WR100 User Manual

Version: 1.01

International Telematics Solutions Innovator

www. queclink .com

Document Title	WR100 User Manual
Version	1.01
Date	2021-11-19
Status	Released

General Notes

Queclink offers this information as a service to its customers, to support application and engineering efforts that use the products designed by Queclink. The information provided is based upon requirements specifically provided to Queclink by the customers. Queclink has not undertaken any independent search for additional relevant information, including any information that may be in the customer's possession. Furthermore, system validation of this product designed by Queclink within a larger electronic system remains the responsibility of the customer or the customer's system integrator. All specifications supplied herein are subject to change.

Copyright

Contents

0. Revision History

Version	Date	Author	Description of change
1.00	2021-09-10	Vincent Zhou	Initial version
1.01	2021-11-19	Vincent Zhou	Added new features

1. Overview

1.1 Description

The Queclink WR100 dual SIM industrial cellular router is a rugged cellular router offering high-speed stable mobile connectivity for machine to machine (M2M) applications. Based on 3G/4G LTE technology, WR100 adopts high-performance 32-bit processor and embedded operating system design. APN/VPDN private network access and dual SIM backup design guarantee data transmission security and provide high-speed, reliable routing and data transmission capabilities. Equipped with 2 Ethernet ports, Wi-Fi, RS232/RS485 port, all of which make it can be widely used in telecommunications, finance, information media, electric industry, retailing, automotive and environmental industries.

1.2 Major Features

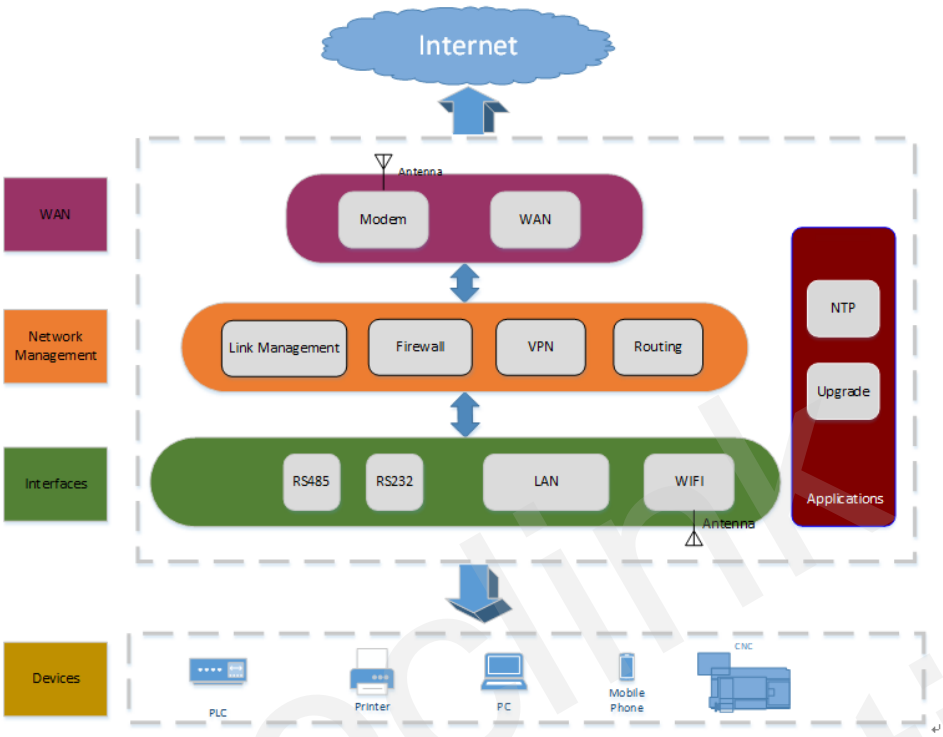
- Dual 4G (LTE) SIM to provide quick access to Internet– Cat 4 DL up to 150 Mbps, UL up to 50 Mbps; compatible with 3G, 2G network.
- 2 Ethernet ports, 1 RS-232/RS-485 to connect to a wide variety of equipment.
- 8-32VDC wide range power supply and -30 °C to 70 °C temperature range to provide high reliability.
- L2TP/PPTP/IPsec/OpenVPN/GRE VPN services to provide highly secure data transmission for devices.
- Static routing, RIPv1, RIPv2 and policy routing to provide various routing functions.

1.3 Technical Specification

Hardware	
CPU	Qualcomm 9531, 650 MHz
RAM	128 MB, DDR2
FLASH memory	16 MB SPI Flash
Mobile module	4G (LTE) – Cat 4 up to 150 Mbps, 3G (WCDMA or CDMA), 2G (GSM)
Ethernet	2 x 10/100 Ethernet ports: 1 x WAN (configurable as LAN), 1 x LAN ports, 10/100 Mbps, comply IEEE 802.3, IEEE 802.3u standards, supports auto MDI/MDIX
Status LEDs	1 x Power LED, 1 x CELL LED, 1 x Wi-Fi LED, 1 x Signal strength LED
SIM	2 x SIM slots (Mini SIM - 2FF), 1.8 V/3 V, external SIM holders
Power	4-pin power connector with 2 pins for input/output
Antennas	2 x SMA for LTE, 2 x RP-SMA for Wi-Fi antenna connectors
RS232/RS485	RS232 (without RTS, CTS), 300-115200 baud rate/ RS485 half-duplex (2 wires), 300-115200 baud rate
Reset	Reset/restore to default button

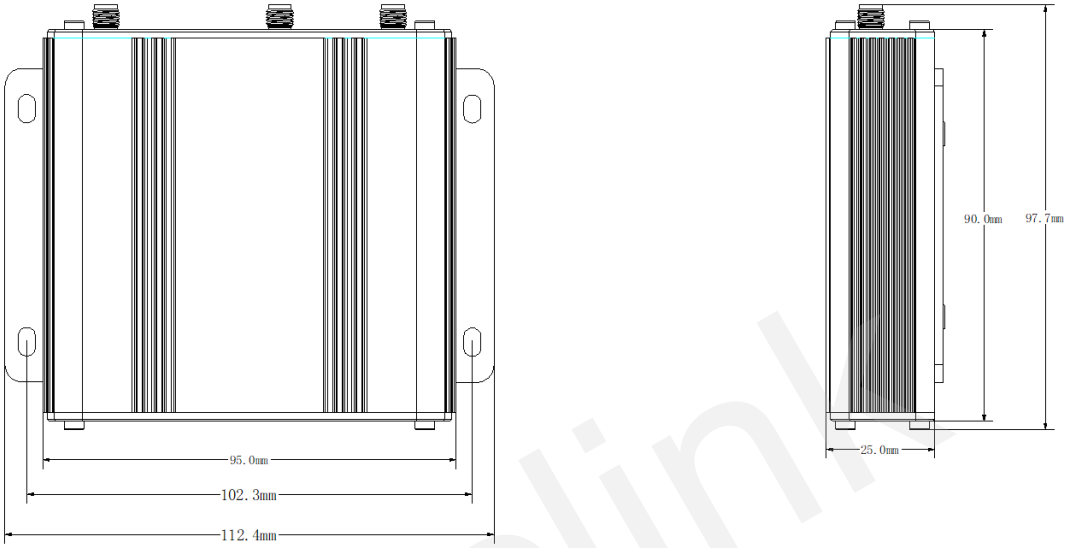
Software	
Operating system	OpenWrt based Linux OS
SIM switch	2 SIM cards, auto-switch cases: weak signal, no network, network denied, data connection fail
Wireless mode	IEEE 802.11b/g/n, Access Point (AP), Station (STA)
Routing	Static routing, dynamic routing (RIP v1/v2)
Network protocols	TCP, UDP, IPv4, ICMP, NTP, DNS, HTTP, FTP, SMTP, SSL v3, TLS, ARP, PPPoE, SSH, DHCP, Telnet
Connection monitoring	Ping Reboot, LCP and ICMP for link inspection
VPN	L2TP, PPTP, OPENVPN, IPSec, GRE tunnel
Physical	
Input voltage range	8 - 32 VDC (4-pin industrial socket), reverse polarity protection; Surge protection >31 VDC 10us max
Power consumption	< 7W
Casing material	Aluminum housing
Dimensions	95 mm x 95 mm x 24 mm (W x D x H)
Weight	200g
Operating Environment	
Operating temperature	-30 °C to 70 °C
Operating humidity	10% to 90% non-condensing
Ingress Protection Rating	IP30

1.4 Software Architecture

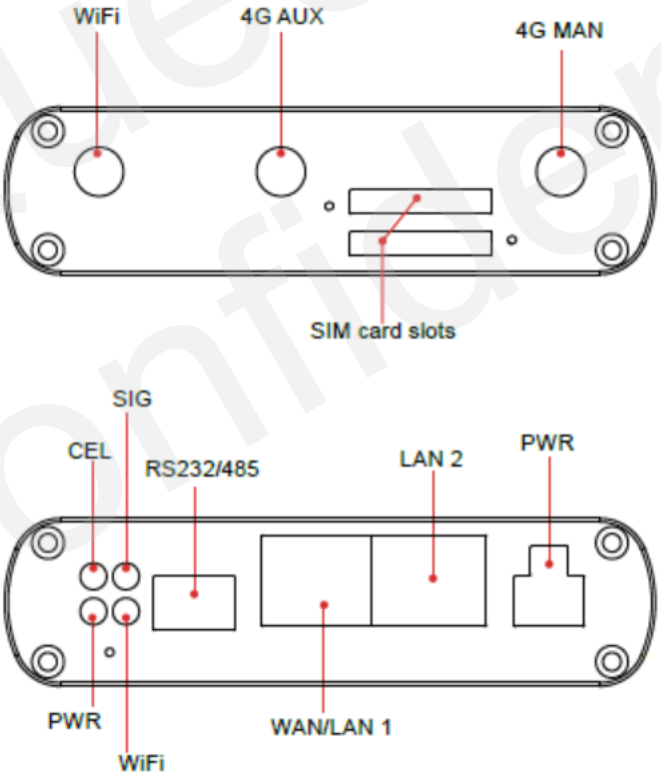


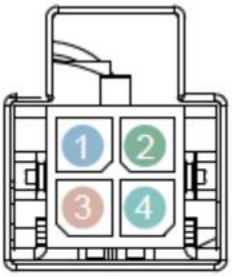
2. Hardware

2.1 Structure



2.2 Interfaces





PWR

1 Power

2 Ground

3 Digital input (0-5 VDC: low logic level/8-40 VDC: high logic level)

4 Digital output (4-pin connector) (30 VDC, 0.3A)

RS232/485

1 TX/A

2 RX/B

3 GND

2.3 LEDs

Name	Status	Description
PWR	Red, solid	Power on
	Off	Power off
Wi-Fi	Orange, solid	Wi-Fi on and working
	Orange blinking every 350ms	Data is being transferred
	Off	Wi-Fi off
CEL	Green, solid	Connecting to 4G network
	Green blinking every 0.5s	Connecting to 2G/3G network
	Off	No SIM or bad PIN
SIGNAL (RSSI)	Blue, solid	23 to 32
	Blue blinking every 1s	11 to 23
	Blue blinking every 0.5s	1 to 10
	Off	0

2.4 Accessories

Item	Quantity	Note
Power adaptor	1	
4G antenna	2	

Wi-Fi antenna	1	
RJ45 cable	1	1 meter long
3-pin connector	1	
Mounting kits	1	

2.5 Installation

1. Insert SIM card:

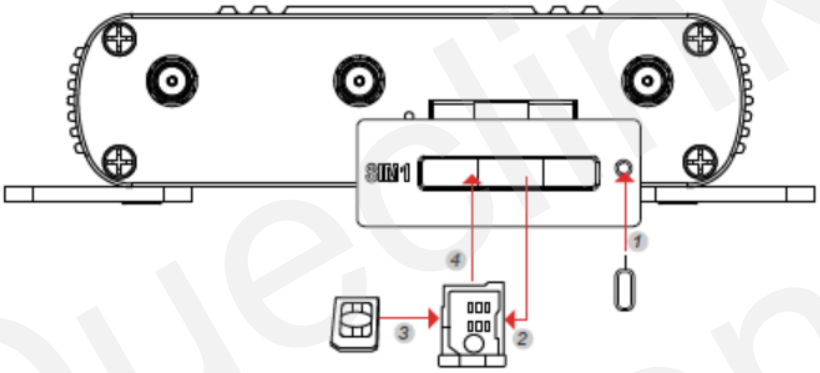
(1) Make sure the router is powered off.

(2) Push the SIM holder button with the SIM ejection pin.

(3) Pull out the SIM holder.

(4) Insert your SIM card into the SIM holder.

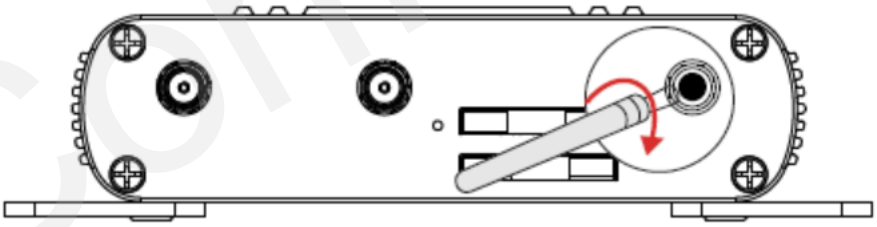
(5) Slide the SIM holder back into the router.



Note: The device is compatible with **mini-SIM (2FF)** size cards.

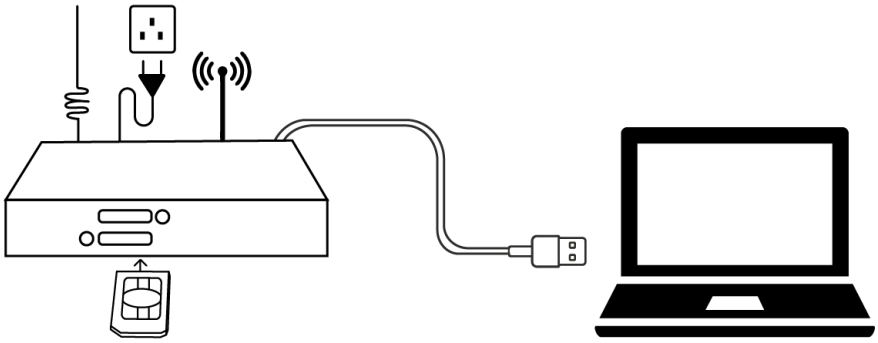
2. Attach External LTE, Wi-Fi and GPS Antennas:

Attach the SMA external antenna to the router's connector and twist tightly. Make sure that the antenna type corresponds to the antenna connector. You can see the antenna type by the printing on the antenna.



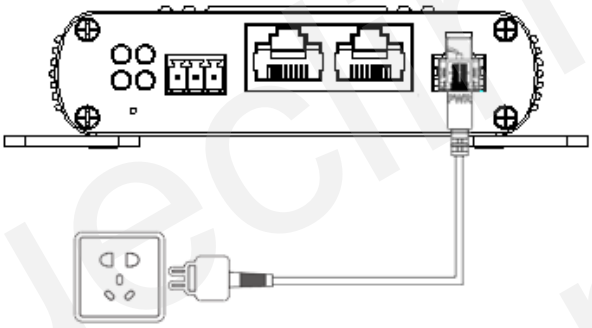
3. Connect the Router to the devices

Connect an Ethernet cable to any port marked ETH0~ETH3 at the bottom of the router, and connect the other end of the cable to your computer or lower end device.



4. Connect the 4-pin power cable to power on the Router.

Connect the power adaptor to the socket on the front of the router and plug the other end of the power adaptor into a power outlet. The router is designed to accept input voltage between 8V DC to 32V DC. Higher voltage input may damage the device.



5. Fix the Router

You can use 4pcs of M6*10 flat-head Phillips screws to fix the router on the wall or other flat surface.

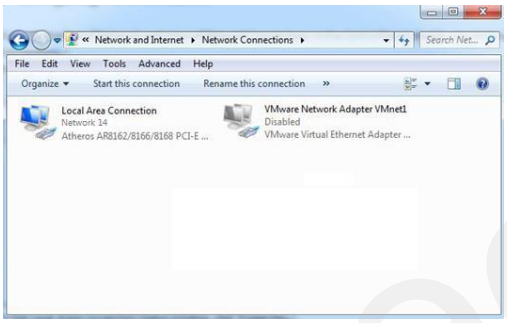
3. Initial Configuration

WR100 has a friendly WebUI. You can very easily configure the device through this UI. Make sure your computer has an Ethernet interface and web browser such as IE, Chrome, Firefox, etc.

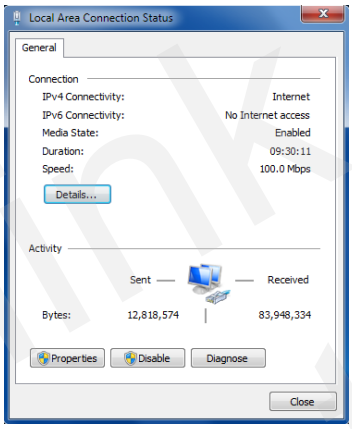
3.1 Configure the PC

There are two methods to get IP address for the PC, one is to obtain an IP address automatically from “Local Area Connection”, and another is to configure a static IP address manually within the same subnet of the router. Please refer to the steps below.

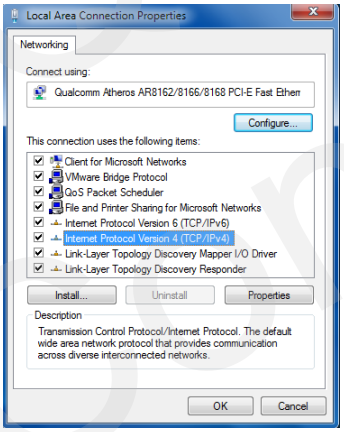
Here takes **Windows 7** as example to configure a static IP address, and the configuration for windows system is similar.

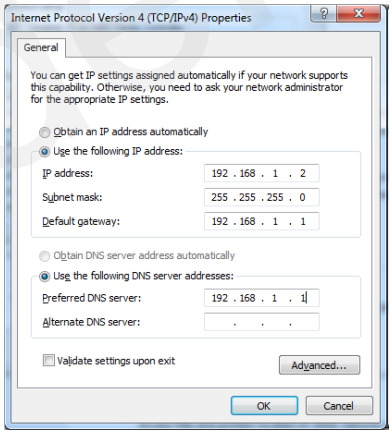


1. Click Start > Control panel, double-click Network and Sharing Center, and then double-click Local Area Connection.



2. Click Properties in the window of Local Area Connection Status.





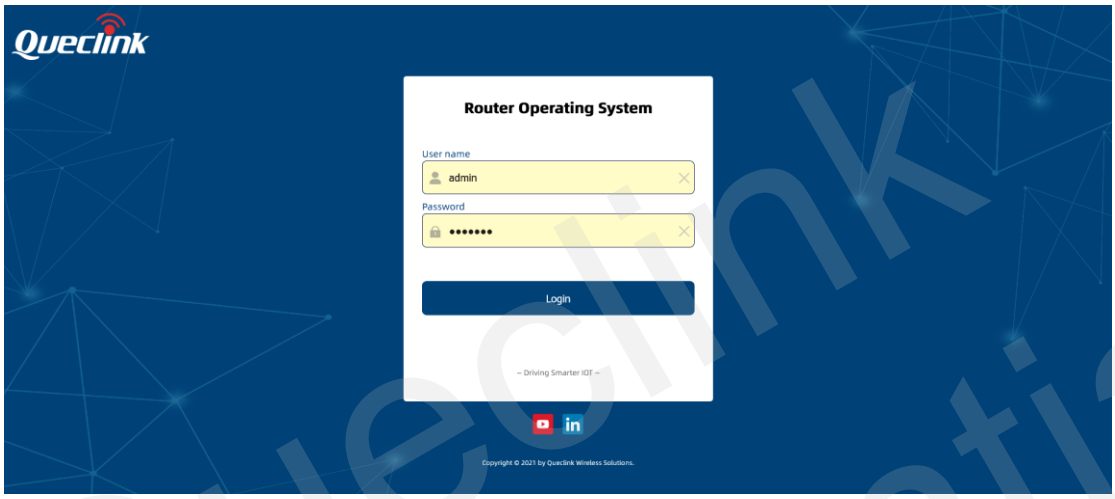
3. Choose Internet Protocol Version 4 (TCP/IPv4) and click Properties.
4. Use the following IP address:

Configure a static IP address manually within the same subnet of the router, the default router IP address is 192.168.1.1.

Click OK to finish the configuration.

3.2 Login to device

1. To enter the router's Web interface (WebUI), type http://192.168.1.1 into the URL field of your Internet browser.
2. Use the following login information when prompted for authentication:

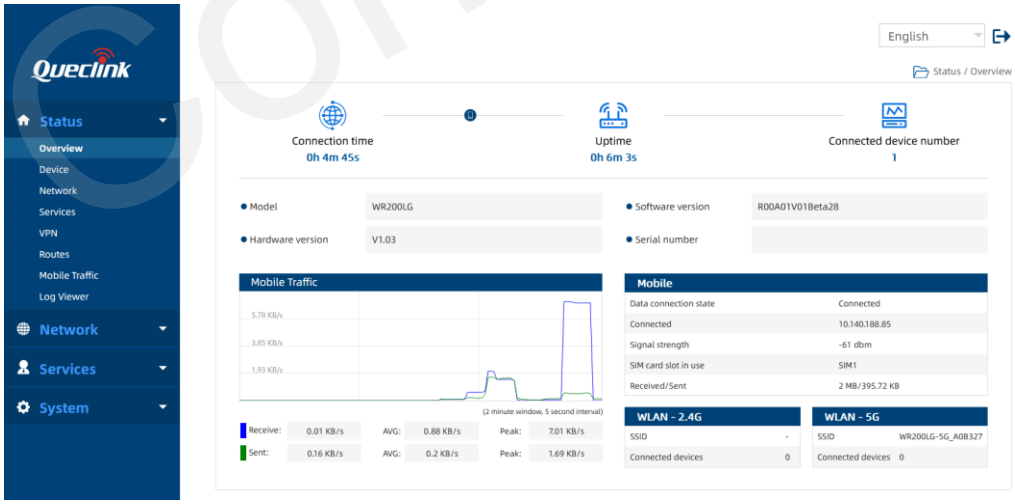


Enter the username and password, and then click Login button. The default username is ‘admin’ and password is ‘admin01’.

3.3 Control Panel

After logging in, the home page of the WR100 Router’s web interface is displayed. The home page is an overview of the router. It displays the network state, mobile connection state and Wi-Fi state of the router.

The page has language selection dropdown menu and exit button in the upper right corner. You can change language setting or logout the system easily.



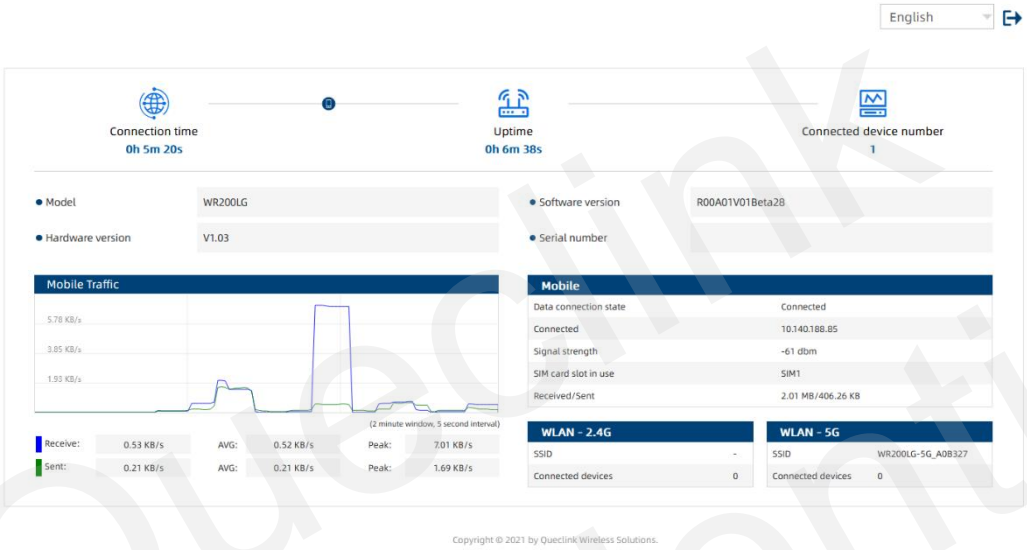
4. Software Configuration

4.1 Status

This section includes the running status of the Router.

