



User Manual

---Apply to WL-R230 Series 4G/3G Router

V1.0

<http://www.wlink-tech.com>

Jan, 2024



Copyright © Shenzhen WLINK Technology Company Limited 2012 ~ 2024

Without our written approval, anyone can't extract, copy whole or part of content of this file and can't spread out in any format.

Important Notice

Due to the nature of cellular/wireless communications, transmission and reception of data can never be guaranteed, Especially the cellular signal quality is not good on the site. Data may be delayed, corrupted (i.e., have errors) or be totally lost, WLINK accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the router, or for failure of the router to transmit or receive such data. Wlink accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the router, or for failure of the router to transmit or receive such data.




Furthermore, due to product updates or functional upgrading, we may renew the content of this file, and this file only for reference. All statement, information, suggestion etc. in this file does not compose any form of guarantee and we WLINK reserves the right of final explanation.

Safety Precautions

- ◆ The router generates radio frequency (RF) power. When using the router, care must be taken on safety issues related to RF interference as well as regulations of RF equipment.
- ◆ Don't use the router in places where cellular products are prohibited.
- ◆ Make sure that the router will not be interfering with nearby equipment. For example: pacemakers or medical equipment. The antenna of the router should be away from computers, office equipment, home appliance, etc.
- ◆ Make sure plug an available SIM card in the router. Don't power on the router without SIM card for long time if router worked on 5G/4G mode.
- ◆ An external antenna must be connected to the router for proper operation. Only uses approved antenna with the router.
- ◆ Always keep the antenna with minimum safety distance of 30 cm or more from human body. Do not put the antenna inside metal box, containers, etc.

Various Signs

The manual also uses a variety of eye-catching signs to indicate the places to which special attention should be paid in operation. The significance of these signs are as follows.

 CAUTION	Caution indication, used to reminder and warning during product operation and testing.
 NOTE	Note indication, use to complement the additional descriptions.
 Configuration Instance	Configuration instance indication, use to show configuration instance as reference.

Version History

Updates between document versions are cumulative. The latest document version contains all updates made to previous version.

Data	Document Version	Firmware Version	Description
2024-1-5	V1.0	Rm.0.2.5-240105-152307.bin	Released.

Shenzhen WLINK Technology Company Limited

Add 2A, F5 Building, TCL International E City, No.1001 Zhongshanyuan Rd.,
Nanshan Dist., Shenzhen, 518052, China

Web <http://www.wlink-tech.com>

Service Email support@wlink-tech.com

Tel 86-755-86089513

Fax 86-755-26059261

Contents

1 Overview	6
1.1 Key Features	6
1.2 Specifications	6
2 Hardware Introduction	9
2.1 WL-R230 Panel	9
2.2 Dimension	10
2.3 LED Indicator	11
2.4 Ethernet Connection	11
2.5 Serial Port Connection	11
2.6 Power Supply	11
2.7 Review	12
3 Router Configuration	13
3.1 Local Configure	13
3.2 Status	14
3.3 Overview	14
3.4 Traffic Stats	15
3.5 Device List	15
3.6 Tool Column	16
3.7 Basic Network	18
3.8 WLAN Setting	28
3.9 Advanced Network Setting	30
3.10 Firewall	39
3.11 VPN Tunnel	41
3.12 Administration	57

4 Configuration Instance	70
4.1 VLAN	70
4.2 WAN Backup (WAN as Main, Cellular Backup)	72
4.3 Port Forwarding	74
4.4 Port Redirecting	75
4.5 IP Passthrough	76
4.6 Captive Portal	78
4.7 GPS Settings	81
4.8 Firewall	84
4.9 VPN Tunnel	85

1 Overview

As an upgraded version of our best-selling R210, the R230 maintains its compact and rugged construction, secure and reliable performance, cost-effective price, but offers more functionalities. Its rich interfaces – three Fast Ethernet ports, two serial ports, and two digital input/output allow users to connect various devices to the Internet.

The R230 performs auto-failover between wired and wireless WAN to ensure uninterrupted connectivity. Users can easily manage thousands of R230 with Wlink RMS, which is a cloud-based system for easy setup, remote monitoring, mass configuration and maintenance. In addition, the R230 is eSIM supported, making it easier to switch from one carrier to another. All these advantages make the R230 an ideal choice for use in critical industrial IoT / M2M applications that require high-speed and stable communications.

Especially, the R230 is eSIM supported, making it easier to switch from one carrier to others.

1.1 Key Features

Dual SIM redundancy for continuous cellular connections, supports 2G/3G/4G.

WAN link management: cellular WAN/Ethernet WAN/WLAN WAN backup.

VPN tunnel: IPSec/OpenVPN/PPTP/L2TP/GRE/Wireguard

Supports Modbus router (Modbus RTU/ASCII to Modbus TCP).

Supports GPS (optional), provides real time location and tracking.

Auto reboot via SMS/Timing.

Supports WLINK M2M management platform.

Flexible Management methods: Web/CLI/SNMP/WLINK M2M Platform.

Firmware upgrade via Web/CLI/USB/SMS/WLINK M2M management Platform.

Various interfaces: RS232/RS485/Ethernet.

Wide range input voltages from 7.5 to 32 VDC and extreme operating temperature.

1.2 Specifications

Cellular

Number of antennas: 2

Connector: SMA, female

SIM slot: 2 (3.0V & 1.8V)

Standards: 5G Redcap/ LTE-A/LTE/LTE CAT1

HSPA/WCDMA/UMTS

EDGE/GPRS

WiFi Interface

Number of antennas: 2

Connector: RP-SMA Male

IEEE 802.11 b/g/n 300Mbps(2T2R)

Output Power 11n HT40 MCS7: 15dBm, 11b CCK: 18dBm, 11g OFDM: 15dBm

Sensitivity

300Mbps: -65dBm

54Mbps: -73dBm

11Mbps: -86dBm

Ethernet Interface

Number of ports: 3x 10/100Mbps, 2 x LAN, 1xWAN

Magnet isolation protection: 1.5 KV

GPS Interface (Optional)

Number of antennas: 1

Connector: SMA Female with 50 ohms impedance

GPS Sensitivity: -160dBm

GPS Accuracy: 2.5m CEP

Update Rate: 1Hz@5Hz

Time to First Fix: Cold Status 27s, Hot status 1s.

Protocol: NMEA-0183 2.3V

Serial Interface

Number of ports: 1xRS232, 1xRS485

Connector: 3.5mm RP female socket

Baud rate: 300bps to 115200bps

RS232: TxD, RxD, GND

RS485: A (Data+), B (Data-), GND

Digital Input / Digital Output

Number of ports: 1xDI (wet contact), 1xDO (wet contact)

Connector: 3.5 mm RP female socket

ESD withstand level: contact: ± 6 K, air: ± 8 K

Absolute maximum VDC: "V+" +5V DC (DI), 30V DC (DO)

USB Port

Number of ports: 1 x Mini USB for configuration/upgrade/troubleshooting

Connector: Mini Female

Speed: 2.0high speed up to 480Mbps

Software (Basic features of WLINKOS)

Network protocols: PPP, TCP, UDP, ICMP, HTTP, HTTPS, DNS, NTP, SMTP, Telnet, SSH2, DDNS, etc.

VPN tunnel: IPsec, OpenVPN, GRE, PPTP/L2TP, Wireguard, Zerotier

Serial port: Transparent, TCP Client/Server, UDP, Modbus RTU

Management: Web, CLI, SMS, WLINK M2M Platform

Consumption

Voltage: DC +9~60V (standard 12V/1.5A power adapter)

SIM/R-UIM Card: 1.8V/3V

Idle: 160mA@+12VDC

Online: 155mA@+12VDC

Other

Galvanized metal with grounding Screw

Dimension: 102mm x 100mm x 42mm (not including antenna)

Weight: 350g (not including accessories)

Operation temperature: -30~+75℃

Store temperature: -40~+85℃

Related humidity: 0~95% (non-condensing)

Guarantee: two years

2 Hardware Introduction

This chapter is mainly for hardware introduction, there would be some difference between the scheme and real object. But the difference won't have any influence to products performance.

2.1 WL-R230 Panel



Interface	Description	Note
Main	4G Main SMA Antenna Connector, 50Ω	
Aux/GPS	4G Aux SMA Antenna Connector, 50Ω.	GPS Optional.
Wi-Fi1	Wi-Fi SMA-RP Antenna Connector, 50Ω.	300Mbps, 2T2R
Wi-Fi2	Wi-Fi SMA-RP Antenna Connector, 50Ω.	300Mbps, 2T2R
USB	USB2.0. Configuration, upgrade and troubleshooting	
Reset	Reset router to default setting.	Press 5s for Reset
LAN1~LAN2	10/100M Base-TX, MDI/MDIX Self-adaptation	
WAN	10/100M Base-TX, MDI/MDIX Self-adaptation	
SIM Cover	Protect SIM cards.	Two SIM slots
DC Interface	Power interface. 9~60VDC	DC5.5mm
Terminal Block	9Pin Bock. Power interface, RS232, RS485, DI, DO	Dual-Power interfaces.
GND	Ground Screw	

2.2 Dimension



2.3 LED Indicator

silk-screen	status		Indication
Signal	Signal LED	Solid Light	LED1 indicates signal is Poor (CSQ0~10) LED2 indicates signal is good (CSQ11~19) LED3 indicates signal is strong (CSQ20~31)
	LED 1	Quick Blink	Offline
		Solid Light	4G Online
		Slow Blink	3G Online
PWR	Solid Light		System power operation.
WLAN	Solid light		WLAN enable, but no data communication.
	Quick Blinking		Data Send
	Dark		WLAN disable
ERR	Dark		System operation and LTE/3G online.
	Solid Light (Red)		System fail indicator such as SIM card/ module fail.
LAN(WAN)	Green	Solid light	Plugged
	Green	Blinking	Data in transmitting.
	Green	Dark	Unplugged

2.4 Ethernet Connection

Connect an Ethernet cable to the port marked ETH0 or ETH1 at the front of the R230 Router, and connect the other end of the cable to your computer.

2.5 Serial Port Connection

The serial port supports RS232 and RS485 ports as default. The serial port feature supports TCP/UDP client/server as optional, also supports Modbus protocol. You may check the feature in Serial App of Advanced Network UI.

2.6 Power Supply

Voltage input range: +9~60VDC.



WL-R230 supports reverse polarity protection, but always refers to the figure above to connect the power adapter correctly.

2.7 Review

After insert the SIM/UIM card and connect Ethernet cable and antenna, connect power supply adaptor or power cable.



Please connect the antenna before power on, otherwise the signal maybe poor because of impedance mismatching.

Notice:

- Step 1 Check the antenna connection.
- Step 2 Check SIM/UIM card, confirm SIM/UIM card is available.
- Step 3 Power on the industrial Router

----END

3 Router Configuration

WL-R230 Series routers support GUI and CLI configuration. This chapter introduce GUI configuration via Ethernet port, if need CLI configuration guide, please contact our technical support department by email: support@wlink-tech.com.

3.1 Local Configure

The router supports to be configured by local Ethernet port, you could specify a static IP or set as DHCP. The default IP address is 192.168.1.1, subnet mask is 255.255.255.0, please refer to following.

- Step 1 Click “start > control panel”, find “Network Connections” icon and double click it to enter, select “Local Area Connection” corresponding to the network card on this page. Refer to the figure below.

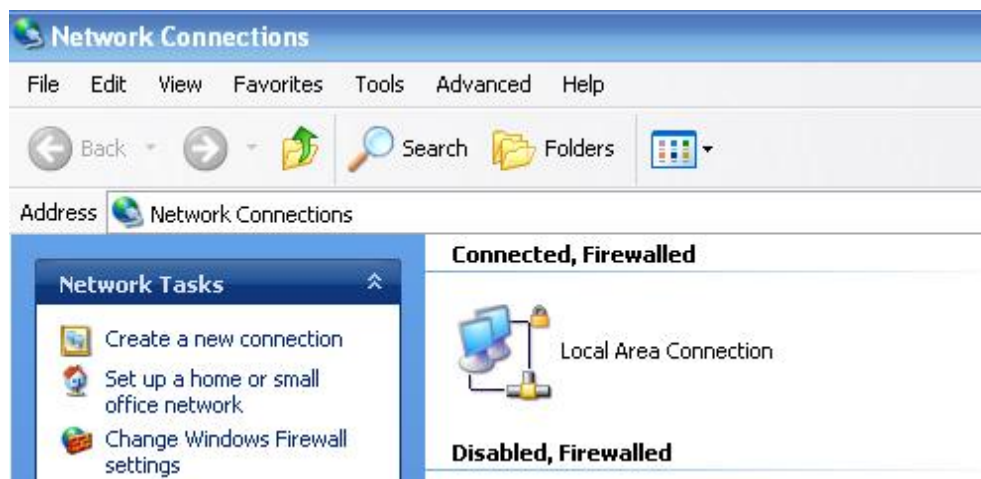


Figure 2-1 Network Connection

- Step 2 Obtain a IP address automatically or set up IP address, 192.168.1.xxx (XXX can be any number between 2~254)

- Step 3 Run an Internet Explorer and visit “<http://192.168.1.1/>”, to enter identify page.

User should use the default user name and password when log in for the first time



Figure 2-2 User Identify Interface

----END

3.2 Status

Check routers information such as status, traffic Stats and device list after login router. Especially, suggest change the password according to the prompts because of security requirement.

You haven't changed the default password for this router. To change router password [click here](#).

The UI will display "already changed login password successfully" after router reboot.

Already changed login password successfully.

3.3 Overview

The overview GUI will be display router system information, Ethernet ports status, VPN connection status, LAN information, 4G connection information and WLAN information,

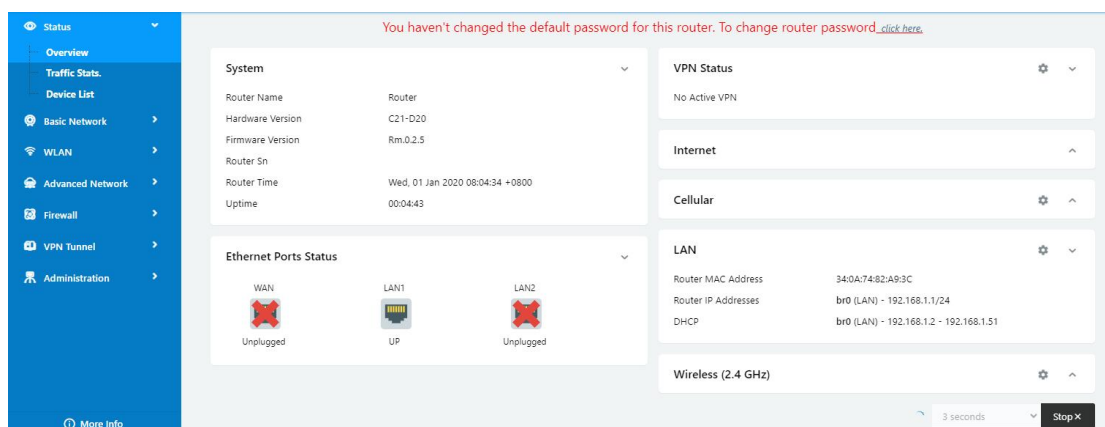


Figure 2-3 Router Status GUI



One Ethernet Port Icon for WL-R100 and WL-R130.
Two Ethernet Port Icons for WL-R200 and WL-R210.
Three Ethernet Port Icons for WL-R230.
Five Ethernet Port Icons for WL-R520.

