

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

This document contains proprietary technical information which is the property of Queclink. Copying of this document, distribution to others or using or communication of the contents thereof is forbidden without express authority. Offenders are liable to the payment of damages. All rights are reserved in the event of a patent grant or registration of a utility model or design. All specifications supplied herein are subject to change without notice at any time.

Copyright © Queclink Wireless Solutions Co., Ltd. 2021



Contents

0. Revision History	6
1. Overview	7
1.1 Description	7
1.2 Major Features	7
1.3 Technical Specification	7
1.4 Software Architecture	9
2. Hardware	10
2.1 Structure	10
2.2 Interfaces	10
2.3 LEDs	
2.4 Accessories	11
2.5 Installation	12
3. Initial Configuration	14
3.1 Configure the PC	14
3.2 Login to device	15
3.3 Control Panel	
4. Software Configuration	
4.1 Status	16
4.1.1 Overview	16
4.1.2 Device	16
4.1.3 Network->Mobile	17
4.1.4 Network->WAN	19
4.1.5 Network->LAN	19
4.1.6 Network->WLAN	20
4.1.7 Applications	21
4.1.8 VPN	21
4.1.9 Routes	22
4.1.10 Traffic	23
4.1.11 Log Viewer	24
4.2 Network	25
4.2.1 Link Management	25



4.2.2 Mobile.		27
	4.2.2.1 General	.27
	4.2.2.2 SIM Management	.28
	4.2.2.3 Data Limit	.30
4.2.3 WAN		30
4.2.4 LAN		34
4.2.5 WLAN		37
4 2 6 Routing		39
1.2.0 1.0000116		20
	4.2.0.1 Statit	.39
	4.2.6.2 KIP	.40
4.2.7 Firewall		41
	4.2.7.1 NAT	.41
	4.2.7.2 Domain Filter	.43
	4.2.7.3 IP/MAC Filter	.43
	4.2.7.4 DMZ	.44
	4.2.7.5 DDOS	.45
4.3 Services		46
		16
4.3.1 VPN		40
	4.3.1.1 PPTP	.46
	4.3.1.2 L2TP	.48
	4.3.1.3 OPENVPN	.50
	4.3.1.4 IPSec	.59
	4.3.1.5 GRE Tunnel	.63
4.3.2 SMS Uti	lities	65
4.3.3 RS232/F	RS485	66
	4 3 3 1 RS232/RS485 Configuration	66
	4 3 3 2 MOTT<->MODBUS RTU	.00
	4 3 3 3 MODBUS TCP<-> MODBUS RTU	72
		72
		72
4.3.5 Auto Re	covery	74
	4.3.5.1 Timing Task	.74
	4.3.5.2 ICMP	.75
4.4 System		76
4.4.2	L Setup Wizard	.76
4.4.2	2 Administration	.77
	4.4.2.1 General	.77
	4.4.2.2 Access Control	.78
	4.4.2.3 Configuration File	.78
4.4.3	3 Reboot	.79





4.4.4 NTP	79
4.4.5 Upgrade	80
4.5 Reset Button	81
5. FAQ	82
5.1 SIM Slot	82
5.2 No Signal	82
5.3 Cannot Find SIM/UIM Card	82
5.4 VPN Cannot Connect	82
Glossary	84



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 highspeed 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.

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

1.3 Technical Specification



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	t	
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







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	Blue, solid	23 to 32
(RSSI)	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.

ile Edit View	 Network and interior w Tools Advance 	ed Help	• • • •	Sear	en IVe	Eur J
Organize 💌	Start this connection	on Rename this connection »		•		0
Ather	os AK8102/8100/8108	SPCI-E Viviware virtuai Etrie	iner Haapter			

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

Networking		
Connect using:		
Qualcomm Athero:	a AR8162/8166/816	8 PCI-E Fast Etherr
		Configure
This connection uses the	following items:	
Client for Micros	oft Networks	
VMware Bridge	Protocol	
🛛 🖳 QoS Packet Sci	heduler	
🗹 📙 File and Printer	Sharing for Microsoft	Networks
Internet Protoco	Version 6 (TCP/IP	(6)
🗹 📥 Internet Protoco	Version 4 (TCP/IP	(4)
🗹 🔺 Link-Layer Topo	ology Discovery Map	per I/O Driver
Link-Layer Topo	logy Discovery Res	oonder
Install	Uninstall	Properties
Description		
Transmission Control F wide area network pro across diverse intercor	Protocol/Internet Pro tocol that provides of nnected networks.	tocol. The default ommunication
	_	

📱 Local Area Conne	ection Status	
General		
Connection		
IPv4 Connectivi	ty:	Internet
IPv6 Connectivi	ty:	No Internet access
Media State:		Enabled
Duration:		09:30:11
Speed:		100.0 Mbps
Details		
Activity —	Sent — 👢	Received
		1
Bytes:	12,818,574	83,948,334
Properties	🚱 Disable 🛛 🛛	Diagnose
		Close

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:

Queclink		
	Router Operating System	
XA	User name	
	Password	
	Login	
	- Driving Smarter 107 -	
	Enzysteph & 2021 by Questink Workers Substants.	

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.

veclink							E	nglish 👻
itus 👻			0	<u> </u>	<u>ه</u>			^
rview ce	Connection Oh 4m 4	time ISS		Uptin Oh 6m	ne 1 3s		Connected de	evice number
rork ces	• Model	WR200LG			 Software version 	R00A01V01	Beta28	
es	 Hardware version 	V1.03			 Serial number 			
ile Traffic	Mobile Traffic				Mobile			
twork •	5.78 KB/s				Data connection state Connected		Connected 10.140.188.85	
rvices 👻	3.85 KB/s 1.93 KB/s		8-		Signal strength SIM card slot in use		-61 dbm SIM1	
item 🝷			(2 minute window	, 5 second interval)	Received/Sent		2 MB/395.72 K	В
	Receive: 0.01 KB/s	AVG: 0.88 KB/s	Peak:	7.01 KB/s	SSID		SSID	WR200LG-5G_A0B32



* E

English

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:

Connection Oh 5m 2) tíme 10s		Upt Oh 6i	time m 38s		Connected device number
• Model	WR200LG			Software version	R00A01V01B	eta28
Hardware version	V1.03			• Serial number		
Mobile Traffic				Mobile		
C 70 VD/-				Data connection state		Connected
2.10 6.072				Connected		10.140.188.85
3.85 KB/s				Signal strength		-61 dbm
1.93 KB/s				SIM card slot in use		SIM1
				Received/Sent		2.01 MB/406.26 KB
-		(2 minute v	vindow, 5 second interval)	WLAN - 2.4G		WLAN - 5G
Receive: 0.53 KB/s	AVG: 0.52 KB/s	Peak:	7.01 KB/s	SSID		SSID WR200LG-5G_A0B327
Sent: 0.21 KB/s	AVG: 0.21 KB/s	Peak:	1.69 KB/s	Connected devices	0	Connected devices 0

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.