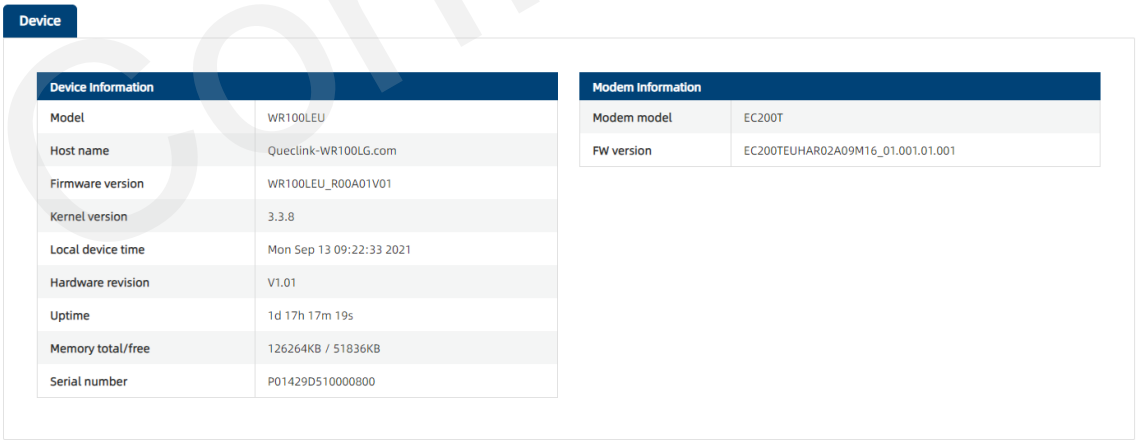
4.1.1 Overview

The **Overview** page contains various information summaries, such as connection state, Wi-Fi state and real-time traffic, etc. It is also the homepage of the WebUI.
The figure bellow is an example of the Overview page:



4.1.2 Device

The **Device page** displays the Router's hardware, software and modem related information. You can find serial number and software version in this page, which are important information of after sales maintenance.

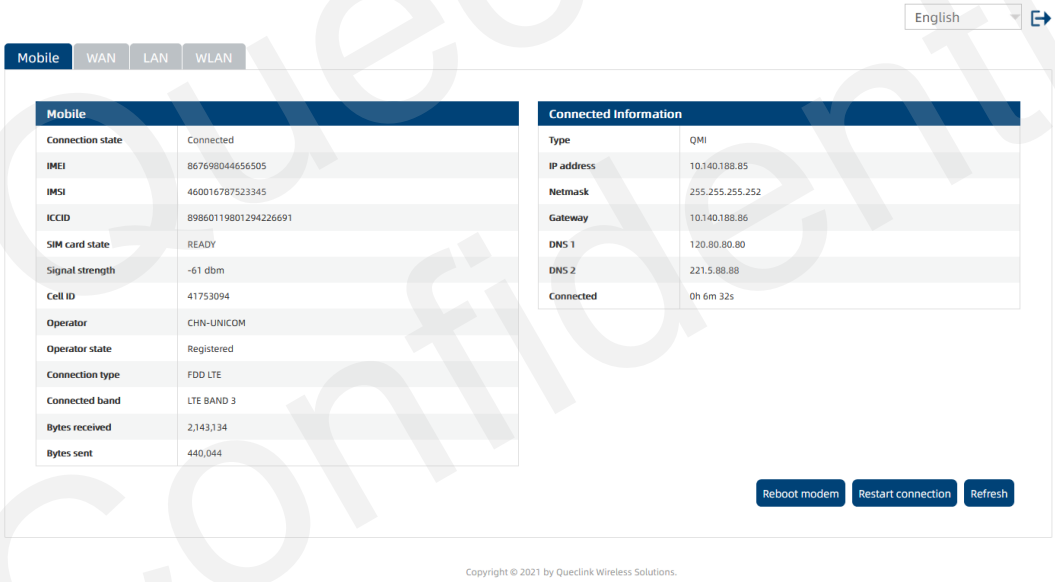


Field Name	Description
Model	Displays model number of the device.
Host name	Displays the device's host name. The hostname can be used

	instead of the LAN IP address to communicate with the device inside the local network.
Firmware version	Displays the firmware version currently used by the device.
Kernel version	Displays the device's kernel version. A kernel is a computer program responsible for connecting a device's software to its hardware
Local device time	Displays the current time as perceived by the device.
Hardware version	Displays the device's hardware version.
Uptime	Displays the running time since the device's last start up.
Memory total/free	Displays the amount of currently unused RAM.
Serial number	A unique device identifier.
Modem Model	The modem's model number
FW version	Modem's current firmware version

4.1.3 Network->Mobile

The Mobile page has two tables, one table displays the wireless information and the SIM card in use, another one displays the connection information, including IP address, DNS, etc. The figure below is an example of the Mobile page:



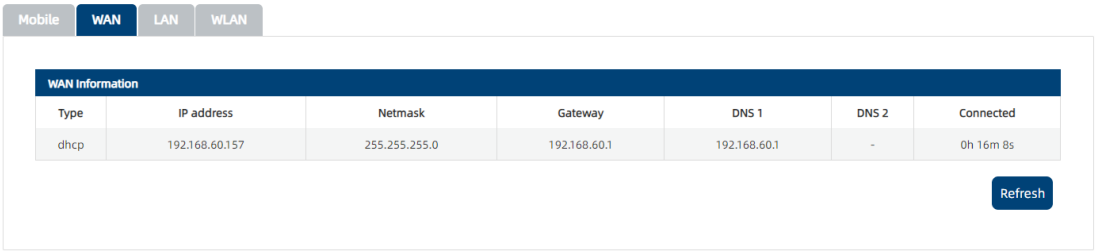
You can click Reboot modem or Restart connection button to restore the connection if the connection is abnormal. The Refresh button is to refresh all information fields in the page.

Field Name	Description
Connection State	Indicates whether the device has an active mobile data connection
IMEI	The IMEI (International Mobile Equipment Identity) is a unique 15 decimal digit number used to identify cellular modules.
IMSI	The IMSI (international mobile subscriber identity) is a unique 15 decimal digit (or less) number used to identify the user of a cellular network.
ICCID	SIM card's ICCID is a unique serial number used to identify the SIM

	chip.
SIM card state	The current SIM card state. Possible values are: • Ready - SIM card is inserted and ready to be used • Inserted - SIM card is inserted • Not inserted - SIM card is not inserted • Unknown - unable to obtain SIM card state value. Possible communication issue between the device and the modem
Signal strength	Received signal strength indicator (RSSI) measured in dBm. Values closer to 0 mean a better signal strength
Cell ID	The ID of the cell that the modem is currently connected with
Operator	Network operator's name
Operator state	Shows whether the network has currently indicated the registration of the mobile device. Possible values are: Unregistered - not registered to a network and the device is not currently searching for a new operator to register to Registered (home) - registered, home network Searching - not registered to a network, but the device is currently searching for a new operator to register to Network denied - registration to network is denied by operator Unknown - operator state is currently unknown Registered (roaming) - registered to network, roaming conditions
Connection type	Mobile connection type. Possible values are: 2G: 2G (GSM), 2G (GPRS), 2G (EDGE) 3G: 3G (WCDMA), 3G (HSDPA), 3G (HSUPA), 3G (HSPA), 3G (HSPA+), 3G (DC-HSPA+), 3G (HSDPA+HSUPA), UMTS 4G: 4G (LTE) N/A - not possible to determine at the moment
Connected band	Currently used frequency band. For more information on supported frequency bands
Bytes received	Amount of data received through the mobile interface
Bytes sent	Amount of data sent through the mobile interface
Restart Modem	Reboots the device's cellular module
Restart Connection	Restarts the mobile connection
Refresh	Refresh all information fields in the page
Type	The dialing mode of the connection
IP address	Router's modem IP address
Netmask	A netmask is used to define how "large" a network is by specifying which part of the IP address denotes the network and which part denotes the device
Gateway	Gateway of the default route - an IP address through which the router reaches the Internet
DNS	DNS servers used by the connection
Connected	Currently used connection uptime

4.1.4 Network->WAN

The **WAN** section displays information about the WAN interface, the connection type, IP address, Netmask, etc.
The figure below is an example of the WAN status page:

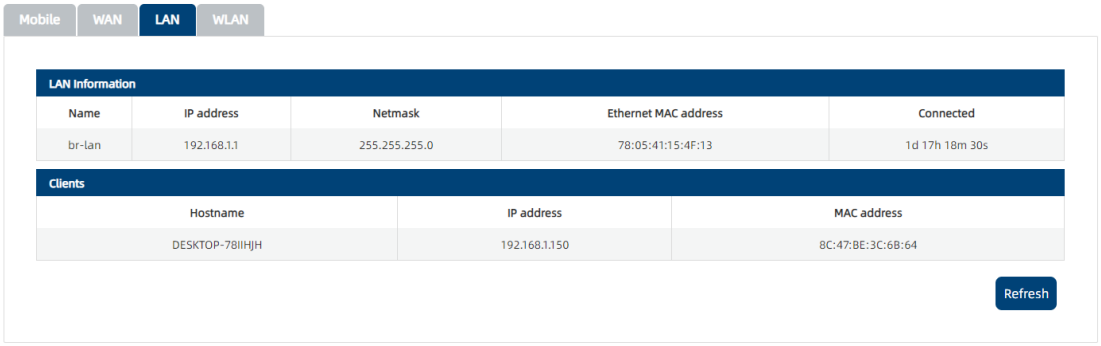


The Refresh button is to refresh all information fields in the page.

Field Name	Description
Type	Static - WAN network interface controller configuration parameters are set manually (used when the WAN gateway is not a DHCP server) DHCP - Dynamic Host Configuration Protocol; the WAN network interface controller acts as a DHCP client, meaning that it receives a dynamically assigned IP address and other network configuration parameters PPPoE - Point-to-Point Protocol over Ethernet; used to establish a Digital Subscriber Line (DSL) Internet service connection
IP address	Router's WAN IP address
Netmask	A netmask is used to define how "large" a network is by specifying which part of the IP address denotes the network and which part denotes the device
Gateway	Gateway of the default route - an IP address through which the router reaches the Internet
DNS	DNS servers used by the main WAN connection
Connected	Currently WAN interface connection uptime
Refresh	Refreshes all information fields in the page

4.1.5 Network->LAN

The **LAN Information** page contains data on the router's LAN interfaces. There are two sections in this page, one is LAN information, including IP, Netmask, MAC address, connected time, and another one is DHCP lease, which contains information of DHCP clients.



The Refresh button is to refresh all information fields in the page.

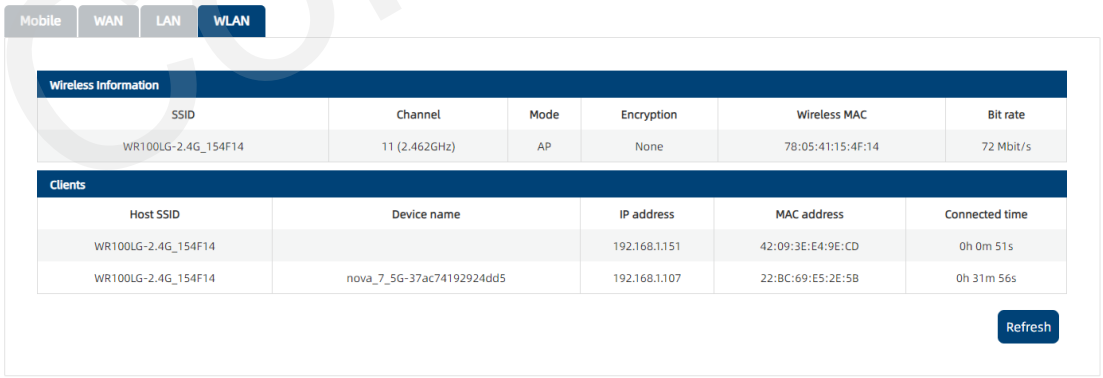
Field Name	Description
LAN Information	
Name	LAN interface name
IP address	Router's LAN IP address
Netmask	A netmask is used to define how "large" a network is by specifying which part of the IP address denotes the network and which part denotes the device
Ethernet MAC address	Router's LAN MAC address
Connected	The time since connection established
Clients	
Hostname	DHCP client's hostname
IP address	DHCP client's IP address
MAC address	DHCP client's MAC address

4.1.6 Network->WLAN

This page displays information about wireless connections and associated Wi-Fi stations. When router works in AP mode, the page displays AP information, otherwise, the page displays the connected station information.

The router can work either in Access Point (AP) mode or Station mode.

The figure below is an example of the WAN status page:



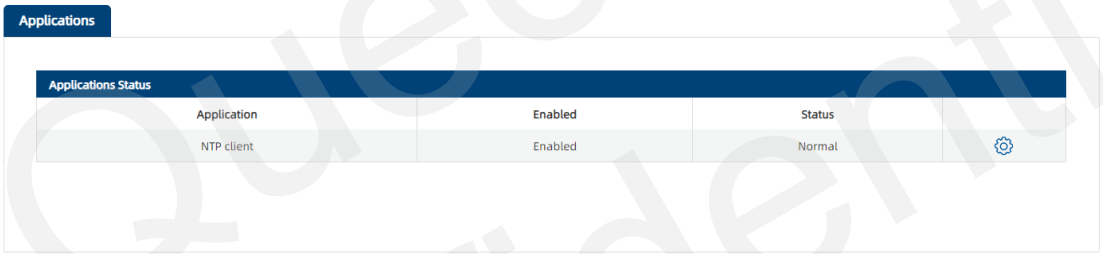
The Refresh button is to refresh all information fields in the page.

Field Name	Description

SSID	The broadcasted SSID (Service Set Identifier) of the wireless network
Channel	Currently used channel. In most countries there are 13 Wi-Fi channels on the 2.4 GHz band (14 in Japan) to choose from
Mode	Connection mode. Can either be Access Point (AP) or Client. In AP mode others can connect to this router's wireless connection. In client mode router connects to other wireless networks
Encryption	The type of Wi-Fi encryption used
Wireless MAC	The MAC (Media Access Control) address of the access point radio
Signal Quality	The signal quality between router's radio and some other device that is connected to the router
Bit rate	The maximum possible physical throughput that the router's radio can handle. Bit rate will be shared between router and other possible devices which connect to local Access Point (AP)

4.1.7 Applications

The Services table displays the status of the device's applications. Applications that are currently disabled are displayed in a red font; services abnormal are also displayed in a red font. The user can click ⚙ icon to direct to the configuration page of the services.



Field Name	Description
Application	Name of the application
Enabled	Display the enable/disable status of this service
Status	Display the working status of this service

4.1.8 VPN

The VPN table displays the status and connection information of all VPN link. The status is connected if a VPN connection is established. You can also see the IP address (work as client) or connected device number (work as server) in this page.

Field Name	Description
Name	Associated VPN name
Status	Destination network address
Mode	Server or client
IP/Client Number	If the VPN is a client, it displays the IP address allocated by the server. If the VPN is a server, it displays the client number connecting to the server.
Time	The total connection time of this connection

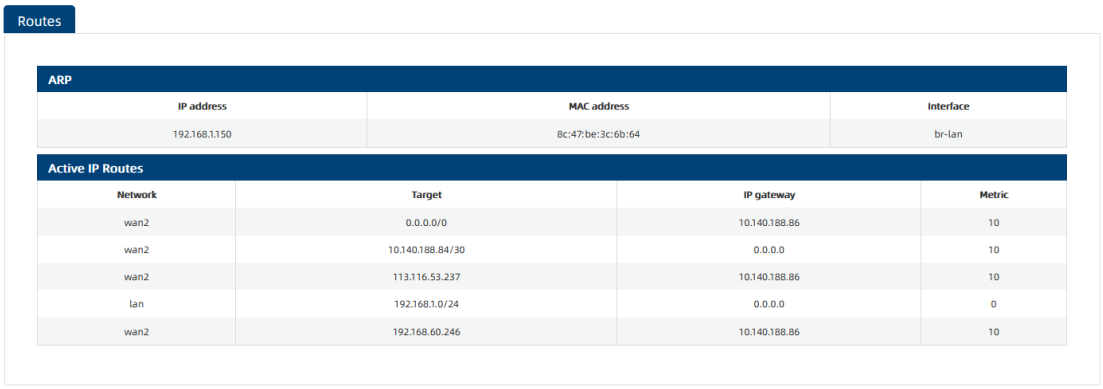
4.1.9 Routes

The **Routes** page displays the router's ARP table and active routes.

The ARP section displays the router's **ARP cache** (also known as ARP table) data. The ARP cache contains information on each known MAC address and its corresponding IP address. When the router receives a packet destined for a local host, the ARP program attempts to find a physical host or MAC address in the ARP cache that matches the IP address. If the ARP cache doesn't contain the needed IP address, ARP broadcasts a request packet to all LAN machines in order to find the device with the IP address in question.

The **Active IP routes** section displays the router's **routing table**. A routing table contains a list of routes to network destinations associated with and known by the router.

The figure below is an example of the ARP and IP routes section:



ARP Parameter description:

Field Name	Value	Description
IP address	ip; Default: none	IP address of a local host
MAC address	mac; Default: none	MAC address of a local host
Interface	string; Default: none	Interface through which the router is associated with the host

Routes Parameter description:

Field Name	Value	Description
Network	string; Default: none	Associated network interface name
Target	ip|ip/netmask; Default: none	Destination network address
IP gateway	ip; Default: none	Indicates the IP address of the gateway through which the target network can be reached
Metric	Integer [0..4,294,967,295]; Default: none	Metrics help the router choose the best route among multiple feasible routes to a destination. The route will go in the direction of the gateway with the lowest metric value

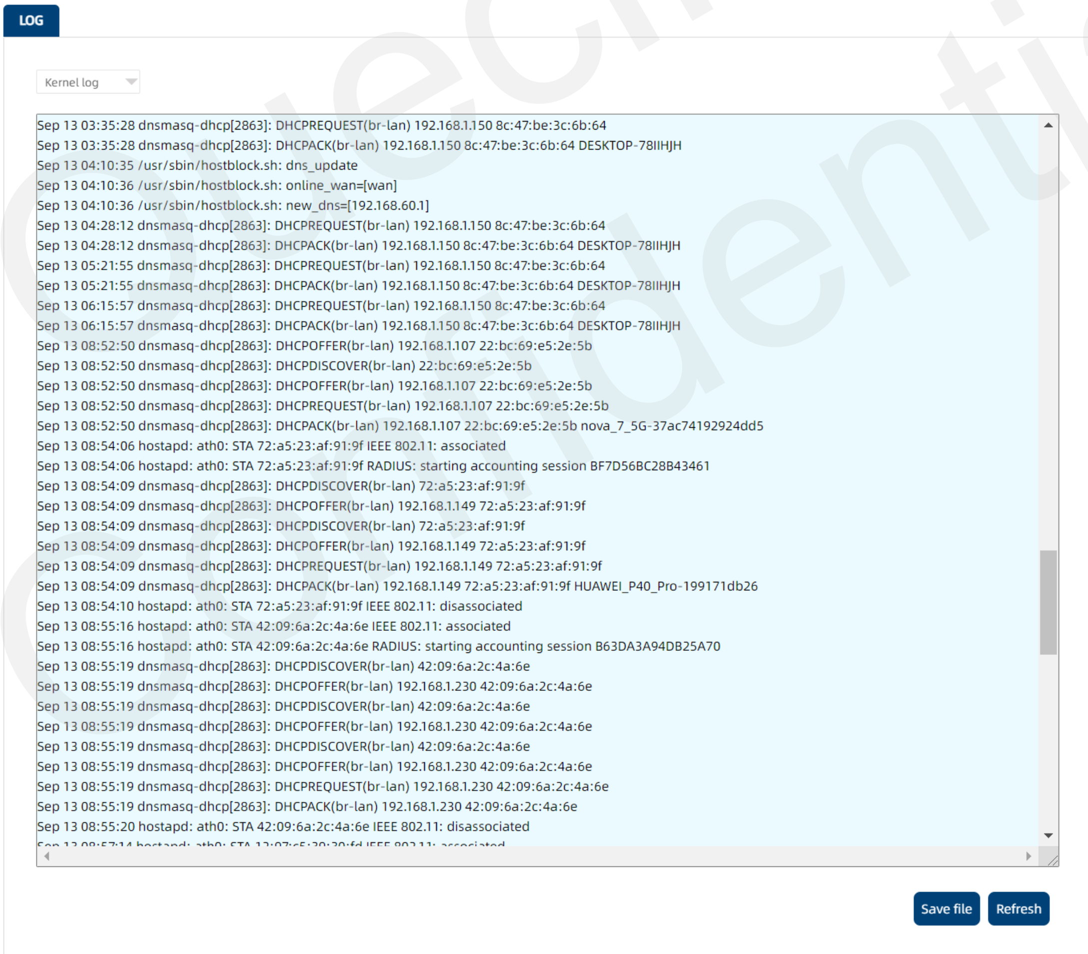
4.1.10 Traffic

The Mobile Traffic section contains graphs that display mobile data usage values over different periods of time. Different tabs of the Mobile Traffic section display mobile data usage values over different periods of time. You can select the period by day, week and month.

The Router accumulates the traffic going through the modem interface; it is not exactly the same as the traffic statistics of operators.

4.1.11 Log Viewer

The Log Viewer page is to display the contents of the router's system log or kernel log. You can select which log file to display with the drop-down box. Refresh button is to refresh the content. You can save the current log as .rar file through the Save button.

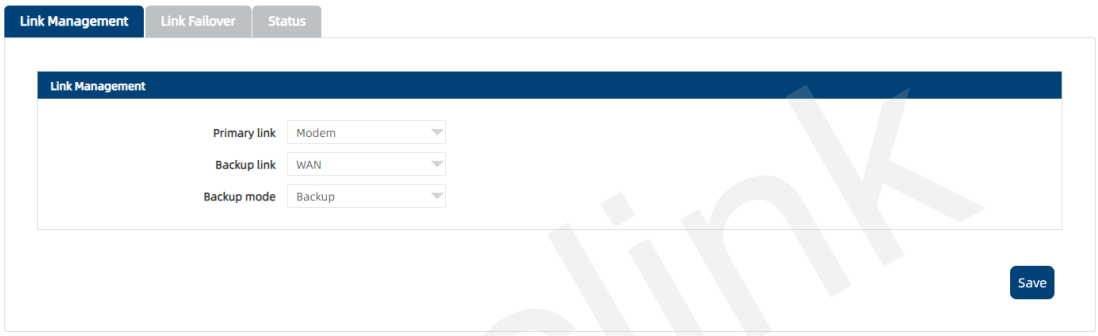


4.2 Network

This section shows you how to configure the network of the Router.

4.2.1 Link Management

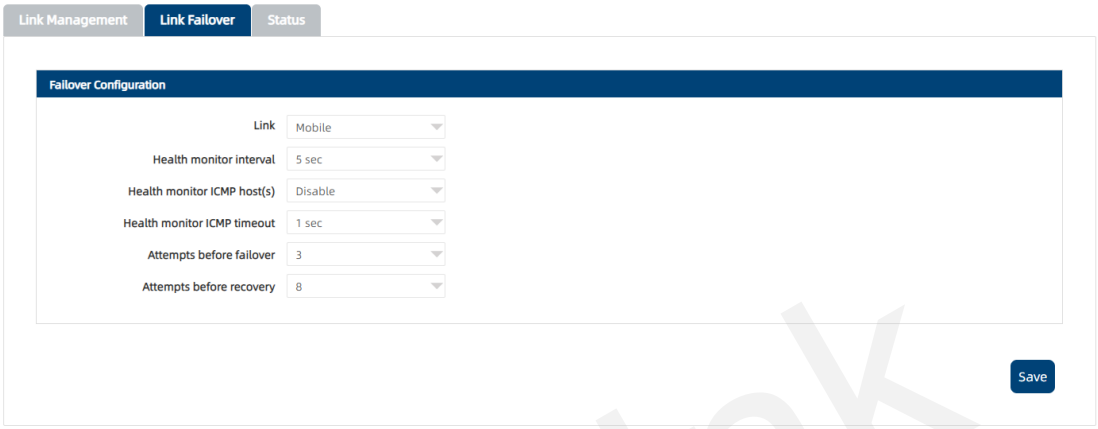
The link management is to manage the WAN connection of the router. The router has three interfaces can work as WAN interface: Mobile, WAN and WLAN (2.4G, station mode). The user can configure one of them as primary link and another one as backup link. If primary link is down, the router can switch to backup link according to the failover configuration. The two links can also work in Load Balancing mode; the router will divide traffic between two interfaces.



