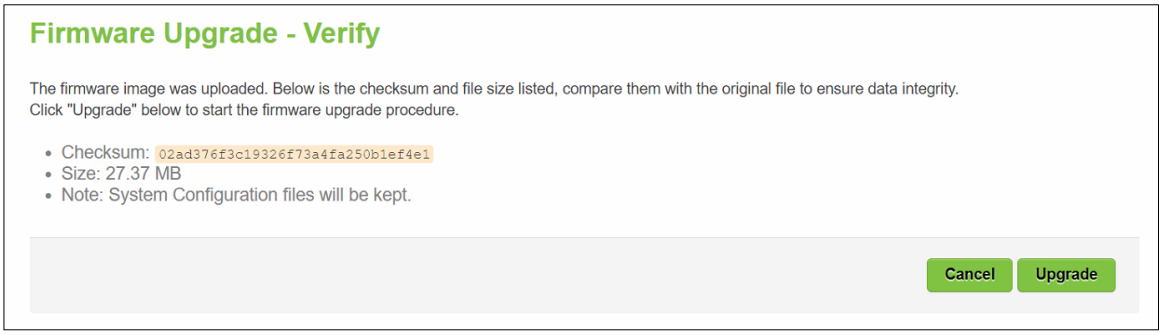
7. Then, click "Flash image" button to start the firmware upgrade process.

Figure 121. System > Firmware



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



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

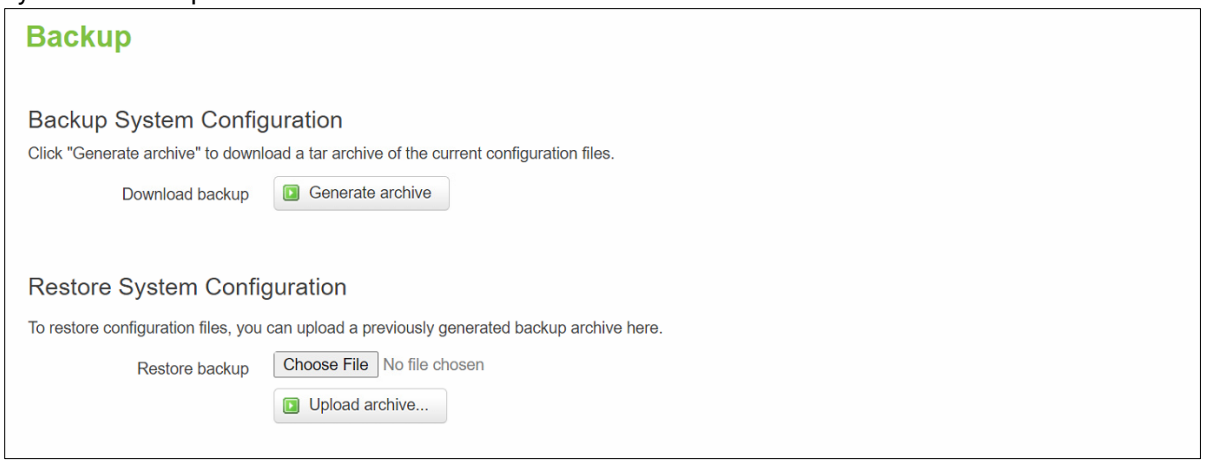
Click the **Generate archive** button to backup configuration files from CWR5805 device to your local host device. These backup configuration files are archived to a **backup-Hostname-yyyy-mm-dd.tar.gz** file.

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** button to start restoring the archive file to the CWR5805 device.