Device Information		Modem Information	Modem Information		
Model	WR100LEU	Modem model	EC200T		
Host name	Queclink-WR100LG.com	FW version	EC200TEUHAR02A09M16_01.001.01.001		
Firmware version	WR100LEU_R00A01V01				
Kernel version	3.3.8				
Local device time	Mon Sep 13 09:22:33 2021				
Hardware revision	V1.01				
Uptime	1d 17h 17m 19s				
Memory total/free	126264KB / 51836KB				

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.
	Displays the device's kernel version. A kernel is a computer
Kernel version	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:

Mobile		Connected Infor	mation
Connection state	Connected	Туре	QMI
IMEI	867698044656505	IP address	10.140.188.85
IMSI	460016787523345	Netmask	255.255.255.252
ICCID	89860119801294226691	Gateway	10.140.188.86
SIM card state	READY	DNS 1	120.80.80.80
Signal strength	-61 dbm	DNS 2	221.5.88.88
Cell ID	41753094	Connected	0h 6m 32s
Operator	CHN-UNICOM		
Operator state	Registered		
Connection type	FDD LTE		
Connected band	LTE BAND 3		
Bytes received	2,143,134		
Bytes sent	440,044		

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
	The IMEI (International Mobile Equipment Identity) is a unique 15
	decimal digit number used to identify cellular modules.
	The IMSI (international mobile subscriber identity) is a unique 15
IMSI	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.
	The current SIM card state. Possible values are:
	• Ready - SIM card is inserted and ready to be used
	Inserted - SIM card is inserted
SIM card state	 Not inserted - SIM card is not inserted
	• Unknown - unable to obtain SIM card state value. Possible
	communication issue between the device and the modem
	Received signal strength indicator (RSSI) measured in dBm. Values
Signal strength	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
	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
Operator state	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
	Mobile connection type. Possible values are:
	2G: 2G (GSM), 2G (GPRS), 2G (EDGE)
Connection type	3G: 3G (WCDMA), 3G (HSDPA), 3G (HSUPA), 3G (HSPA), 3G (HSPA+),
connection type	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
Туре	The dialing mode of the connection
IP address	Router's modem IP address
	A netmask is used to define how "large" a network is by specifying
Netmask	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:

tion					
IP address	Netmask	Gateway	DNS 1	DNS 2	Connected
192.168.60.157	255.255.255.0	192.168.60.1	192.168.60.1	-	0h 16m 8s
	ion IP address 192.168.60.157	IP address Netmask 192.168.60.157 255.255.255.0	IP address Netmask Gateway 192.168.60.157 255.255.255.0 192.168.60.1	Ip address Netmask Gateway DNS 1 192.168.60.157 255.255.255.0 192.168.60.1 192.168.60.1	IP address Netmask Gateway DNS 1 DNS 2 192.168.60.157 255.255.255.0 192.168.60.1 192.168.60.1 192.168.60.1

Field Name Description 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 Type 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 A netmask is used to define how "large" a network is by specifying Netmask which part of the IP address denotes the network and which part denotes the device Gateway of the default route - an IP address through which the router Gateway 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

The Refresh button is to refresh 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.



Name	IP address	Netmask	Ethernet MA	AC address	Connected	
br-lan	192.168.1.1	255.255.255.0	78:05:41:15:4F:13		1d 17h 18m 30s	
Clients						
	Hostname		IP address		MAC address	
	DESKTOP-78IIHJH		192.168.1.150	8	C:47:BE:3C:6B:64	

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
	A netmask is used to define how "large" a network is by specifying
Netmask	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:

SSID	Channel	Mode	Encryption	Wireless MAC	Bit rate	
WR100LG-2.4G_154F14	11 (2.462GHz)	AP	None	78:05:41:15:4F:14	72 Mbit/s	
lients						
Host SSID	Device name		IP address	MAC address	Connected time	
WR100LG-2.4G_154F14			192.168.1.151	42:09:3E:E4:9E:CD	0h 0m 51s	
WR100LG-2.4G_154F14	nova_7_5G-37ac74192924dd	5	192.168.1.107	22:BC:69:E5:2E:5B	0h 31m 56s	

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

Field Name Description	
------------------------	--



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

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 ③ icon to direct to the configuration page of the services.

lications				
Applications Status				
	Application	Enabled	Status	
	NTP client	Enabled	Normal	0

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.



VPN

рртр				
Name	Status	Mode	IP/Client Number	Time
1	Disabled	Client	-	-
PPTP	Disabled	Server		
L2TP				
Name	Status	Mode	IP/Client Number	Time
1	Disconnected	Client		
L2TP	Disabled	Server		
OpenVPN				
Name	Status	Mode	IP/Client Number	Time
wr200	Disabled	Server		
1	Disabled	Client	-	-
IPsec				
Name	Status	Mode	IP	Time
www	Enabled	Main		•
GRE Tunnel				
Name	Status	Source	IP	Time

Copyright © 2021 by Queclink Wireless Solution

Field Name	Description
Name	Associated VPN name
Status	Destination network address
Mode	Server or client
	If the VPN is a client, it displays the IP address allocated by the
IP/Client Number	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:



Routes

ARP							
IP address	MAC ac	MAC address					
192.168.1.150	8c:47:be:	8c:47:be:3c:6b:64					
Active IP Routes							
Network	Target	IP gateway	Metric				
wan2	0.0.0/0	10.140.188.86	10				
wan2	10.140.188.84/30	0.0.0.0	10				
wan2	113.116.53.237	10.140.188.86	10				
lan	192.168.1.0/24	0.0.0.0	0				
wan2	192.168.60.246	10.140.188.86	10				

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: sone	Interface through which the router is
Interface	string; Default: none	associated with the host
<u> </u>	1 	

Routes Parameter description:

Field Name	Value	Description
Network	string; Default: none	Associated network interface name
Target	ip ip/netmask; Default: none	Destination network address
		Indicates the IP address of the gateway
IP gateway	ip; Default: none	through which the target network can
		be reached
		Metrics help the router choose the
	Integer [0, 4, 204, 067, 205].	best route among multiple feasible
Metric	Default: none	routes to a destination. The route will
	Default: none	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.



Mobile Traffi

Card:	SIM1			Perio	od:	Day																
Last 24 H	ours																					
5h 16h	17h	18h	19h	20h	21h	22h	23h	0h	1h	2h	3h	4h	5h	6h	7h	8h	9h	10h	11h	12h	13h	14
54.49 MB																						
36.33 MB																						
18.16 MB																						
																			(1 da	iy windov	, 1 hour	inte
									_										(1 da	iy windov	v, 1 hour	i

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.