3.4 Traffic Stats.

Click Status->Traffic Stats. to enter the traffic stats.GUI.to check Cellular/WAN traffic in real-time.

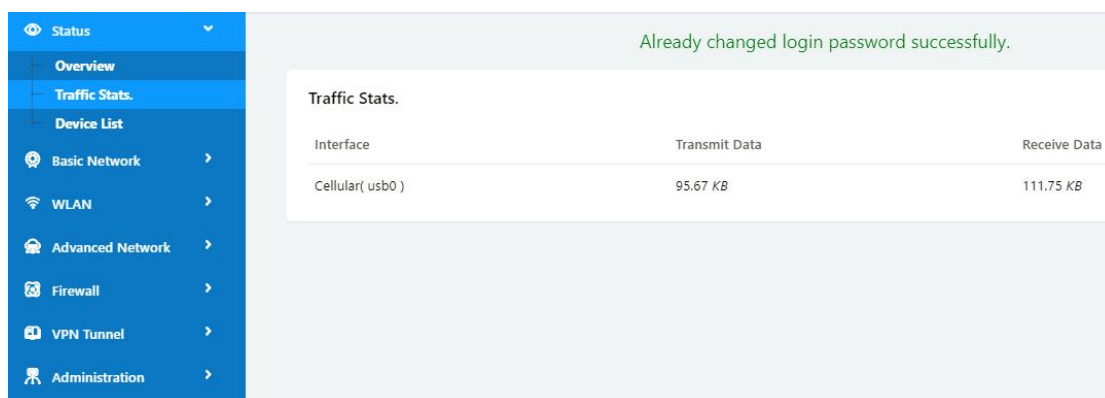


Figure 2-4 Traffic Stats. GUI

3.5 Device List

Click Status->Device List to enter the device list GUI.to check the connected devices information in the list.

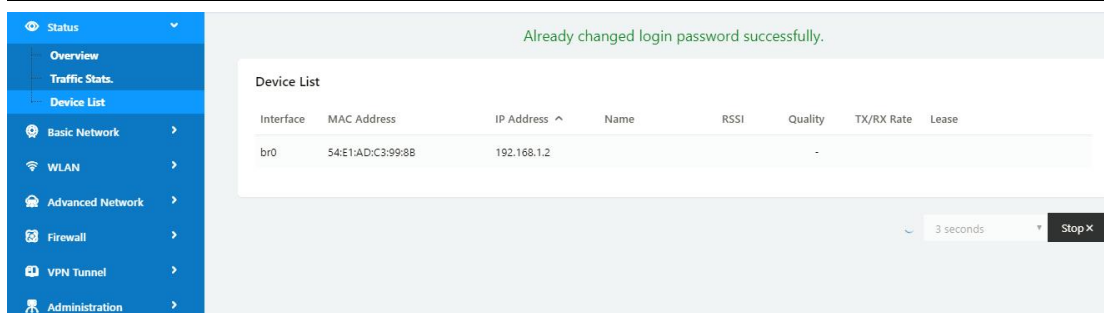


Figure 2-5 Device List GUI

3.6 Tool Column

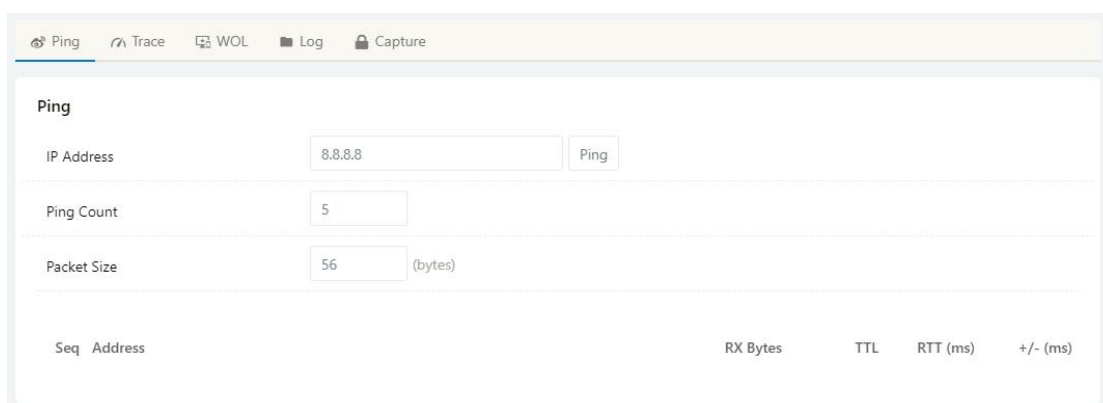


Figure 2-6 Tool Column GUI

3.6.1 Tools

3.6.1.1 Ping

Click Tools->Ping to enter ping test GUI. Used to test the reachability of a host on an Internet IP network and to measure the round-trip time for messages sent from the originating host to a destination server.



3.6.1.2 Trace

Click Tools->Trace to enter trace test GUI. diagnostic tool for displaying the route and measuring transit delays of packets across an Internet IP network.

3.6.1.3 WOL

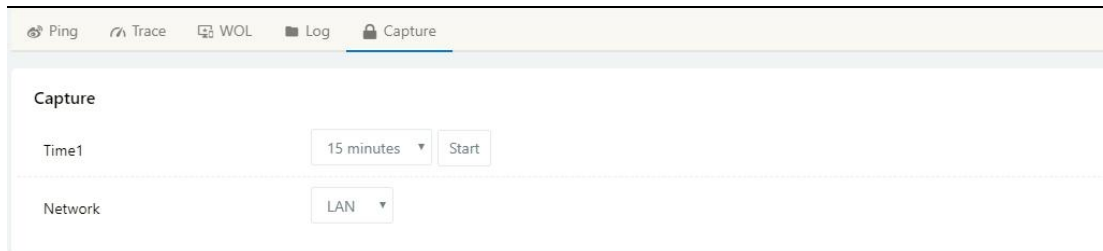
Click Tools-> WOL to enter WOL(Wake On Lan) GUI. Used to wake up those connected devices via WOL protocol. Click left mouse button to wake up the device.

3.6.1.4 Log

Click Tools-> Log to enter Log GUI. Use to check logs in GUI, download GUI and send logs to server.

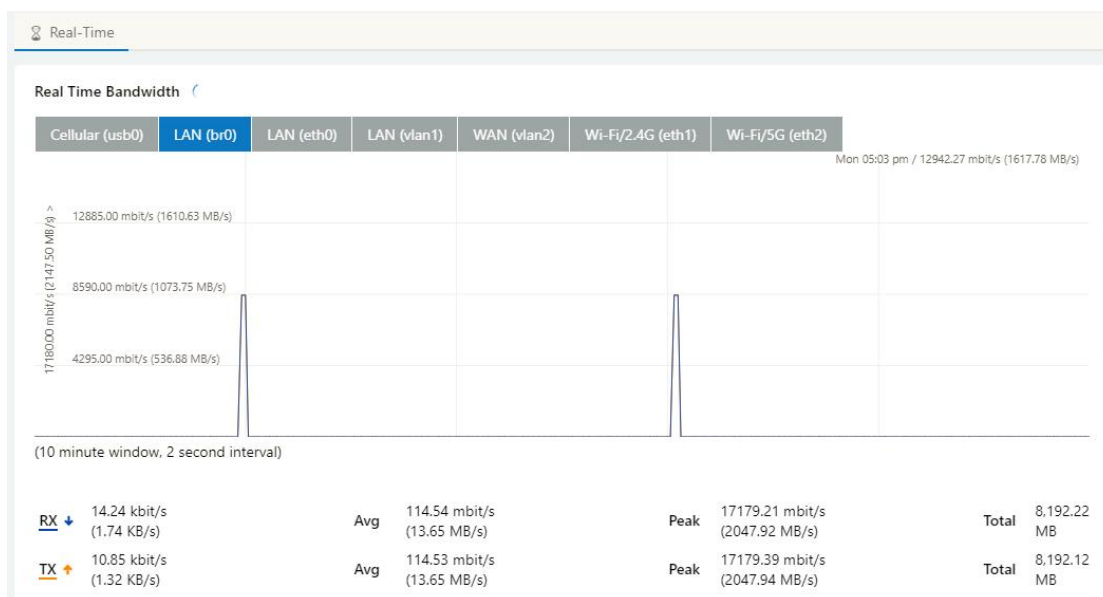
3.6.1.5 Capture

Click Tools-> Capture to enter capture data GUI. Use to capture LAN/WAN data packet to analyse what happen in the router.



3.6.2 Bandwidth

Click Bandwidth to enter bandwidth graphic GUI. Used to check cellular/LAN/Wi-Fi real-time bandwidth.



3.6.3 System

Click system to choose software reboot, hardware reboot and logout GUI.



3.7 Basic Network

3.7.1 WAN Setting

Step 1 Basic Network>WAN to enter below interface.

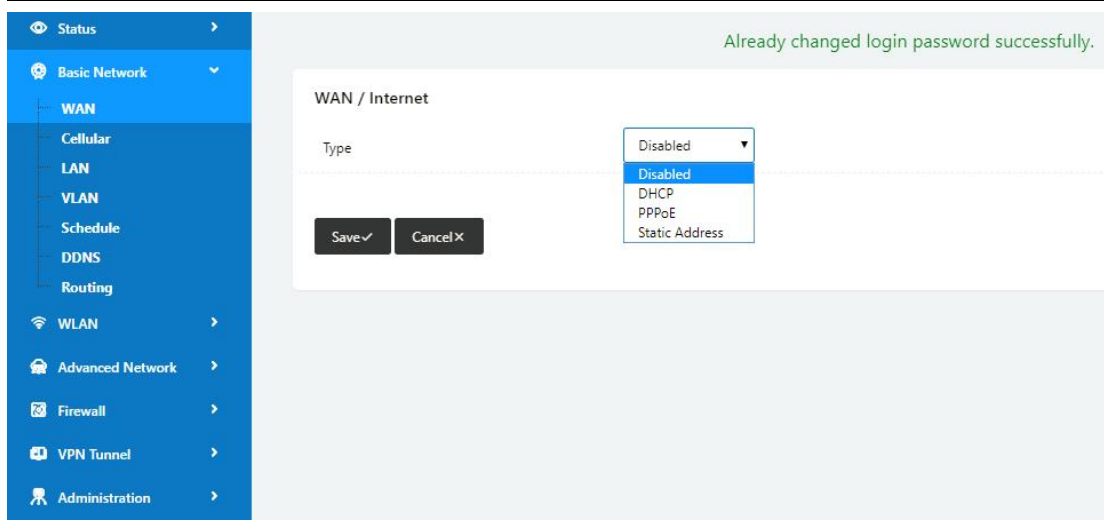


Table 2-1 WAN Setting Instruction

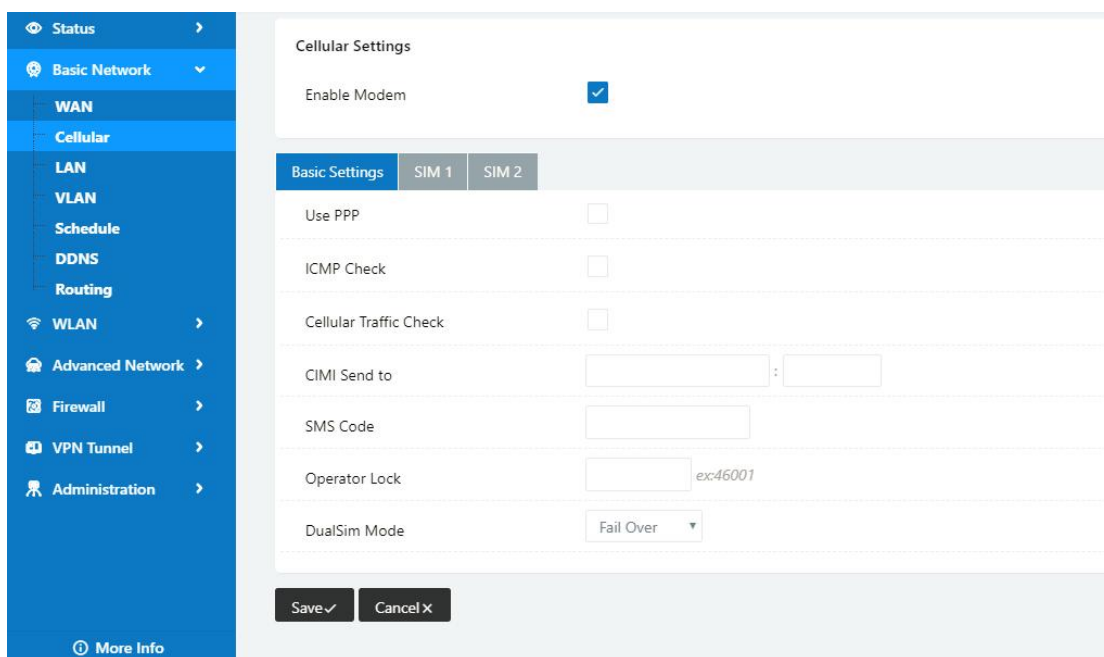
Parameter	Instruction
Type	Support DHCP, PPPoE, Static IP address

Step 2 After setting, please click “save” to finish, the device will reboot.

----End

3.7.2 Cellular Setting

Step 1 Basic Network-> Cellular, you can modify relevant parameter according to the application.





WL-R100 supports single SIM.
WL-R230 supports dual-SIM as default.
WL-R200/R520 supports dual-SIM as optional.
WL-R210 supports dual-SIM as default.
WL-R230 supports dual-SIM as default.

Table 2-2 Cellular Setting Instruction

Parameter	Instruction
Enable Modem	Enable/Disable 4G mode.
Use PPP	ECM dialup as default. PPP optional.
ICMP check	If enable ICMP check and setup a reachable IP address as destination IP, the router will reconnect/reboot once ICMP check failed.
Cellular Traffic Check	The router will reconnect/reboot once there's no Rx/Tx data.
CIMI Send to	Send CIMI to a defined IP and port by TCP protocol.
SMS Code	Remote control the router by SMS. Only the configured SMS code will work.
Operator Lock	Lock a specified operator for the router by MCC/MNC code.
Dual SIM Mode	【Fail Over】 Two SIM cards mutual backup. Once SIM1 failed,

Parameter	Instruction
	<p>it'll switch to SIM2 and work on SIM2, and vice versa.</p> <p>【SIM1 Only】 Only SIM1 works.</p> <p>【SIM2 Only】 Only SIM2 works.</p> <p>【Backup】 SIM1 is the primary SIM. Once SIM1 failed, it'll switch to SIM2 and work on SIM2 for a specified period of time, then it switches back to SIM1.</p>
Connect Mode	<p>【Auto】 The router will automatically connect to 3G/4G networks and give priority to 4G.</p> <p>【LTE】 Router will connect to 4G only.</p> <p>【3G】 Router will connect to 3G only.</p>
Pin Code	Some SIM cards are locked with a Personal Identification Number (PIN) code in case they are lost or stolen.
APN	APN is provided by local ISP, usually CDMA/EVDO networks do not need this parameter.
User	SIM card user name is provided by ISP
Password	SIM card password is provided by ISP
Auth. Type	Auto/PAP/Chap/MS-Chap/MS-Chapv2 authentication optional.
SIM Local IP Address	Fix SIM IP. The feature is available if carrier can provide this service.