Figure 123. System > Backup



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

3.6 Logout

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

Figure 125. System > Logout

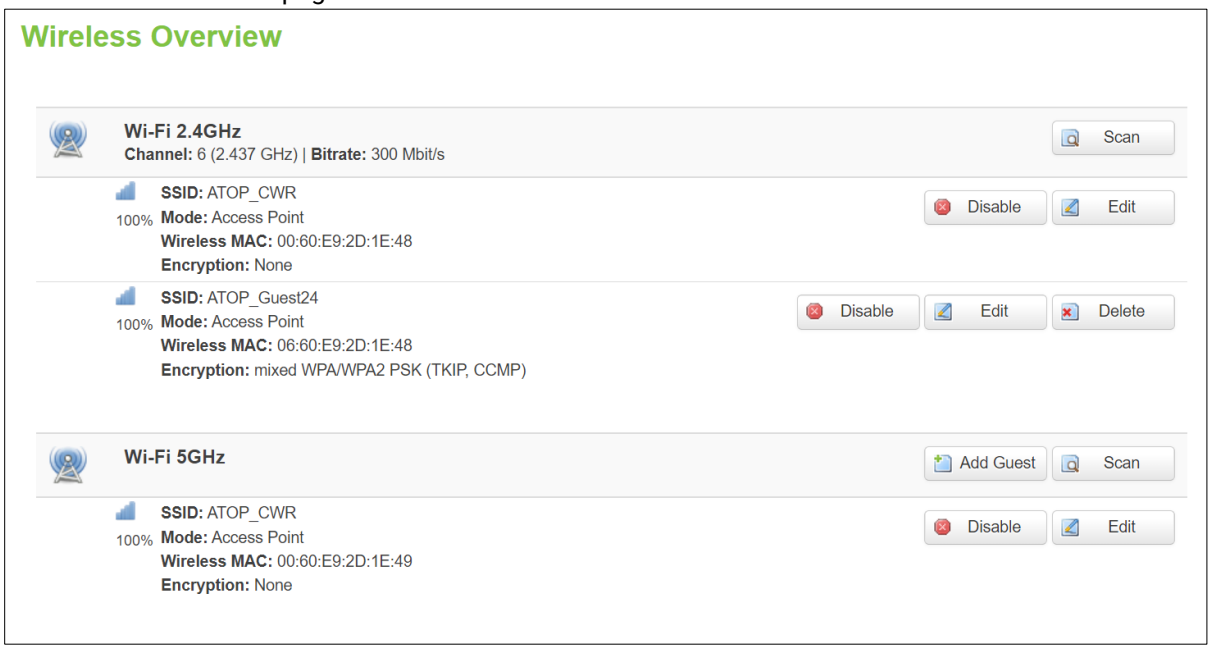
4 Tutorials

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

4.1 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 126. Wireless Overview Webpage under Wifi Menu



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 device.

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

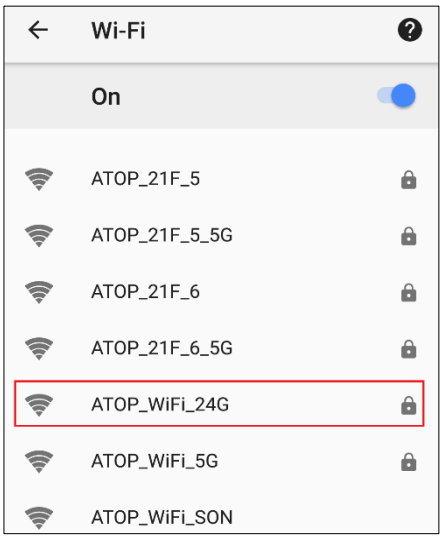
Select the **Settings** icon to enter Settings and then select **Network & Internet** to enter the Network & Internet screen. As shown in the Figure below, select the Wi-Fi item and turn WiFi on.

Figure 127. Network & Internet Settings on the Android System

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.

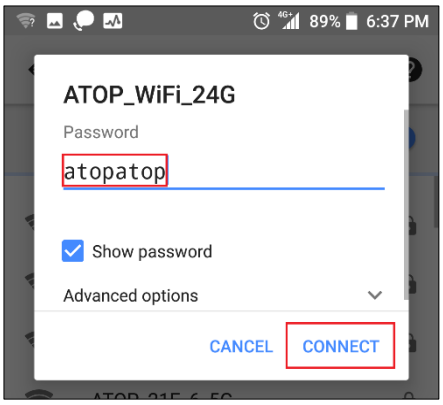
Figure 128. Select ATOP_WiFi_24G AP under Network & Internet Menu



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.