Kernel log 🔍		
20 13 03:35:28 dnsmasq-dncp[2863]: DHCPREQUEST(DF-tan)	192.168.1.150 80:47:De:30:60:64	
20 13 03:35:26 distriasq-dicp[2605]. DrcPACK(bi-tail) 192.1	56.1.150 8C.47.DE.5C.6D.64 DESKTOP-78IIHJH	
p 13 04:10:35 /usi/sbin/hostblock.sii: uns_update		
ap 13 04:10:36 /usr/sbin/hostblock.sh: online_wan-[wan]	11	
ap 13 04:10:30 / dsmacg-dbcp[2863]: DHCPPEOUEST(br-lap)	-''] 107 168 1150 8c:47:be:3c:6b:64	
p 13 04:28:12 drsmasq-drcp[2863]: DHCPACK(br-lap) 1921	581150 8c:47:be:3c:6b:64 DESKTOP-78IIHIH	
ep 13 05:21:55 dosmasq-dbcp[2863]: DHCPREOLIEST(br-lan)	192 168 1 150 8c:47:be:3c:6b:64	
20 13 05:21:55 drismasq dhcp[2863]: DHCPACK(br-lan) 1921	581150 8c:47:be:3c:6b:64 DESKTOP-78IIHIH	
p 13 06:15:57 dnsmasg-dhcp[2863]: DHCPREQUEST(br-lan)	192.168.1.150 8c:47:be:3c:6b:64	
ep 13 06:15:57 dnsmasg-dhcp[2863]: DHCPACK(br-lan) 192.1	68.1.1 50 8c:47:be:3c:6b:64 DESKTOP-78IIHIH	
ep 13 08:52:50 dnsmasg-dhcp[2863]: DHCPOFFER(br-lan) 19	.168.1.107 22:bc:69:e5:2e:5b	
p 13 08:52:50 dnsmasg-dhcp[2863]: DHCPDISCOVER(br-lan)	22:bc:69:e5:2e:5b	
p 13 08:52:50 dnsmasg-dhcp[2863]: DHCPOFFER(br-lan) 19	.168.1.107 22:bc:69:e5:2e:5b	
p 13 08:52:50 dnsmasg-dhcp[2863]: DHCPREQUEST(br-lan)	192.168.1.107 22:bc:69:e5:2e:5b	
p 13 08:52:50 dnsmasq-dhcp[2863]: DHCPACK(br-lan) 192.1	58.1.107 22:bc:69:e5:2e:5b nova_7_5G-37ac74192924dd5	
ep 13 08:54:06 hostapd: ath0: STA 72:a5:23:af:91:9f IEEE 802	.11: associated	
p 13 08:54:06 hostapd: ath0: STA 72:a5:23:af:91:9f RADIUS:	starting accounting session BF7D56BC28B43461	
ep 13 08:54:09 dnsmasq-dhcp[2863]: DHCPDISCOVER(br-lan)	72:a5:23:af:91:9f	
p 13 08:54:09 dnsmasq-dhcp[2863]: DHCPOFFER(br-lan) 19	.168.1.149 72:a5:23:af:91:9f	
ep 13 08:54:09 dnsmasq-dhcp[2863]: DHCPDISCOVER(br-lan)	72:a5:23:af:91:9f	
ep 13 08:54:09 dnsmasq-dhcp[2863]: DHCPOFFER(br-lan) 192	.168.1.149 72:a5:23:af:91:9f	
ep 13 08:54:09 dnsmasq-dhcp[2863]: DHCPREQUEST(br-lan)	192.168.1.149 72:a5:23:af:91:9f	
ep 13 08:54:09 dnsmasq-dhcp[2863]: DHCPACK(br-lan) 192.1	58.1.149 72:a5:23:af:91:9f HUAWEI_P40_Pro-199171db26	
ep 13 08:54:10 hostapd: ath0: STA 72:a5:23:af:91:9f IEEE 802	.11: disassociated	
ep 13 08:55:16 hostapd: ath0: STA 42:09:6a:2c:4a:6e IEEE 80	2.11: associated	
p 13 08:55:16 hostapd: ath0: STA 42:09:6a:2c:4a:6e RADIUS	: starting accounting session B63DA3A94DB25A70	
ep 13 08:55:19 dnsmasq-dhcp[2863]: DHCPDISCOVER(br-lan)	42:09:6a:2c:4a:6e	
ep 13 08:55:19 dnsmasq-dhcp[2863]: DHCPOFFER(br-lan) 192	.168.1.230 42:09:6a:2c:4a:6e	
p 13 08:55:19 dnsmasq-dhcp[2863]: DHCPDISCOVER(br-lan)	42:09:6a:2c:4a:6e	
ep 13 08:55:19 dnsmasq-dhcp[2863]: DHCPOFFER(br-lan) 192	.168.1.230 42:09:6a:2c:4a:6e	
p 13 08:55:19 dnsmasq-dhcp[2863]: DHCPDISCOVER(br-lan)	42:09:6a:2c:4a:6e	
p 13 08:55:19 dnsmasq-dhcp[2863]: DHCPOFFER(br-lan) 192	.168.1.230 42:09:6a:2c:4a:6e	
p 13 08:55:19 dnsmasq-dhcp[2863]: DHCPREQUEST(br-lan)	92.168.1.230 42:09:6a:2c:4a:6e	
p 13 08:55:19 dnsmasq-dhcp[2863]: DHCPACK(br-lan) 192.1	8.1.230 42:09:6a:2c:4a:6e	
ep 13 08:55:20 hostapd: ath0: STA 42:09:6a:2c:4a:6e IEEE 80	2.11: disassociated	
an 12 NOVEZ(14 hostandy athov CTA 12)NZVCEV2NVSH IEEE 0N3	11: accoriated	Þ



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.

Link Management	Link Failover Sta	atus			
Link Management	:				1
	Primary link	Modem			
	Backup link	WAN			
	Backup mode	Backup			
	buckup moue	outrap			
					Save

Field Name	Value	Description		
Primary Link		Select from "Modem", "WAN" or		
		"Wi-Fi2.4G".		
		Modem: Select to make mobile		
	Madam MANUMI 52 4C	as the primary link		
	Widdening WAN WI-Fiz.40	WAN: Select to make WAN as		
		the primary link		
		Wi-Fi2.4G: Select to make Wi-		
		Fi 2.4G as the primary link		
Deduce Link		Select from "None", "Modem",		
	None Modem WAN Wi-Fi2.4G	"WAN" or "Wi-Fi2.4G".		
		None: Do not select any backup		
		link		
		Modem: Select to make mobile		
Васкир шик		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		
		Select from "Backup" or "Load		
		Balancing".		
Backup mode	Backup Load Balancing	Backup: The inactive link is on		
		standby		
		Load Balancing: Use two links		



	simultaneously, eac	n 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.

Link	Mobile	r
Health monitor interval	5 sec	
Health monitor ICMP host(s)	Disable	
Health monitor ICMP timeout	1 sec	
Attempts before failover	3	r
Attempts before recovery	8	

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	Disphal DNS	Indicates the host try to ping, select
Health monitor	Disable DNS	custom to manually configure an IP
ICIVIP nost(s)	server Gateway Custom	address to ping.
	integer [04,294,967,295];	
IPV4 address	Default: none	The IP address of the host
Health monitor	1 sec 3 sec 4 sec 5	Set the ping timeout
ICMP timeout	sec 10sec	set the ping timeout.
		Set the max ping tries. Switch to
Attempts before	1121518115120	another link or take emergency
failover	1 3 3 8 13 20	action if the max continuous ping
		tries reached.
Attempts before		Set the max ping tries. Switch to
	1 3 5 8 15 20	primary link if the max continuous
recovery		ping tries reached.