NOTE ICMP Check and Cellular Traffic Check are alternative.

【ICMP Check】

Enable ICMP, Router will automatically check whether the defined IP address is reachable per 60s. If the IP address is unreachable and ICMP check is timeout at the first time, it will check 2 times every 3 seconds. If the third time is still failed, the router will redial.

The ICMP Check IP is a public IP or company server IP address.

ICMP Check	<input checked="" type="checkbox"/>
Check IP	8.8.8.8
Check IP (Optional)	4.4.4.4
Interval	60 (seconds)
Retries	3 (Times)
Fail Action	Reboot System ▼

【Cellular Traffic Check】

【Check Mode】 there are Rx(Receive), Tx(Transmission) and Rx/Tx check modes.

【Rx】 Router will check the 3G/LTE cellular receiver traffic. If no receiver traffic within the defined check interval, the router will implement the specified action reconnect or reboot.

Cellular Traffic Check	<input checked="" type="checkbox"/>
Check Mode	Rx ▼
Check Interval	10 (minutes) Range: 1 ~ 1440
Fail Action	Cellular Reconnect ▼

Step 2 After Setting, please click “save” icon.

----End

3.7.3 LAN Setting

Step 1 Basic Network>LAN to enter below interface

Already changed login password successfully.

Status
Basic Network
WAN
Cellular
LAN
VLAN
Schedule
DDNS
Routing
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
More Info

LAN

Bridge ^	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)
br0	192.168.1.1	255.255.255.0	✓	192.168.1.2 - 51	1440
1					

Add +

Save ✓ Cancel ✕

LAN

Bridge ^	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)
br0	192.168.1.1	255.255.255.0	✓	192.168.1.2 - 51	1440
1					

Add +

Save ✓ Cancel ✕

Table 2-3 LAN Setting Instruction

Parameter	Instruction
Bridge	Supports 4 LAN IP address for br0 to br3 interface. If need to support VLAN, please go to VLAN GUI.
Router IP Address	Router IP address, default IP is 192.168.1.1
Subnet Mask	Router subnet mask, default mask is 255.255.255.0
DHCP	Dynamic allocation IP service, after enable, it will show the IP address range and options of lease
IP Pool	IP address range within LAN
Lease	The valid time, unit as minute
Add	Add LAN IP address, supports 4 LAN IP addresses.

Step 2 After setting, please click “save” to finish, the device will reboot.

----End

3.7.4 VLAN

Step 1 Basic Network->VLAN to enter the VLAN setting page.

VLAN

VID ^	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
1	✓	✗	✓	✗	✓	✗	✓	✗	✓	✗	br0
2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	WAN
0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	none

Add+

Save✓

Cancel✕

Table 2-4 LAN Setting Instruction

Parameter	Instruction
VID	VLAN ID number. The VID range is from 1 to 15.
LAN1~LAN4, WAN	LAN
Tagged	Enable to make router can encapsulate and de-encapsulate the VLAN tag.
Bridge	Routers interface br0, br1, br2, br3 and WAN

Step 2 Please Click “Save” to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

3.7.5 Schedule

Step 1 Basic Network->VLAN to enter the Schedule setting page.

Status

Basic Network

WAN

Cellular

LAN

VLAN

Schedule

DDNS

Routing

WLAN

Advanced Network

Firewall

VPN Tunnel

Administration

More Info

Enabled Links

Link Name	Link Type	Description
modem	ECM/QMI	

ICMP Check

On	Link	Destination	Interval	Retries	Description
<input checked="" type="checkbox"/>					

Add +

Schedule

On	Link 1	Link 2	Policy	Description
<input checked="" type="checkbox"/>	modem	modem	FAILOVER	

Add +

Enabled Links

Link Name	Link Type	Description
modem	ECM/QMI	

ICMP Check

On	Link	Destination	Interval	Retries	Description
<input checked="" type="checkbox"/>					

Add +

Schedule

On	Link 1	Link 2	Policy	Description
<input checked="" type="checkbox"/>	modem	modem	FAILOVER	

Add +

Save ✓

Cancel ✕

Step 2 Please Click “Save” to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

3.7.6 Dynamic DNS Setting

Step 1 Basic Network->DDNS to enter the DDNS setting page.

Already changed login password successfully.

Dynamic DNS

IP Address: Use WAN IP Address 0.0.0.0 (recommended)

Auto refresh every: 28 minutes (0 = Disabled)

Dynamic DNS1

Service: None

Dynamic DNS2

Service: None

Save ✓ Cancel ✕

Dynamic DNS

IP Address: Use WAN IP Address 0.0.0.0 (recommended)

Auto refresh every: 28 minutes (0 = Disabled)

Dynamic DNS1

Service: None

Dynamic DNS2

Service: None

Save ✓ Cancel ✕

Table 2-5 DDNS Setting Instruction

parameter	Instruction
IP address	Default is standard DDNS protocol, for customized protocol, please contact Wlink engineer. Usually, use default IP 0.0.0.0
Auto refresh time	Set the interval of the DDNS client obtains new IP, suggest 240s or above
Service provider	Select the DDNS service provider that listed.

Step 2 Please Click “Save” to finish.

----End

3.7.7 Routing Setting

Step 1 Basic Network->Routing to enter the DDNS setting GUI.

Status

Basic Network

WAN

Cellular

LAN

VLAN

Schedule

DDNS

Routing

WLAN

Advanced Network

Firewall

VPN Tunnel

Administration

More Info

Current Routing Table

Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
192.168.1.0	*	255.255.255.0	0	LAN
127.0.0.0	*	255.0.0.0	0	lo

Static Routing Table

Destination	Gateway	Subnet Mask	Metric	Interface	Description
	0.0.0.0		0	LAN	

Add +

Miscellaneous

Mode

Gateway

RIPv1 & v2

Disabled

DHCP Routes

☒

Spanning-Tree Protocol

☐

Save

Cancel

Current Routing Table

Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
192.168.1.0	*	255.255.255.0	0	LAN
127.0.0.0	*	255.0.0.0	0	lo

Static Routing Table

Destination	Gateway	Subnet Mask	Metric	Interface	Description
	0.0.0.0		0	LAN	

Add +

Miscellaneous

Mode

Gateway

RIPv1 & v2

Disabled

DHCP Routes

☒

Spanning-Tree Protocol

☐

Save

Cancel

Table 2-6 Routing Setting Instruction

Parameter	Instruction
Destination	Router can reach the destination IP address.
router	Next hop IP address which the router will reach
Subnet Mask	Subnet mask for destination IP address
Metric	Metrics are used to determine whether one particular route should be chosen over another.
Interface	Interface from router to router.
Description	Describe this routing name.

Step 2 Please Click “ Save ” to finish.

----End

3.8 WLAN Setting

It's mainly for router which support Wi-Fi, you can modify and configure WLAN parameter through Web GUI, below is the common setting.



WL-R100 doesn't support Wi-Fi feature.

WL-R200 Wi-Fi feature is optional.

WL-R230/WL-R520 supports Wi-Fi feature as default.

3.8.1 Basic Setting

Step 1 WLAN->Basic Setting to configure relative parameter

Wireless(2.4 GHz)	
Enable WLAN	<input checked="" type="checkbox"/>
MAC Address	00:34:4C:06:50:2F
Wireless Mode	Access Point
Wireless Network Mode	Auto
SSID	router-wifi_06502F
Broadcast SSID	<input checked="" type="checkbox"/>
Channel	7 - 2.442 GHz Scan
Channel Width	40 MHz
Control Sideband	Upper
Maximum Clients	128 (range: 1 - 255)
Security option	Disabled

Table 2-7 Basic of WLAN Setting Instruction

Parameter	Instruction
Radio Mode	2.4G model, Wi-Fi bandwidth for 1300Mbps
Enable wireless	Enable or Disable the Wireless
Wireless mode	Support AP mode.
Wireless Network protocol	Support Auto/b/g/n optional for 2.4G. Support Auto/A/N optional for 2.5G.
SSID	The default is router, can be modified as per application.
Channel	The channel of wireless network, suggest keep the default

Parameter	Instruction
Channel Width	20MHz and 40MHz alternative for 2.4G. 20MHz, 40MHz and 80MHz alternative for 2.4G.
Security	Support various encryption method as requested.

Step 2 Please click “Save” to finish.

----End

3.8.2 MultiSSID

Step 1 WLAN> MultiSSID.

Already changed login password successfully.

MultiSSID

Overview eth1 (wlan) wlan0.1 wlan0.2 wlan0.3

Interface	Enabled	SSID	Mode	Bridge
eth1 (wlan)	Yes	router-wifi_06502F	Access Point	LAN (br0)
wlan0.1	Yes	router-wifi_1	Access Point	LAN (br0)
wlan0.2	Yes	router-wifi_2	Access Point	LAN (br0)
wlan0.3	Yes	router-wifi_3	Access Point	LAN (br0)

wlan0.1 ☒ Access Point

[Add +](#)

[Save ✓](#) [Cancel ✕](#)

Step 2 Please Click “Save “ to finish.



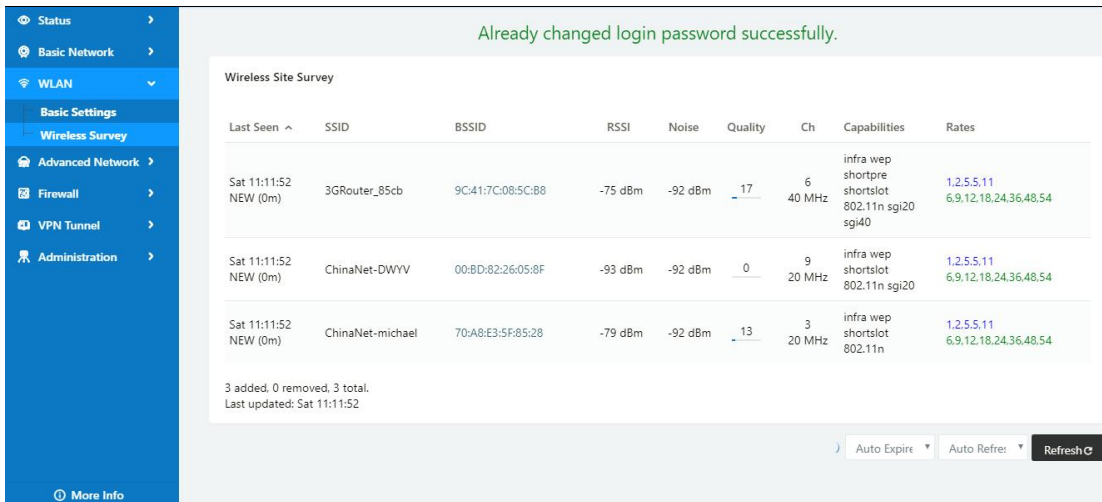
Support 4 SSIDs as Max

----End

3.8.3 Wireless Survey

Step 1 WLAN> Wireless Survey to check survey.

The Router will automatically scan neighbour SSIDs.



Step 2 Please Click “Stop” to change refresh by manual.

----End

3.9 Advanced Network Setting

3.9.1 Port Forwarding

Step 1 Advanced Network > Port Forwarding to enter the GUI, you may modify the router name, Host name and Domain name according to the application requirement.

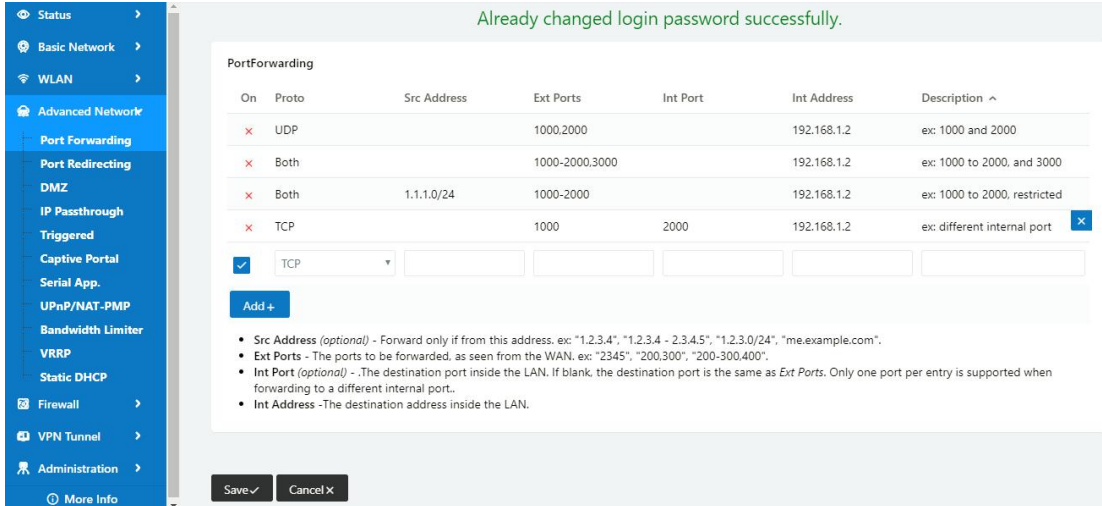


Table 2-8 Port Forwarding Instruction

Parameter	Instruction
Protocol	Support UDP, TCP, both UDP and TCP
Src. Address	Source IP address. Forward only if from this address.
Ext. Ports	External ports. The ports to be forwarded, as seen from the WAN.
Int. Port	Internal port. The destination port inside the LAN. If blank, the destination port is the same as Ext Ports. Only one port

Parameter	Instruction
	per entry is supported when forwarding to a different internal port.
Int. Address	Internal Address. The destination address inside the LAN.
Description	Remark the rule

Step 2 Please click "save" to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

---End

3.9.2 Port Redirecting

Step 1 Advanced Network > Port Redirecting to enter the GUI, you may modify the router name, Host name and Domain name according to the application requirement.

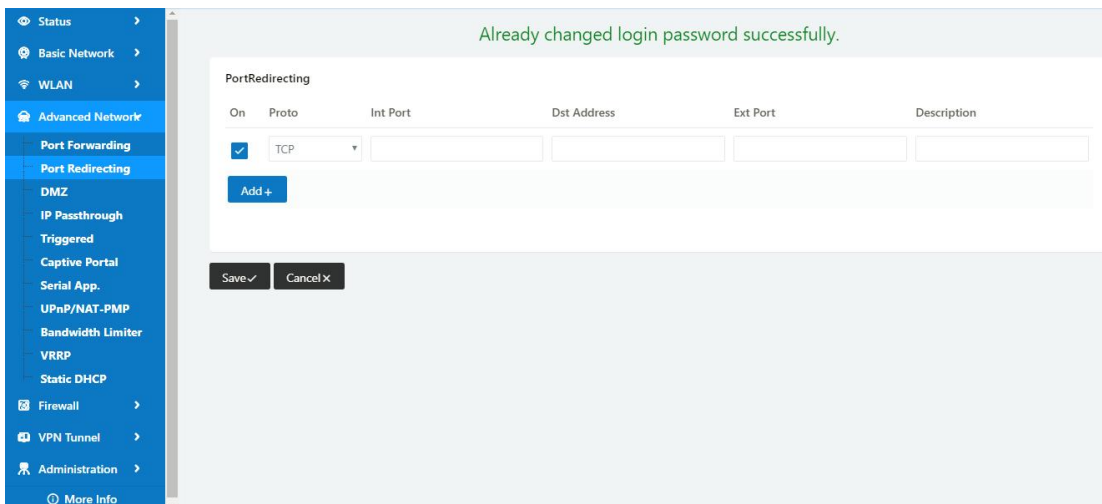


Table 2-9 Port Redirecting Instruction

Parameter	Instruction
Protocol	Support UDP, TCP, both UDP and TCP
Int Port	Internal port.
Dst. Address	The redirecting IP address.
Ext. Ports	External port for redirection.
Description	Remark the rule

Step 2 Please click "save" to finish.