Field Name	Value	Description
Primary Link	Modem|WAN|Wi-Fi2.4G	Select from “Modem”, “WAN” or “Wi-Fi2.4G”. Modem: Select to make mobile as the primary link WAN: Select to make WAN as the primary link Wi-Fi2.4G: Select to make Wi-Fi 2.4G as the primary link
Backup Link	None|Modem|WAN|Wi-Fi2.4G	Select from “None”, “Modem”, “WAN” or “Wi-Fi2.4G”. None: Do not select any backup link Modem: Select to make mobile as the backup link WAN: Select to make WAN as the backup link Wi-Fi2.4G: Select to make Wi-Fi2.4G as the backup link
Backup mode	Backup|Load Balancing	Select from “Backup” or “Load Balancing”. Backup: The inactive link is on standby Load Balancing: Use two links

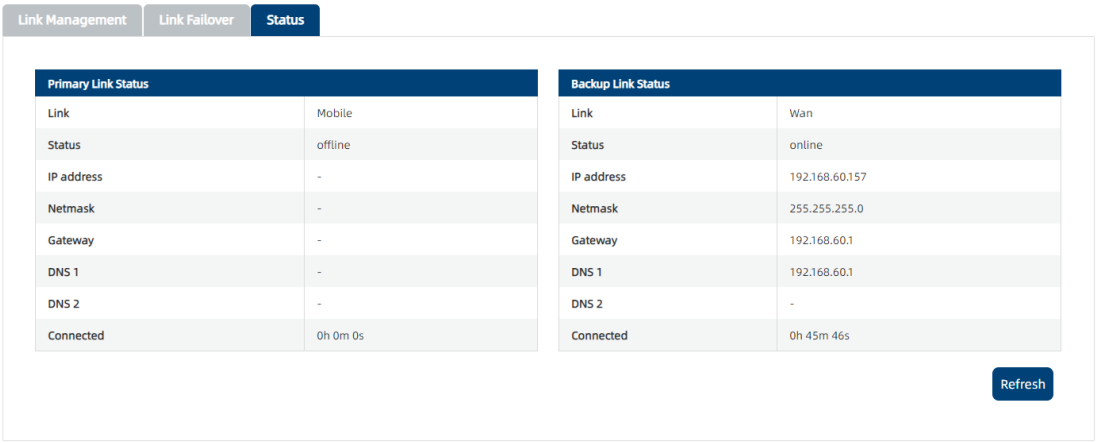
		simultaneously, each link bear specific traffic ratio.

The failover configuration section is to configure the rule of switchover rule. The router uses ICMP to check the status of the link. If link is abnormal, the router will switch to another backup link.



Field Name	Value	Description
Link	Modem|WAN	Associated interface to configure the failover strategy.
Health monitor interval	ip|ip/netmask; Default: none	Destination network address
Health monitor ICMP host(s)	Disable|DNS server|Gateway|Custom	Indicates the host try to ping, select custom to manually configure an IP address to ping.
IPv4 address	integer [0..4,294,967,295]; Default: none	The IP address of the host
Health monitor ICMP timeout	1 sec|3 sec|4 sec|5 sec|10sec	Set the ping timeout.
Attempts before failover	1|3|5|8|15|20	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.
Attempts before recovery	1|3|5|8|15|20	Set the max ping tries. Switch to primary link if the max continuous ping tries reached.

The status page displays the connecting link and parameters of the current connection.



4.2.2 Mobile

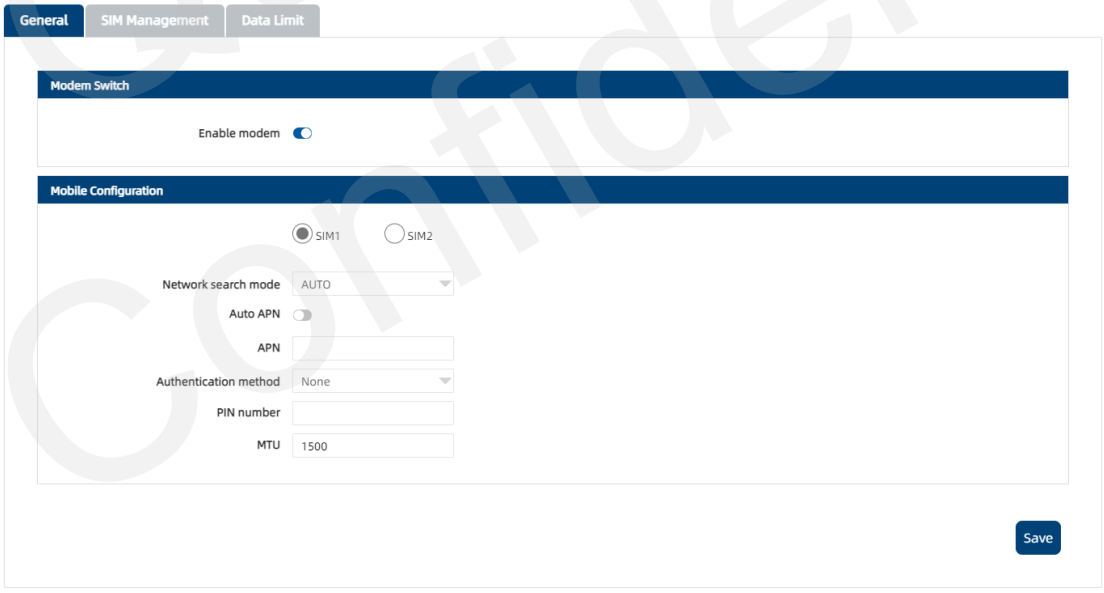
The **Mobile** page is used for setting parameters related to the mobile data connection. There are two SIM slots in the router. Each slot can insert a SIM card, and the user can select one SIM as the primary SIM and allow the switchover between two SIMs.

The Router has a mechanism to automatically detect SIM card and use appropriate dialing parameters in the system. Even if no parameters are configured, the device still can try to automatically dial to establish a connection.

4.2.2.1 General

The **Mobile Configuration** section is used to configure SIM card parameters.

Refer to the figure below for information on the fields contained in the section.



Field	Value	Description
Network search mode	Auto|GSM only|WCDMA only|LTE only; default: Auto	Network connection type preference. Users can specify that only one network is to be searched.

Auto APN	checkbox; default: enabled	Auto APN scans an internal Android APN database and selects an APN based on the SIM card's operator and country. If the first automatically selected APN doesn't work, it attempts to use the next existing APN from the database.
APN	string; default: none	An Access Point Name (APN) is a gateway between a GSM, GPRS, 3G or 4G mobile network and another computer network. Depending on the contract, some operators may require you to use an APN just to complete the registration on a network. In other cases, APN is used to get special parameters from the operator (e.g., a public IP address) depending on the contract. An APN Network Identifier cannot start with any of the following strings: • rac; • lac; • sgsn; • rnc; it cannot end in: • .gprs; and it cannot contain the asterisk symbol (*).
Authentication method	CHAP|PAP|None; default: None	Authentication method that your network carrier uses to authenticate new connections on its network. If you select PAP or CHAP, you will also be required to enter a username and password.
PIN number	string; default: none	A 4-digit long numeric password used to authenticate the modem to the SIM card. **Reminder:** First boot will not reset the PIN number, it must be changed manually
MTU	integer [0..1500]; default: 1500	Sets the maximum transmission unit (MTU) size. It is the largest size of a protocol data unit (PDU) that can be transmitted in a single network layer transaction.

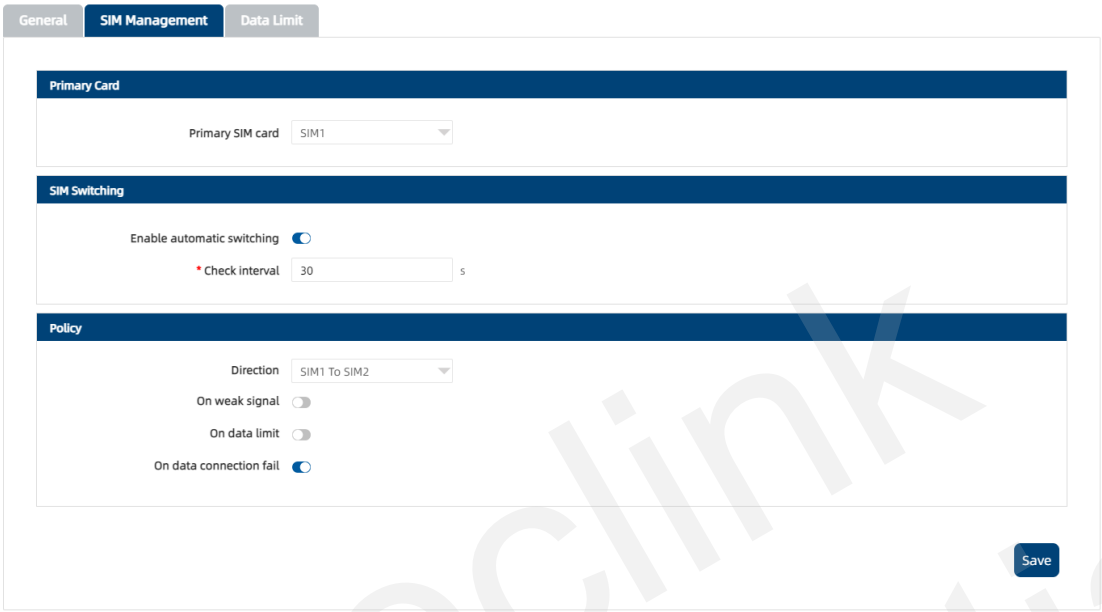
Click Save button to save the configuration and establish the connection.

4.2.2.2 SIM Management

The **SIM Management** section provides you with the function to configure which SIM card is the primary one and which one is slave one, you can setup SIM switching rules between two SIM cards. SIM switching is the failover mechanism when the user has two SIM cards. For example, if the user has two SIM cards with limited data, you can setup a rule that switches the in use SIM card to the slave SIM card when the data limit is reached. You can setup similar rules for signal strength and more.

The **Primary card** section is used to select which SIM slot will host the router's primary SIM card. The primary SIM card is the one which is active by default, while the secondary card stays inactive until switchover happen.

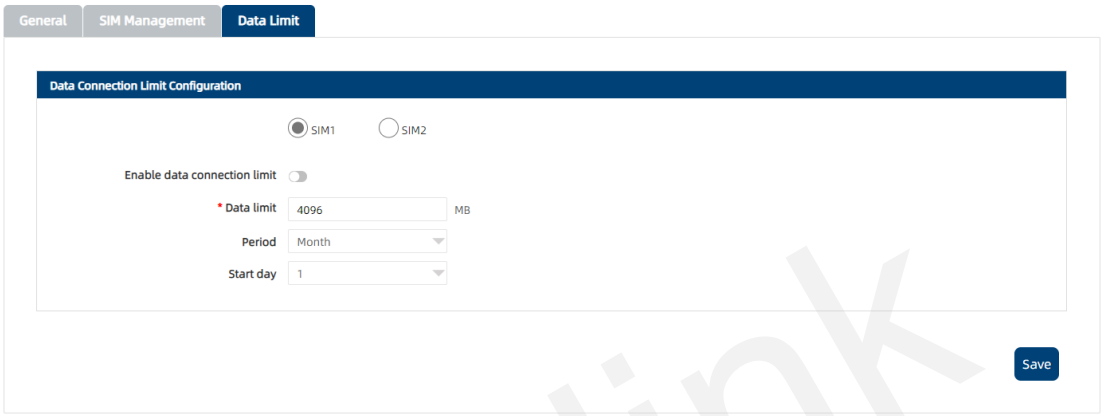
The **SIM switching** section is used to enable automatic SIM switching and to set the SIM switching check interval.



Field	Value	Description
Enable automatic switching*	yes|no; default: no	Turns automatic SIM switching on or off.
Check interval	integer; default: 30	The frequency at which the router will check for condition changes corresponding to SIM switch rules. If such a condition happens, the router will perform a switchover, if not, it will check for the same conditions again after the amount of time specified in this field.
On weak signal	yes|no; default: no	Performs a SIM switch when signal strength value (RSSI in dBm) falls below a specified threshold. When this field is checked you will see an additional field for entering the minimum signal strength value appears.
On data limit	yes|no; default: no	Performs a SIM switch when the SIM card reaches the specified data limit for the designated period. Mobile data limit can be configured in the Services → Mobile → Mobile Data Limit page.
On data connection fail	yes|no; default: no	Performs a SIM switch when the router does establish network connection.

4.2.2.3 Data Limit

The Data Limit section is used to configure custom mobile data limits for your SIM card(s). When the mobile data limit set for the SIM card(s) is reached, the router will no longer use the mobile connection to establish a data connection until the limit period is over or the limit is reset by the user.

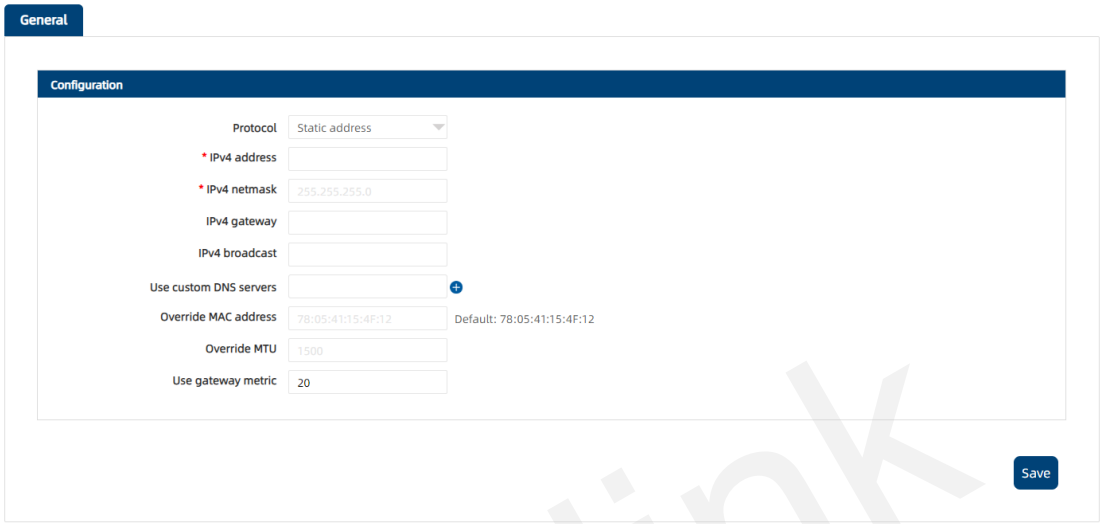


Field	Value	Description
Enable data connection limit	yes|no; default: no	Turns mobile data limitations on or off.
Data limit* (MB)	integer; default: none	The amount of data that is allowed to be downloaded over the specified period of time. When the limit is reached, the router will no longer be able to establish a data connection until the period is over or the data limit is reset. **Note:** after the router has reached the data limit it will not switch to using the secondary SIM card. If you wish to configure a SIM switch system based on received data limit, instructions can be found in the SIM Switching rules section of this page.
Period	Month|Week|Day; default: Month	Data limit period after which the data counter is reset on the specified Start day.
Start day|Start hour	day [1..31]|day [Monday..Sunday]|hour [1..24]; default: day 1	Specifies when the period of counting data usage should begin. After the period is over, the limit is reset and the count begins over again.

4.2.3 WAN

The WAN page is used to configure different protocols for WAN interfaces. The router supports Static, DHCP and PPPoE protocol. You can click Switch Protocol button to display and configure the parameters. The content will change according to which network protocol is selected.

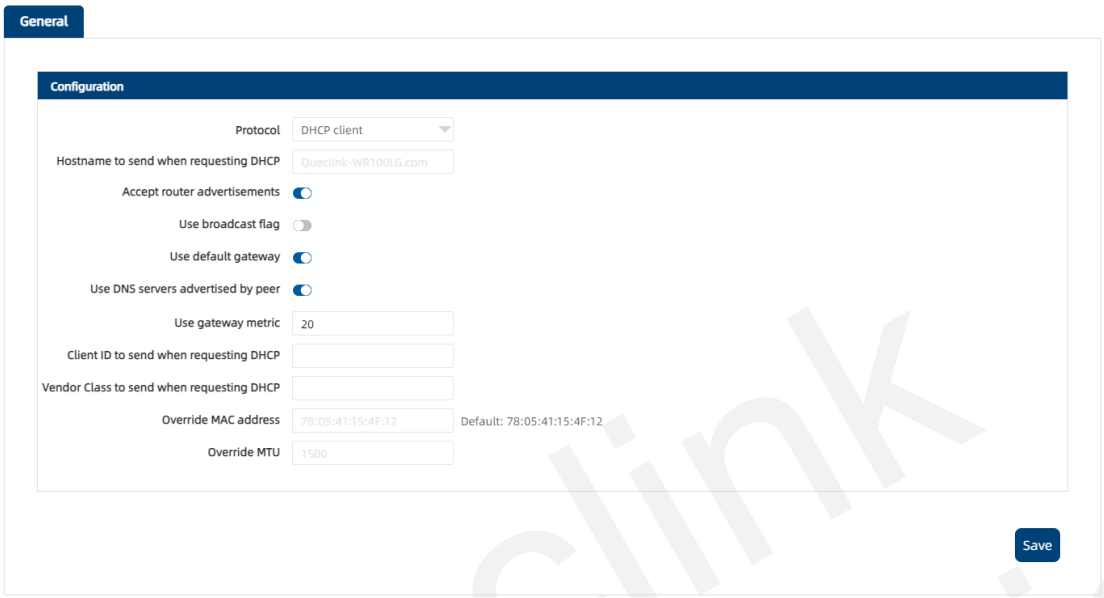
The Static protocol is used when there is no DHCP server available. Therefore, in order to connect to the internet, you configure a static IP address in accordance to that source. The following is an example of static configuration page:



Field Name	Value	Description
Protocol	Static|DHCP|PPPoE; default: **DHCP**	The protocol used by the WAN interface
IPv4 address	ip; default: **none**	Your router's address on the WAN network
IPv4 netmask	ip; default: **255.255.255.0**	Netmask defines how "large" a network is
IPv4 gateway	ip; default: **none**	The address where the router will send all the outgoing traffic
IPv4 broadcast	ip; default: **none**	IP broadcasts are used by BOOTP and DHCP clients to find and send requests to their respective servers
Use custom DNS servers	ip; default: **none**	Custom DNS server configured by user
Override MAC address	mac; default: **router's mac**	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 (i.e., that IP will only work with your computer but not with your router). In this field you can enter your computer's MAC address and fool the gateway into thinking that it is communicating with your computer
Override MTU	integer [0..1500]; default: **1500**	Maximum Transmission Unit (MTU) – specifies the largest possible size of a data packet
Use gateway metric	integer; default: **0**	The WAN configuration by default generates a routing table entry. In this

		field you can alter the metric of that entry. Higher metric means higher priority

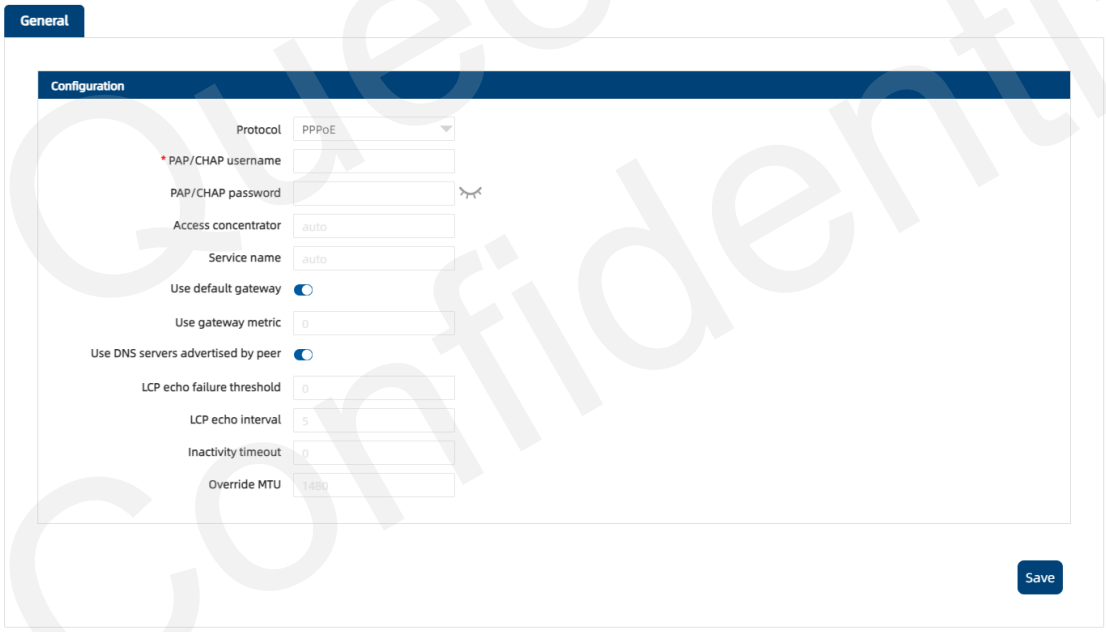
The DHCP protocol should be used when the source of your internet has a DHCP server. The following is an example of DHCP configuration page:



Field Name	Value	Description
Protocol	Static|DHCP|PPPoE; Default: DHCP	The protocol used by the WAN interface
Hostname to send when requesting DHCP	ip | hostname; Default: router's hostname	Host name to which the DHCP request will be sent to
Accept router advertisements	yes|no; Default: yes	Toggles to allow to accept the advertisements from upper router, including link and network parameters
Use broadcast flag	yes|no; Default: no	Required for certain ISPs (Internet Service Providers), e.g. Charter with DOCSIS 3
Use default gateway	yes|no; Default: yes	Uses the default gateway obtained through DHCP. If left unchecked, no default route is configured
Use DNS servers advertised by peer	yes|no; Default: yes	Uses DNS servers obtained from DHCP. If left unchecked, the advertised DNS server addresses are ignored
Use gateway metric	ip; Default: " "	The WAN configuration by default generates a routing table entry. In this field you can alter the metric of that entry. Higher metric means higher priority
Client ID to send when requesting DHCP	string; Default: " "	Client ID which will be sent when requesting a DHCP lease

Vendor class to send when requesting DHCP	string; Default: " "	Vendor class which will be sent when requesting a DHCP lease
Override MAC address	mac; Default: router's mac	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 (i.e., that IP will only work with your computer but not with your router). In this field you can enter your computer's MAC address and fool the gateway into thinking that it is communicating with your computer
Override MTU	integer [0..1500]; Default: 1500	Maximum Transmission Unit (MTU) – specifies the largest possible size of a data packet

The PPPoE protocol is used if you have a DSL internet provider. In this case, you can select the PPPoE protocol to connect with the internet. The following is an example of PPPoE configuration page:

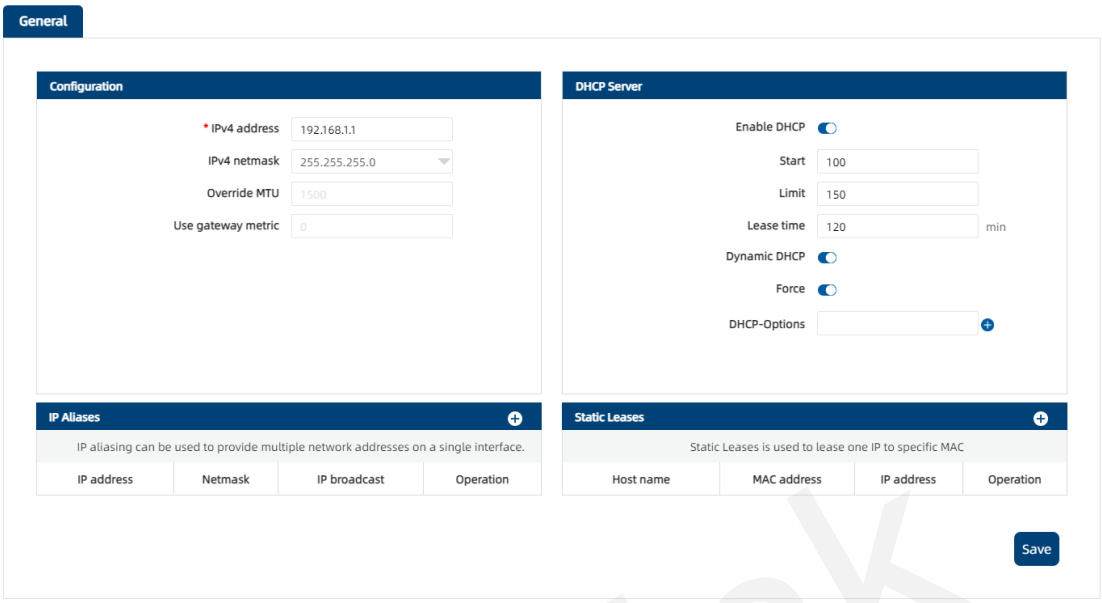


Field Name	Value	Description
Protocol	Static|DHCP|PPPoE; default: **DHCP**	The protocol used by the WAN interface
PAP/CHAP username	string; default: **none**	The username that you use to connect to your carrier's network
PAP/CHAP password	string; default: **none**	The password that you use to connect to your carrier's network
Access concentrator	string; default: **none**	The name of the access concentrator.