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



Primary Link Status		Backup Link Status	
Link	Mobile	Link	Wan
Status	offline	Status	online
IP address	-	IP address	192.168.60.157
Netmask		Netmask	255.255.255.0
Gateway	-	Gateway	192.168.60.1
DNS 1	-	DNS 1	192.168.60.1
DNS 2		DNS 2	
Connected	0h 0m 0s	Connected	0h 45m 46s

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.

ral SIM Management Data Li	mit
Modem Switch	
Enable modem	
Mobile Configuration	
	€ SIM1 SIM2
Network search mode	OTUA
Auto APN	
APN	
Authentication method	None
PIN number	
МТО	1500
	Sav
	_

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 that your network carrier
Authentication	CHAP PAP None;	uses to authenticate new connections on its
method	default: None	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
		Sets the maximum transmission unit (MTU) size
	integer [0, 1500].	It is the largest size of a protocol data unit (DDU)
MTU	dofault: 1500	that can be transmitted in a single network layer
		transaction
		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.

Primary Card	
Primary SIM card	SIM1
SIM Switching	
Enable automatic switching Check interval	30 s
Policy	
Direction On weak signal On data limit On data connection fail	SIM1 To SIM2

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
On weak signal	yes no; default: no	amount of time specified in this field. 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 \rightarrow Mobile \rightarrow 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.

	(12		
Enable da	ata connection limit	3			
	* Data limit	4096	MB		
	Period	Month	-		
	Start day	1	-		

Field	Value	Description
Enable data	yes no; default: no	Turns mobile data limitations on or off.
connection limit		
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;	Data limit period after which the data
	default: Month	counter is reset on the specified Start day.
Start day Start	day [131] day	Specifies when the period of counting data
hour	[MondaySunday] hour	usage should begin. After the period is over,
	[124]; default: day 1	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:

Configuration		
Protocol	Static address	
* IPv4 address		
* IPv4 netmask		
IPv4 gateway		
IPv4 broadcast		
Use custom DNS servers		•
Override MAC address		Default: 78:05:41:15:4F:12
Override MTU		
Use gateway metric	20	

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 [01500]; 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:

comgutation		
Protocol	DHCP client	
Hostname to send when requesting DHCP		
Accept router advertisements		
Use broadcast flag		
Use default gateway		
Use DNS servers advertised by peer		
Use gateway metric	20	
Client ID to send when requesting DHCP		
/endor Class to send when requesting DHCP		
Override MAC address		Default: 78:05:41:15:4F:12
Override MTU		

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 [01500]; 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:

General Configu Protocol PPPoE PAP/CHAP username PAP/CHAP password Access concentrator Service name Use default gateway 💽 Use gateway metric Use DNS servers advertised by peer 🛛 🕥 LCP echo failure threshold LCP echo interval Inactivity timeout Override MTU Save

Field Name	Value	Description		
Drotocol	Static DHCP PPPoE;	The protocol used by the MAN interface		
Protocol	default: DHCP	The protocol used by the WAN interface		
РАР/СНАР	string dofault: none	The username that you use to connect to		
username	string; default. none	your carrier's network		
	string default neme	The password that you use to connect to		
PAP/CHAP password	string; default: none	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		
		Uses the default gateway obtained		
Use default gateway	yes no; default: yes	through DHCP. If left unchecked, no default		
		route is configured		
		The WAN configuration by default		
Liso gatoway motric	integer: default: 0	generates a routing table entry. In this field		
Use galeway metho	Integer; default: U	you can alter the metric of that entry.		
		Higher metric means higher priority		
		Uses DNS servers obtained from DHCP. If		
ose DNS servers	yes no; default: yes	left unchecked, the advertised DNS server		
auvertised by peer		addresses are ignored		
LCD ocho failura		Presumes peer to be dead after given		
threshold	integer; default: 0	amount of LCP echo failures. Leave it at 0		
threshold		to ignore failures		
		Sends LCP echo requests at the given		
LCD acho intorval	internet defaulte F	interval in seconds. This function is only		
LCP echo interval	integer; default: 5	effective in conjunction with failure		
		threshold		
		Close inactive connection after the given		
Inactivity timeout	integer; default: 0	amount of seconds. Leave it at 0 to persist		
		connection		
	integer [0, 1500], defeuilte	Maximum Transmission Unit (MTU) -		
Override MTU		specifies the largest possible size of a data		
	1200	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.



					Fachla Direct		
	 IPv4 address 	192.168.1.1			Enablé DHCP		
	IPv4 netmask	255.255.255.0	-		Start	100	
	Override MTU				Limit	150	
	Use gateway metric				Lease time	120	min
					Dynamic DHCP	C	
					Force	C	
					DHCP-Options		Ð
IP Aliases			÷	Static Leases			e
IP aliasing can b	e used to provide multi	ple network addresses or	a single interface.	Sta	tic Leases is used to	lease one IP to specific MA	.C
ID address	Netmask	IP broadcast	Operation	Host name	MAC addres	s IP address	Operation

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 [01500]; 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		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
	integer [1253]; Default:	to be in the range of
	100	[192.168.2.0192.168.2.254]
		(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		How many addresses the DHCP server can
		lease out. Continuing from the above
		example: if the start address is
	integer [1 4294967296]	192 168 2 100 and the server can lease out
	Default: 150	150 (default limit value) available
	Delault. 150	addresses will be from 192 168 2 100 to
		$102, 168, 2, 249, (100 \pm 150 - 1 - 249)$ this is
		192.108.2.249 (100 + 150 - 1 = 249) (118 IS
		The duration of on ID losse lossed out
Lease time		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
	time in 'h' (nours) or 'm'	after half of the specified amount of time
	(minutes); Default: 12h	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 broadcasts are used by BOOTP and DHCP
	ip; Default: " "	clients to find and send requests to their
		respective servers
Dynamic DHCP		Enables Dynamic allocation of client
	yes no; Default: yes	addresses. If this is disabled, only clients that
		have static IP leases will be served


		The DHCP force function ensures that the		
		router will always start it's DHCP server, even		
		if there is another DHCP server already		
Force	yes no; Default: no	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		
		Overrides your LAN netmask, thus making		
IPv4 netmask	ip; Default: 255.255.255.0	the DHCP server think that it's serving a		
		larger or smaller network than it actually is		
		Additional options to be added to the DHCP		
		server. For example with '26,1470' or		
		'option:mtu, 1470' you can assign an MTU		
DHCP Options	DHCP options; Default: " "	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.

orking mode AP	-				
WLAN Information					Ð
OFF/ON	SSID	Encryption	Channel	Operation	
•	WR100LG-2.4G_154F14	None	11	6 0	

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.