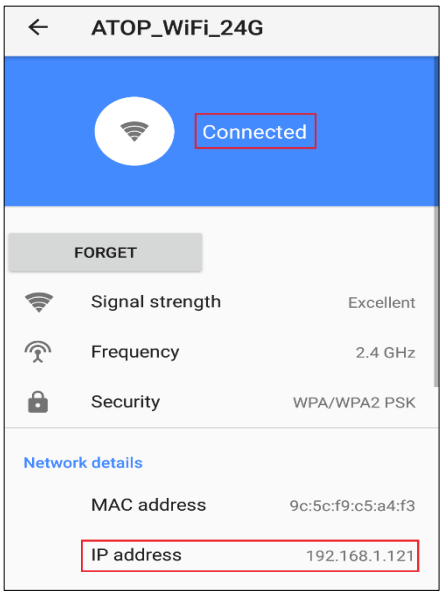
Figure 129. Input Password (Network Key) for WiFi Connection

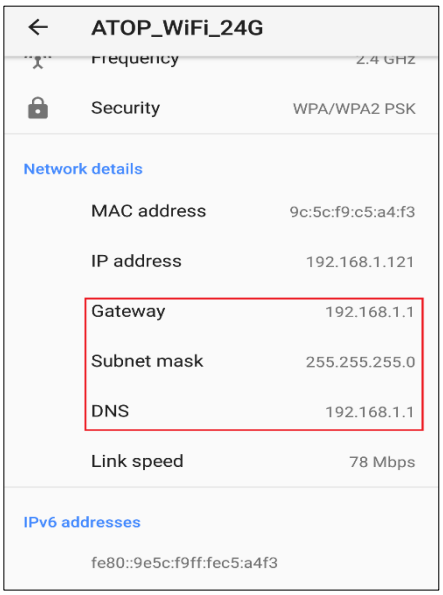


Step 4: *Wi-Fi Connected Infomation*

After Wi-Fi connection is established successfully, push the **SSID** named **ATOP_WiFi_24G** again to enter the connection details screen. As shown in Figure 130, the assigned IPv4 address, subnet mask, gateway, and DNS come from bridged interface (br-lan) of CWR5805 device.

Figure 130. Wi-Fi Connected Information





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.

4.2 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.

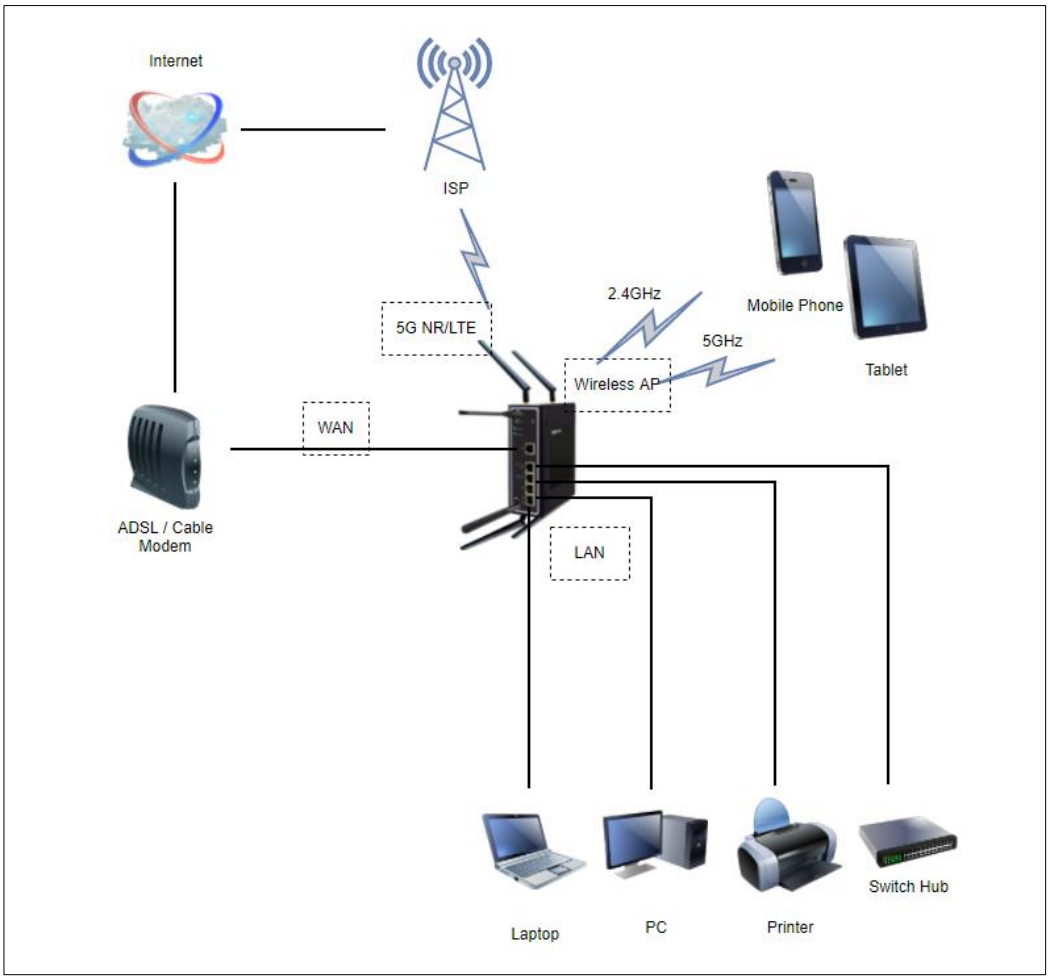
As shown in the Figure below, DHCP client devices connected to the LAN port or wireless 2.4GHz/5GHz interface are under the same network domain of **192.168.1.x**. This means that all DHCP clients can communicate with each other.