		Leave empty to auto detect
Service name	string; default: **none**	The name of the service. Leave empty to auto detect
Use default gateway	yes|no; default: **yes**	Uses the default gateway obtained through DHCP. If left unchecked, no default route is configured
Use gateway metric	integer; default: **0**	The WAN configuration by default generates a routing table entry. In this field you can alter the metric of that entry. Higher metric means higher priority
Use DNS servers advertised by peer	yes|no; default: **yes**	Uses DNS servers obtained from DHCP. If left unchecked, the advertised DNS server addresses are ignored
LCP echo failure threshold	integer; default: **0**	Presumes peer to be dead after given amount of LCP echo failures. Leave it at 0 to ignore failures
LCP echo interval	integer; default: **5**	Sends LCP echo requests at the given interval in seconds. This function is only effective in conjunction with failure threshold
Inactivity timeout	integer; default: **0**	Close inactive connection after the given amount of seconds. Leave it at 0 to persist connection
Override MTU	integer [0..1500]; default: **1500**	Maximum Transmission Unit (MTU) – specifies the largest possible size of a data packet

4.2.4 LAN

This page allows you to set the related parameters for LAN port, such as IP address, IP Netmask, etc. There are four LAN ports on WR100. The following is the example configuration page of LAN port.



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). The router can configure as DHCP server. If you connect a device that has been configured to obtain an IP address automatically, the router will lease out an IP address from the available IP pool and the device will be able to communicate within the private network. You can configure DHCP in DHCP section. Advanced setting is also available in this section.

Static IP leases are used to reserve specific IP addresses for specific devices by binding them to their MAC address. This is useful when you have a stationary device connected to your network that you need to reach frequently, e.g., printer, server, etc. You can configure setting in static leases section.

IP Aliases section allows you to set multi IP address for the router. It is a way of defining or reaching a subnet that works in the same space as the regular network. This is useful if you need to reach the router that is located in the same network but in a different subnet.

Field Name	Value	Description
Configuration		
IP address	ip; Default: 192.168.1.1	IP address that the device uses on the LAN network
IP netmask	ip; Default: 255.255.255.0	A netmask is used to define how “large” the LAN network is
Override MTU	integer [0..1500]; Default: 1500	MTU (Maximum Transmission Unit) specifies the largest possible size of a data packet
Use gateway metric	integer; Default: 0	The LAN configuration generates an entry in the routing table. In this field you can alter the metric of that entry. Higher metric means higher priority
DHCP Server		
DHCP	Enable|Disable|DHCP	Enables or disables DHCP Server. If DHCP

	Relay; Default: Enable	Relay is selected, you will be prompted to enter an IP address of another DHCP server in your LAN. In this case, whenever a new device connects to the router, the router will redirect any DHCP requests to the specified DHCP Server
Start	integer [1..253]; Default: 100	The starting IP address value. e.g., if your router's LAN IP is 192.168.2.1 and your subnet mask is 255.255.255.0 that means that in your network a valid IP address has to be in the range of [192.168.2.0..192.168.2.254] (192.168.2.255 is a special unavailable address). If the Start value is set to 100 then the DHCP server will only lease out addresses starting from 192.168.2.100
Limit	integer [1..4294967296]; Default: 150	How many addresses the DHCP server can lease out. Continuing from the above example: if the start address is 192.168.2.100 and the server can lease out 150 (default limit value), available addresses will be from 192.168.2.100 to 192.168.2.249 (100 + 150 – 1 = 249; this is because the first address is inclusive)
Lease time	time in 'h' (hours) or 'm' (minutes); Default: 12h	The duration of an IP 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. However, if the device stays connected, its lease will be renewed after half of the specified amount of time passes, e.g., if the lease time is 12 hours, then every 6 hours the device will send a request to the DHCP server asking to renew its lease. Lease time can be set in hours (h) or minutes (m). The minimal amount of time that can be specified is 2min (2m)
IP broadcast	ip; Default: " "	IP broadcasts are used by BOOTP and DHCP clients to find and send requests to their respective servers
Dynamic DHCP	yes|no; Default: yes	Enables Dynamic allocation of client addresses. If this is disabled, only clients that have static IP leases will be served

Force	yes|no; Default: no	The DHCP force function ensures that the router will always start it's DHCP server, even if there is another DHCP server already running in the router's network. By default, the router's DHCP server will not start when it is connected to a network segment that already has a working DHCP server
IPv4 netmask	ip; Default: 255.255.255.0	Overrides your LAN netmask, thus making the DHCP server think that it's serving a larger or smaller network than it actually is
DHCP Options	DHCP options; Default: " "	Additional options to be added to the DHCP server. For example with '26,1470' or 'option:mtu, 1470' you can assign an MTU value per DHCP. You can find more information on DHCP Options here.You can add more options by clicking the plus symbol (+) located next to the field

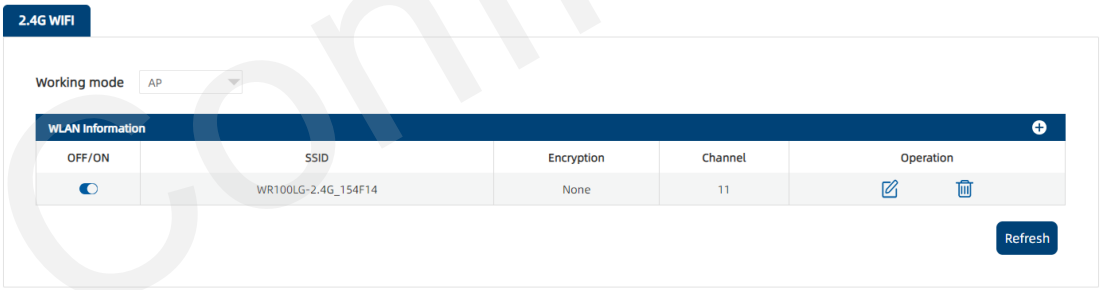
4.2.5 WLAN

WR100 supports IEEE 802.11b/g/n wireless technologies.

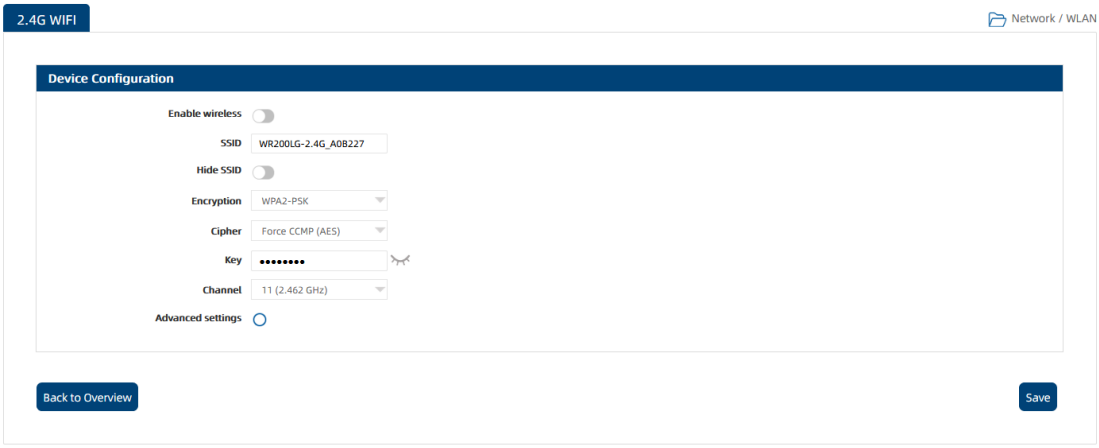
You can configure 2.4GHz as Wi-Fi Access Points (AP) and Wi-Fi Stations (STA). You can select the Wi-Fi mode from the dropdown menu.

a) Wireless Access Point:

The page will display the overview of the Wireless Configuration. It displays all configured access points and stations. You can disable or enable the Wi-Fi interfaces, remove unwanted access points or stations or enter a configuration window of any Wi-Fi interface, where you can configure this interface more comprehensively. You can click the 'Edit' button next to the Wi-Fi interface that you wish to configure to go to the configuration page.

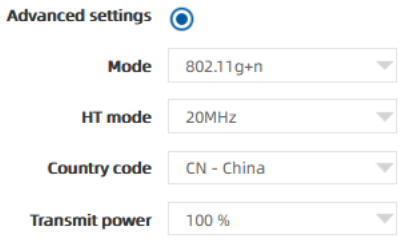


You can configure a Wi-Fi channel according to the busyness of other channels. Use a channel with no other active Access Points and preferably one that has no active Access Point on two adjacent channels on each side as well or set the channel field to auto and the router will pick the least busy channel in your location automatically. **SSID** is the name of your Wi-Fi interface. Wi-Fi client devices can scan the area for Wi-Fi networks will see your network with this name. Hide SSID is used to make your Access Point invisible to other devices. To use a hidden Wi-Fi Access Point, first un-hide it, connect your device to it, then hide it again.



Field Name	Value	Description
SSID	string; default: **none**	Name of a Wi-Fi AP.
Hide SSID	yes|no; Default: **no**	Toggles to make your Access Point invisible to other devices. To use a hidden Wi-Fi Access Point, first un-hide it, connect your device to it, then hide it again.
Encryption*	No encryption|WPA-PSK|WPA2-PSK |WPA-PSK/WPA2-PSK mixed mode; Default: No encryption	The type of Wi-Fi encryption used.
Cipher	Auto|Force CCMP (AES)|Force TKIP|Force TKIP and CCMP (AES); Default: Auto	An algorithm for performing encryption or decryption
Key	string; default: **none**	Pre-shared key, a custom passphrase used for user authentication (at least 8 characters long).
Enable wireless	yes|no; Default: **no**	Toggles to enable or disable this access point.
Channel	1-11	Configure the channel of this Wi-Fi

You can select 'Advanced setting' button to display the advanced parameters. It is used to configure the hardware operating settings of the Wi-Fi radio. The settings available in this section are mostly used to find the best Wi-Fi performance conditions.



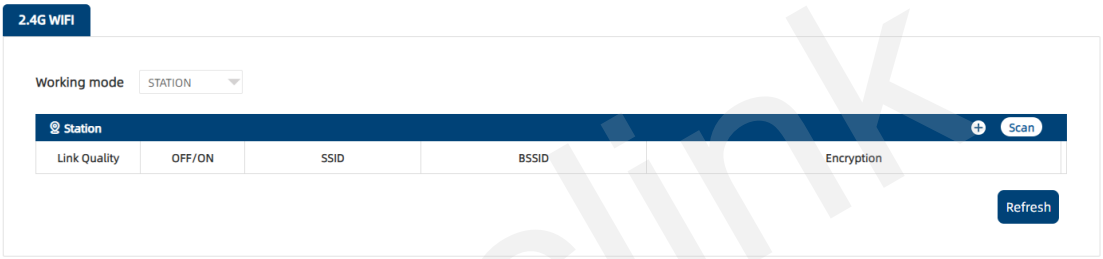
Mode	Auto|802.11b|802.11g|	Wireless protocol used. Different modes

	802.11g+n; Default: 802.11g+n	provide different wireless standard support which directly impacts the radio's throughput performance
Country code	country code; Default: 0 - World	SO/IEC 3166 alpha2 country codes as defined in ISO 3166-1 standard
Transmit power	100%|80%|60%|40%|20%; Default: 100%	Wi-Fi signal power. The percentage of the maximum output power. Reduce the power will reduce the signal coverage.

b) Wireless Station:

WR100 can also work as a Wi-Fi client.

Click Scan button to rescan the surrounding area and try to connect to a new wireless access point.

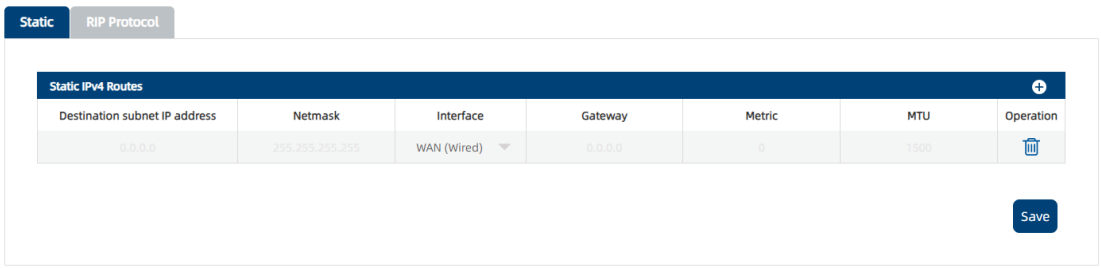


After the scan finishes, you will see a list of Wi-Fi Access Points. Choose one according to your liking and click the Join button next to it, enter the password to connect to that access point.

4.2.6 Routing

4.2.6.1 Static

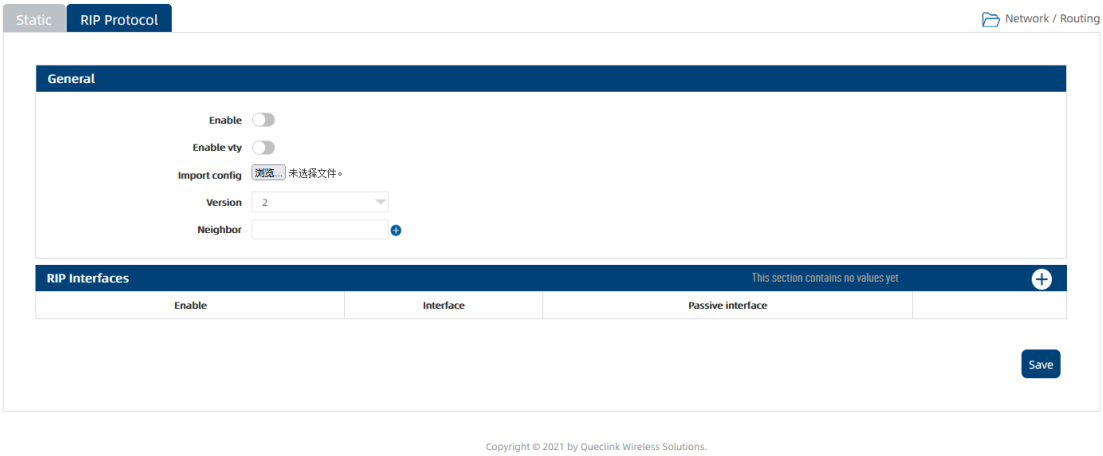
Static routes specify over which interface and gateway a certain host or network can be reached. You can configure your own custom routes in this page. You can configure multi static routes in the router.



Field Name	Value	Description
Destination address*	ip; Default: **0.0.0.0**	The address of the destination network
Netmask*	ip; Default: **0.0.0.0**	A Mask that is applied to the Target to determine to what actual IP addresses the routing rule applies
Interface	LAN|WAN(Wired)| WAN2(Mobile)|WAN3(Wi-Fi) |VPN instances; Default: **WAN(Wired)**	The zone where the target network resides
Gateway	ip; Default: " "	Defines where the router should send all the traffic that applies to the rule
Metric	integer; default: **none**	The **Metric** value is used as a sorting measure. If a packet about to be routed fits two rules, the one with the higher metric is applied.
MTU	integer [0..1500]; default: 1500	Sets the maximum transmission unit (MTU) size. It is the largest size of a protocol data unit (PDU) that can be transmitted in a single network layer transaction.

4.2.6.2 Rip

The **Routing Information Protocol (RIP)** is a distance-vector routing protocol which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. The maximum number of hops allowed for RIP is 15, which limits the size of networks that RIP can support. A hop count over 16 is considered an infinite distance and the route is unreachable.



You can click 'Add' button to a new RIP interface and click 'Save' button to save the configuration.

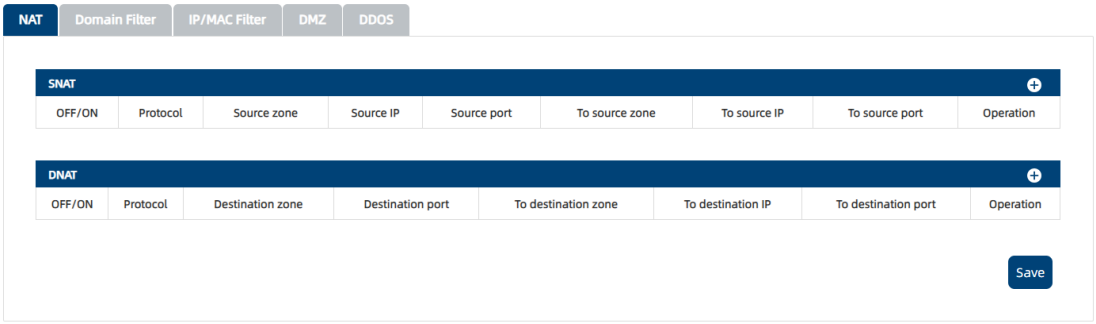
Field Name	Value	Description
Enable	yes|no; Default: **no**	Toggles RIP Protocol ON or OFF
Enable vty	yes|no; Default: **no**	Toggles vty access from LAN ON or OFF
Import config	-	Uses imported RIP configurations
Version	2|1; Default: **2**	Specifies the version of RIP
Neighbor	ip; Default: " "	Neighbor IP address
Enable	yes|no; Default: **no**	Toggles RIP Interface ON or OFF
Interface	network interface; Default: **no**	Network interface to be used with the RIP interface
Passive interface	yes|no; Default: **no**	Sets the specified interface to passive mode. On passive mode interface, all receiving packets are processed as normal and rip does not send either multicast or unicast RIP packets

4.2.7 Firewall

4.2.7.1 NAT

Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more global IP address (SNAT) and vice versa in order to provide Internet access to the local hosts (DNAT). Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table.

The router supports both SNAT (Source NAT) and DNAT (Destination NAT). You can Click ⊕ icon to add a new instance and can configure the setting in the corresponding section. You need to Click Save button to save all parameters you configured.

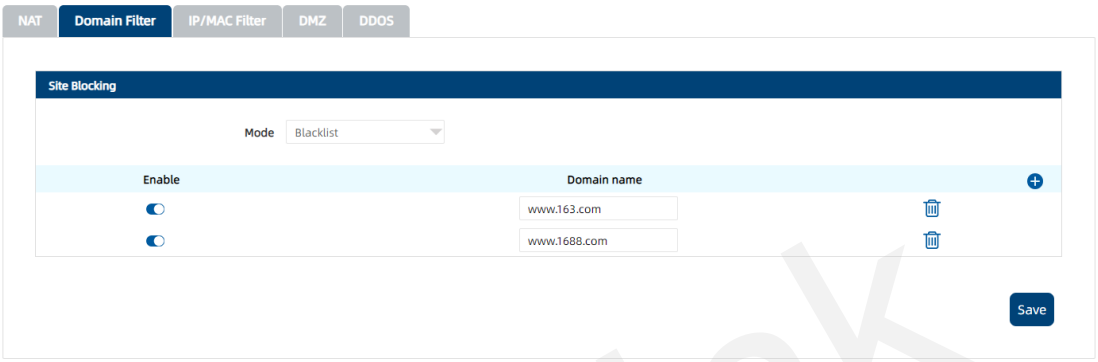


Field Name	Value	Description
OFF/ON	ON|OFF	To turn on/off the section
Protocol	all|tcp|udp|icmp Default: all	Select the protocol to translate the IP and Port.
Source IP	A.B.C.D	The initial IP address to be translated.
Source Port	1~65535	The initial port to be translated
To source zone	LAN|WAN|VPN default: WAN	The source zone of the section
To source zone	lan|modem1| modem2|WAN Default: **Lan**	Interface name, available when initial address type selects “interface”
To source IP	A.B.C.D	The translated IP address
To source Port	1~65535	The translated port

Field Name	Value	Description
OFF/ON	ON|OFF	To turn on/off the section
Protocol	all|tcp|udp|icmp Default: **all**	Select the protocol to translate the IP and Port.
Destination zone	WAN|VPN default: WAN	The destination zone of the section
Destination port	1~65535	The initial port to be translated
To destination zone	LAN default: LAN	The destination zone of the section
To destination IP	A.B.C.D	The translated IP address
To destination Port	1~65535	The translated port

4.2.7.2 Domain Filter

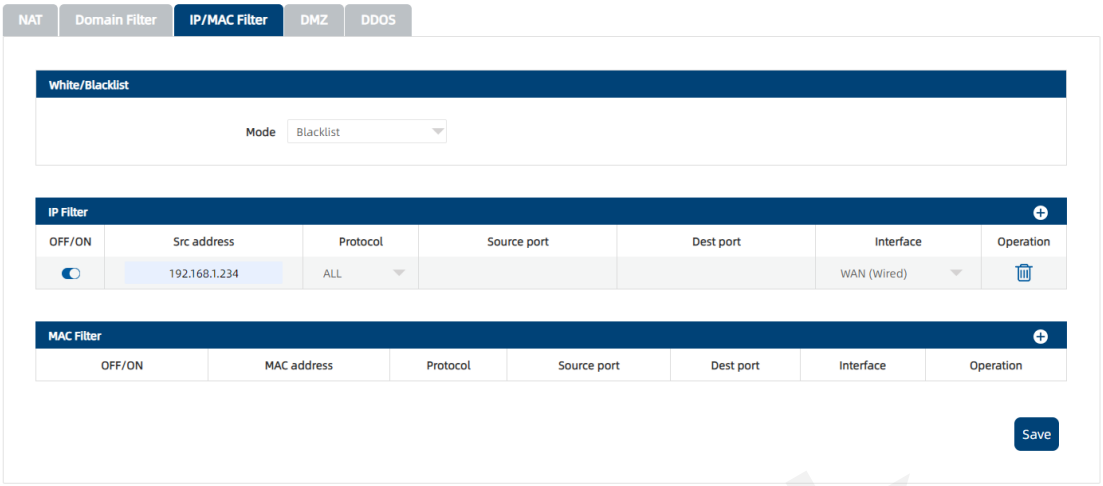
The domain filter function provides you with the possibility to set up lists of wanted or unwanted websites (Blacklists or Whitelists). If the mode is whitelist, the router allows every site included in the list and blocks everything else. If the mode is Blacklist, the router blocks every site included in the list and allows everything else.



Field Name	Value	Description
Enable	yes|no; Default: **no**	Turns Site Blocking on or off.
Mode	Blacklist|Whitelist; Default: **Whitelist**	Mode of operation. • **Whitelist** - allow every site included in the list and block everything else. • **Blacklist** - block every site included in the list and allow everything else.
Hosts list	text file; Default: **none**	Provides a possibility to upload a text file containing a list of hosts instead of adding hosts individually via the WebUI. Different hosts must be separated by line breaks (one host per line) in the text file.
Enable	yes|no; Default: **yes**	Turns an entry of the list to an active or inactive state. Inactive entries are not considered to be a part of the list until they are activated.
Hostname	host; Default: **none**	Website name. The formats accepted are either *www.website.com* or *website.com*, i.e., the protocol and subdomains can be not specified. The rules will also be applicable for the subdomains of the specified site.

4.2.7.3 IP/MAC Filter

The domain filter function provides you an easy way to set up lists of blocking or unblocking client base on IP/MAC address. If the mode is whitelist, the router allows every IP/MAC address included in the list and blocks everything else. If the mode is Blacklist, the router blocks every IP/MAC address included in the list and allows everything else.



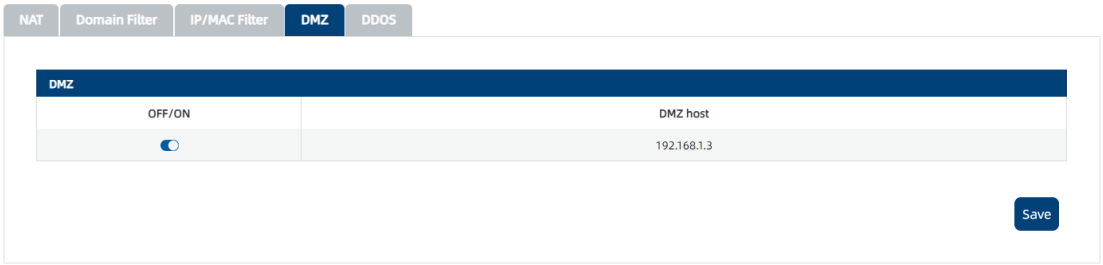
Field Name	Value	Description
Enable	yes|no; Default: **no**	Turns Client Blocking on or off.
Mode	Blacklist|Whitelist; Default: **Whitelist**	Mode of operation. • **Whitelist** - allow every IP/MAC address included in the list and block everything else. • **Blacklist** - block every IP/MAC address included in the list and allow everything else.
Src address	ip; Default: **0.0.0.0**	The IP address of client to be configured.
MAC address	mac; Default: none	The MAC address of client to be configured.
Protocol	All|TCP|UDP|TCP+UDP|ICMP|; Default: **All**	Specifies the protocol to blocked/unblock.
Source Port	integer [0..65535]; default: none	TCP/UDP port number. **Note:** traffic on the selected port will be automatically allowed in the router's firewall rules.
Dest Port	integer [0..65535]; default: none	TCP/UDP port number. **Note:** traffic on the selected port will be automatically allowed in the router's firewall rules.
Interface	WAN(Wired)| WAN2(Mobile) default: WAN(Wired)	Interface to block/unblock this IP/MAC address

4.2.7.4 DMZ

A DMZ (Demilitarized Zone), is a perimeter network that enables organizations to protect their internal networks. It enables organizations to provide access to untrusted networks, such as the internet, while keeping private networks or local-area networks (LANs) secure.