Enable wireless		
SSID	WR200LG-2.4G_A0B227	
Hide SSID		
Encryption	WPA2-PSK	
Cipher	Force CCMP (AES)	
Кеу	•••••	<u>}</u> ∼≺
Channel	11 (2.462 GHz)	
Advanced settings	0	

	Copyright © 2021	by Queclink Wireless Solutions.		
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-	The type of Wi-Fi encryption used.		
	Default: No encryption			
	Auto Force CCMP			
Cipher	(AES) Force TKIP Force TKIP	An algorithm for performing encryption or		
Cipiter	and CCMP (AES); Default:	decryption		
	Auto			
		Pre-shared key, a custom passphrase used		
Кеу	string; default: none	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.

Advanced settings	۲	
Mode	802.11g+n	-
HT mode	20MHz	-
Country code	CN - China	$\overline{}$
Transmit power	100 %	

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



	802.11g+n; Default:	provide different wireless standard support		
	802.11g+n	which directly impacts the radio's		
		throughput performance		
Country code	country code; Default: 0 -	SO/IEC 3166 alpha2 country codes as		
Country code	World	defined in ISO 3166-1 standard		
	1000/1000/1000/1000/1000/	Wi-Fi signal power. The percentage of the		
Transmit power	100% 80% 00% 40% 20%	maximum output power. Reduce the power		
	Delault: 100%	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.

2.4G WIFI					
Working mode	STATION				
Station					Scan
Link Quality	OFF/ON	SSID	BSSID	Encryption	
					Refresh

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.

50	SSID	Encryption	
all	queclink_sz	WPA2PSK	Join
all	HWFL59522C	mixed WPA/WPA2PSK	Joir
att	queclink	WPA2PSK	Joir
al	WR100LG-2.4G_gopro	OPEN	Join
af	FAST_mark	mixed WPA/WPA2PSK	Join
al	queclink	WPAJPSK	Join
	360	WPA2PSK	Join
n	queclink_zoom	mbed WPA/WPA2PSK	Join
all la	CMCC	mixed WPA/WPA2P5K	Join
a C	queclink	WPA2PSK	Join
all	queclink	WPA2P5K	Join
- aC	MERCURY_AE30	OPEN	Join
all a	queclink	WPA295K	Join
- C	RUT_4652_2G	WPAPSK	Join
aff	Queclink_Office	WPA2P5K	Join
.d	ChinaNet-bWqW	mbed WPA/WPAJP5K	Join
all a	WR200LG-2.4G_AABBC0	WPA2PSK	Join
	RUT955_C6A0	WPA2PSK	Join
	#25+2.4G	mixed WPA/WPA2PSK	Join
	CHCC_2	WPA2PSK	Join
	off sta	OPEN	loin

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.



Static RIP Protocol

Destination subnet IP address	Netmask	Interface	Gateway	Metric	MTU	Operation
		WAN (Wired)				Ū

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 [01500]; 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.



Static	RIP Protocol								Petwork / Routing
_									
G	ieneral								
		Enable							
		Enable vty							
		Import config	浏览 未选择文件。						
		Version	2	-					
		Neighbor		Ð					
R	IP Interfaces					TI	his section contains no values	; yet	+
		Enable			Interface	Passive interfac	ie -		
									Save
									_

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:	Network interface to be used with the RIP
Interface	no	interface
		Sets the specified interface to passive mode.
		On passive mode interface, all receiving
Passive interface	yes no; Default: no	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 \bigcirc 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.



т	Doma	in Filter	IP/MAC Filter	DMZ	DDOS						
SN (NAT DFF/ON	Protoco	l Source z	one	Source IP	Source	port	To source zone	To source IP	To source port	Operation
DI	NAT										÷
0											

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.

IAT Domain Filter IP/MAC Filter	DDDS	
Site Blocking		
Mode	lacklist 🔍	
Enable	Domain name	•
C	www.163.com	<u>ال</u>
C	www.1688.com	۱
		Save

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 <i>www.website.com</i> or <i>website.com</i> , 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 address included in the list and allows everything else.





	, and the second s								
		Mode	Blacklist	~					
IP Filter									e
OFF/ON	Src ad	dress	Protocol	Sou	urce port	Dest port	Interf	ace	Operatio
	192.168	3.1.234	ALL	r			WAN (Wired		Ū
MAC Filter									e
0	FF/ON	MAC a	ddress	Protocol	Source por	t Dest po	ort Interface	0	peration

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 ICM P ; Default: All	Specifies the protocol to blocked/unblock.
Source Port	integer [065535]; 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 [065535]; 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.

T Domain Filter IP/MAC Filter	DMZ DDOS
DMZ	
OFF/ON	DMZ host
	192.168.1.3
	Sau

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.

			DMZ
s	SYN Flood Protection		
	Enable S	YN flood protection	0
		SYN flood rate	250
		SYN flood burst	50
		TCP SYN cookies	
R	Remote ICMP Requests		
	Er	able ICMP requests	
		Enable ICMP limit	•
		Limit period	Second
		Limit	10
		Limit burst	5
s	SSH Attack Prevention		
		Enable SSH limit	•
		Limit period	Second
		Limit	10
		Limit burst	5
	ITTP Attack Prevention		
		Enable HTTP limit	
		Limit period	Second
		Limit	10
		Limit	10
		Limit burst	10

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.

OFF/ON	Tunnel name	Туре	Operation	
•	РРТР	Server	e b	
Role: Client	New configuration name:	e		

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.



PPTP	L2TP	OpenVPN	IPsec	GRE Tunnel	
PPT	P Client Inst	ance: queclink	r		
м	ain Settings		-		
	un seungs		Enable		
		D	efault route	0	
		Clie	ent to client		
		* Ser	ver address		
		•	User name		
			* Password		> ,
Ва	ick to Overv	iew			Save
					_

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.

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

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).



Main Setti	ngs				
	Enable				
	* Local IP				
	* Remote IP range start				
	* Remote IP range end				
Client					G
	User name	Password		PPTP client's IP	
	wr100		\succ		<u></u>

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.

	OFF/ON		Tunnel name	Туре	Oper	ation
			L2TP	Server	Ø	<u>ال</u>
Role:	Client	- New c	configuration name:	•		



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.

L2TP Client Instar	nce: queclink					
Main Settings						
	Enable					
	Default route					
	Client to client					
	* Server address	10.65.17.45				
	* User name	admin				
	* Password		\succ			
Back to Overvie	w					Save

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.		
		Frequency (in seconds) at which LCP echo		
Koon alivo	integor: default: none	requests are sent to the remote instance in		
Reep alive	integer, deladit. none	order to determine the health of the		
		connection.		
Server	ip host; default: none	IP address or hostname of an L2TP server.		
Usornamo	string: default: none	Username used for authentication to the L2TP		
Osername	stillig, deladit. hone	server.		
Password	string: default: none	Password used for authentication to the L2TP		
Passworu	sunig, default. none	server.		
		When turned on, this connection will become		
		the router's default route. This means that all		
		traffic directed to the Internet will go through		
Dofault routo	voslad: dofault: no	the L2TP server and the server's IP address		
Deladit Toute	yesfilo, deladit. Ilo	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).