The Port redirecting feature will be unavailable when enable Captive Portal function.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

3.9.3 DMZ Setting

Step 1 Advanced Network> DMZ to check or modify the relevant parameter.

Table 2-10 DMZ Instruction

parameter	Instruction
Destination Address	The destination address inside the LAN.
Source Address Restriction	If no IP address inside, it will allow all IP address to access. If define IP address, it will just allow the defined IP address to access.
Leave Remote Access	

Step 2 Please click "save" to finish

----End

3.9.4 IP Passthrough Setting

Step 1 Advanced Network> IP Passthrough to check or modify the relevant parameter.

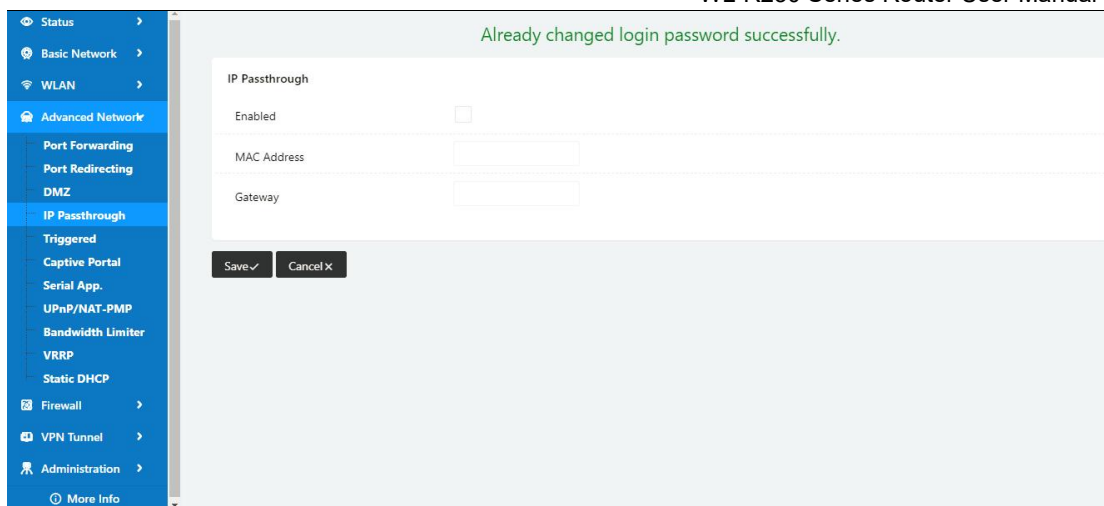


Table 2-11 IP Passthrough Instruction

parameter	Instruction
Enable	Enable IP Passthrough
MAC Address	Enable DHCP of device. Configure device Mac. Device will be assigned SIM IP.
router	If WL-Rxx router connect to multiple device, input other device router. The device might access to router GUI.

Step 2 Please click "save" to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

3.9.5 Triggered Setting

Step 1 Advanced Network> Triggered to check or modify the relevant parameter.

Already changed login password successfully.

Triggered Port Forwarding

On	Protocol	Trigger Ports	Forwarded Ports	Description
<input checked="" type="checkbox"/>	TCP	3000-4000	5000-6000	ex: open 5000-6000 if 3000-4000
<input checked="" type="checkbox"/>	TCP			

Add +

- (200-300).
- These ports are automatically closed after a few minutes of inactivity.

Save ✓ Cancel ✕

Table 2-12 Triggered Instruction

parameter	Instruction
Protocol	Support UDP, TCP, both UDP and TCP
Triggered Ports	Trigger Ports are the initial LAN to WAN "trigger".
Transferred Ports	Forwarded Ports are the WAN to LAN ports that are opened if the "trigger" is activated.
Note	Port triggering opens an incoming port when your computer is using a specified outgoing port for specific traffic.

Step 2 Please click "save" to finish.

----End

3.9.6 Captive Portal

Step 1 Advanced Network> Triggered to check or modify the relevant parameter.

Captive Portal

Enabled ☐

Auth Type

WEB Root

WEB Host

Portal Host

Login Timeout Minutes

Idle Timeout Minutes

Ignore LAN ☒

Redirecting http://

MAC Address Whitelist

Download QOS ☐

Unload QOS ☐

Table 2-13 Captive Portal Instruction

Parameter	Instruction
Enable	Enable Captive portal feature.
Auth Type	Reserved.
Web Root	Choose captive portal file storage path. Default: Captive portal file is in the firmware as default. In-storage: Captive portal file is in router's Flash. Ex-storage: Captive portal file is in extended storage such as SD card.
Web Host	Configure domain name for the captive portal access. For example, Configure as wlink.tech.com, we might directly access to captive portal page in the website as wlink.tech.com
Portal Host	Reserved.
Logged Timeout	Maximum time user has connectivity. User need to re-login Captive Portal page after defined time.
Idle Timeout	Maximum time user has connectivity if no network activity from Wi-Fi User.If User need to re-login Captive page to surf internet.
Ignore LAN	If enabled, LAN devices will bypass the Captive Portal page.
Redirecting	Router will redirect to the defined link after accepting the terms and conditions on the Captive Portal page.
MAC Whitelist	No captive portal page for Wi-Fi device.
Download QoS	Enable to apply the Download and Upload per user limits.
Upload Qos	Maximum download speed available to each user.

Step 2 Please click "save" to finish.



WL-R100 doesn't support Captive Portal feature.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

3.9.7 Serial App. Setting

Step 1 Advanced Network> Serial App to check or modify the relevant parameter.

Already changed login password successfully.

Serial to TCP/IP

IPoC Mode: Serial

Serial to TCP/IP Mode: Disabled

Save ✓ Cancel ✕

Serial to TCP/IP

IPoC Mode: Serial

Serial to TCP/IP Mode: Client

Server IP/Port: 8.8.8.8 : 40002

Socket Type: TCP

Socket Timeout: 500 (milliseconds)

Serial Timeout: 500 (milliseconds)

Packet Payload: 1024 (bytes)

Heart-Beat Content:

Heart-Beat Interval: 2 (seconds)

Port Type: RS485/RS232

Cache Enable: ☒

Debug Enable: ☐

Baud Rate: 57600

Parity Bit: none

Data Bit: 8

Stop Bit: 1

Save ✓ Cancel ✕

Table 2-14 Serial App Instruction

Parameter	Instruction
Serial to TC/IP	Support Disable, Server and Client mode. Such as Client.

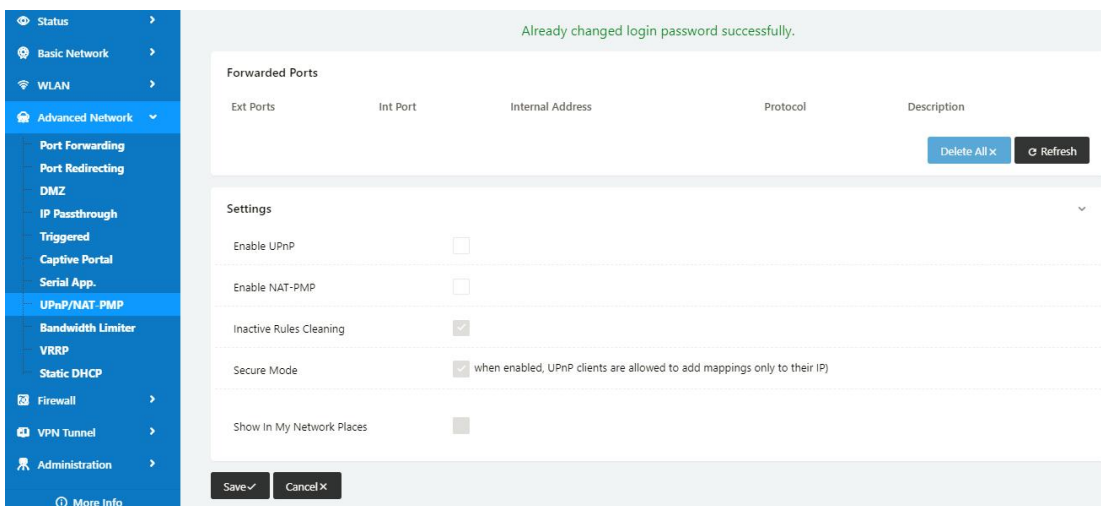
Parameter	Instruction
mode	
Server IP/Port	IP address and domain name are acceptable for Server IP
Socket Type	Support TCP/UDP protocol
Socket Timeout	Router will wait the setting time to transmit data to serial port.
Serial Timeout	Serial Timeout is the waiting time for transmitting the data package that is less the Packet payload. If the last package equals to the Packet payload, Serial port will transmit it immediately. The default setting is 500ms.
Packet payload	Packet payload is the maximum transmission length for serial port data packet. The default setting is 1024bytes.
Heart-beat Content	Send heart beat to the defined server to keep router online. Meantime, it's convenient to monitor router from server.
Heart beat Interval	Heart beat interval time
Baud Rate	115200 as default
Parity Bit	None as default
Data Bit	8bit as default
Stop Bit	1bit as default

Step 2 Please click "save" to finish.

----End

3.9.8 UPnP/NAT-PMP Setting

Step 1 Advanced Network> Upnp/NAT-PMP to check or modify the relevant parameter.



Step 2 Please click "save" to finish.

----End

3.9.9 Bandwidth Control Setting

Step 1 Advanced Network> Bandwidth Control to check or modify the relevant parameter.

Table 2-15 Bandwidth Control Instruction

Max Available Download	Speed limit for router.
Max Available Upload	Speed limit for router.
IP/ IP Range/ MAC Address	Limit devices speed for specified IP/IP Range/ MAC Address.
DL Rate	Mix Download rate
DL ceil	Max download rate
UL Rate	Mix Upload rate
UL ceil	Max upload rate
Priority	The priority of a specific user.
Default Class	If no specified IP/MAC, the download and upload limit for total speed for all of device.

Step 2 Please click "save" to finish.

----End

3.9.10 VRRP Setting

Step 1 Advanced Network> VRRP to check or modify the relevant parameter.

Already changed login password successfully.

VRRP

Enable VRRP ☐

Mode

Virtual IP

Virtual Router ID

Priority

Authentication ☐

Script Type

Check Interval

Weight

Step 2 Please click "save" to finish.

----End

3.9.11 Static DHCP Setting

Step 1 Advanced Network> Static DHCP to check or modify the relevant parameter.

Already changed login password successfully.

Static DHCP

MAC Address	IP Address	Hostname ^	Description
<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="192.168.1.2"/>	<input type="text"/>	<input type="text"/>
<input type="text" value="00:00:00:00:00:00"/>			

Step 2 Please click "save" to finish.

----End

3.10 Firewall

3.10.1 IP/URL Filtering

Step 1 Firewall> IP/URL Filtering to check or modify the relevant parameter.

Status

Basic Network

WLAN

Advanced Network

Firewall

IP/URL Filtering

Domain Filtering

VPN Tunnel

Administration

More Info

IP/MAC/Port Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
<input checked="" type="checkbox"/>				NOH			Accey	
Add +								

Key Word Filtering

On	Key Word	Description
<input checked="" type="checkbox"/>		
Add +		

URL Filtering

On	URL	Description
<input checked="" type="checkbox"/>		
Add +		

IP/MAC/Port Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
<input checked="" type="checkbox"/>				NOH			Accey	
Add +								

Key Word Filtering

On	Key Word	Description
<input checked="" type="checkbox"/>		
Add +		

URL Filtering

On	URL	Description
<input checked="" type="checkbox"/>		
Add +		

Access Filtering

Save ✓ Cancel x

Table 2-16 IP/URL Filtering Instruction

Parameter	Instruction
IP/MAC/Port Filtering	Support IP address, MAC address and port filter. Accept/Drop options for filter policy.
Key Word Filtering	Support key word filter.
URL Filtering	Support URL filter.
Access Filtering	Support Access Filter.



Please check Firewall rule in Configuration instance.

Step 2 Please click "save" to finish.

---End

3.10.2 Domain Filtering

Step 1 Firewall> Domain Filtering to check or modify the relevant parameter.

Table 2-17 Domain Filtering Instruction

Parameter	Instruction
Default Policy	Support black list and white list
Local IP Address	Local IP address for LAN.
Domain	Support Domain filter.

Step 2 Please click "save" to finish.

----End

3.11 VPN Tunnel

3.11.1 Wireguard Setting

Step 1 VPN Tunnel> Wireguard to check or modify the relevant parameter.

Wireguard

Enabled ☒

Mode Client

Peer IP/Port :

Local Key

Local IP/Mask ex. 192.168.88.5/24

Peer Key

Preshared Key

Persistent Keepalive

Allowed IPS ex. 192.168.88.0/24 or 192.168.88.0/24,192.168.99.0/24

Peer Subnet IP/Mask ex. 192.168.88.0/24 or 192.168.88.0/24,192.168.99.0/24

Table 2-18 Wireguard Client Instruction

Parameter	Instruction
Enable	Enable Wireguard.
Model	Wireguard client and server modes optional
Peer IP/Port	Server IP and port
Local Key	VPN local key
Local IP/Mask	Wireguard VPN tunnel local IP and mask. The VPN local IP address and peer IP address are different subnet segment.
Peer Key	VPN peer key
Preshared Key	Wireguard Pre-shared key
Keepalive	Keepalive interval, unit for second
Allowed IPs	Allowed VPN subnet IP addresses
Peer Subnet IP/Mask	Wireguard VPN tunnel Peer IP and mask.

Wireguard

Enabled

☒

Mode

Server ▾

Bind Port

51820

Local Key

test

Local IP/Mask

192.168.88.1/24

ex. 192.168.88.5/24

Peer Subnet IP/Mask

ex. 192.168.88.0/24 or 192.168.88.0/24,192.168.99.0/24

Allowd IPS

Persistent Keepalive

Peer Key

0.0.0.0/0

25

Add +

Save ✓

Cancel ✕

Table 2-19 Wireguard Sever Instruction

Parameter	Instruction
Enable	Eenable Wireguard.
Model	Wireguard client and server modes optional
Bind Port	Wireguard server port
Local Key	VPN local key
Local IP/Mask	Wireguard VPN tunnel local IP and mask. The VPN server local IP address and client IP address are different subnet segments.
Preshared Key	Wireguard Pre-shared key
Keepalive	Keepalive interval,unit for second
Allowed IPs	Allowed VPN subnet IP addresses
Peer Key	VPN peer key

Step 2 Please click "save" to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

3.11.2 GRE Setting

Step 3 VPN Tunnel> GRE to check or modify the relevant parameter.