Section 3.5.1.2.1 illustrates how to test a communication by DHCP client with other devices using ping utility such as PingTools.

In section 3.3.8, 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 131. Multiple Devices are Assigned Dynamic IP Addresses by CWR5805 for Internet Connection



4.2.1 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**.

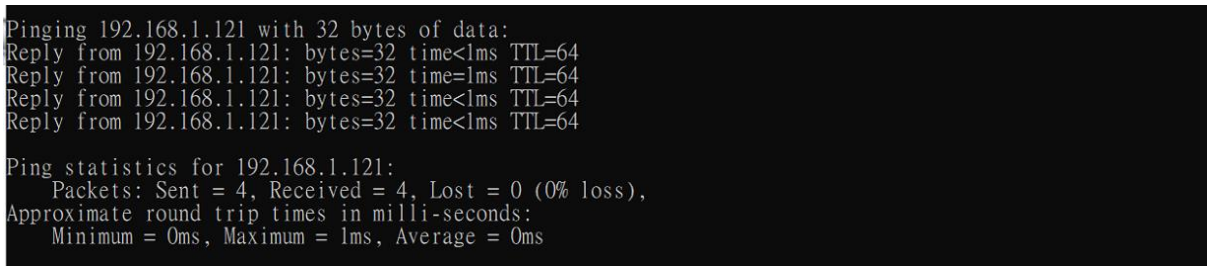
***Step 2**: Assign a dynamic IPv4 address to a mobile phone*