PPTP L2TP OpenVPN IPsec	GRE Tunnel				
L2TP Server Instance: L2TP					
Main Settings					
Enable					
* Local IP	192.168.2.1				
* Remote IP range start	192.168.2.10				
* Remote IP range end	192.168.2.30				
Client		B 1			÷
User name		Password	\sim	L2TP client's IP	<u>⊡</u>
user			· · · ·		
Back to Ourseinu					Com.
Back to overview					Save

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	ip;	L2TP IP address leases will begin from the		
begin	default: 192.168.0.20	address specified in this field.		
Remote IP range	ip;	L2TP IP address leases will end with the address		
end	default: 192.168.0.30	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.



penVPN Configuration						
OFF/ON	Tunnel name	Туре	TUN/TAP	Protocol	Port	Operation
	wr100	Server	TUN	UDP	1194	r ti
Role: Client	New configur	ation name:		•		

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.

enVPN Client Instance: queclink	
Main Settings	
Enable	0
Enable OpenVPN config from file	0
TUN/TAP	TUN (tunnel)
Protocol	UDP
Port	1194
LZO	0
Authentication	TLS
Encryption	BF-CBC 128 (default)
TLS cipher	All
• Remote host/IP address	queclink.com
Resolve retry	infinite
Keep alive	60 120
Remote network IP address	
Remote network IP netmask	
HMAC authentication algorithm	SHA1 (default)
Additional HMAC authentication	None
Extra options	0
Use PKCS #12 format	
Certificate authority	Browse No file is selected
Client certificate	Browse No file is selected
Client key	Browse No file is selected
Private key decryption password (optional)	*

Field Name	Value	Description		
Enable OpenVPN	unal nas dafasilts na	Enables custom OpenVPN configuration from		
config from file	yes mo; default. no	file.		
Enable	yes no; default: no	Turns the OpenVPN instance on or off.		
	TUN (tunnel) TAP	Virtual network device type.		
TUN/TAP	(bridged); default:	TUN - a virtual point-to-point IP link which		
	TUN (tunnel)	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.
		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
	UDP TCP;	issue occurs. It should be used when reliability
Protocol	default: UDP	is crucial (for example, in file transfer).
		User Datagram Protocol (UDP) - packets are
	1	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).
		TCP/UDP port number used for the
		connection. Make sure it matches the port
	integer [065535];	number specified on the server side.
Port	default: 1194	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 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:
	TLS Static Key Password	Certificate Authority (CA)
Authentication		Client certificate
	ILS/Password;	Client key
	default: TLS	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.
	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	
Encryption	128 AES-192-CFB	Algorithm used for packet encryption.
	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	
TIS: TIS cipher	All DHE+RSA Custom;	Packet encryption algorithm cinhor
res. res cipiter	default: All	
TLS: Allowed TLS	All DHE+RSA Custom;	A list of TLS ciphers accepted for this
ciphers	default: All	connection.
Remote host/IP	in dofaulti nono	IP address or hostname of an OpenVPN
address	ip; default. none	server.
		In case server hostname resolve fails, this field
Decelue notre	integer infinite;	indicates the amount of time (in seconds) to
Resolve retry	default: infinite	retry the resolve. Specify infinite to retry
		indefinitely.
	two integers	Defines two-time intervals: the first is used to
Keep alive	separated by a space;	periodically send ICMP requests to the
	default: none	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.
		Certificate authority (CA) is an entity that
TLS/Password:	ca filo, dofault, nono	issues digital certificates. A digital certificate
Certificate authority	.ca me, default. none	certifies the ownership of a public key by the
		named subject of the certificate.
	.crt file; default: none	Client certificate is a type of digital certificate
		that is used by client systems to make
TIS: Client cortificate		authenticated requests to a remote server.
TLS. Chefit Certificate		Client certificates play a key role in many
		mutual authentication designs, providing
		strong assurances of a requester's identity.
TIS: Client kov	.key file; default: none	Authenticates the client to the server and
TLS. Chefit Rey		establishes precisely who they are.
TLS: Private key		A password used to decrypt the server's
decryption	string; default: none	private key. Use only if server's .key file is
password (optional)		encrypted with a password.
Static key: Static	kov filo: dofault: popo	Uploads a secret key file used for server-
pre-shared key	.key me, default. none	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.

PPTP L2TP OpenVPN IPsec	GRE Tunnel
OpenVPN Server Instance: wr100	
Main Settings	
Enable	
Enable OpenVPN config from file	
TUN/TAI	> TUN (tunnel)
Protoco	L UDP
Por	t 1194
LZC	
Authentication	static key
Encryption	BF-CBC 128 (default)
Local tunnel endpoint I	172.16.0.3
Remote tunnel endpoint II	172.16.0.2
Remote network IP address	5
Remote network netmas	t 255.255.0
Static pre-shared ke	/ Browse No file is selected
Back to Overview	Save



Field Name	Value	Description	
Enable OpenVPN	vestor default: no	Enables custom OpenVPN configuration from	
config from file	yes mo, default. no	file.	
Enable	yes no; default: no	Turns the OpenVPN instance on or off.	
		Virtual network device type.	
		TUN - a virtual point-to-point IP link which	
	TUN (tunnel) TAP	operates at the network layer (OSI layer 3),	
TUN/TAP	(bridged);	used when routing is required.	
	default: TUN (tunnel)	TAP - a virtual Ethernet adapter (switch),	
		operates at the data link layer (OSI layer 2),	
		used when bridging is required.	
		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	
	1	receive packets in the order they were sent by	
		numbering, analyzing response messages,	
		checking for errors and resending them if an	
	UDP TCP; default: UDP	issue occurs. It should be used when reliability	
Protocol		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).	
		TCP/UDP port number used for the	
		connection. Make sure it matches the port	
	integer [065535];	number specified on the server side.	
Port	default: 1194	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 mode, used to secure data	
		sessions.	
		Static key is a secret key used for server-client	
	TLS Static Key	authentication.	
Authentication	TLS/Password;	TLS authentication mode uses X.509 type	
	default: TLS	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.
	DES-CBC 64 RC2-CBC	
	128 DES-EDE-CBC	
	128 DES-EDE3-CBC	
	1921DESX-CBC	
	192 BC2-40-CBC	
	128 RC2-64-CRC	
	64 ΔFS-128-CER	
	178 AFS-178-CER1	
	120 ALS-120-CLD1	
	128 ALS-128-CI B8	
	120 AES-120-OFB	
	120 AES-120-CBC	
	128 AES-128-GUM	
Incryption	128 AES-192-CFB	Algorithm used for packet encryption.
	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	
Static key: Local	ip: default: none	IP address of the local OpenVPN network
tunnel endpoint IP		interface.
Static key: Remote	in: default: none	IP address of the remote OpenVPN network
tunnel endpoint IP		(client) interface.
Static key: Remote	in: default: nono	I AN IP address of the remote network (client)
network IP address		
Static key: Remote	netmask;	LAN IP subnet mask of the remote network
network IP netmask	default: none	(client).
TLS/TLS/Password:	All DHE+RSA	
TLS cipher	Custom; default: All	Packet encryption algorithm cipher.