Table 2-20 GRE Instruction

Parameter	Instruction
IDx	GRE tunnel number
Tunnel Address	GRE Tunnel local IP address which is a virtual IP address.
Tunnel Source	Router's 3G/WAN IP address.
Tunnel Destination	GRE Remote IP address. Usually a public IP address
Keep alive	GRE tunnel keep alive to keep GRE tunnel connection.
Interval	Keep alive interval time.
Retries	Keep alive retry times. After retry times, GRE tunnel will be re-established.
Description	

Step 4 Please click "save" to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

3.11.3 OpenVPN Client Setting

Step 1 VPN Tunnel> OpenVPN Client to check or modify the relevant parameter.

The screenshot displays the 'OpenVPN Client' configuration interface. On the left, a blue sidebar contains a navigation menu with options: Basic Network, WLAN, Advanced Network, Firewall, VPN Tunnel (expanded), GRE, OpenVPN Client (selected), PPTP/L2TP Client, IPSec, and Administration. The main content area is titled 'OpenVPN Client' and has tabs for 'Client 1' and 'Client 2'. Below the tabs are sub-tabs: 'Basic', 'Advanced', 'Keys', and 'Status'. The 'Basic' tab is active, showing the configuration for 'VPN Client #1 (Stopped)'. The configuration parameters are as follows:

- Start with WAN: ☐
- Interface Type: TUN (dropdown)
- Protocol: UDP (dropdown)
- Server Address: 1194 (text input)
- Firewall: Automatic (dropdown)
- Authorization Mode: TLS (dropdown)
- Username/Password Authentication: ☐
- HMAC authorization: Disabled (dropdown)
- Create NAT on tunnel: ☒

At the bottom of the configuration area, there is a 'Start Now' button.

OpenVPN Client

Client 1

Client 2

Basic

Advanced

Keys

Status

VPN Client #1 (Stopped)

Start with WAN

Interface Type

TUN ▼

Protocol

UDP ▼

Server Address

1194

Firewall

Automatic ▼

Authorization Mode

TLS ▼

Username/Password Authentication

HMAC authorization

Disabled ▼

Create NAT on tunnel

☒

Start Now

Save ✓

Cancel ✕

Table 2-21 Basic of OpenVPN Instruction

Parameter	Instruction
Start with WAN	Enable the Openvpn feature for 4G/3G/WAN port.
Interface Type	Tap and Tun type are optional. Tap is for bridge mode and Tunnel is for routing mode.
Protocol	UDP and TCP optional.
Server Address	The Openvpn server public IP address and port.

Parameter	Instruction
Firewall	Auto, External only and Custom are optional
Authorization Mode	TLS, Static key and Custom are optional.
User name/Password Authentication	As the configuration requested.
HMAC authorization	As the configuration requested.
Create NAT on tunnel	Configure NAT in Openvpn tunnel.

Basic Advanced Keys Status

VPN Client #1 (Stopped) ▶

Poll Interval (in minutes, 0 to disable)

Redirect Internet traffic ☐

Accept DNS configuration

Encryption cipher

Compression

TLS Renegotiation Time (in seconds, -1 for default)

Connection retry (in seconds; -1 for infinite)

Verify server certificate (tls-remote) ☐

Custom Configuration

Start Now

Table 2-22 Advanced of OpenVPN Instruction

Parameter	Instruction
Poll Interval	Openvpn client check router's status as interval time.
Redirect Internet Traffic	Configure Openvpn as default routing.
Access DNS	As the configuration requested.
Encryption	As the configuration requested.
Compression	As the configuration requested.
TLS Renegotiation Time	TLS negotiation time. -1 as default for 60s.
Connection Retry Time	Openvpn retry to connection interval.
Verify server certificate	As the configuration requested.

Parameter	Instruction
Custom Configuration	As the configuration requested.

Basic Advanced **Keys** Status

VPN Client #1 (Stopped)

For help generating keys, refer to the OpenVPN HOWTO.

Certificate Authority

Client Certificate

Client Key

Start Now

Table 2-23 Keys of OpenVPN Instruction

Parameter	Instruction
Certificate Authority	Keep certificate as the same as server
Client Certificate	Keep client certificate as the same as server
Client Key	Keep client key as the same as server

OpenVPN Client

Client 1 Client 2

Basic Advanced **Keys** **Status**

VPN Client #1 (Stopped)

Client is not running or status could not be read.

Refresh Status

Start Now

Table 2-24 Status of OpenVPN Instruction

Parameter	Instruction
Status	Check Openvpn status and data statistics.

Step 2 Please click "save" to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

3.11.4 PPTP/L2TP Client Setting

Step 1 VPN Tunnel> VPN Client to check or modify the relevant parameter.

The screenshot shows the configuration page for PPTP/L2TP Client. The left sidebar contains navigation links: Status, Basic Network, WLAN, Advanced Network, Firewall, VPN Tunnel (selected), GRE, OpenVPN Client, PPTP/L2TP Client (selected), IPsec, and Administration. The main content area has four sections:

- L2TP/PPTP Basic:** Includes a table with columns: On, Protocol, Name, Server, Username, Password, Firewall, Default Route, Local IP. The 'On' checkbox is checked. The 'Protocol' dropdown is set to L2TP. The 'Name', 'Server', 'Username', 'Password', 'Local IP' fields are empty. The 'Firewall' and 'Default Route' checkboxes are unchecked. An 'Add +' button is at the bottom.
- L2TP Advanced:** Includes a table with columns: On, Name, Accept DNS, MTU, MRU, Tunnel Auth, Tunnel Password, Custom Options. The 'On' checkbox is checked. The 'Name' field is empty. The 'Accept DNS' dropdown is set to NO. The 'MTU' and 'MRU' fields are empty. The 'Tunnel Auth' checkbox is unchecked. The 'Tunnel Password' and 'Custom Options' fields are empty. An 'Add +' button is at the bottom.
- PPTP Advanced:** Includes a table with columns: On, Name, Accept DNS, MTU, MRU, MPPE, MPPE Stateful, Custom Options. The 'On' checkbox is checked. The 'Name' field is empty. The 'Accept DNS' dropdown is set to NO. The 'MTU' and 'MRU' fields are empty. The 'MPPE' and 'MPPE Stateful' checkboxes are unchecked. The 'Custom Options' field is empty. An 'Add +' button is at the bottom.
- Schedule:** Includes a table with columns: On, Name 1, Name 2, Policy, Description. The 'On' checkbox is checked. The 'Name 1' and 'Name 2' fields are empty. The 'Policy' dropdown is set to FAILOVER. The 'Description' field is empty. An 'Add +' button is at the bottom.

Table 2-25 PPTP/L2TP Basic Instruction

parameter	Instruction
On	VPN enable
Protocol	VPN Mode for PPTP and L2TP
Name	VPN Tunnel name
Server Address	VPN Server IP address.
User name	As the configuration requested.
Password	As the configuration requested.
Firewall	Firewall For VPN Tunnel
Local IP	Defined Local IP address for tunnel

Table 2-26 L2TP Advanced Instruction

On	L2TP Advanced enable
Name	L2TP Tunnel name
Accept DNS	As the configuration requested.
MTU	MTU is 1450bytes as default
MRU	MRU is 1450bytes as default

Tunnel Auth.	L2TP authentication Optional as the configuration requested.
Tunnel Password	As the configuration requested.
Custom Options	As the configuration requested.

Table 2-27 PPTP Advanced Instruction

On	PPTP Advanced enable
Name	PPTP Tunnel name
Accept DNS	As the configuration requested.
MTU	MTU is 1450bytes as default
MRU	MRU is 1450bytes as default
MPPE	As the configuration requested
MPPE Stateful	As the configuration requested
Customs	As the configuration requested

Table 2-28 SCHEDULE Instruction

On	VPN SCHEDULE feature enable
Name1	VPN tunnel name
Name2	VPN tunnel name
Policy	Support VPN tunnel backup and failover modes optional
Description	As the configuration requested

Step 2 Please click "save" to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

---End

3.11.5 IPSec Setting

Already changed login password successfully.

IPSec

IPSec 1 | IPSec 2 | Schedule

Group Setup | Basic Setup | Advanced Setup

Enable IPSec ☐

IPSec Extensions Normal

Local Security Gateway Interface 3G Cellular

Local Security Group Subnet/Netmask 192.168.1.0/24 ex. 192.168.1.0/24

Local Security Firewalling ☒

Remote Security Gateway IP/Domain

Remote Security Group Subnet/Netmask 10.0.0.0/24 ex. 192.168.88.0/24

Remote Security Firewalling ☒

Save ✓ Cancel ✕

3.11.5.1 IPSec Group Setup

Step 1 IPSec> Group Setup to check or modify the relevant parameter.

Group Setup | Basic Setup | Advanced Setup

Enable IPSec ☐

IPSec Extensions Normal

Local Security Gateway Interface 3G Cellular

Local Security Group Subnet/Netmask 192.168.1.0/24 ex. 192.168.1.0/24

Local Security Firewalling ☒

Remote Security Gateway IP/Domain

Remote Security Group Subnet/Netmask 10.0.0.0/24 ex. 192.168.88.0/24

Remote Security Firewalling ☒

Table 2-29 IPSec Group Setup Instruction

parameter	Instruction
IPSec Extensions	Support Standard IPSec, GRE over IPSec, L2TP over IPSec
Local Security Interface	Defined the IPSec security interface
Local Subnet/Mask	IPSec local subnet and mask.
Local Firewall	Forwarding-firewalling for Local subnet

parameter	Instruction
Remote IP/Domain	IPsec peer IP address/domain name.
Remote Subnet/Mask	IPSec remote subnet and mask.
Remote Firewall	Forwarding-firewalling for Remote subnet

Step 2 Please click "save" to finish.

---End

3.11.5.2 IPSec Basic Setup

Step 1 IPSec >Basic Setup to check or modify the relevant parameter.

Group Setup	Basic Setup	Advanced Setup
Keying Mode IKE with Preshared Key		
Phase 1 DH Group Group 2 - modp1024		
Phase 1 Encryption 3DES (168-bit)		
Phase 1 Authentication MD5 HMAC (96-bit)		
Phase 1 SA Life Time 28800 seconds		
Phase 2 DH Group Group 2 - modp1024		
Phase 2 Encryption 3DES (168-bit)		
Phase 2 Authentication MD5 HMAC (96-bit)		
Phase 2 SA Life Time 3600 seconds		
Preshared Key <input type="text"/>		

Table 2-30 IPSec Basic Setup Instruction

parameter	Instruction
Keying Mode	IKE preshared key
Phase 1 DH Group	Select Group1, Group2, Group5 from list. It must be matched to remote IPSec setting.
Phase 1 Encryption	Support 3DES, AES-128, AES-192, AES-256

parameter	Instruction
Phase 1 Authentication	Support HASH MD5 and SHA
Phase 1 SA Life Time	IPSec Phase 1 SA lifetime
Phase 2 DH Group	Select Group1, Group2, Group5 from list. It must be matched to remote IPSec setting.
Phase 2 Encryption	Support 3DES, AES-128, AES-192, AES-256
Phase 2 Authentication	Support HASH MD5 and SHA
Phase 2 SA Life Time	IPSec Phase 2 SA lifetime
Preshared Key	Preshared Key

Step 2 Please click "save" to finish.

---End

3.11.5.3 IPSec Advanced Setup

Step 1 IPSec >Advanced Setup to check or modify the relevant parameter.

Group Setup	Basic Setup	Advanced Setup
Aggressive Mode		<input type="checkbox"/>
Compress(IP Payload Compression)		<input type="checkbox"/>
Dead Peer Detection(DPD)		<input type="checkbox"/>
ICMP Check		<input type="checkbox"/>
IPSec Custom Options 1		<input type="text"/>
IPSec Custom Options 2		<input type="text"/>
IPSec Custom Options 3		<input type="text"/>
IPSec Custom Options 4		<input type="text"/>

Table 2-31 IPSec Advanced Setup Instruction

parameter	Instruction
Aggressive Mode	Default for main mode
ID Payload Compress	Enable ID Payload compress
DPD	To enable DPD service
ICMP	ICMP Check for IPSec tunnel
IPSec Custom Options	IPSec advanced setting such as left/right ID.

Step 2 Please click "save" to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

3.11.6 DMVPN Setting

Step 1 VPN Tunnel> DMVPN to check or modify the relevant parameter.

Status	
Basic Network	
Advanced Network	
Firewall	
VPN Tunnel	
Wireguard	
GRE	
OpenVPN Client	
OpenVPN Server	
PPTP/L2TP Server	
PPTP/L2TP Client	
L2TP V3	
IPSec	
DMVPN	
Administration	

DMVPN

Enable DMVPN ☐

Tunnel Address

Tunnel Netmask

Tunnel MTU

Tunnel Key

Tunnel Source

NHRP Server Address

NHRP Tunnel Address

NHRP Server Address 2

NHRP Tunnel Address 2

NHRP Key

Keying Mode

Phase 1 DH Group

Phase 1 Encryption

Phase 1 Authentication

VPN Tunnel

- Wireguard
- GRE
- OpenVPN Client
- OpenVPN Server
- PPTP/L2TP Server
- PPTP/L2TP Client
- L2TP V3
- IPSec
- DMVPN**

Administration

Phase 1 Authentication MD5 HMAC (96-bit)

Phase 1 SA Life Time 28800 seconds

Phase 2 DH Group Group 2 - modp1024

Phase 2 Encryption 3DES (168-bit)

Phase 2 Authentication MD5 HMAC (96-bit)

Phase 2 SA Life Time 3600 seconds

Preshared Key

Dead Peer Detection(DPD)

IPSec Custom Options 1

IPSec Custom Options 2

IPSec Custom Options 3

IPSec Custom Options 4

Save **Cancel**

More Info

Table 2-32 DMVPN Client Instruction

Parameter	Instruction
Enable	Eenable DMVPN
Tunnel Address	GRE tunnel address
Tunnel Mask	GRE tunnel subnet mask
Tunnel MTU	GRE tunnel MTU
Tunnel Key	GRE tunnel secret key
Tunnel Source	modem(4G/5G);WAN;STA/STA2(WIFI2.4/5.8) Optional
NHRP Server Address	NHRP Server IP address
NHRP Tunnel Address	NHRP Tunnel address
NHRP Key	NHRP Secret key
Keying Mode	IKEv1/IKEv2 optional
Phase1 DH Group	Select Group1, Group2, Group5 from list. It must be matched to remote IPSec setting.

Parameter	Instruction
Phase1 Encryption	Support 3DES, AES-128, AES-192, AES-256
Phase1 Authentication	Support HASH MD5 and SHA
Phase1 SA Lifetime	IPSec Phase 1 SA lifetime
Phase2 DH Group	Select Group1, Group2, Group5 from list. It must be matched to remote IPSec setting.
Phase2 Encryption	Support 3DES, AES-128, AES-192, AES-256
Phase2 Authentication	Support HASH MD5 and SHA
Phase2 SA Lifetime	IPSec Phase 2 SA lifetime
Preshared Key	IPsec preshared key
Dead Peer Detection(DPD)	Dead Peer Detection
IPSec Custom Options	IPSec custom configuration according to server.