By enabling DMZ for a specific internal host, you will expose that host and its services to the

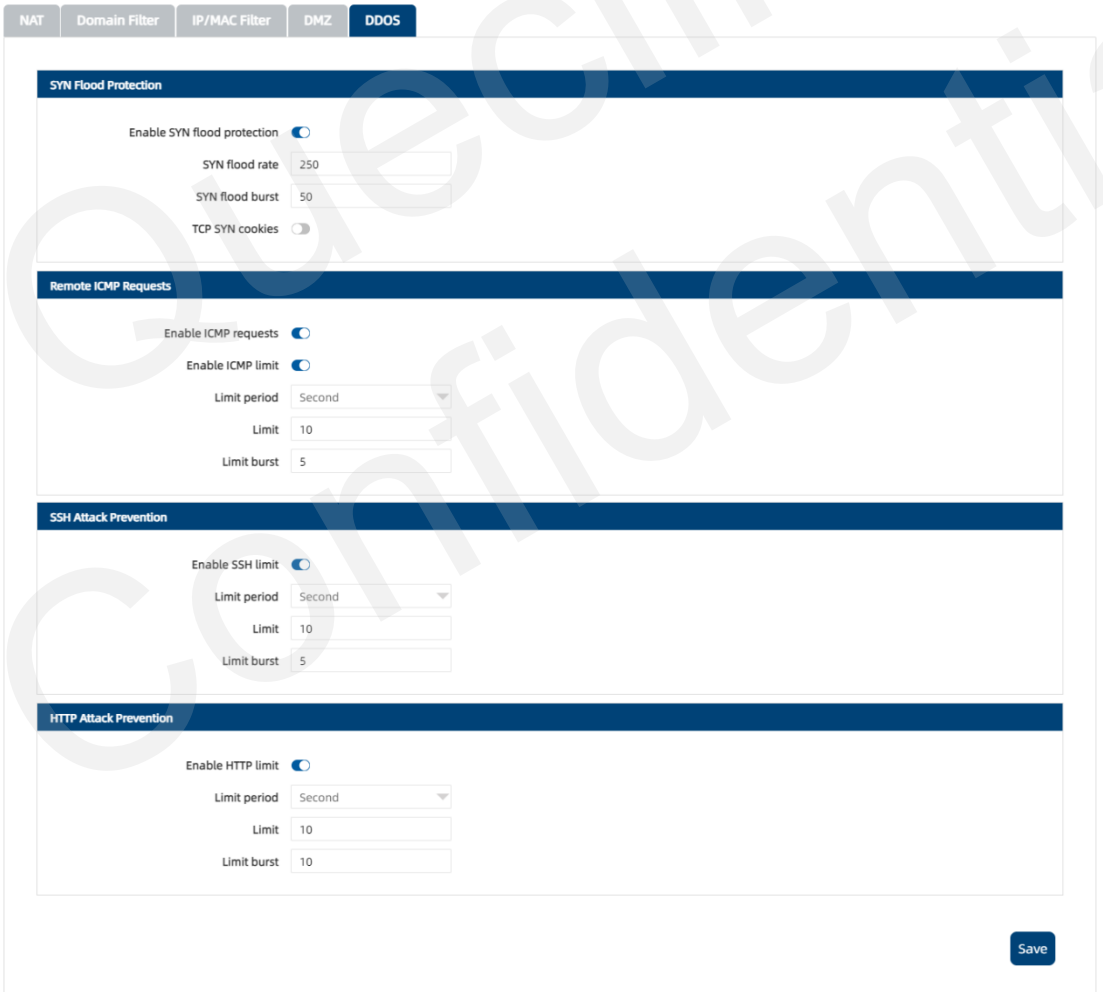
external network.



Field Name	Value	Description
OFF/ON	yes|no; Default: **no**	Toggles DMZ On or Off
DMZ host	ip; Default: " "	Internal host to which the DMZ rule will be applied

4.2.7.5 DDOS

The DDOS Prevention page allows you to set up protections from various types of DDOS attacks. You will find information on all of these methods below.



SYN Flood Protection:

SYN Flood Protection allows you to protect yourself 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 over-saturation.

Remote ICMP Requests:

Some attackers use ICMP echo request packets directed to IP broadcast addresses from remote locations to generate denial-of-service attacks. You can set up some custom restrictions to help protect your router from ICMP bursts.

SSH Attack Prevention:

Prevent SSH (allows a user to run commands on a machine's command prompt without them being physically present near the machine) attacks by limiting connections in a defined period.

HTTP Attack Prevention:

An HTTP attack sends 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 (e.g. 1 byte/100 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.

4.3 Services

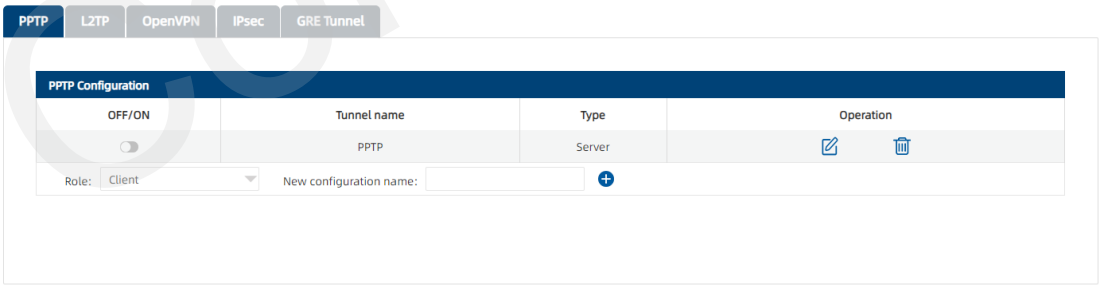
This section shows you how to configure the service applications of the Router.

4.3.1 VPN

A virtual private network (VPN), is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. WR100 router provides multiple VPN functions, which can be applied in different industries and application.

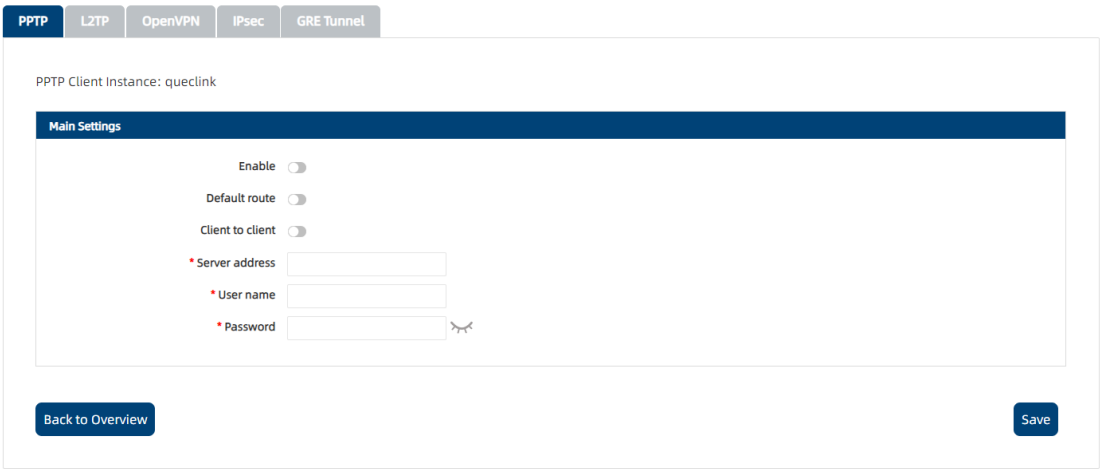
4.3.1.1 PPTP

Point-to-Point Tunneling Protocol (**PPTP**) is a type of VPN protocol that uses a TCP control channel and a Generic Routing Encapsulation tunnel to encapsulate PPP packets.



PPTP client:

A **PPTP client** is an entity that initiates a connection to a PPTP server. Select *Role as Client*, enter a custom name and click the Add icon to create a new client instance, then click edit icon to go to PPTP client configuration page. You can click edit button on the right to edit an existing PPTP instance.

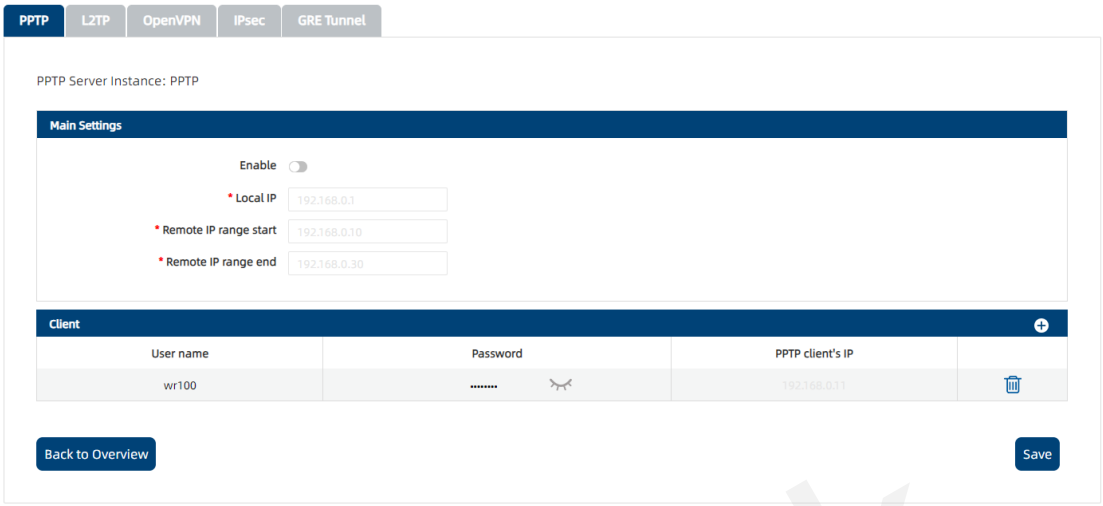


Refer to the figure and table below for information on the PPTP client's configuration fields:

Field Name	Value	Description
Enable	yes|no; default: no	Turns the PPTP instance on or off.
Use as default gateway	yes|no; default: no	When turned on, this connection will become the router's default route. This means that all traffic directed to the Internet will go through the PPTP server and the server's IP address will be seen as this device's source IP to other hosts on the Internet. **Note:** this can only be used when WAN Failover is turned off.
Client to client	yes|no; default: no	Adds a route that makes other PPTP clients accessible within the PPTP network.
Server	ip|host; default: none	IP address or hostname of a PPTP server.
Username	string; default: none	Username used for authentication to the PPTP server.
Password	string; default: none	Password used for authentication to the PPTP server.

PPTP server:

An **PPTP server** is an entity that waits for incoming connections from PPTP clients. To create a new server instance, select Role as Server, enter a custom name and click the Add icon to create a new server instance, then click edit icon go to PPTP server configuration page. You can click edit button to edit an existing PPTP instance. Only one PPTP server instance is allowed to be added. A server needs to have a public IP address in order to be available from the public network (the Internet).

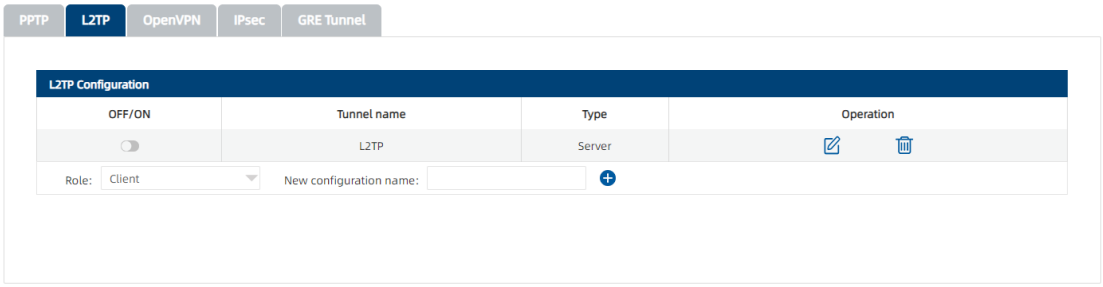


Refer to the figure and table below for information on the PPTP client's configuration fields:

Field Name	Value	Description
Enable	yes|no; default: no	Turns the PPTP instance on or off.
Local IP	ip; default: 192.168.0.1	IP address of this PPTP network interface.
Remote IP range start	ip; default: 192.168.0.20	PPTP IP address leases will begin from the address specified in this field.
Remote IP range end	ip; default: 192.168.0.30	PPTP IP address leases will end with the address specified in this field.
User name	string; default: youruser	Username used for authentication to this PPTP server.
Password	string; default: yourpass	Password used for authentication to this PPTP server.
PPTP Client's IP	ip; default: none	Assigns an IP address to the client that uses the adjacent authentication info. This field is optional and if left empty the client will simply receive an IP address from the IP pool defined above.

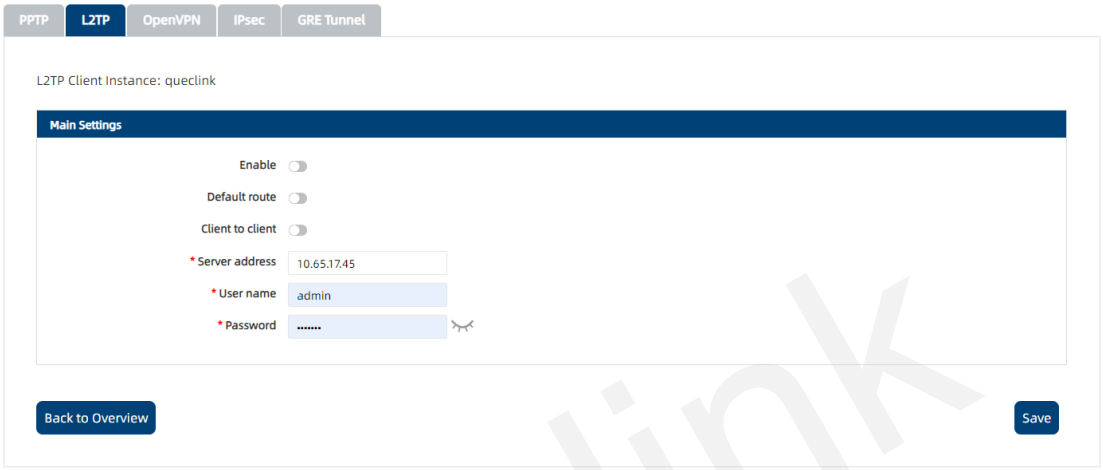
4.3.1.2 L2TP

Layer 2 Tunneling Protocol (**L2TP**) is a tunneling protocol used to support virtual private networks (VPNs). It can work as client or server mode.



L2TP client:

An L2TP client is an entity that initiates a connection to an L2TP server. To create a new client instance, select Role as Client, enter a custom name and click the Add icon to create a new instance, then click Edit icon to go to L2TP client configuration page. You can click Edit icon on the right to edit an existing L2TP instance.

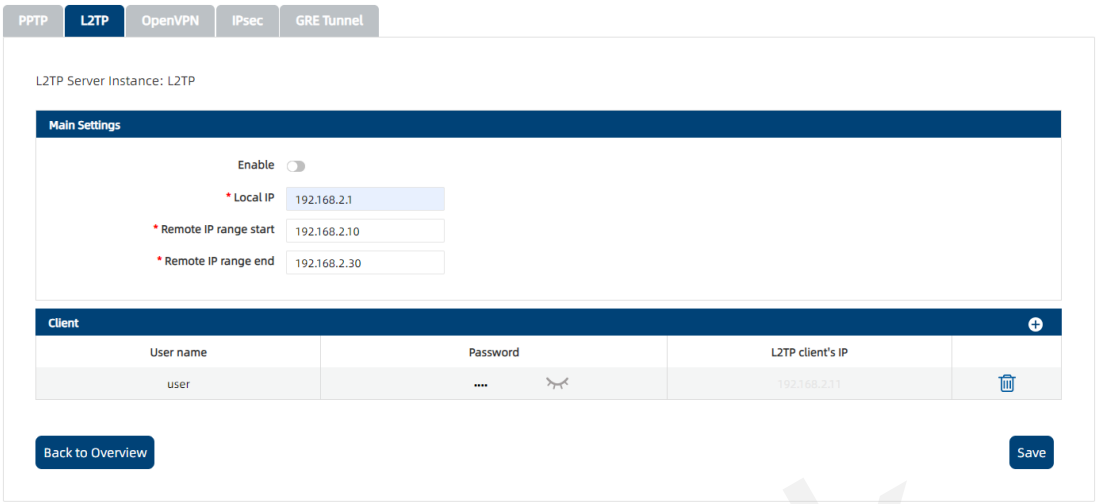


Refer to the figure and table below for information on the L2TP client's configuration fields:

Field Name	Value	Description
Enable	yes|no; default: no	Turns the L2TP instance on or off.
Keep alive	integer; default: none	Frequency (in seconds) at which LCP echo requests are sent to the remote instance in order to determine the health of the connection.
Server	ip|host; default: none	IP address or hostname of an L2TP server.
Username	string; default: none	Username used for authentication to the L2TP server.
Password	string; default: none	Password used for authentication to the L2TP server.
Default route	yes|no; default: no	When turned on, this connection will become the router's default route. This means that all traffic directed to the Internet will go through the L2TP server and the server's IP address will be seen as this device's source IP to other hosts on the Internet. **Note:** this can only be used when WAN Failover is turned off.

L2TP server:

An **L2TP server** is an entity that waits for incoming connections from L2TP clients. To create a new server instance, select Role as Server, enter a custom name and click the Add icon to go to L2TP server configuration page. You can click edit icon to edit an existing L2TP instance. Only one L2TP server instance is allowed to be added. A server needs to have a public IP address in order to be available from the public network (the Internet).

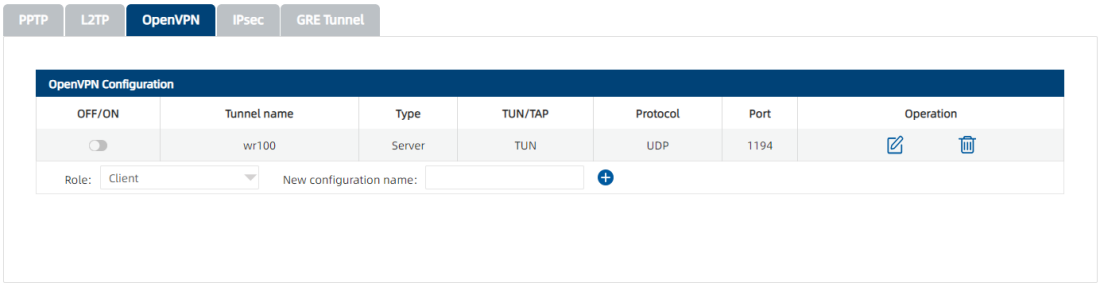


Refer to the figure and table below for information on the L2TP client's configuration fields:

Field Name	Value	Description
Enable	yes|no; default: no	Turns the L2TP instance on or off.
Local IP	ip; default: 192.168.0.1	IP address of this L2TP network interface.
Remote IP range begin	ip; default: 192.168.0.20	L2TP IP address leases will begin from the address specified in this field.
Remote IP range end	ip; default: 192.168.0.30	L2TP IP address leases will end with the address specified in this field.
User name	string; default: user	Username used for authentication to this L2TP server.
Password	string; default: pass	Password used for authentication to this L2TP server.
L2TP Client's IP	ip; default: none	Assigns an IP address to the client that uses the adjacent authentication info. This field is optional and if left empty the client will simply receive an IP address from the IP pool defined above.

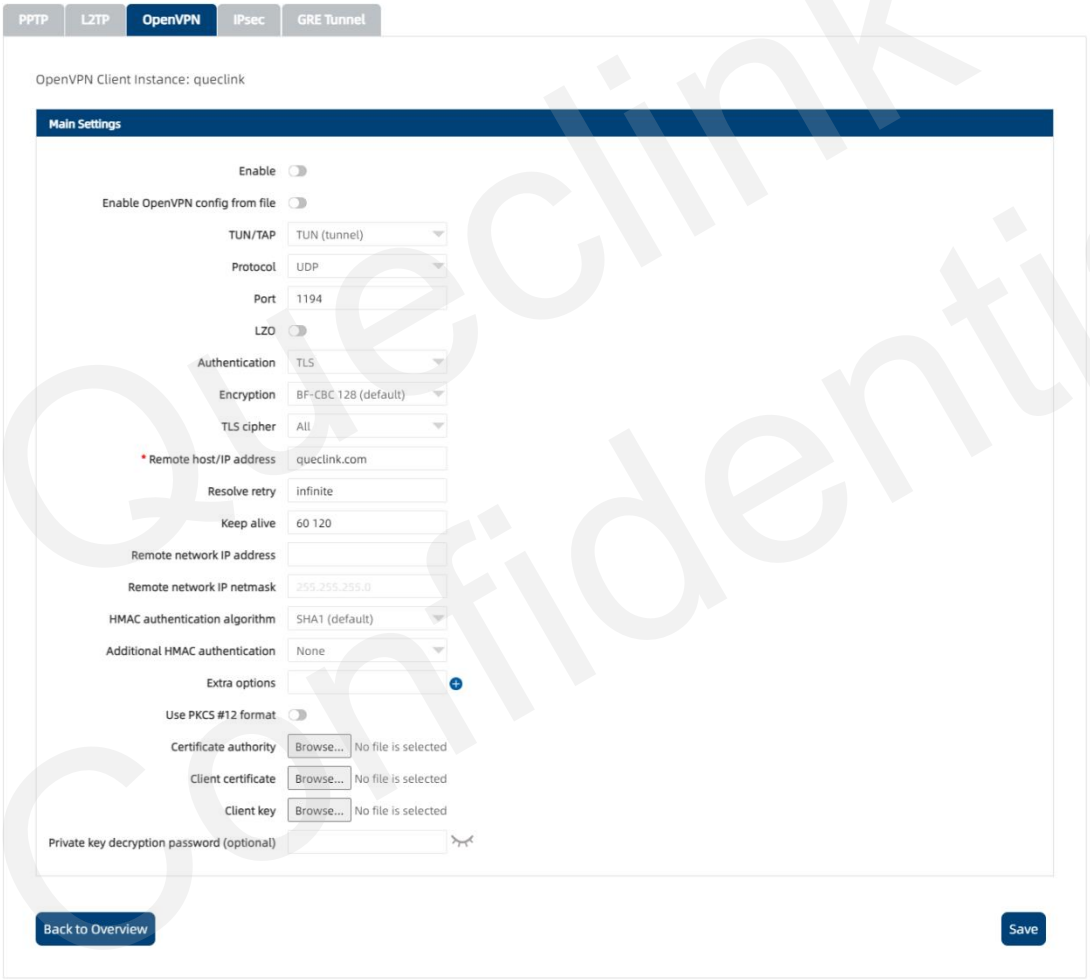
4.3.1.3 OPENVPN

OpenVPN is an open-source software application that implements virtual private network (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.



OpenVPN client:

An OpenVPN client is an entity that initiates a connection to an OpenVPN server. To create a new client instance, select Role as Client, enter a custom name and click the Add icon to go to OpenVPN client configuration page. You can click edit icon on the right to edit an existing OpenVPN instance. A maximum of six OpenVPN client instances are allowed to be added.