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*

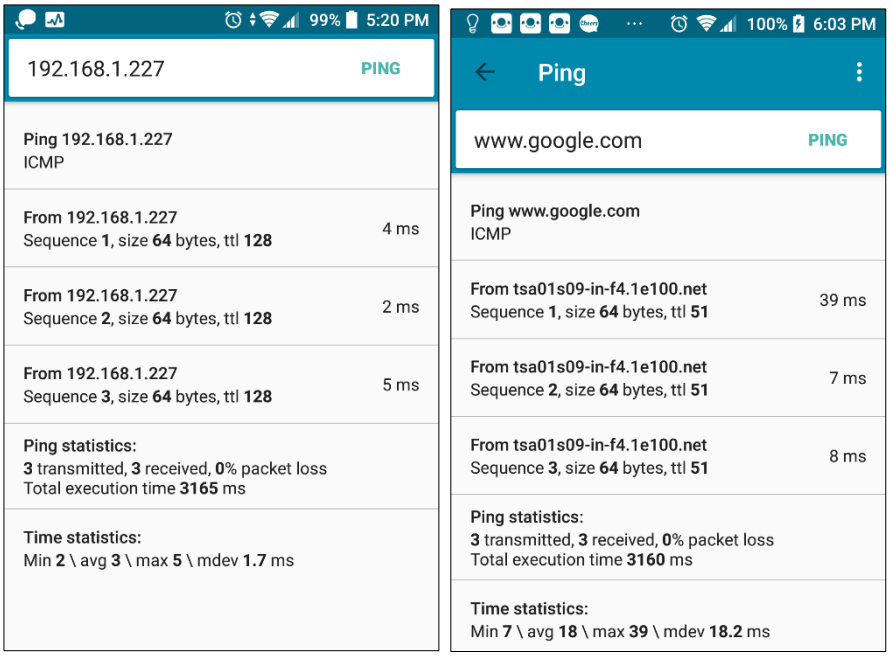
On the personal computer, open Windows' command prompt window, type in the "**ping 192.168.1.121**" command. As shown in the Figure below, the personal computer is receiving the response packets from the remote mobile phone side.

Figure 132. Local Personal Computer ping Android Mobile Phone



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 133. Android Mobile Phone ping Local Personal Computer



***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 134. 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.

4.2.2 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 3.3.2 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 3.3.1 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 Figure 63, 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 135, 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 136, 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 135. Traceroute Test on Command Prompt Window of Local Computer

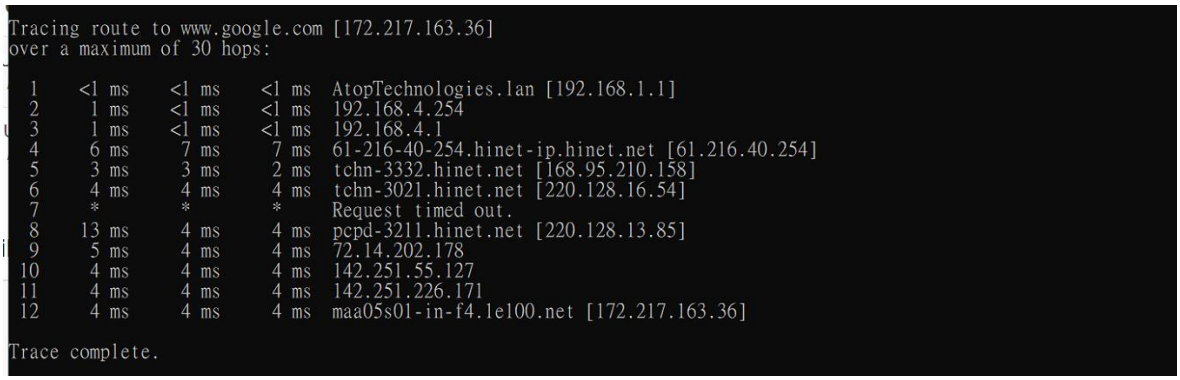
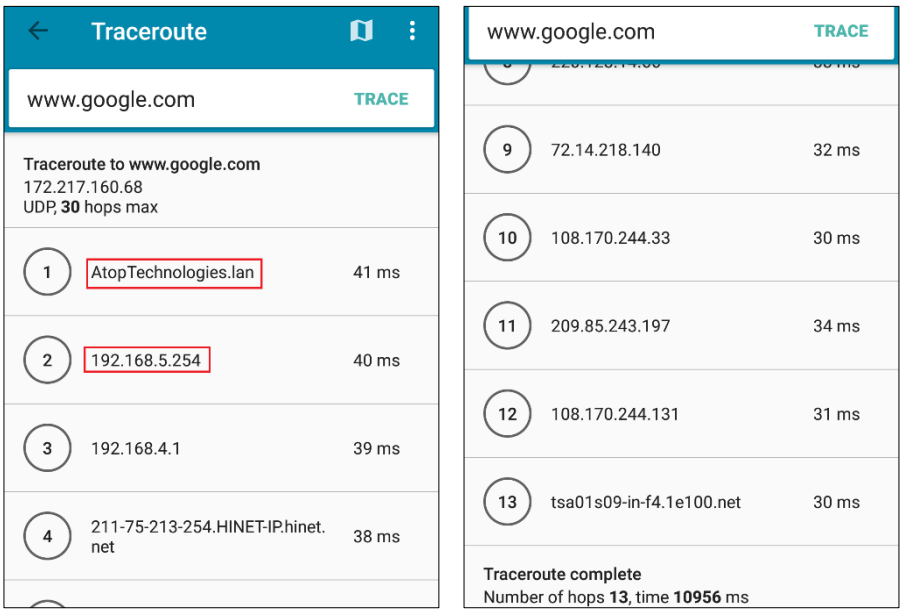