Step 2 Please click "save" to finish.

----End

3.12 Administration

3.12.1 Identification Setting

Step 1 Please click "Administrator> Identification" to enter the GUI, you may modify the router name, Host name and Domain name according to self-requirement.

Router Identification

Router Name Router

Hostname Router

Domain Name

Save Cancel

Router Identification

Router Name

Router

Hostname

Router

Domain Name

Save

Cancel

Table 2-33 Router Identification Instruction

Parameter	Instruction
Router name	Default is router, can be set maximum 32 character
Host name	Default is router, can be set maximum 32 character
Domain name	Default is empty, support maximum up to 32 character, it is the domain of WAN, no need to configure for most application.

Step 2 Please click "save" to finish

---End

3.12.2 Time Setting

Step 1 Please click “Administrator> time” to check or modify the relevant parameter.

The screenshot shows the 'Time' configuration page in the router's web interface. The left sidebar has 'Administration' expanded, with 'Time' selected. The main panel shows the following settings:

- Router Time:** Sat, 01 Jan 2000 09:01:24 +0800. A 'Clock Sync' button is next to it.
- Time Zone:** A dropdown menu showing 'UTC+08:00 China, Hong Kong, Western Australia, Singapore, Taiwan'.
- Auto Daylight Savings Time:** A checked checkbox.
- Auto Update Time:** A dropdown menu showing 'Every 4 Hours'.
- Trigger Connect On Demand:** An unchecked checkbox.
- NTP Time Server:** A dropdown menu showing 'Asia'. Below it, a list of NTP servers is displayed: 0.asia.pool.ntp.org, 1.asia.pool.ntp.org, 2.asia.pool.ntp.org.

At the bottom of the configuration area are 'Save' and 'Cancel' buttons.



If the device is online but time update is fail, please try other NTP Time Server.

Step 2 Please click “save to finish.”

----End

3.12.3 Admin Access Setting

Step 1 Please click “Administrator>Admin” to check and modify relevant parameter.

In this page, you can configure the basic web parameter, make it more convenient for usage. Please note the “password” is the router system account password.

Step 2 Please click save icon to finish the setting

----End

3.12.4 Schedule Reboot Setting

Step 1 Please click “Administrator>Schedule Reboot” to check and modify relevant parameter.

Step 2 Please click save icon to finish the setting

----End

3.12.5 SNMP Setting

Step 1 Please click “Administrator>SNMP” to check and modify relevant parameter.

Step 2 Please click save icon to finish the setting

----End

3.12.6 Storage Setting

Step 1 Please click “Administrator>Storage Setting” to check and modify relevant parameter.

Step 2 Please click save icon to finish the setting



NOTE WL-R100/R200 series router doesn't support extra storage. The storage path is Router as default.

----End

3.12.7 M2M Access Setting (Apply to M2M Management Platform installation application only)

Step 1 Please click “Administrator>M2M Access” to check and modify relevant parameter.

m2m	
M2M Enabled	<input type="checkbox"/>
Fail Action	Restart M2M
Device ID	<input type="text"/>
M2M Server/Port	<input type="text"/> : 8000
Heartbeat Intval	60 (seconds)
Heartbeat Retry	10 (Range:10-1000)
Named-Pipe Enabled	Remote Connect
Named-Pipe Server Port	8002 (Range:1024-65535)
Named-Pipe Status	Offline
Named-Pipe Address	0.0.0.0

Step 2 Please click save iron to finish the setting

----End

3.12.8 DI/DO Setting(Apply to WL-R230 only)

Step 1 Please click “Administrator>DI/DO Setting” to check and modify relevant parameter.

Already changed login password successfully.

DI Setting	
Enabled	Port1 <input type="checkbox"/> Port2 <input type="checkbox"/>

DO Setting	
Enabled	<input checked="" type="checkbox"/>
Alarm Source	DI Control <input type="checkbox"/> SMS Control <input type="checkbox"/>
Alarm Action	ON
Power On Status	OFF
Keep On	1 (*100ms)

Save ✓ Cancel ✕

3.12.8.1 DI Configure

DI Setting

Enabled

Port1 ☒

Port2 ☐

Port1Mode

ON

Filter

1

(*100ms)

SMS Alarm

☐

DO Setting

Enabled

☒

Alarm Source

DI Control ☐

SMS Control ☐

Alarm Action

ON

Power On Status

OFF

Keep On

1

(*100ms)

Save ✓

Cancel ✕

Table 2-34 DI Instruction

Parameter	Instruction
Enable	Enable DI. Port1 is for I/O1 and Port2 is I/O2. Both I/O1 and I/O2 are DI ports
Mode	<p>Selected from OFF, ON and EVENT_COUNTER modes.</p> <p>OFF Mode: DI from high level(3.3v~5V) to low level(0V), it will trigger alarm.</p> <p>ON Mode: DI from low level(0V) to high level(3.3v~5V), it will trigger alarm.</p> <p>EVENT_COUNTER Model: Enter EVENT_COUNTER mode.</p>
Filter	<p>Software filtering is used to control switch bounces. Input (1~100)*100ms.</p> <p>Under OFF and ON modes, WL-G510 detects pulse signal and compares with first pulse shape and last pulse shape. If both are the same level, WL-G510 will trigger alarm.</p>

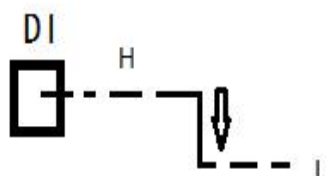
Parameter	Instruction
	Under EVENT_COUNTER mode, if first pulse shape and last pulse shape are not the same level, WL-G510 will trigger alarm according to Counter Action setting.
Counter Trigger	Available when DI under Event Counter mode Input from 0 to 100. (0=will not trigger alarm) It will trigger alarm when counter reaches this value. After triggering alarm, DI will keep counting but no trigger alarm again.
Counter Period	It's a reachable IP address. Once the ICMP check is failed, GRE will be established again.
Counter Recover	it will re-count after counter trigger alarm. The value is 0~30000(*100ms). 0 means no counter.
Counter Action	HI_TO_LO and LO_TO_HI is available when DI under Event Counter mode. In Event Counter mode, the channel accepts limit or proximity switches and counts events according to the ON/OFF status. When LO_TO_HI is selected, the counter value increase when the attached switch is pushed. When HI_TO_LO is selected, the counter value increases when the switch is pushed and released.
Counter Start	Available when DI under EVENT_COUNTER mode. Start counting when enable this feature.
SMS Alarm	The alarm SMS will send to specified phone group. Each phone group include up to 2 phone numbers.
SMS Content	70 ASCII Char Max
Number 1	SMS receiver phone number.
Number 2	SMS receiver phone number.

Step 2 Please click "save" to finish.



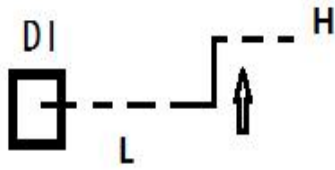
OFF Mode

DI from high level 3.3~5V to low level 0V will be triggered.



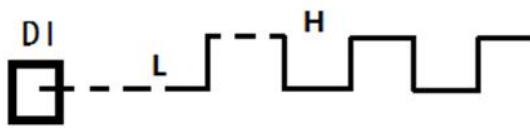
ON Mode

Data input from low level 0V to high level 3.3~5V will be triggered.



EVENT_COUNTER Model

The counted number of pulses will be triggered.



3.12.8.2 DO Configure

DO Configure

Enable

☐

Alarm Source

DI Alarm ☒
SMS Control ☒
M2M Control ☐

Alarm Action

Pulse ▾

Power On Status

ON ▾

Delay

(*100ms)

Low

(*100ms)

High

(*100ms)

Output

SMS Trigger Content

70 ASCII Char Max

SMS Replay Content

70 ASCII Char Max

SMS Manager Num1

SMS Manager Num2

backup receiver

Table 2-35 DO Instruction

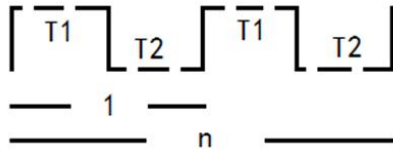
Parameter	Instruction
Enable	1 DO as selected
Alarm Source	Digital output initiates according to different alarm source. Select from DI Alarm, SMS Control and M2M Control. Selections can be one or more. DI Alarm: Digital Output triggers the related action when there is alarm from Digital Input.

Parameter	Instruction
	SMS Control: Digital Output triggers the related action when receiving SMS from the number in phone book. M2M Control: it's not ready.
Alarm Action	Digital Output initiates when there is an alarm. Selected from "OFF", "ON", "Pulse". OFF: Open from GND when triggered. ON: Short contact with GND when triggered. Pulse: Generates a square wave as specified in the pulse mode parameters when triggered.
Power on Status	Specify the digital Output status when power on. Selected from OFF and ON. OFF: how high(0V). ON: high lever(4.8-5.0V)
Keep On	Available when digital output Alarm On Action/Alarm Off Action status is ON, input the Digital Output keep on status time. Input from 0 to 255 seconds. (0=keep on until the next action)
Delay	Available when enable Pulse in Alarm On Action/Alarm Off Action. The first pulse will be generated after a "Delay" . Input from 0 to 30000ms. (0=generate pulse without delay)
Low	Available when enable Pulse in Alarm On Action/Alarm Off Action. In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The low level widths are specified here. Input from 1 to 30000 ms.
High	Available when enable Pulse in Alarm On Action/Alarm Off Action. In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The high level widths are specified here. Input from 1 to 30000 ms.
Output	Available when enable Pulse in Alarm On Action/Alarm Off Action. The number of pulses, input from 0 to 30000. (0 for continuous pulse output)
SMS Trigger Content	Available when enable SMS Control in Alarm Source. Input the SMS content to enable "Alarm On Action" by SMS (70 ASCII char max).
SMS Reply Content	Input the SMS content, which will be sent after DO was triggered. (70 ASCII char max).
Number 1	SMS receiver phone number.
Number 2	SMS receiver phone number.

Step 3 Please click "save" to finish.



DO might be customized pulse width ratio: T1, T2 duration and n value.



---End

3.12.9 Configuration Setting

Step 4 Please click “ Administrator> Configuration ” to do the backup setting

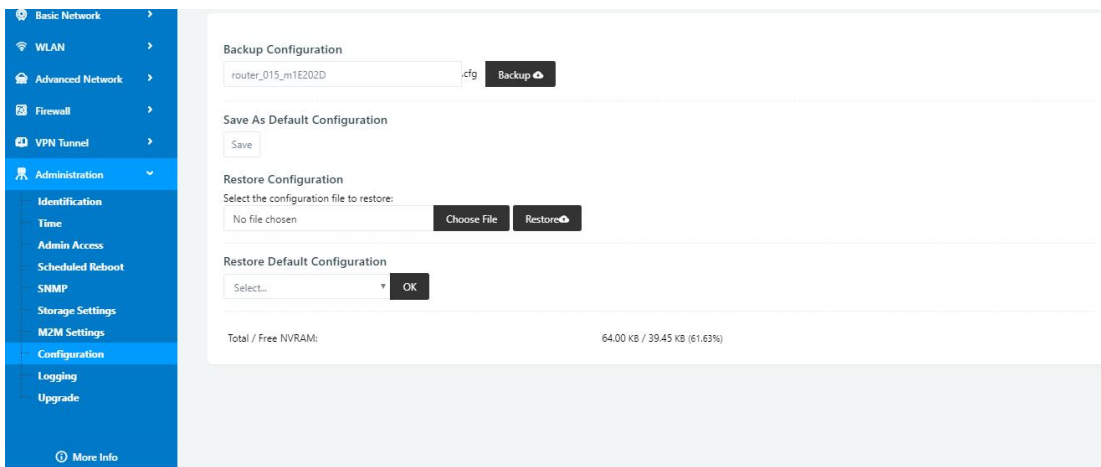


Figure 3-1 Backup and Restore Configuration GUI



Restore Default would lose all configuration information, please be careful.

Step 5 After setting the backup and restore configuration. The system will reboot automatically.

----End

3.12.10 System Log Setting

Step 6 Please click “Administrator> Logging” to start the configuration, you can set the file path to save the log (Local or remote sever).

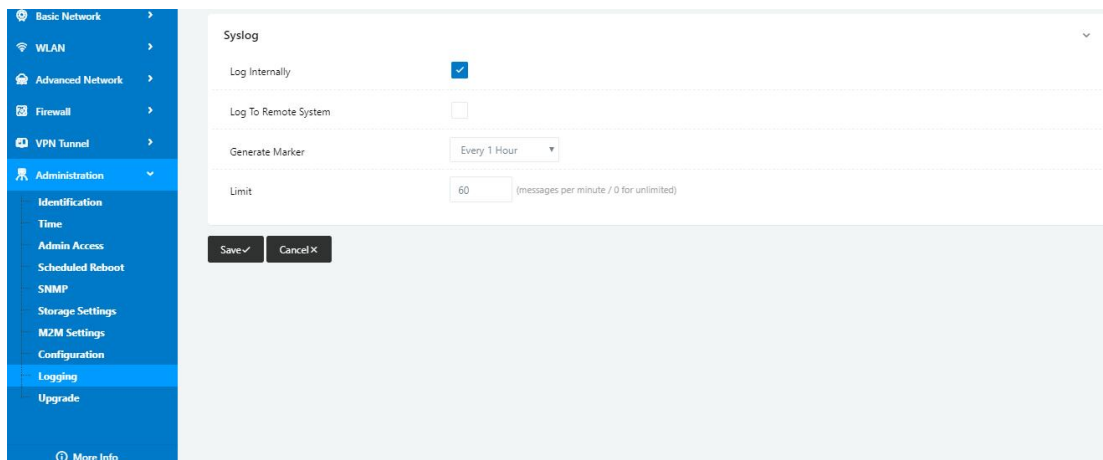


Figure 3-2 System log Setting GUI

Step 7 After configure, please click “Save” to finish.

----End

3.12.11 Firmware upgrade

Step 8 Please click “Administrator>firmware upgrade” to open upgrade firmware tab.

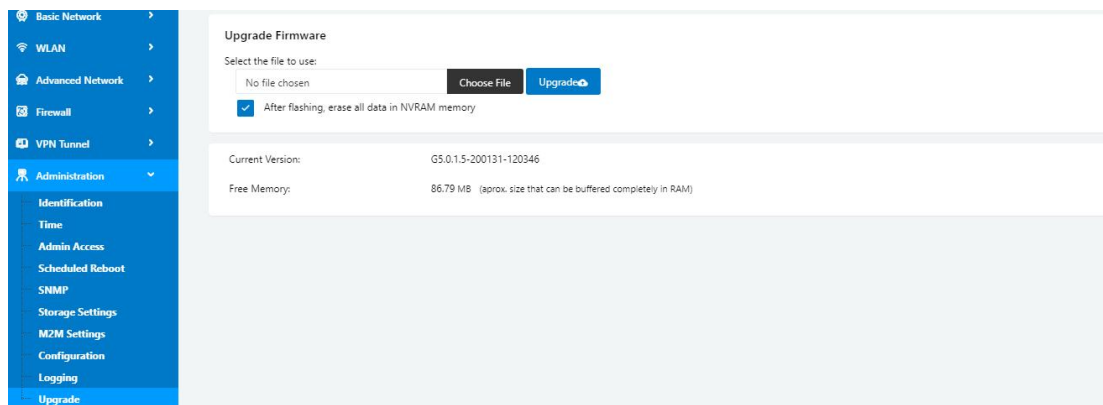


Figure 3-3 Firmware Upgrade GUI



Please don't cut off the power during upgrading. The upgrade period is about 4mins.