Field Name	Value	Description
Enable OpenVPN config from file	yes|no; default: no	Enables custom OpenVPN configuration from file.
Enable	yes|no; default: no	Turns the OpenVPN instance on or off.
TUN/TAP	TUN (tunnel)|TAP (bridged); default: TUN (tunnel)	Virtual network device type. TUN - a virtual point-to-point IP link which operates at the network layer (OSI layer 3),

		used when routing is required. TAP - a virtual Ethernet adapter (switch), operates at the data link layer (OSI layer 2), used when bridging is required.
Protocol	UDP|TCP; default: UDP	Transfer protocol used for the OpenVPN connection. Transmission Control Protocol (TCP) - most commonly used protocol in the Internet Protocol (IP) suite. It ensures the recipient will receive packets in the order they were sent by numbering, analyzing response messages, checking for errors and resending them if an issue occurs. It should be used when reliability is crucial (for example, in file transfer). User Datagram Protocol (UDP) - packets are sent to the recipient without error-checking or back-and-forth quality control, meaning that when packets are lost, they are gone forever. This makes it less reliable but faster than TCP; therefore, it should be used when transfer speed is crucial (for example, in video streaming, live calls).
Port	integer [0..65535]; default: 1194	TCP/UDP port number used for the connection. Make sure it matches the port number specified on the server side. **Note:** traffic on the selected port will be automatically allowed in the router's firewall rules.
LZO	yes|no; default: no	Turns LZO data compression on or off.
Authentication	TLS|Static Key| Password| TLS/Password; default: TLS	Authentication mode, used to secure data sessions. Static key is a secret key used for server–client authentication. TLS authentication mode uses X.509 type certificates: Certificate Authority (CA) Client certificate Client key All mentioned certificates can be generated using OpenVPN or Open SSL utilities on any type of host machine. One of the most popular utilities used for this purpose is called Easy-RSA. Password is a simple username/password

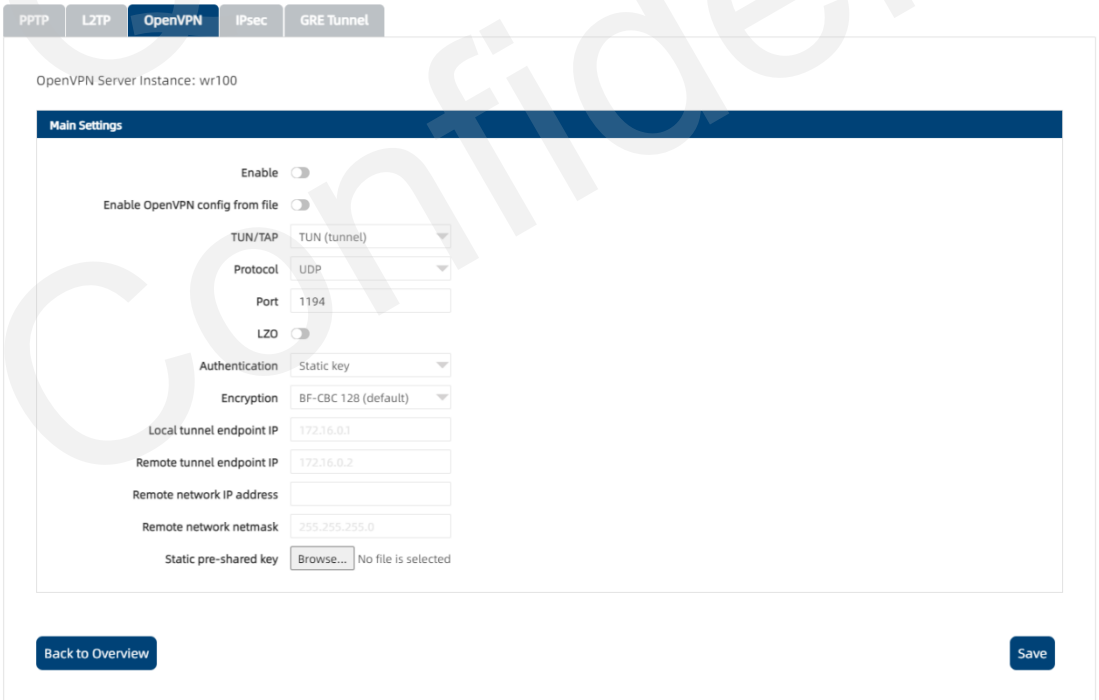
		based authentication where the owner of the OpenVPN server provides the login data. TLS/Password uses both TLS and username/password authentication.
Encryption	DES-CBC 64|RC2-CBC 128|DES-EDE-CBC 128|DES-EDE3-CBC 192|DESX-CBC 192|RC2-40-CBC 40|CAST5-CBC 128|RC2-64-CBC 64|AES-128-CFB 128|AES-128-CFB1 128|AES-128-CFB8 128|AES-128-OFB 128|AES-128-CBC 128|AES-128-GCM 128|AES-192-CFB 192|AES-192-CFB1 192|AES-192-CFB8 192|AES-192-OFB 192|AES-192-CBC 192|AES-192-GCM 192|AES-256-CFB 256|AES-256-CFB1 256|AES-256-CFB8 256|AES-256-OFB 256|AES-256-CBC 256|AES-256-GCM 256|none; default: BF-CBC 128	Algorithm used for packet encryption.
TLS: TLS cipher	All|DHE+RSA|Custom; default: All	Packet encryption algorithm cipher.
TLS: Allowed TLS ciphers	All|DHE+RSA|Custom; default: All	A list of TLS ciphers accepted for this connection.
Remote host/IP address	ip; default: none	IP address or hostname of an OpenVPN server.
Resolve retry	integer|infinite; default: infinite	In case server hostname resolve fails, this field indicates the amount of time (in seconds) to retry the resolve. Specify infinite to retry indefinitely.
Keep alive	two integers separated by a space; default: none	Defines two-time intervals: the first is used to periodically send ICMP requests to the OpenVPN server, the second one defines a

		time window, which is used to restart the OpenVPN service if no ICMP response is received during the specified time slice. When this value is specified on the OpenVPN server, it overrides the 'keep alive' values set on client instances. Example: 10 120
Static key: Local tunnel endpoint IP	ip; default: none	IP address of the local OpenVPN network interface.
Static key: Remote tunnel endpoint IP	ip; default: none	IP address of the remote OpenVPN network (server) interface.
Remote network IP address	ip; default: none	LAN IP address of the remote network (server).
Remote network IP netmask	netmask; default: none	LAN IP subnet mask of the remote network (server).
Password: User name	string; default: none	Username used for authentication to the OpenVPN server.
Password: Password	string; default: none	Password used for authentication to the OpenVPN server.
Extra options	string; default: none	Extra OpenVPN options to be used by the OpenVPN instance.
Use PKCS #12 format	yes|no; default: no	Use PKCS #12 archive file format to bundle all the members of a chain of trust.
PKCS #12 passphrase	string; default: none	Passphrase to decrypt PKCS #12 certificates.
PKCS #12 certificate chain	string; default: none	Uploads PKCS #12 certificate chain file.
TLS/Password: HMAC authentication algorithm	none|SHA1|SHA256|SHA384|SHA512; default: SHA1	HMAC authentication algorithm type.
TLS/Password: Additional HMAC authentication	none|Authentication only (tls-auth)|Authentication and encryption (tls-crypt); default: none	An additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks.
TLS/Password: HMAC authentication key	.key file; default: none	Uploads an HMAC authentication key file.
TLS/Password: HMAC key direction	0|1|none; default: 1	The value of the key direction parameter should be complementary on either side (client and server) of the connection. If one side uses 0, the other side should use 1, or

		both sides should omit the parameter altogether.
TLS/Password: Certificate authority	.ca file; default: none	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.
TLS: Client certificate	.crt file; default: none	Client certificate is a type of digital certificate that is used by client systems to make authenticated requests to a remote server. Client certificates play a key role in many mutual authentication designs, providing strong assurances of a requester's identity.
TLS: Client key	.key file; default: none	Authenticates the client to the server and establishes precisely who they are.
TLS: Private key decryption password (optional)	string; default: none	A password used to decrypt the server's private key. Use only if server's .key file is encrypted with a password.
Static key: Static pre-shared key	.key file; default: none	Uploads a secret key file used for server–client authentication.

OpenVPN server:

An **OPENVPN server** is an entity that waits for incoming connections from OpenVPN clients. To create a new server instance, select Role as Server, enter a custom name and click the 'Add New' button to go to OpenVPN server configuration page. You can click edit button to edit an existing OpenVPN instance. Only one OpenVPN server instance is allowed to be added.



Field Name	Value	Description
Enable OpenVPN config from file	yes|no; default: no	Enables custom OpenVPN configuration from file.
Enable	yes|no; default: no	Turns the OpenVPN instance on or off.
TUN/TAP	TUN (tunnel)|TAP (bridged); default: TUN (tunnel)	Virtual network device type. TUN - a virtual point-to-point IP link which operates at the network layer (OSI layer 3), used when routing is required. TAP - a virtual Ethernet adapter (switch), operates at the data link layer (OSI layer 2), used when bridging is required.
Protocol	UDP|TCP; default: UDP	Transfer protocol used for the connection. Transmission Control Protocol (TCP) - most commonly used protocol in the Internet Protocol (IP) suite. It ensures the recipient will receive packets in the order they were sent by numbering, analyzing response messages, checking for errors and resending them if an issue occurs. It should be used when reliability is crucial (for example, file transfer). User Datagram Protocol (UDP) - packets are sent to the recipient without error-checking or back-and-forth quality control, meaning that when packets are lost, they are gone forever. This makes it less reliable but faster than TCP; therefore, it should be used when transfer speed is crucial (for example, video streaming, live calls).
Port	integer [0..65535]; default: 1194	TCP/UDP port number used for the connection. Make sure it matches the port number specified on the server side. **Note:** traffic on the selected port will be automatically allowed in the router's firewall rules.
LZO	yes|no; default: no	Turns LZO data compression on or off.
Authentication	TLS|Static Key|TLS/Password; default: TLS	Authentication mode, used to secure data sessions. Static key is a secret key used for server–client authentication. TLS authentication mode uses X.509 type certificates: Certificate Authority (CA) Client certificate Client key

		All mentioned certificates can be generated using OpenVPN or Open SSL utilities on any type of host machine. One of the most popular utilities used for this purpose is called Easy-RSA. TLS/Password uses both TLS and username/password authentication.
Encryption	DES-CBC 64|RC2-CBC 128|DES-EDE-CBC 128|DES-EDE3-CBC 192|DESX-CBC 192|RC2-40-CBC 40|CAST5-CBC 128|RC2-64-CBC 64|AES-128-CFB 128|AES-128-CFB1 128|AES-128-CFB8 128|AES-128-OFB 128|AES-128-CBC 128|AES-128-GCM 128|AES-192-CFB 192|AES-192-CFB1 192|AES-192-CFB8 192|AES-192-OFB 192|AES-192-CBC 192|AES-192-GCM 192|AES-256-CFB 256|AES-256-CFB1 256|AES-256-CFB8 256|AES-256-OFB 256|AES-256-CBC 256|AES-256-GCM 256|none; default: BF-CBC 128	Algorithm used for packet encryption.
Static key: Local tunnel endpoint IP	ip; default: none	IP address of the local OpenVPN network interface.
Static key: Remote tunnel endpoint IP	ip; default: none	IP address of the remote OpenVPN network (client) interface.
Static key: Remote network IP address	ip; default: none	LAN IP address of the remote network (client).
Static key: Remote network IP netmask	netmask; default: none	LAN IP subnet mask of the remote network (client).
TLS/TLS/Password: TLS cipher	All|DHE+RSA |Custom; default: All	Packet encryption algorithm cipher.

TLS/Password: Allowed TLS ciphers	All|DHE+RSA |Custom; default: All	A list of TLS ciphers accepted for this connection.
TLS/TLS/Password: Client to client	yes|no; default: no	Allows OpenVPN clients to communicate with each other on the VPN network.
TLS/TLS/Password: Keep alive	two integers separated by a space; default: none	Defines two-time intervals: the first is used to periodically send ICMP requests to the OpenVPN server, the second one defines a time window, which is used to restart the OpenVPN service if no ICMP response is received during the specified time slice. When this value is specified on the OpenVPN server, it overrides the 'keep alive' values set on client instances. Example: 10 120
TLS/TLS/Password: Virtual network IP address	ip; default: none	IP address of the OpenVPN network.
TLS/TLS/Password: Virtual network netmask	netmask; default: none	Subnet mask of the OpenVPN network.
TLS/TLS/Password: Push option	OpenVPN options; default: none	Push options are a way to "push" routes and other additional OpenVPN options to connecting clients.
TLS/TLS/Password: Allow duplicate certificates	yes|no; default: no	When enabled allows multiple clients to connect using the same certificates.
Use PKCS #12 format	yes|no; default: no	Use PKCS #12 archive file format to bundle all the members of a chain of trust.
PKCS #12 passphrase	string; default: none	Passphrase to decrypt PKCS #12 certificates.
PKCS #12 certificate chain	string; default: none	Uploads PKCS #12 certificate chain file.
TLS/Password: User name	string; default: none	Username used for authentication to this OpenVPN server.
TLS/Password: Password	string; default: none	Password used for authentication to this OpenVPN server.
Static key: Static pre-shared key	.key file; default: none	Uploads a secret key file used for server–client authentication.
TLS/TLS/Password: Certificate authority	.ca file; default: none	Certificate authority is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.
TLS/TLS/Password: Server certificate	.crt file; default: none	A type of digital certificate that is used to identify the OpenVPN server.

TLS/TLS/Password: Server key	.key file; default: none	Authenticates clients to the server.
TLS/TLS/Password: Diffie Hellman parameters	.pem file; default: none	DH parameters define how OpenSSL performs the Diffie-Hellman (DH) key-exchange.
TLS/TLS/Password: CRL file (optional)	.pem file|.crl file; default: none	A certificate revocation list (CRL) file is a list of certificates that have been revoked by the certificate authority (CA). It indicates which certificates are no longer accepted by the CA and therefore cannot be authenticated to the server.

A server needs to have a public IP address in order to be available from the public network (the Internet).

4.3.1.4 IPSec

To create a new IPsec instance, go to the Services → VPN → IPsec section, enter a custom name and click Add icon.

Field Name	Value	Description
Enable	yes|no; default: no	Turns the IPsec instance on or off.
IKE version	IKEv1|IKEv2; default: IKEv1	Internet Key Exchange (IKE) version used for key exchange. IKEv1 - more commonly used but contains known issues, for example, dealing with NAT. IKEv2 - updated version with increased and improved capabilities, such as integrated NAT support, supported multihosting, deprecated exchange modes (does not use main or aggressive mode; only 4 messages required to establish a connection).

Mode	Main|Aggressive; default: Main	Internet Security and Key Management Protocol (ISAKMP) phase 1 exchange mode. Main - performs three two-way exchanges between the initiator and the receiver (a total of 9 messages). Aggressive - performs fewer exchanges than main mode (a total of 6 messages) by storing most data into the first exchange. In aggressive mode, the information is exchanged before there is a secure channel, making it less secure but faster than main mode.
Type	Tunnel|Transport; default: Tunnel	Type of connection. Tunnel - protects internal routing information by encapsulating the entire IP packet (IP header and payload); commonly used in site-to-site VPN connections; supports NAT traversal. Transport - only encapsulates IP payload data; used in client-to-site VPN connections; does not support NAT traversal; usually implemented with other tunneling protocols (for example, L2TP).
On startup	Ignore|Add|Route|Start; default: Start	Defines how the instance should act on router startup. Ignore - does not start the tunnel. Add - loads a connection without starting it. Route - starts the tunnel only if there is traffic. Start - starts the tunnel on router startup.
My identifier	ip|string; default: none	Defines how the user (IPsec instance) will be identified during authentication.
Tunnel: Local IP address/Subnet mask	ip/netmask|default: none	Local IP address and subnet mask used to determine which part of the network can be accessed in the VPN network. Netmask range [0..32]. If left empty, IP address will be selected automatically.
Left firewall	off|on; default: on	Adds necessary firewall rules to allow traffic of this IPsec instance on this router.
Force encapsulation	yes|no; default: no	Forces UDP encapsulation for ESP packets even if a "no NAT" situation is detected.
Dead Peer Detection	yes|no; default: no	A function used during Internet Key Exchange (IKE) to detect a "dead" peer. It used to reduce traffic by minimizing the

		number of messages when the opposite peer in unavailable and as failover mechanism.
Dead Peer Detection: Delay (sec)	integer; default: none	The frequency of checking whether a peer is still available or not.
Dead Peer Detection: Timeout (sec)	integer; default: none	Time limit after which the IPsec instance will stop checking the availability of a peer and determine it to be "dead" if no response is received.
Authentication type	Pre-shared key|X.509; default: Pre-shared key	Here you can choose authentication type accordingly to your IPSec configuration
Certificate file	.crt file; default: none	Uploads a certificate file.
Key file	.key file; default: none	Uploads a key file.
CA certificate	.crt file; default: none	Uploads a Certificate authority (CA) file.
Remote participant's certificate	.crt file; default: none	Remote participant's certificate is used to authenticate remote peer
Use additional xauth authentication	yes|no; default: no	Adds additional xauth authentication options.
Xauth: Xauth password	string; default: none	Password for additional peer authentication.
Remote VPN endpoint	host|ip; default: none	IP address or hostname of the remote IPsec instance.
Remote identifier	ip|string; default: none	Defines remote IPsec instance identification.
Tunnel: Remote IP address/subnet mask	ip/netmask; default: none	Remote network IP address and subnet mask used to determine which part of the network can be accessed in the VPN network. Netmask range [0..32]. This value must differ from the device's LAN IP.
Right firewall	yes|no; default: yes	Adds necessary firewall rules to allow traffic of from the opposite IPsec instance on this router.
Transport: Use with DMVPN	yes|no; default: no	Adds several necessary options to make DMVPN work.
Passthrough networks	None|LAN|Wired|Wi-Fi|Mobile|custom; default: none	Select networks which should be passthrough and excluded from routing through tunnel
Enable keepalive	yes|no; default: no	When enabled, the instance sends ICMP packets to the specified host at the specified frequency. If no response is

		received, the router will attempt to restart the connection.
Host	host|ip; default: none	Hostname or IP address to which keepalive ICMP packets will be sent to.
Ping period (sec)	integer [0..9999999]; default: none	The frequency at which keepalive ICMP packets will be sent to the specified host or IP address.
Allow WebUI access	yes|no; default: no	Allows WebUI access for hosts in the VPN network.
Custom options	ipsec options; default: none	Provides the possibility to further customize the connection by adding extra IPsec options.

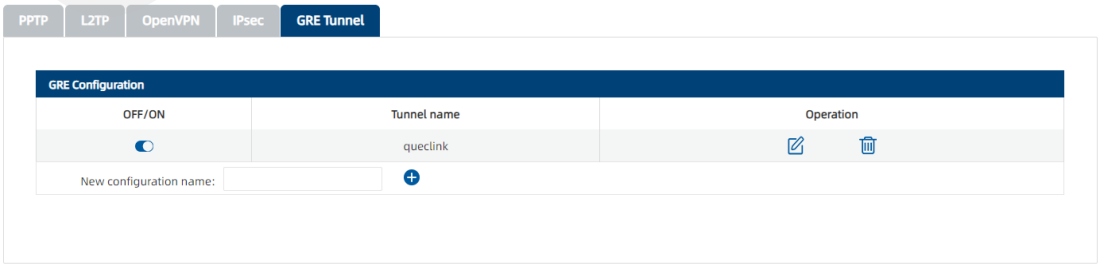
IKE (Internet Key Exchange) is a protocol used to set up security associations (SAs) for the IPsec connection. This process is required before the IPsec tunnel can be established. It is done in two phases:

Field Name	Value	Description
Encryption algorithm	DES|3DES|AES128|AES192|AES256; default: 3DES	Algorithm used for data encryption.
Authentication /Hash algorithm	MD5|SHA1|SHA256|SHA384|SHA512; default: SHA1	Algorithm used for exchanging authentication and hash information.
DH group/PFS group	MODP768|MODP1024|MODP1536|MODP2048|MODP3072|MODP4096; default: MODP1536	Diffie-Hellman (DH) group used in the key exchange process. Higher group numbers provide more security, but take longer and use more resources to compute the key.
Lifetime	integer; default: 8 hours	Defines a time period after which the phase will re-initiate its exchange of information.

4.3.1.5 GRE Tunnel

Generic Routing Encapsulation (**GRE**) is a tunneling protocol used to establish point-to-point connections between remote private networks. GRE tunnels encapsulate data packets in order to route other protocols over IP networks.

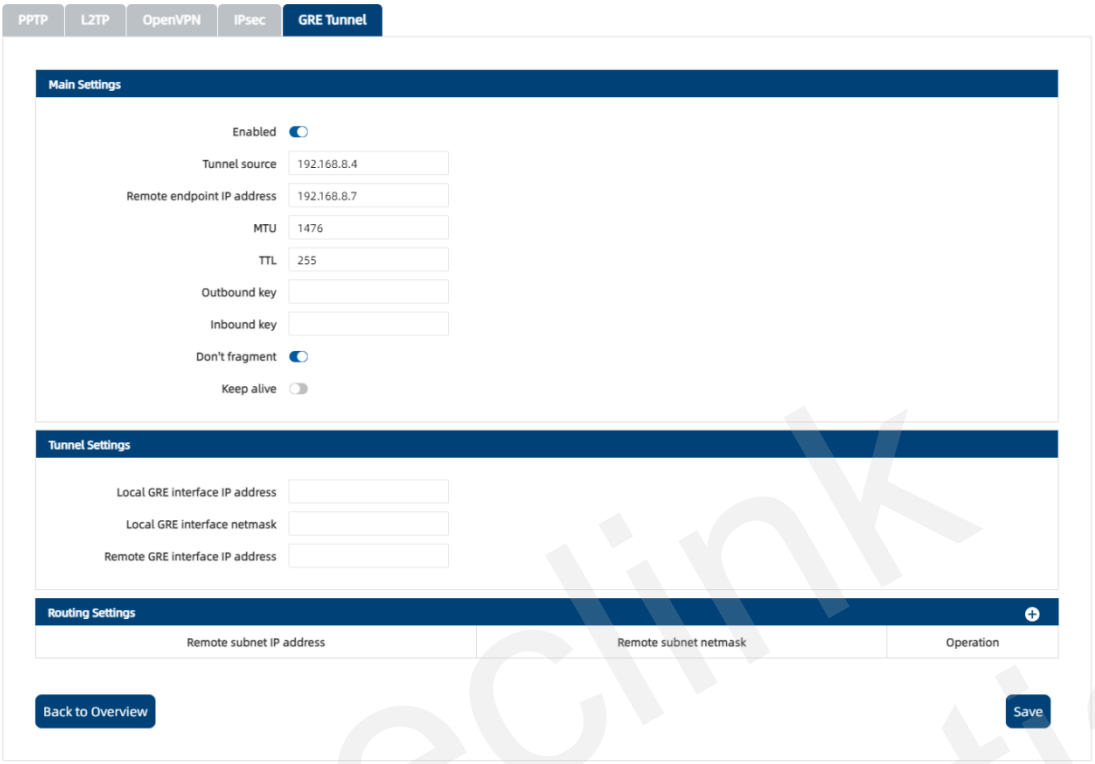
To create a new GRE Tunnel instance, enter a custom name and click the 'Add' button to go the configuration page.



You can click edit button on the right to edit an existing GRE tunnel instance.

Routing settings are used to configure routes to networks that are behind the device that hosts the

opposite GRE instance. To add a new route, simply click the 'Add' button. For information on configuring the route refer to the figure and table below.



Field Name	Value	Description
Enabled	yes|no; default: no	Turns the GRE Tunnel instance on or off.
Tunnel source	network interface; default: none	Network interface used to establish the GRE Tunnel.
Remote endpoint IP address	ip; default: none	External IP address of another GRE instance used to establish the initial connection between peers.
MTU	integer; default: 1476	Sets the maximum transmission unit (MTU) size. It is the largest size of a protocol data unit (PDU) that can be transmitted in a single network layer transaction.
TTL	integer [0..255]; default: 255	Sets a custom TTL (Time to Live) value for encapsulated packets. TTL is a field in the IP packet header which is initially set by the sender and decreased by 1 on each hop. When it reaches 0 it is dropped and the last host to receive the packet sends an ICMP "Time Exceeded" message back to the source.
Outbound key	integer [0..65535]; default: none	A key used to identify outgoing packets. A This value should match the "Inbound key" value set on the opposite GRE instance or

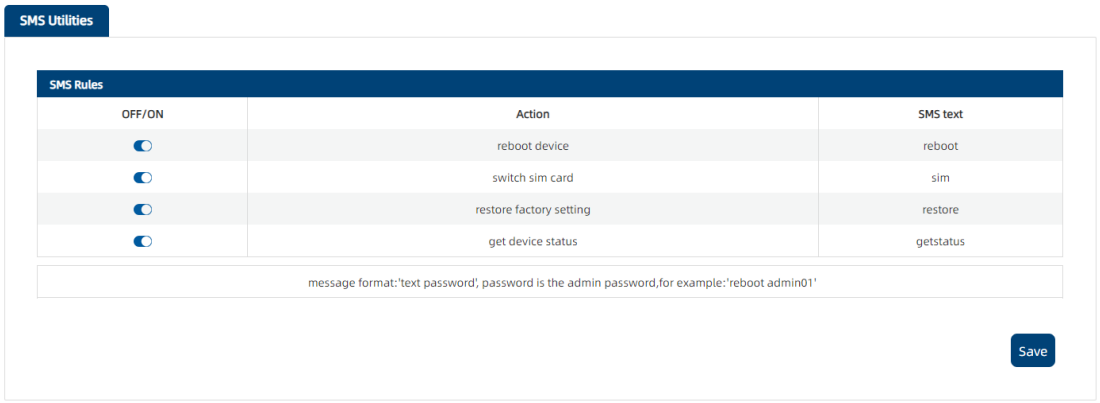
		both key values should be omitted on both sides.
Inbound key	integer [0..65535]; default: none	A key used to identify incoming packets. This value should match the "Outbound key" value set on the opposite GRE instance or both key values should be omitted on both sides.
Don't fragment	yes|no; default: yes	When unchecked, sets the nopmtudisc option for tunnel. Cannot be used together with the TTL option.
Keep alive	yes|no; default: no	Turns "keep alive" on or off. The "keep alive" feature sends packets to the remote instance in order to determine the health of the connection. If no response is received, the device will attempt to re-establish the tunnel.
Keep alive interval	integer [0..255]; default: none	Frequency (in seconds) at which "keep alive" packets are sent to the remote instance.
Local GRE interface IP address	ip; default: none	IP address of the local GRE Tunnel network interface.
Local GRE interface netmask	netmask; default: none	Subnet mask of the local GRE Tunnel network interface.