TLS/Password:	AII DHE+RSA	A list of TLS ciphers accepted for this
Allowed TLS ciphers	Custom; default: All	connection.
TLS/TLS/Password:	veslno: default: no	Allows OpenVPN clients to communicate with
Client to client		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 \rightarrow VPN \rightarrow IPsec section, enter a custom name and click Add icon.



		_
sec Configuration		
Enable		
IKE version	IKEv1 🔍	
Mode	Main	
Туре	Tunnel T	
My identifier type	FQDN T	
On startup	Start 👻	
My identifier		
Local IP address/Subnet mask	0	
Left firewall		
Force encapsulation		
Dead peer detection		
Remote VPN endpoint		
Remote IP address/Subnet mask	0	
Right firewall	0	
Enable keep alive		
Host		
Ping period	S	
Allow webbi access		
custom options		
ase 1		
IKE encountion algorithm		
IKE authentication	SH41	
IKE DH group	MODP1536	
• IKE lifetime	28800 5	
nase 2		
ESP encryption algorithm		
ESP nash algorithm		
ESP PFS group	M0DP1530	
- ESP key lifetime	3000	

Field Name	Value	Description
Enable	yes no; default: no	Turns the IPsec instance on or off.
		Internet Key Exchange (IKE) version used for
		key exchange.
		IKEv1 - more commonly used but contains
		known issues, for example, dealing with
		NAT.
IKE version	IKEv1 IKEv2; default: IKEv1	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.
Туре	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 [032]. 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	Pre-shared key X.509;	Here you can choose authentication type
type	default: Pre-shared key	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 [032]. 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.
Ding pariod	od integer [09999999]; default: none	The frequency at which keepalive ICMP
		packets will be sent to the specified host or
(sec)		IP address.
Allow WebUI		Allows WebUI access for hosts in the VPN
access	yes no; default: no	network.
		Provides the possibility to further customize
Custom options	ipsec options; default: none	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	DES 3DES AES128 AES192	Algorithm used for data energy tion
algorithm	AES256; default: 3DES	Algorithm used for data encryption.
Authentication	MD5 SHA1 SHA256	Algorithm used for exchanging
/Hash	SHA384 SHA512;	Algorithm used for exchanging
algorithm	default: SHA1	authentication and hash information.
	MODP768 MODP1024	Diffie-Hellman (DH) group used in the key
DH group/PFS	MODP1536 MODP2048	exchange process. Higher group numbers
group	MODP3072 MODP4096;	provide more security, but take longer and
	default: MODP1536	use more resources to compute the key.
Lifetime	integer; default: 8 hours	Defines a time period after which the phase
Liletime		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.

GRE	E Configurat	ion			
	(DFF/ON	Tunnel name	Oper	ation
			queclink	Ľ	I
	New con	figuration name:	•		

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.

Main Settings			
En	abled 💽		
Tunnel s	source 192.168.8.4		
Remote endpoint IP ad	ddress 192.168.8.7		
	MTU 1476		
	TTL 255		
Outbour	nd key		
Inbour	nd key		
Don't frac	gment 💽		
Keep	palive		
Tunnel Settings			
	11		
Local GRE Interface IP ac	ldress		
Local GRE interface net	tmask		
Remote GRE interface IP ad	ddress		
couting Settings			
Remote sub	bnet IP address	Remote subnet netmask	Operation

Field Name	Value	Description
Enabled	yes no; default: no	Turns the GRE Tunnel instance on or off.
Turnel course	network interface;	Network interface used to establish the GRE
runner source	default: none	Tunnel.
Romoto ondpoint		External IP address of another GRE instance
IP address	ip; default: none	used to establish the initial connection
		between peers.
		Sets the maximum transmission unit (MTU)
MTU	integer; default: 1476	size. It is the largest size of a protocol data
		unit (PDU) that can be transmitted in a
		single network layer transaction.
		Sets a custom TTL (Time to Live) value for
	integer [0255]; default: 255	encapsulated packets. TTL is a field in the IP
		packet header which is initially set by the
TTI		sender and decreased by 1 on each hop.
116		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.
	integer [0 65535].	A key used to identify outgoing packets. A
Outbound key	dofault: nono	This value should match the "Inbound key"
		value set on the opposite GRE instance or



	r	F
		both key values should be omitted on both
		sides.
		A key used to identify incoming packets.
	integer [0, CEE25].	This value should match the "Outbound
Inbound key	Integer [U.05535];	key" value set on the opposite GRE instance
	default: none	or both key values should be omitted on
		both sides.
		When unchecked, sets the nopmtudisc
Don't fragment	yes no; default: yes	option for tunnel. Cannot be used together
		with the TTL option.
	yes no; default: no	Turns "keep alive" on or off. The "keep
		alive" feature sends packets to the remote
Keep alive		instance in order to determine the health of
		the connection. If no response is received,
		the device will attempt to re-establish the
		tunnel.
	integer [0255]; default:	Frequency (in seconds) at which "keep
Keep alive interval		alive" packets are sent to the remote
	none	instance.
Local GRE		ID address of the local CBE Tuppel network
interface IP	ip; default: none	interface
address		Interface.
Local GRE	notmask: dofault: none	Subnet mask of the local GRE Tunnel
interface netmask	neunask, uerault. none	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	in default, none	IP address of the network behind the device
address	ip; default. none	that hosts the remote GRE instance.
Remote subnet	notmoski dofoulti nono	Subnet mask of the network behind the
netmask	netmask; default. none	device that hosts the remote GRE instance.
Lifatima	integer; default: 8 hours	Defines a time period after which the phase
Lifetime		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.



SMS Utilities

OFF/ON	Action	SMS text	
	reboot device	reboot	
	switch sim card	sim	
	restore factory setting	restore	
	get device status	getstatus	
message format:'text password', password is the admin password, for example:'reboot admin01'			

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.



RS232/RS485 MQTT<->MODBUS RTU MODBUS TCP

RS232/RS485 Serial Configuration		
Enabled		
Baud rate	115200	-
Data bits	8	-
Parity	None	-
Stop bits	1	~
Flow control	None	-
Serial type	Console	-
Echo		

Save

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;	Specifies the serial connection type
	Default: Console	specifies the serial conflection type.
		Toggles RS232 echo ON or OFF. RS232 echo
Echo	yes no; Default: no	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:



RS232/RS485 MQTT<->MODBUS RTU MODBUS TCP

RS232/RS485 Serial Configuration

Enabled	
Baud rate	115200
Data bits	8
Parity	None
Stop bits	1
Flow control	None
Serial type	Over IP 📃
Protocol	тср
Mode	Server
Port	7001