3.12.12 “Reset” Button for Restore Factory Setting

If you couldn't enter web interface for other reasons, you can also use this way.

“Reset” button is near to Console port in WL-Rxx panel, This button can be used when the router is in use or when the router is turned on.

Press the “RST” button and keep more than 8 seconds till the NET light stopping blink. The system will be reverted to factory.

Table 2-36 System Default Instruction

Parameter	Default setting
LAN IP	192.168.1.1
LAN Subnet Mask	255.255.255.0
DHCP server	Enable
User Name	admin
Password	admin



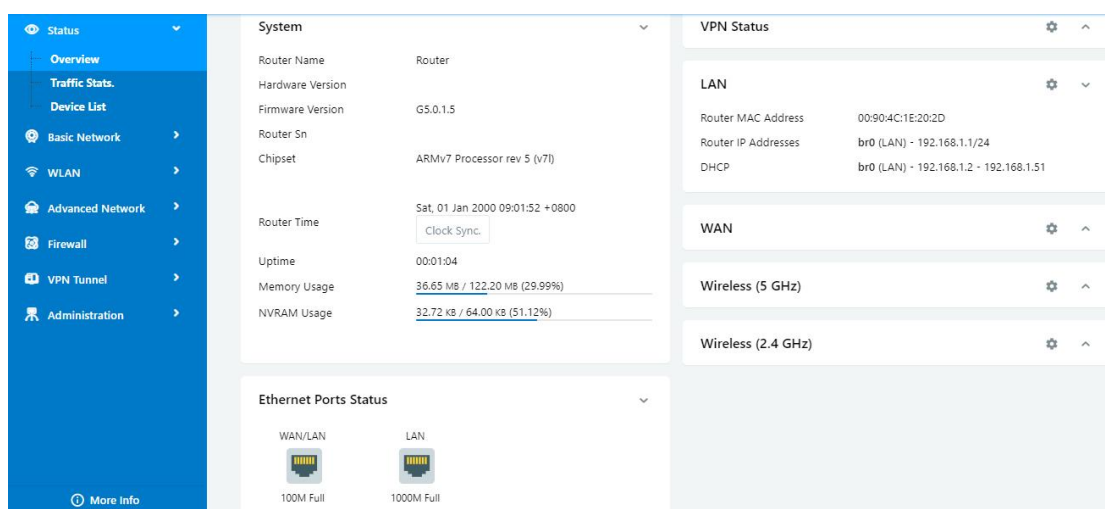
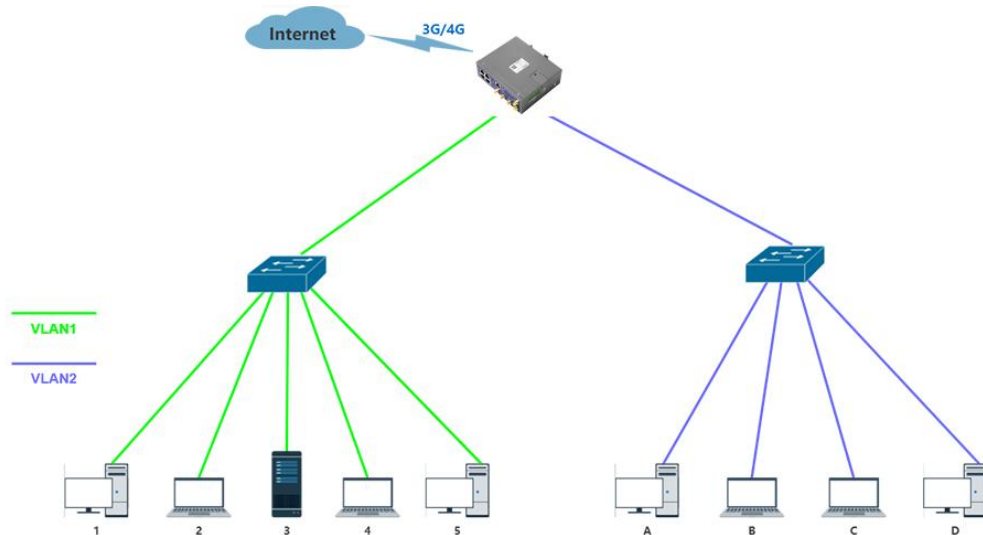
After reboot, the previous configuration would be deleted and restore to factory settings.

4 Configuration Instance

This chapter is mainly for configured test case, there would be some difference between the scheme and real object. But the difference doesn't have any influence to products performance.

4.1 VLAN

WL-R200/R210/R520 supports VLAN partition based on Ethernet port (LAN1~LAN5)



1) Configure LAN with Basic Network.

You haven't changed the default password for this router. To change router password [click here](#).

LAN

Bridge ^	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)
br0	192.168.1.1	255.255.255.0	✓	192.168.1.2 - 51	1440
br1	192.168.10.1	255.255.255.0	✓	192.168.10.100 - 120	1440
br2	192.168.20.1	255.255.255.0	✓	192.168.20.100 - 120	1440

3 ☐

Add+

Save✓ **Cancel✕**

2) If untag for br1 and br2, it won't be accessed between SW1 and SW2.

You haven't changed the default password for this router. To change router password [click here](#).

VLAN

VID ^	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
0	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	br1
1	✗	✗	✓	✗	✓	✗	✗	✗	✓	✗	br0
2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	WAN
3	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	br2
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	none

Add+

Save✓ **Cancel✕**

3) If tag for br1 and br2, it will be accessed between sw1 and sw2.

You haven't changed the default password for this router. To change router password [click here](#).

VLAN

VID ^	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
0	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	br1
1	✗	✗	✓	✗	✓	✗	✗	✗	✓	✗	br0
2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	WAN
3	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	br2
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	none

Add+

Save✓ **Cancel✕**

---End

4.2 WAN Backup (WAN as Main, Cellular Backup)

The WAN and Cellular backup feature can quickly switch traffic to Cellular (link2) when WAN (link1) fails, and WL-Rxx brings you a stable network experience.

- 1) Navigate to **Basic Network > WAN**, you may configure the WAN parameters with your situation

You haven't changed the default password for this router. To change router password [click here](#).

WAN / Internet

Type: Static Address (Dropdown menu: Static Address, Disabled, DHCP, PPPoE)

IP Address:

Subnet Mask:

Gateway:

MTU: Default (Dropdown menu: Default, 1500)

Primary DNS:

Secondary DNS:

[Save ✓](#) [Cancel ✕](#)

- 2) Navigate to **Basic Network > VLAN**, enable the LAN1 as WAN Ethernet

You haven't changed the default password for this router. To change router password [click here](#).

VLAN

VID	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
1	✓	✕	✓	✕	✓	✕	✓	✕	✕	✕	br0
2	✕	✕	✕	✕	✕	✕	✕	✕	✓	✕	WAN

[Add +](#)

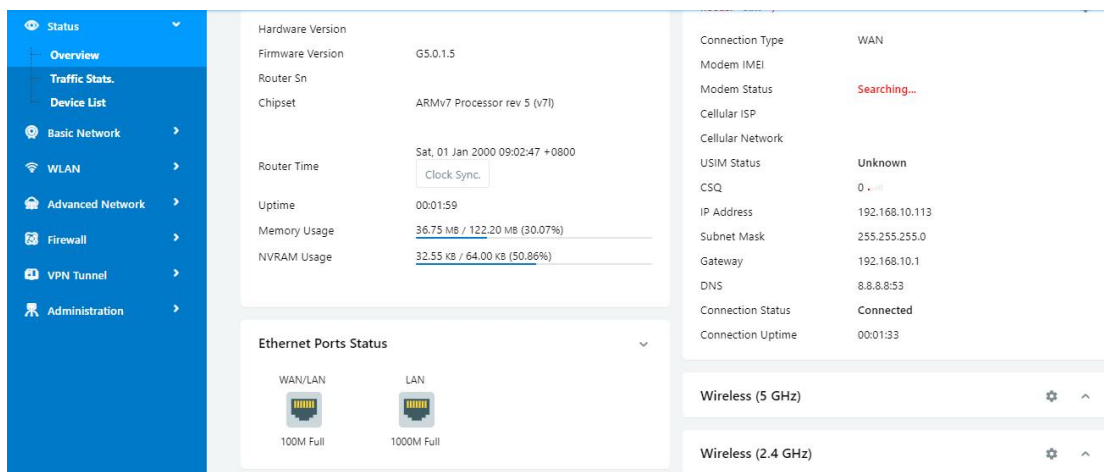
[Save ✓](#) [Cancel ✕](#)

- 3) Navigate to **Basic network > Cellular**, configure the APN as your SIM

- 4) Navigate to **Basic Network > Schedule**, configure WAN (Link1) preferred, Cellular backup (Link2)
Add ICMP Check to WAN
Set the working mode (Schedule)

Parameters	Instruction
modem	The router dial-up to network via modem
wan	The router dial-up to network via WAN (DHCP, PPPOE, Static IP) Ethernet
ICMP Check	When the ICMP Check fails, the switching action between Link1 and Link2 will be triggered
Link1	The preferred link
Link2	The alternate link
BACKUP	Backup mode, Link1 and Link2 will remain online at the same time
FAILOVER	Failover mode, Link2 will dial-up to network when link1 fails

- 5) Status: WAN working



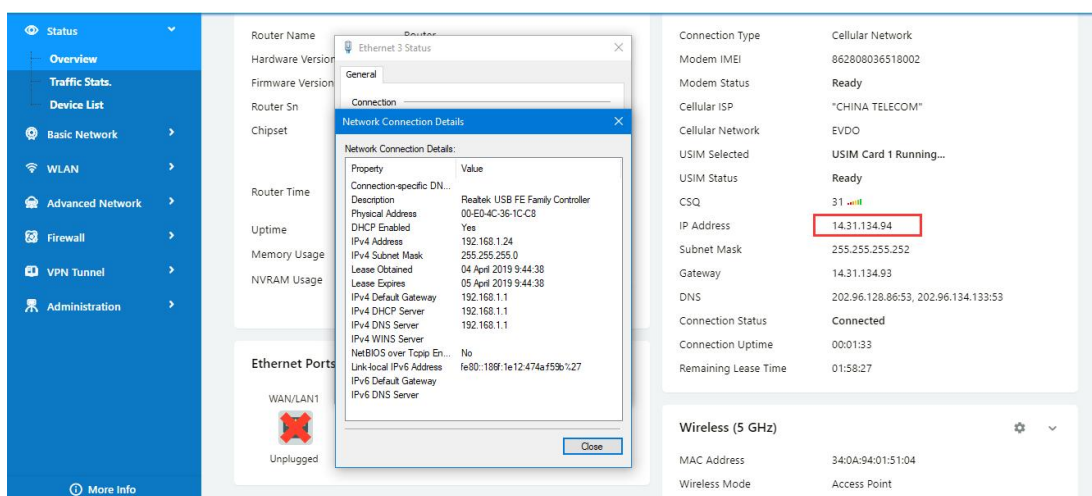
- 6) The system quickly switches traffic to Cellular when the WAN fails
---End

4.3 Port Forwarding

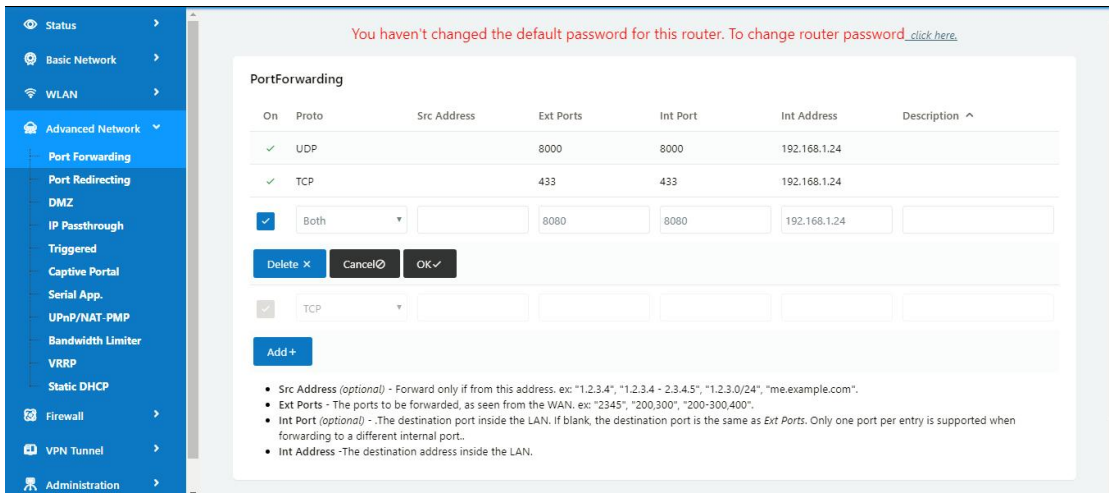
- 1) The router online and got a public IP address 14.31.134.94

Note: It's based on SIM card carrier

- 2) The PC is connected to router and got IP address 192.168.1.24



- 3) Configuration

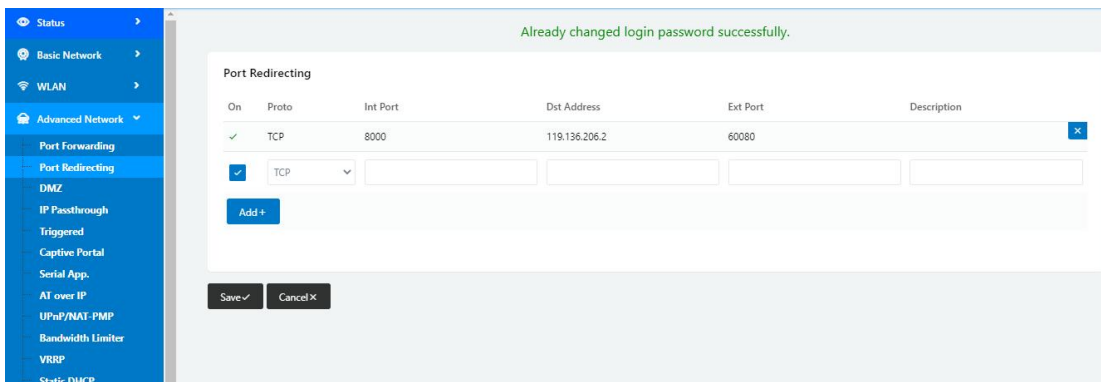


4) The PC can be accessed via 14.31.134.94:443 over Internet

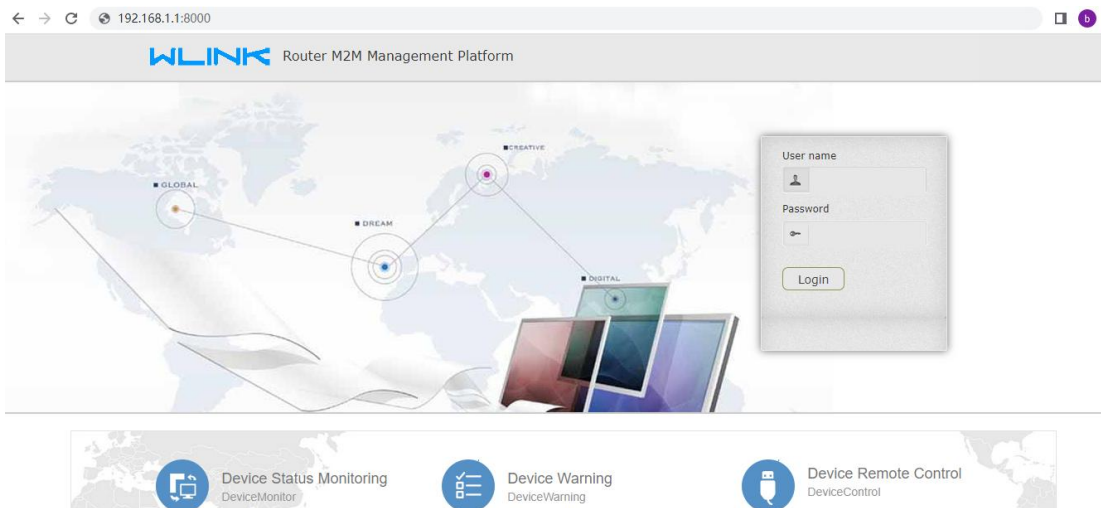
---End

4.4 Port Redirecting

Please click “Advanced Network> Port Redirecting” to check or modify the relevant parameter.