Routing settings are used to configure routes to networks that are behind the device that hosts the opposite GRE instance. To add a new route, simply click the 'Add' button. For information on configuring the route refer to the figure and table below.

Field Name	Value	Description
Remote subnet IP address	ip; default: none	IP address of the network behind the device that hosts the remote GRE instance.
Remote subnet netmask	netmask; default: none	Subnet mask of the network behind the device that hosts the remote GRE instance.
Lifetime	integer; default: 8 hours	Defines a time period after which the phase will re-initiate its exchange of information.

4.3.2 SMS Utilities

The Mobile Utilities page is used to configure SMS commands related device control. It contains a list of rules that perform certain actions when they are activated by SMS messages.



The entire list contains 4 commands. You can reboot, switch sim card, restore to factory setting or get device status by sending a SMS text following the rule: test password, for example, to reboot a device, you can send 'reboot admin01' SMS to the mobile number of this device.

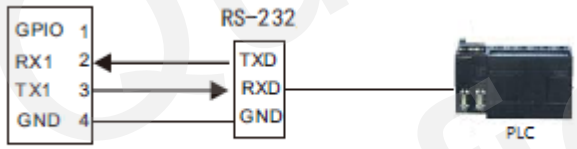
4.3.3 RS232/RS485

RS232 and RS485 functions are to use the available serial interfaces to transfer to data through Router to the Internet. This section allows the user to set the parameters of serial ports. WR100 supports one RS232 and one RS485 port. Serial port provides a way to transfer serial data to IP network, or vice versa.

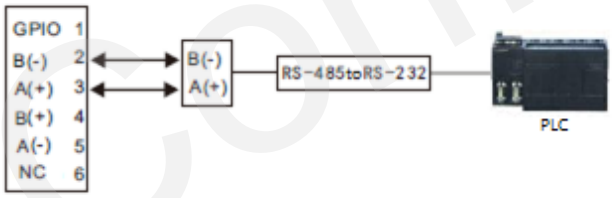
Hardware connection:

The following is figure show you how to connect the lower end device through serial port.

RS232 connection:

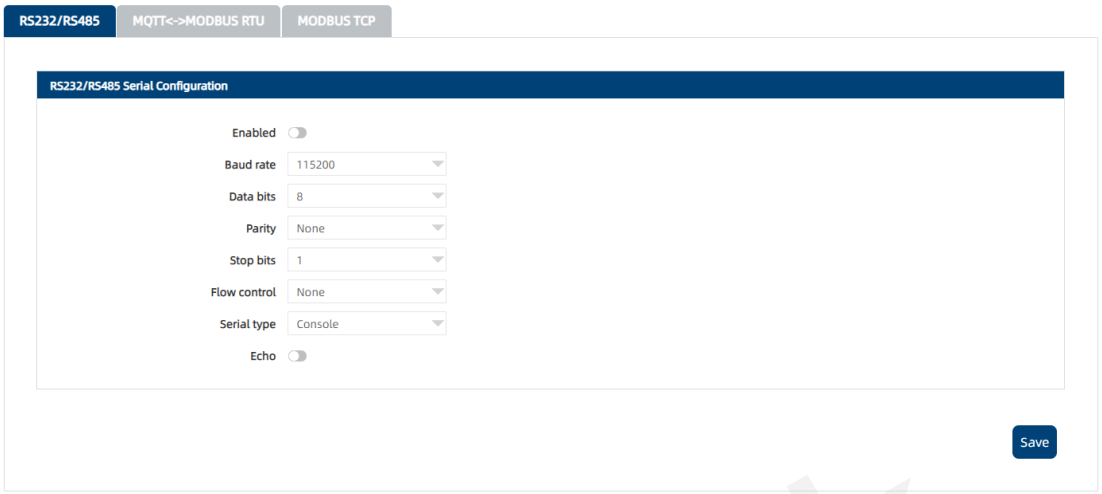


RS485 connection:



4.3.3.1. RS232/RS485 Configuration

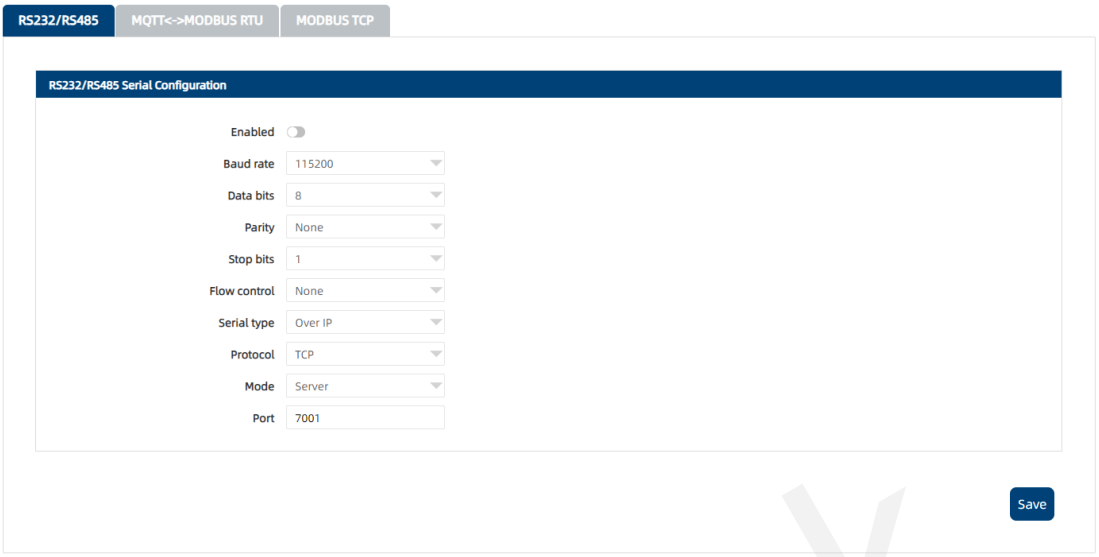
The user can configure the parameters of RS232/RS485 port, including baud rate, data bits, etc. The serial type is the working type of RS232/RS485. By default, RS232/RS485 is working as a console port.



Field Name	Value	Description
Enabled	yes|no; Default: **no**	When checked, enables the RS232 service
Baud rate	300|1200|2400|4800| 9600|19200|38400| 57600|115200; Default: **115200**	Sets the data rate for serial data transmission (in bits per second)
Data bits	5|6|7|8; Default: **8**	The number of data bits for each character
Parity	None|Odd|Even; Default: **None**	In serial transmission, parity is a method of detecting errors. An extra data bit is sent with each data character, arranged so that the number of 1 bit in each character, including the parity bit, is always odd or always even. If a byte is received with the wrong number of 1s, then it must have been corrupted. However, an even number of errors can pass the parity check. **None** (**N**) - no parity method is used **Odd** (**O**) - the parity bit is set so that the number of "logical ones (1s)" has to be odd **Even** (**E**) - the parity bit is set so that the number of "logical ones (1s)" has to be even
Stop bits	1|2; Default: **1**	Stop bits sent at the end of every character allow the receiving signal hardware to detect the end of a character and to re-synchronize with the character stream. Electronic devices usually use one stop bit. Two stop bits are required if slow electromechanical devices are used
Flow control	None|RTS/CTS|Xon/Xoff;	In many circumstances a transmitter

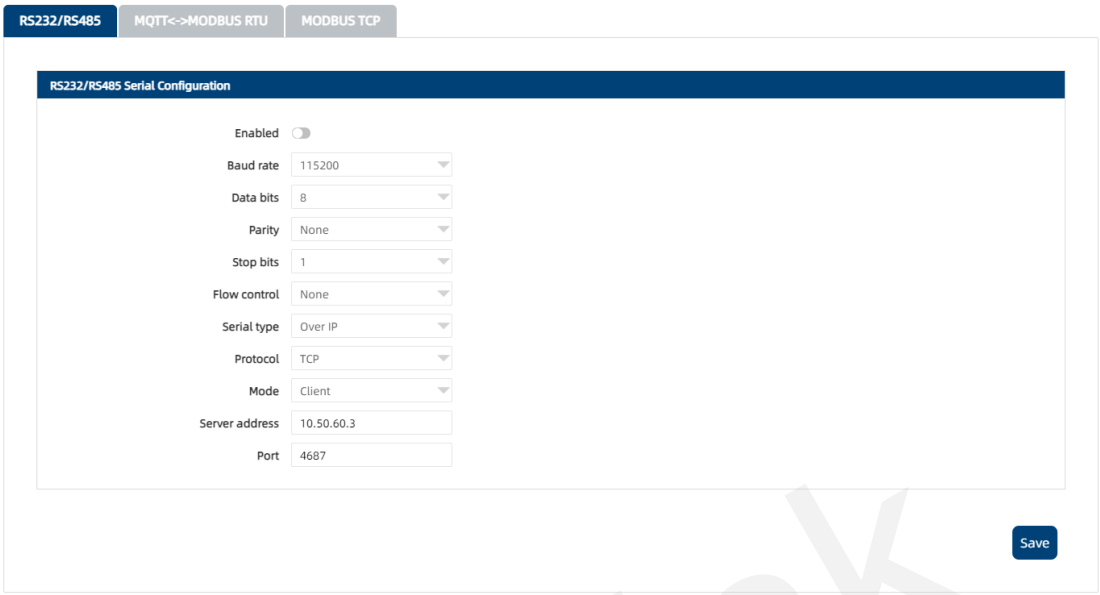
	Default: **None**	might be able to send data faster than the receiver is able to process it. To cope with this, serial lines often incorporate a "handshaking" method, usually distinguished between hardware and software handshaking. **RTS/CTS** - hardware handshaking. RTS and CTS are turned OFF and ON from alternate ends to control data flow, for instance when a buffer is almost full **Xon/Xoff** - software handshaking. The Xon and Xoff characters are sent by the receiver to the sender to control when the sender will send data, i.e., these characters go in the opposite direction to the data being sent. The circuit starts in the "sending allowed" state. When the receiver's buffers approach capacity, the receiver sends the Xoff character to tell the sender to stop sending data. Later, after the receiver has emptied its buffers, it sends an Xon character to tell the sender to resume transmission
Serial type	Console|Over IP; Default: **Console**	Specifies the serial connection type.
Echo	yes | no; Default: **no**	Toggles RS232 echo ON or OFF. RS232 echo is a loopback test usually used to check whether the RS232 cable is working properly

The router can transfer the data between RS232/RS385 ports and IP network. When selecting serial type as “Over IP” and “Mode” as “Server”, the page will display IP configuration parameters:



Field Name	Value	Description
Protocol	TCP; Default: **TCP**	Specifies the protocol used in the communication process
Mode	Server|Client|Bidirect; Default: **Server**	Specifies the device's role in the connection: **Server** - the device waits for incoming connections **Client** - the device initiates the connection **Bidirect** - acts as client by default but waits for incoming connections at the same time
No leading zeros	yes|no; Default: **no**	Specifies that the first hex zeros should be skipped
TCP port	integer [0..65535]; Default: " "	The port number used to connect to the server
Timeout (s)	integer; Default: " "	Disconnects clients after the amount of inactivity time (in seconds) specified in this field

When select serial type as “Over IP” and “Mode” as “Client”, the page will display IP configuration parameters:

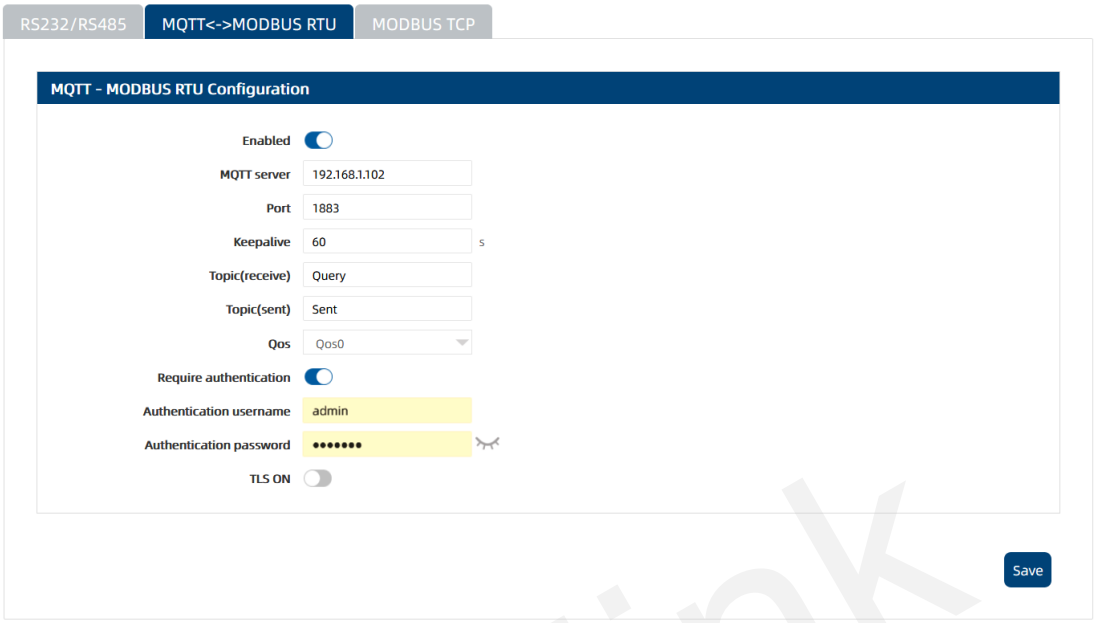


Field Name	Value	Description
Protocol	TCP; Default: **TCP**	The protocol used for data transmission
Mode	Server|Client|Bidirect; Default: **Server**	**Server** - waits for incoming connection **Client** - initiates the connection **Bidirect** – acts as a client by default, but at the same time waits for incoming connections
No leading zeros	yes|no; Default: **no**	Skips first hex zeros
Server address	host|ip; Default: **no**	Server address to which the client will connect to
TCP port	integer [0..65535]; Default: " "	The port number used to listen for incoming connections
Reconnect intervals (s)	integer; Default: " "	Indicates the time period between reconnection attempts

When select serial type as “MODBUS”, the serial port will work as a MODBUS RTU slave device. You can configure data transmission in ‘MQTT<->MODBUS RTU’ and ’MODBUS TCP<->MODBUS RTU’ to transmit data from serial port to the server.

4.3.3.2. MQTT<->MODBUS RTU

This page is used to transfer the Modbus data from the serial port to the server over MQTT. When it is enabled, the device subscribes to a Request topic and publishes on a Response topic on a specified MQTT broker.



Field Name	Value	Description
MQTT server	ip|host; default: 127.0.0.1	IP address or hostname of an MQTT broker.
Port	integer [0..65535]; default: 1883	Port number of the MQTT broker.
Keepalive	yes|no; Default: no	Skips first hex zeros
Topic(receive)	string; default: request	MQTT topic for sending requests.
Topic(sent)	string; default: response	MQTT topic for subscribing to responses.
Username	string; default: none	Username for authentication to the MQTT broker. Leave empty if you do not use client authentication.
Password	string; default: none	Password for authentication to the MQTT broker. Leave empty if you do not use client authentication.

The router communicates with MQTT server with JSON format. The format from the MQTT server to the router is:

Field Name	Value	Description
ID	Integer	Id of the message, to identify the message
slave	Integer	MODBUS slave ID
function	Integer	Function code, 3 represents read register and 6represents write register
address	Integer	The start address of the register,
length	Integer	The length of register

Field Name	Value	Description
crc	Integer	Modbus Crc checking.

For example, {"id":1, "slave":1, "function":3, "address":1, "length":3, "crc":21515}

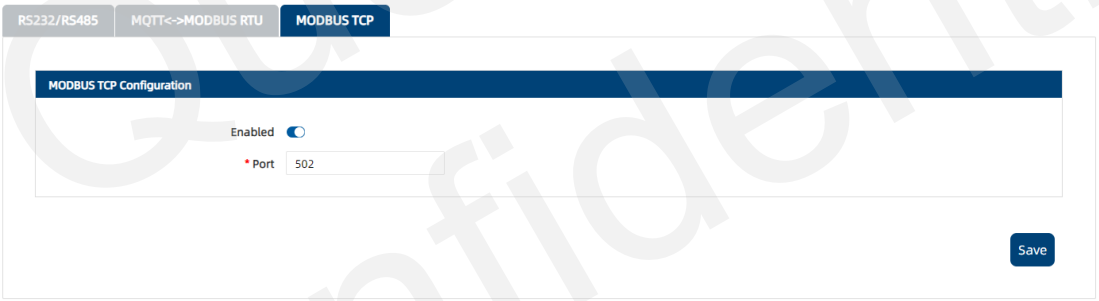
Return message format is:

Field Name	Value	Description
id	Integer	Id of the message, to identify the message
slave	Integer	MODBUS slave ID
function	Integer	Function code,
data_len	Integer	The length of register
data	String	Read data, The length of the string = data_len*2.
crc	Hex	Modbus Crc checking,

For example, {"id":1, "slave":1, "function":3, "data_len":6, "data":"040200080008", "crc":D935}

4.3.3.3. MODBUS TCP<-> MODBUS RTU

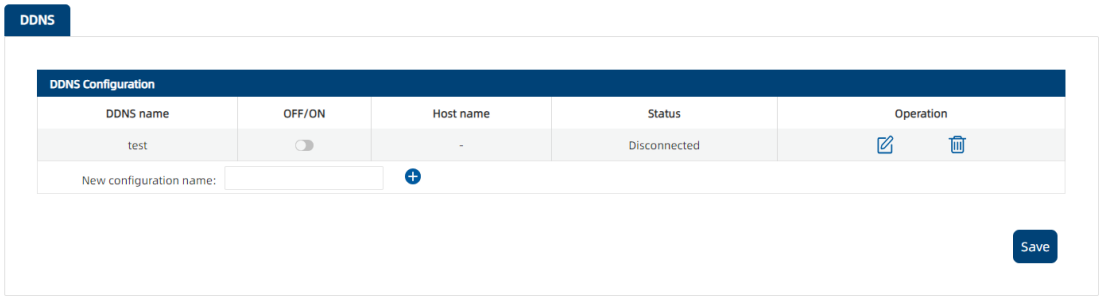
The page allows redirecting MODBUS TCP data coming to a specified port to MODBUS RTU, which allow the user to use MODBUS TCP mater tool to request the data from MODBUS RTU.



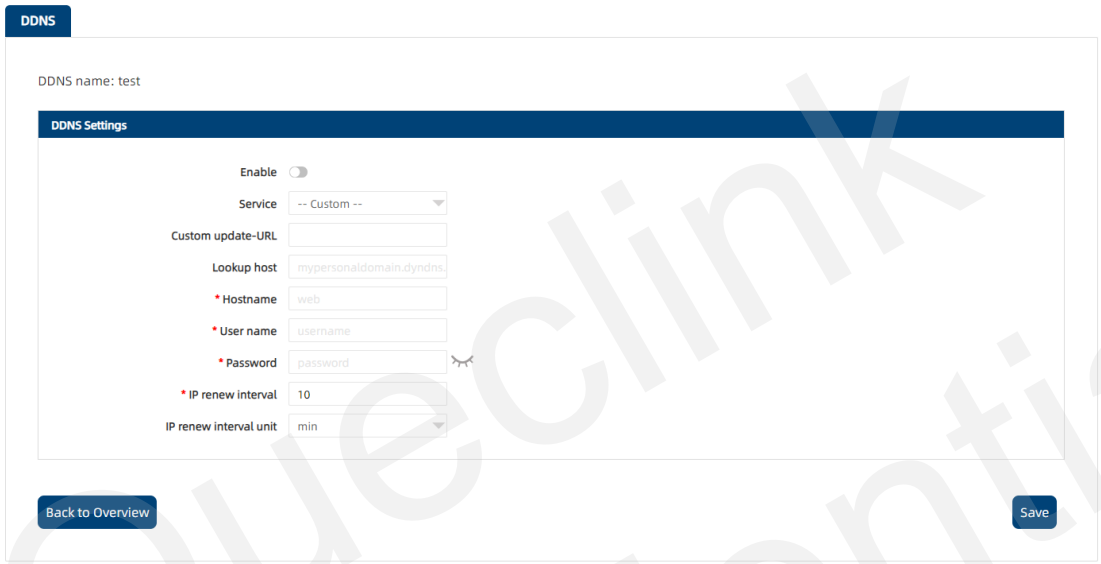
4.3.4 DDNS

Dynamic DNS (DDNS or DynDNS) is a method of automatically updating a name server in the Domain Name System (DNS). This is most often utilized when the end user has a dynamic IP address and wants to bind it to a static hostname.

The router is compatible with many different third party DNS services that provide the possibility to create a custom hostname and bind it to an IP address. The DDNS service periodically updates the IP address information of the hostname, making sure that the device remains reachable via the same hostname even in cases when its IP address has changed.



To configure a DDNS instance, click the Add icon button or the Edit icon of the existing instance. The figure below is an example of the edit page of the default DDNS instance:



Field Name	Value	Description
Enable	yes|no; Default: **no**	Turns the DDNS instance ON or OFF
Service	third party DNS service (chosen from list*)|-- custom --; Default: **dyn.com**	Third party DNS service provider
Lookup host	host; Default: **yourhost.example.com**	Fully qualified domain name (FQDN) of your defined host. This is required to verify what the hostname's current IP address at DNS is (using *nslookup/host* command)
Hostname	host; Default: **yourhost.example.com**	Hostname that will be linked with the router's IP address
Username	string; Default: **your_username**	User name required to login to the third-party DNS service; used to periodically login to your DNS service account and make necessary updates.
Password	string; Default: **your_password**	Password required to login to the third-party DNS service; used to periodically login to your DNS service account and

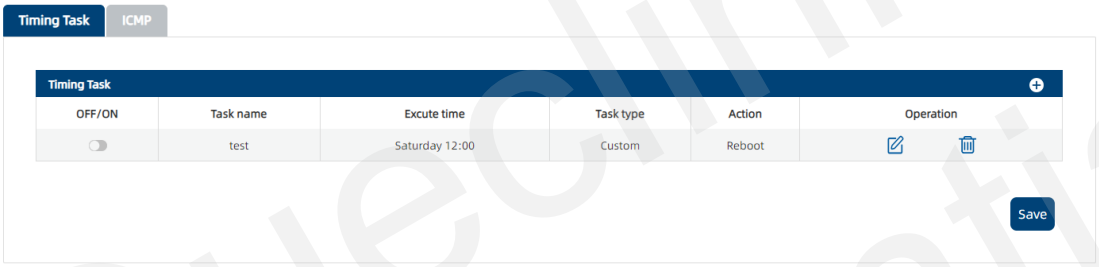
		make necessary updates.
IP renew interval	integer [5..600000]; Default: **10**	Frequency at which the device will check whether it's IP address has changed
IP renew interval unit	Minutes|Hours|Days; Default: **Minutes**	Unit which is used in IP renew interval

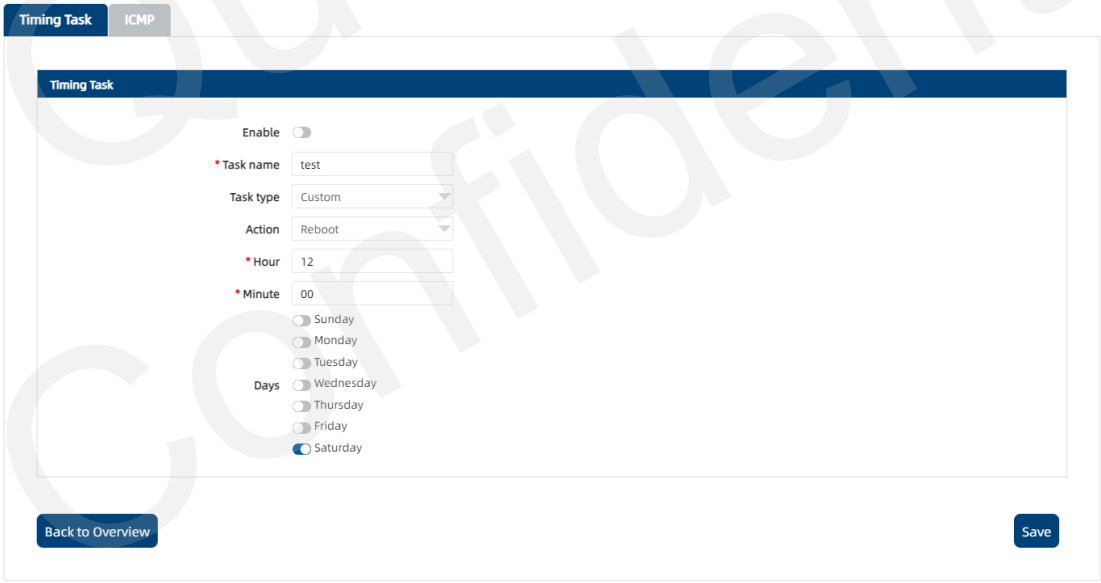
4.3.5 Auto Recovery

Auto Recovery pages provides you several applications as a precautionary measure to ensures the device will recover from unexpected issues, such as mobile connection is down.