Field Name	Value	Description			
Protocol	TCD: Default: TCD	Specifies the protocol used in the			
FIOLOCOI	TCF, Delault. TCF	communication process			
		Specifies the device's role in the			
		connection:			
	Sorver Client Didirect:	Server - the device waits for incoming			
Mode	Mode Default: Server	connections			
		Client - the device initiates the connection			
		Bidirect - acts as client by default but waits			
		for incoming connections at the same time			
No loading zoros	voslao: Dofault: no	Specifies that the first hex zeros should be			
No leading zeros	yes[110, Delault. 110	skipped			
TCD port	integer [065535]; Default:	The port number used to connect to the			
		server			
		Disconnects clients after the amount of			
Timeout (s)	integer; Default: " "	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:



RS232/RS485 Serial Configuration			
Enabled			
Baud rate	115200		
Data bits	8		
Parity	None		
Stop bits	1		
Flow control	None		
Serial type	Over IP	•	
Protocol	TCP	•	
Mode	Client	•	
Server address	10.50.60.3		
Port	4687		

Field Name	Value	Description		
Protocol	TCP; Default: TCP	The protocol used for data transmission		
		Server - waits for incoming connection		
Mode	Server Client Bidirect; Default: Server	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		
Common delanas	host ip; Default: no	Server address to which the client will		
Server address		connect to		
TCD nort	integer [065535]; Default:	The port number used to listen for		
TCP port		incoming connections		
Reconnect	integer Default. ""	Indicates the time period between		
intervals (s)	integer; Delault:	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.



Enabled				
MQTT server	192.168.1.102			
Port	1883			
Keepalive	60	s		
Topic(receive)	Query			
Topic(sent)	Sent			
Qos	Qos0			
Require authentication				
Authentication username	admin			
Authentication password	•••••	~		
TLS ON				

Field Name	Value	Description		
MOTT server	in host: default: 127.0.0.1	IP address or hostname of an MQTT		
		broker.		
Dort	integer [065535];	Port number of the MOTT broker		
POIL	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.

5232/RS485 MQTT<->MOI	DBUS RTU MODBUS TO	CP CP		
MODBUS TCP Configuration				
	Enabled 💽			
	* Port 502			
				_
				Save

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.


DDNS Configuration				
DDNS name	OFF/ON	Host name	Status	Operation
test		-	Disconnected	2
New configuration name:		•		

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:

DDNS Settings		
Enable	•	
Service	Custom 💌	
Custom update-URL		
Lookup host		
* Hostname		
* User name		
* Password	password 😽	
* IP renew interval	10	
IP renew interval unit	min	

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



		make necessary updates.
IP renew interval		Frequency at which the device will
	integer [5600000]; Default: 10	check whether it's IP address has
		changed
IP renew interval	Minutes Hours Days;	Unit which is used in ID renow interval
unit	Default: Minutes	Onit 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.

Task ICMP						
OFF/ON	Task name	Excute time	Task type	Action	Operation	÷
	test	Saturday 12:00	Custom	Reboot	C I	Ì
						Save
Task ICMP						
ming Task						
	Enable 🕥					
	* Task name test					
	Task type Cus	tom				
	Action Reb	oot				
	* Hour 12					
	* Minute 00					
	3	unday				
		londay				
		uesday Iodoosday				
	Days 0	hursday				
		riday				
		aturdav				
ck to Overview						Sav

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 [023]; Default: 23	The hour of the day on which the router will
		reboot
Minute	integer [059]; Default: 0	The minute of the hour on which the router
		will reboot
Days	Monday Tuesday	The day or multiple days on which the router
	Wednesday Thursday	will reboot
	Friday Saturday Sunday;	
	Default: none	

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.

ng Task ICMI	Р				
ICMP Checking			•		÷
Enable	Name	Action	Host to ping	Backup address	Operation
	test	Reboot	8.8.8.8	114.114.114.114	C ū
					Save

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

CMP Checking Configuration				
Enable				
* Name	test			
Action if no echo is received	Reboot			
Interval between pings	5 mins			
* Ping timeout (sec)	5			
* Packet size	56			
* Retry count	2			
Interface	WAN	-		
* Host to ping	8.8.8.8			
Backup host to ping	114.114.114.114			

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 [19999]; 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 [19999]; 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	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.

Time Mobile	LAN WLAN		
Time Zone Settings			
	Current system time F	ri Sep 10 18:27:12 2021 💮	
	Time zone A	sia/Hong Kong 💌	
			_
		Skip Wizard	Next

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



	SIM1			
Auto APN				
Authentication method	None	-		
PIN number				
MTU	1500			

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

* IP address	192.168.1.1		
* Netmask	255.255.255.0		
HCP Server			
Enable DHCP	0		
Start	100		
Limit	150		
Limit Lease time	150 min		
Limit Lease time	150 120 min		

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

WiFi-2.4G Configuration					
Enable wireless	•				
* SSID	WR100LG-2.4G_154F14				
Encryption	No Encryption	-			
Mode	802.11g+n				
					Skip Wizard Fini

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.

Host Name				
• Host nam	e Queclink-WR100LG.com]		
Administrator Password Password requirements: Minimum 4 ch	aracters; Maximum 32 characters			
Current passwo	d	`		
New passwo Confirm new passwo	d	$\overset{\star}{\prec}$		
				Save

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.

Enabling ren	note SSH access makes your device reachable fro	n WAN, this might pose a security risk, especially if you are u	sing a weak or default user password!	
	Enable SSH access			
	Remote SSH access			
	* Port 22			
нттр				
Enabling ren	note HTTP access makes your device reachable fr	om WAN, this might pose a security risk, especially if you are	using a weak or default user password!	
	Remote HTTP access			
	* Port 80			
	Port Bo			

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 [065535]; 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.

eral	Access Control	Configuration		
Backup	p Configuration		Restore Configuration	
	Backup archive	Download		Restore from file
Restor	e Default Settings		Restore from backup	选择文件
	Restore to default	Restore		Upload archive

4.4.3 Reboot

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

Reboot	
Reboot	
Warning! During reboot you will temporarily lose the connection.	

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.



neral		
Current system time	Sat Sep 11 10:57:43 2021 💿	
Time zone	Asia/Hong Kong 🔍	
Enable NTP		
* Update interval	600 s	
ne Servers		
	Host name	Operation
	pool.ntp.org	<u> </u>
	cn.ntp.org.cn	Ū.
	time.windows.com	.

Field Name	Value	Description
Current system time		Current local time of the router.
Time zone	time tong, default: LITC	The router will sync time in accordance with
	time zone; default. OIC	the selected time zone.
Enable NTP	yes no; default: yes	Turns NTP on or off.
Update interval (in	integer default 2000	Defines how often the router will update the
seconds)	integer; default: 3000	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.

irrent Firmware Information		Patche	s	
Firmware version:	R00A01V01Beta28		Name	Version
Firmware build date:	2021-05-13, 15:52:45		Modem driver	00.06.06.1
Kernel version:	3.3.8			
Bootloader version:				
rmware Upgrade Settings				
rmware Upgrade Settings Keep all settings Upgrade from file) ware image file _ 演宽… 未选择文件。			



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

Upload file format error, please select the correct format file upload.

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
СНАР	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
РАР	Password Authentication Protocol
PC	Personal Computer
PIN	Personal Identity Number
РРР	Point-to-point Protocol
РРТР	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