Figure 136. Traceroute Test on PinTools App of Android Mobile Phone



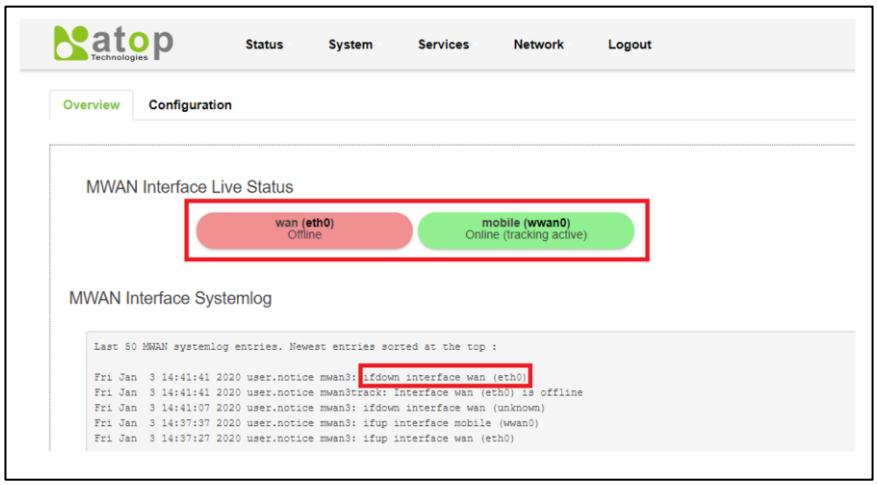
Step 3: *Disconnect WAN Interface*

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



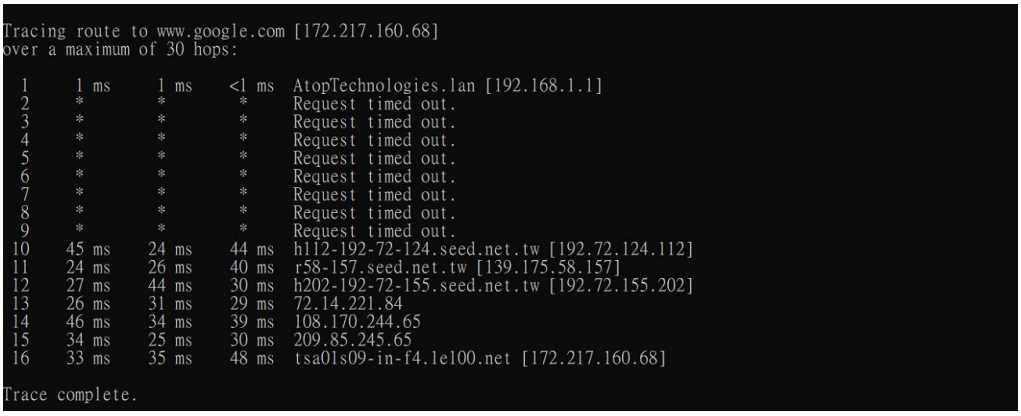
Step 4: *Traceroute outbound host/FQDN again*

In local personal computer side, open Windows' command prompt window, type in the "**tracert www.google.com**" command. As shown in Figure 138, 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 138. Traceroute Test Again on Command Prompt Window of Local Computer



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 95. 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 40 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 139. WAN/LAN Port on RJ45 with Pin Numbering of CWR5805 Device

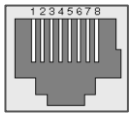


Table 96. Assignment for RJ-45 Connector of CWR5805 Device

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