4.3.5.1 Timing Task

Timing Task is a function that executes a specified action at a specified time interval. It can be used as prophylactic measure to recover the Router back to normal condition, for example, to reboot the router one time at the mid night of each day.



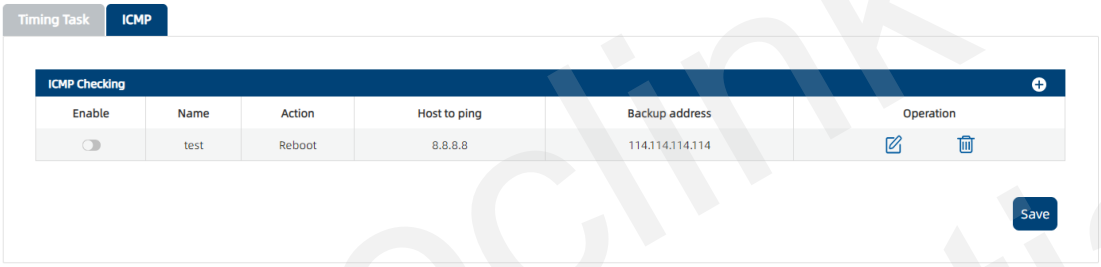


Field Name	Value	Description
Enable	yes|no; Default: **no**	Turns the rule ON or OFF
Task Name	string	Name of ICMP rule
Action if no echo is received	Reboot|Modem restart |Restart mobile connection| none; Default: **Reboot**	The action that will be taken if no ICMP echo is received

Hour	integer [0..23]; Default: **23**	The hour of the day on which the router will reboot
Minute	integer [0..59]; Default: **0**	The minute of the hour on which the router will reboot
Days	Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday; Default: **none**	The day or multiple days on which the router will reboot

4.3.5.2 ICMP

The ICMP is a function periodically sending Ping commands to a specified IP address and wait for received responses. If no response is received, the device will execute specified actions if sending a defined number of times at a defined frequency.



The figure below is an example of that rule and the table below provides information on the fields that make up that rule:

Field Name	Value	Description
Enable	yes|no; Default: **no**	Turns the rule ON or OFF
Name	string	Name of ICMP rule
Action if no echo is received	Reboot|Modem restart|Restart mobile connection|(Re) register|none; Default:	The action that will be taken if no ICMP echo is received

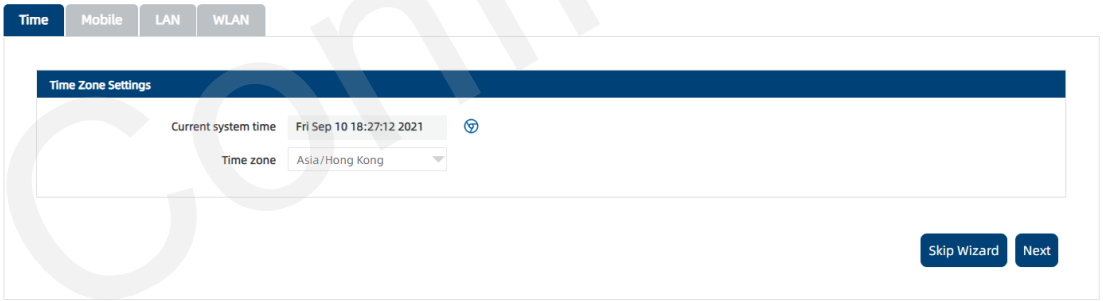
	Reboot	
Interval between pings	5 mins|15 mins|30 mins|1 hour|2 hours; Default: **5 mins**	Interval at which ping requests are sent to the specified host
Ping timeout (sec)	integer [1..9999]; Default: **5**	Maximum response time (in seconds). If no echo is received after the amount of time specified in this field, the ping request is considered to have failed
Retry count	integer [1..9999]; Default: **2**	Indicates how many additional times the device will try sending ping requests if the initial one fails
Interface	Automatically selected| Ping from mobile; Default: **Automatically selected**	Specifies through which interface the pings will be sent. If **Automatically selected** is set, the pings will go through the main WAN interface
Host to ping	host|ip; Default: **8.8.8.8**	Indicates the host to which ping requests will be sent
Backup host to ping	host|ip; Default: **114.114.114.114**	Indicates the backup host to which ping requests will be sent

4.4 System

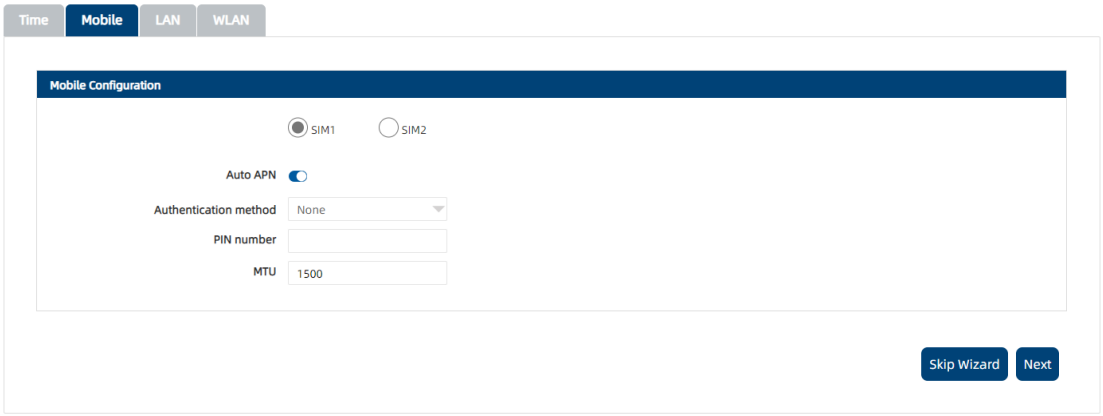
This section shows you how to configure the system setting of the Router.

4.4.1 Setup Wizard

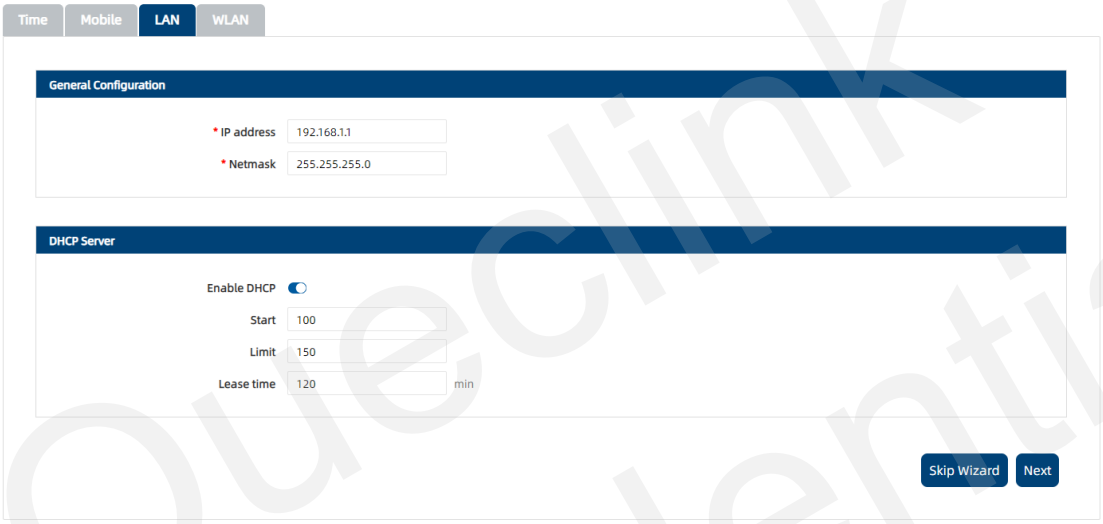
The **Setup Wizard** is to offer a simplified version of other WebUI pages used to set some of the router's most relevant parameters. It's a quick and easy way for you to setup the router.
Step1 is used to configure the router's time settings. Time is very important for many applications, such as scheduled task.



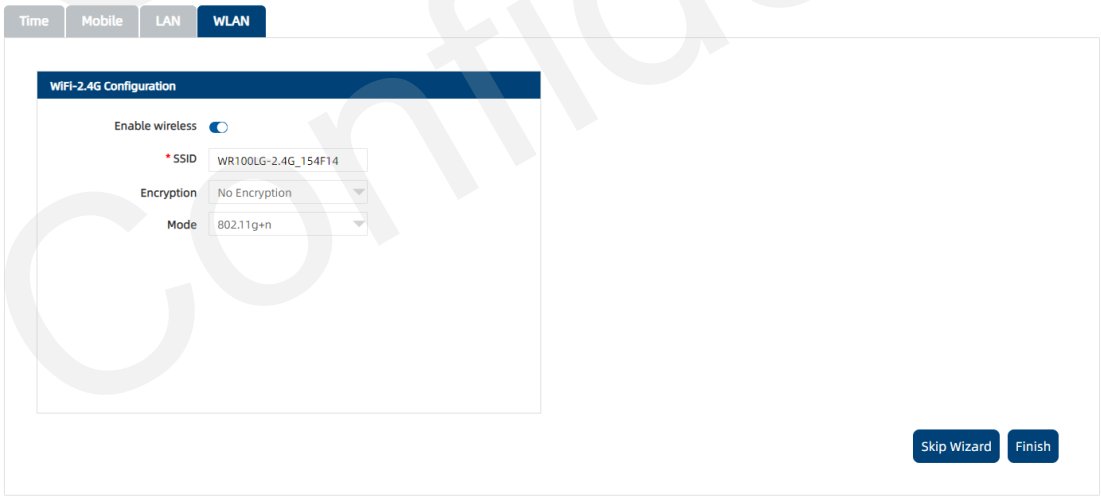
Step2 is used to configure the router's SIM card parameters.



Step3 is used to configure the router's local area network (LAN) and DHCP server settings.



Step4 is used to configure the router's Wi-Fi access point (AP).



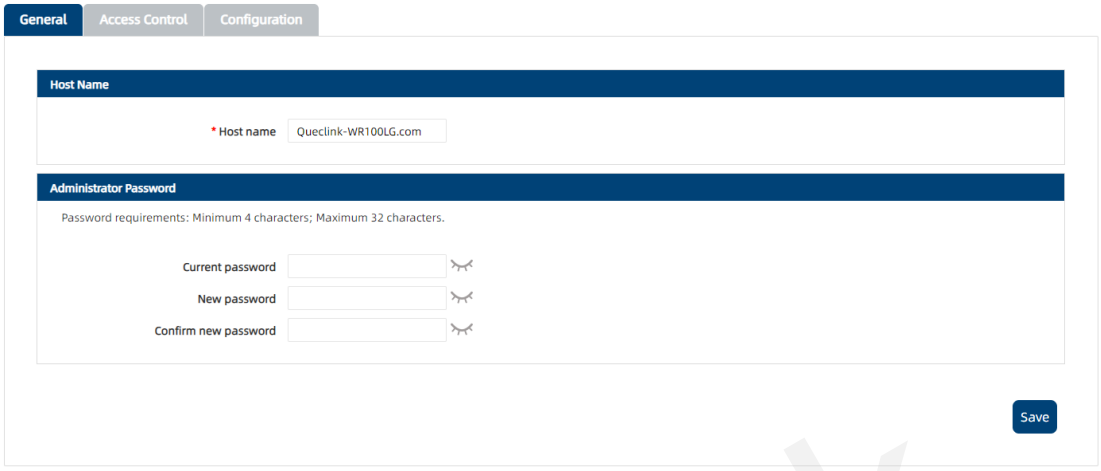
You can also skip any of above steps and configure the setting later in the according section.

4.4.2 Administration

4.4.2.1 General

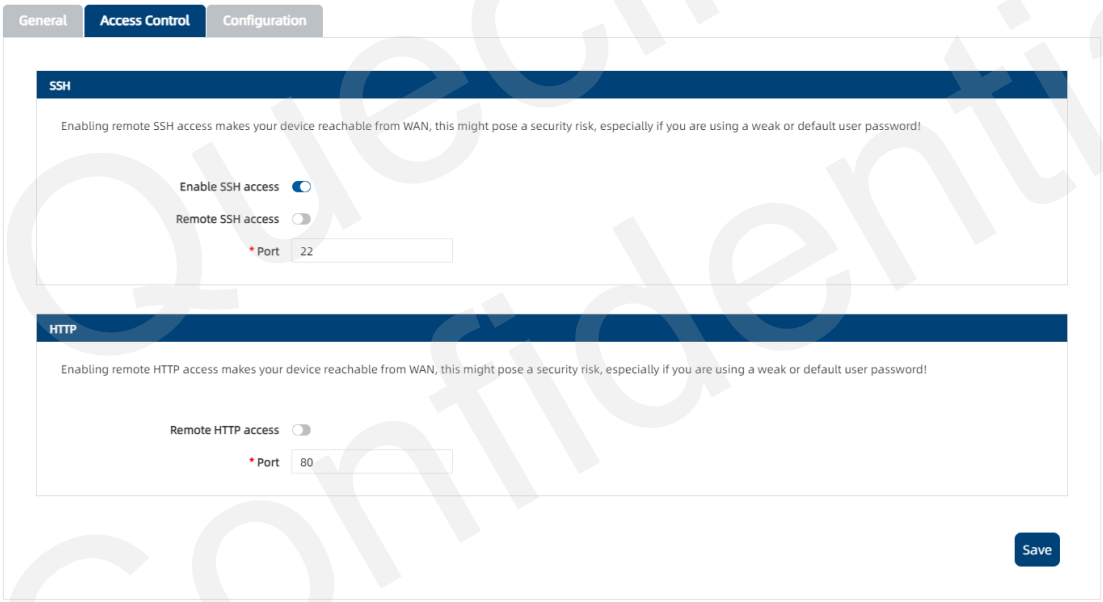
This page is for you to set up some of the router's system parameters, such as password, host name.

To change password, you must input your current password then enter your new password.



4.4.2.2 Access Control

The section is used to manage SSH, HTTP(S) and CLI access to the router. You can click check box to enable or disable access by other devices remote or locally, enable access might pose a security risk to the router, especially if you are using a weak or default user password.



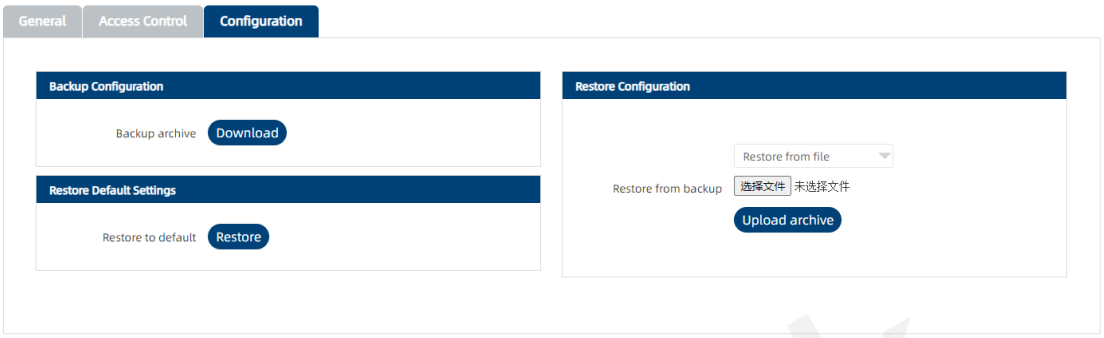
Field Name	Value	Description
Enable SSH access	yes|no; default: **yes**	Turns SSH access from the local network (LAN) on or off.
Remote SSH access	yes|no; default: **no**	Turns SSH access from remote networks (WAN) on or off.
Port	integer [0..65535]; default: **22**	Selects which port to use for SSH access.

4.4.2.3 Configuration File

The **Configuration** page is used to generate the user's defaults configuration and download or

upload backup files to the router.

Backup files can be uploaded only from identical devices with same model. Once a backup file is uploaded to a router, that router will have same configuration as the router from which the backup file originated.



4.4.3 Reboot

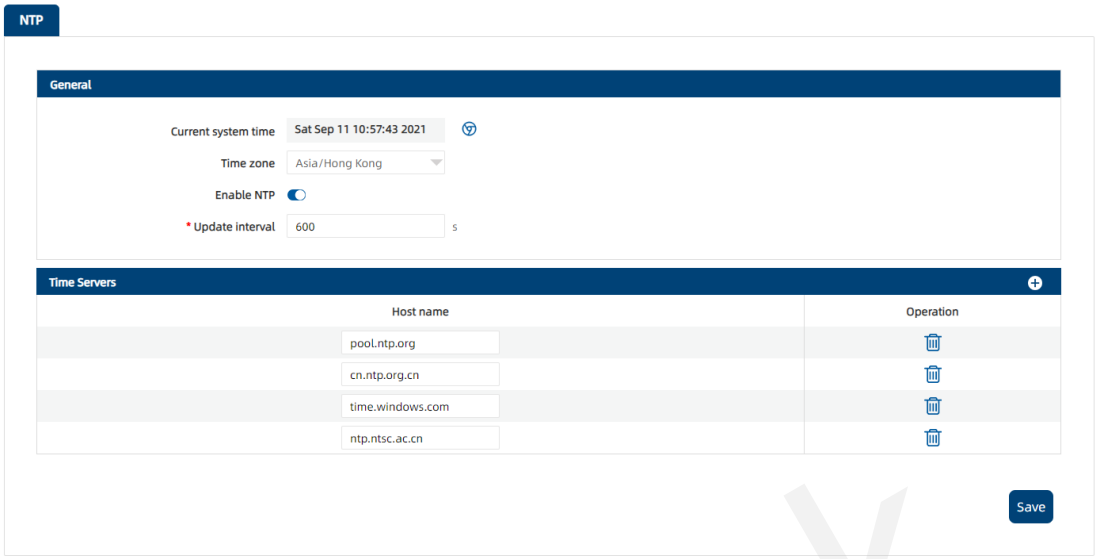
This page is used only to reboot the device. Click the Reboot button if you wish to reboot the device.

4.4.4 NTP

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

In general section, you can configure general router time settings, like selecting the local time zone, setting a time update interval, synchronizing the time, etc.

The Time Servers section displays the NTP servers that the router uses, you can configure maximum four time servers in this section.

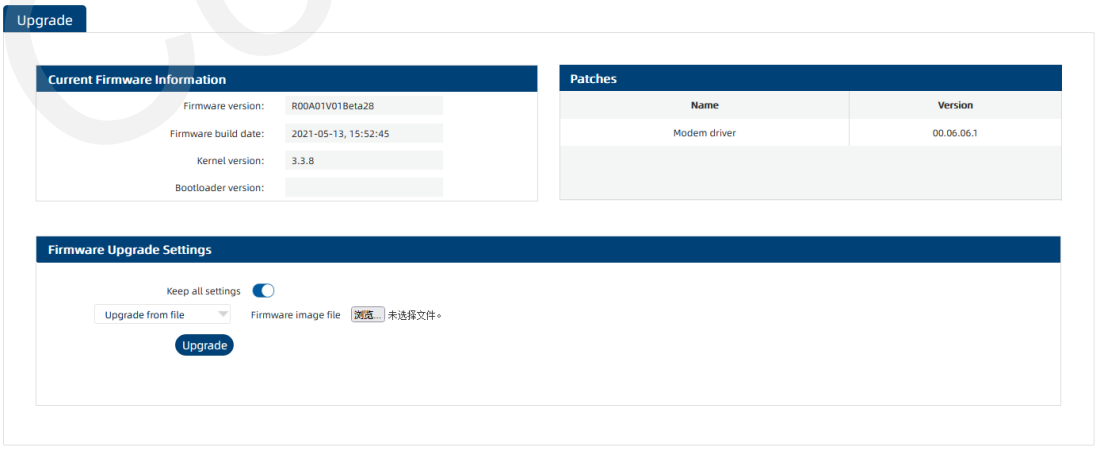


Field Name	Value	Description
Current system time		Current local time of the router.
Time zone	time zone; default: **UTC**	The router will sync time in accordance with the selected time zone.
Enable NTP	yes|no; default: **yes**	Turns NTP on or off.
Update interval (in seconds)	integer; default: **3660**	Defines how often the router will update the time.
Hostname	String	The name of NTP server.

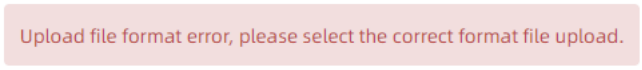
4.4.5 Upgrade

This section is to check the current firmware version of the Router and to upgrade the Router's firmware. Firmware can be upgraded either from server or from an image file uploaded from your computer.

Click Browse button to select the new software from your computer and click Upgrade to upgrade the software. During the upgrade, please do not power off the route, the LEDs of the router will flash at the same time. After upgrade finished, the router will restart automatically. The whole upgrade process will take 5 minutes.



If the uploaded firmware file that is incompatible with your Router, you will see a warning as below:



4.5 Reset Button

WR100 Router has a reset button to return the router back to its default factory settings, please kindly note returning to default factory setting means the router will delete all custom configurations. We strongly recommend you to back up the configuration before the operation.
The reset button has two functions:

- **Reboot the device.** If the reset button is pressed for up to 4 seconds, the device will reboot. Start of the reboot will be indicated by the flashing of all 4 signal strength LEDs together with the green mobile status LED.
- **Factory reset.** If the reset button is pressed for at least 5 seconds (by default), the device will perform a factory reset and then reboot. Signal strength LEDs indicate the elapsed time while holding the reset button. When all 4 LEDs light up, it indicates that 5 seconds have passed and the reset button can be released. Start of the factory reset will be indicated by flashing of all 4 together with a red mobile status LED.

5. FAQ

5.1 SIM Slot

Phenomenon:

Discontinue during dialing, dial failure

Possible Reason:

- SIM card network type do not match
- SIM charges owed
- Power supply do not match
- Modem setting wrong

Solution:

- Change to a suitable SIM card
- Recharge SIM card
- Change to suitable power supply
- Change Modem setting, please check related chapter

5.2 No Signal

Phenomenon:

Modem status show no signal

Possible Reasons:

- Antenna connection wrong
- Modem cannot online
- Modem offline

Solution:

- Connect suitable antenna
- Modem cannot be online, check SIM and modem setting
- Modem offline, check router setting, such as wake-up setting, ICMP setting, check if there are any setting make router offline

5.3 Cannot Find SIM/UIM Card

Phenomenon:

Cannot find SIM card

Possible Reason:

- SIM card damage
- SIM bad contact

Solution:

- Replace SIM card
- Re-install SIM card

5.4 VPN Cannot Connect

Phenomenon

VPN cannot establish connection

Possible Reason:

- VPN port abnormal
- VPN parameter setting wrong
- VPN peer server abnormal

Solution:

- Make sure the Router is online
- Set the correct port to VPN
- Check all VPN parameters
- Check VPN peer server

Glossary

Abbr.	Description
APN	Access Point Name
CHAP	Challenge Handshake Authentication Protocol
dB	Decibel
DC	Direct Current
DI	Digital Input
DO	Digital Output
FDD LTE	Frequency Division Duplexing Long Term Evolution
GRE	generic route encapsulation
GSM	Global System for Mobile Communications
HSPA	High Speed Packet Access
ID	Identification data
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IPsec	Internet Protocol Security
L2TP	Layer 2 Tunneling Protocol
LAN	local area network
M2M	Machine to Machine
MS	Mobile Station
OpenVPN	Open Virtual Private Network
PAP	Password Authentication Protocol
PC	Personal Computer
PIN	Personal Identity Number
PPP	Point-to-point Protocol
PPTP	Point to Point Tunneling Protocol
RF	Radio Frequency
SIM	subscriber identification module
SMA antenna	Stubby antenna or Magnet antenna
SMS	Short Message Service
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VSWR	Voltage Stationary Wave Ratio
WAN	Wide Area Network