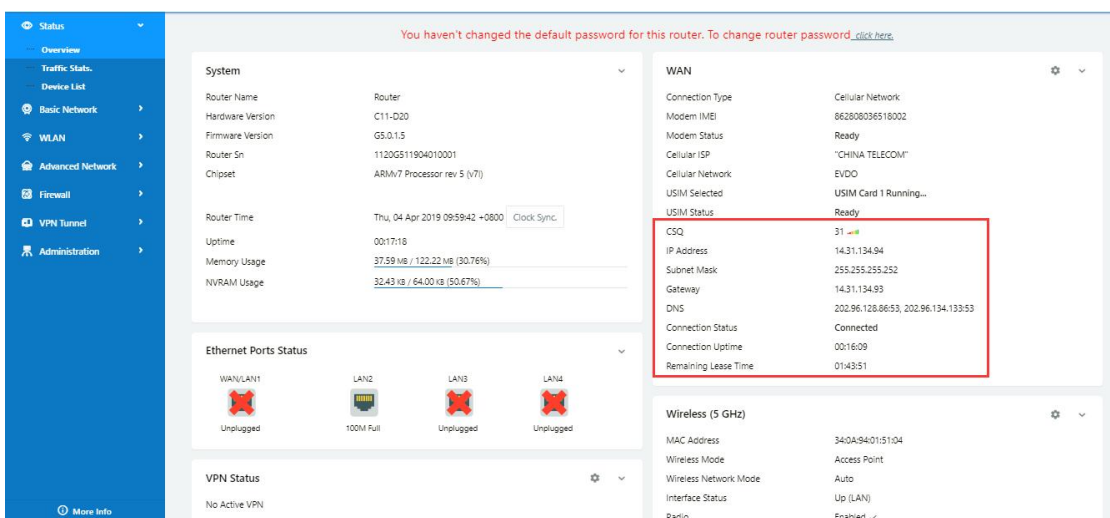
Configure Internal port as 8000, the Destination IP address as 119.136.206.2 and External port 60080(M2M Platform Server IP and Port as example). Access to 192.168.1.1:8000 in browser, the router will redirect to 119.136.206.2: 60080.



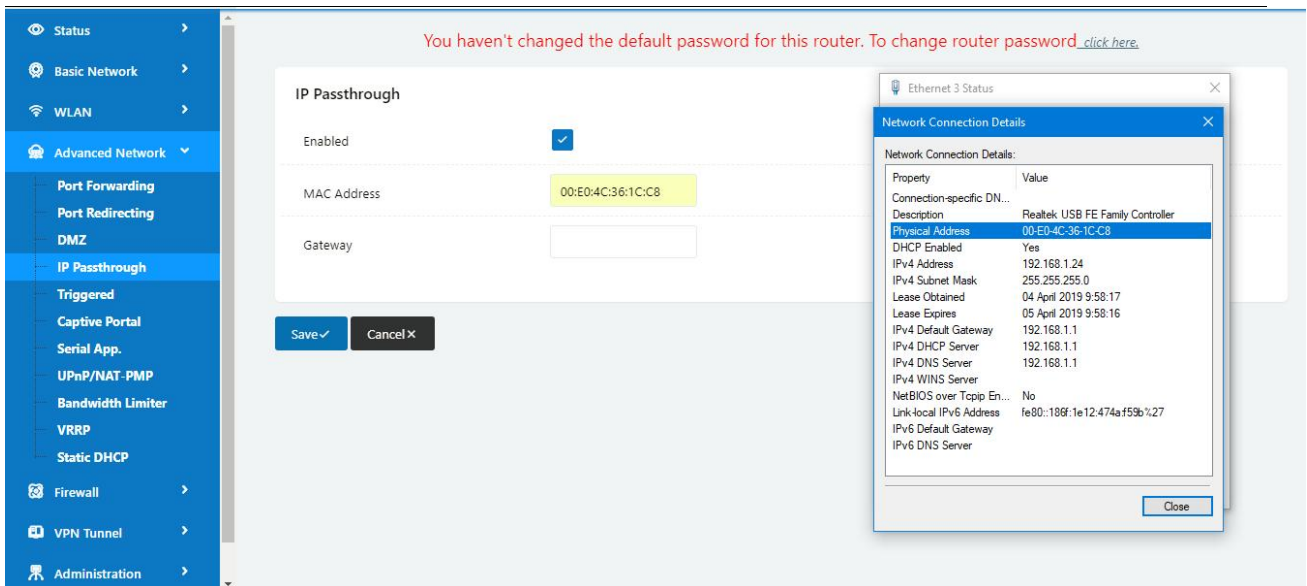
---End

4.5 IP Passthrough

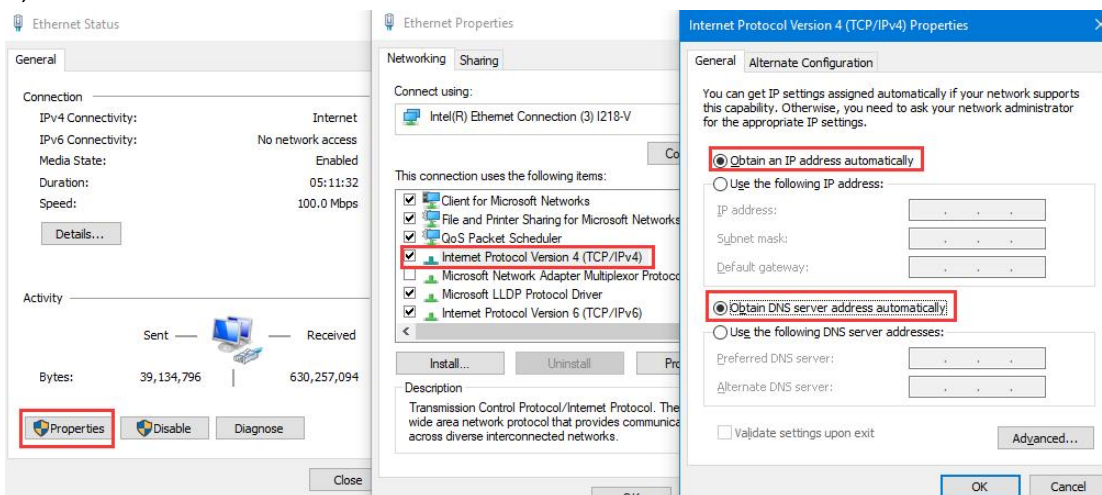
1) The router online



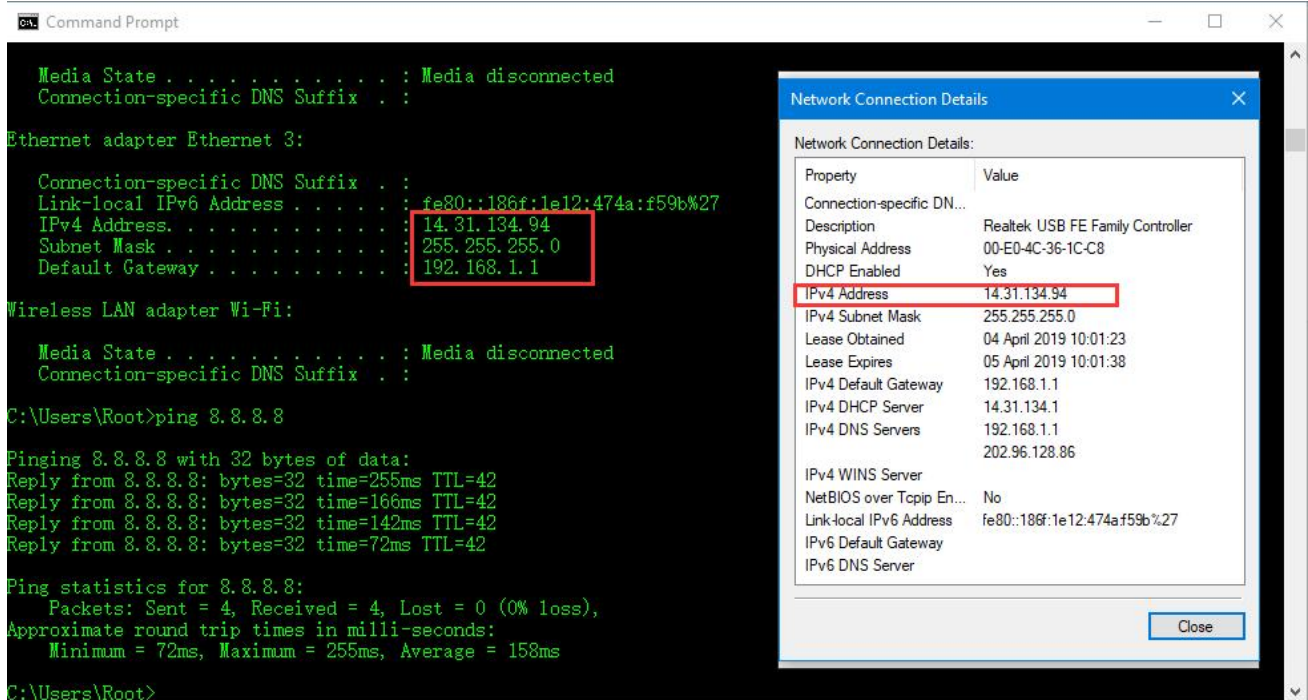
2) Configure IP passthrough destination MAC address (PC Ethernet MAC)



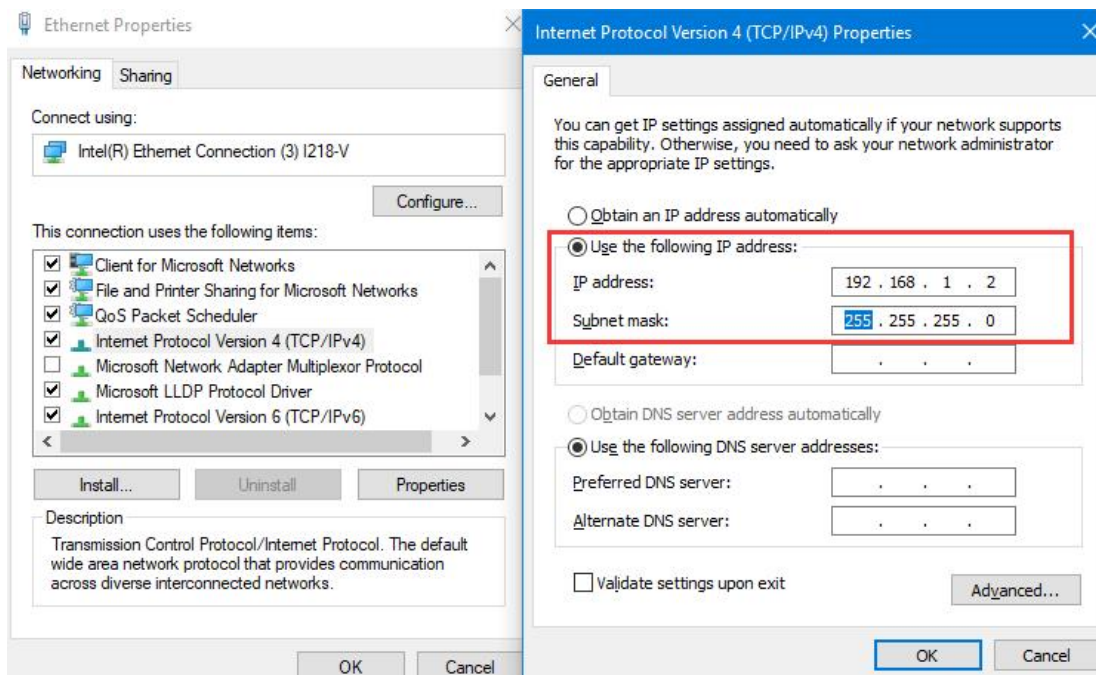
3) Set the PC to DHCP



4) Check the Ethernet status and ping test



5) Set the PC Ethernet as DHCP to release the IP and access to router GUI again



---End

4.6 Captive Portal

Please click "Advanced Network> Captive Portal" to check or modify the relevant parameter.

1) Upload Portal file and Splash.html by local

Upload portal images and splash.html in router for the Slider (0001_portal.png, 0002_portal.png, and 0003_portal.png) to the Router under the “Administration / Storage Settings” menu.

Furthermore, also might upload splash with images together.

Each Ad file just supports 3 Ad portal images. Picture format is acceptable for png/jpg and image size is less than 100Kbytes and resolution is 800*600. Picture name is 0001_portal.png, 0002_portal.png and 0003_portal.png. Furthermore, please keep image names the same between portal file and splash.html.

- Status
- Basic Network
- WLAN
- Advanced Network
- Firewall
- VPN Tunnel
- Administration
 - Identification
 - Time
 - Admin Access
 - Scheduled Reboot
 - SNMP
 - Storage Settings
 - M2M Settings
 - DI/DO Setting
 - Configuration
 - Logging
 - Upgrade
- More Info

Storage settings

Storage Router Total :5,632.00 KB Free:5,100.00 KB

Upload new file

No file chosen Choose File Upload

Current file list

File name	File size	File operation
0001_portal.png	23.8K	✖ 📄
0002_portal.png	45.3K	✖ 📄
0003_portal.png	46.0K	✖ 📄
bootstrap_portal.css	124.3K	✖ 📄
jquery_portal.js	289.7K	✖ 📄
splash.html	3.4K	✖ 📄

```

<!-- <hr> -->

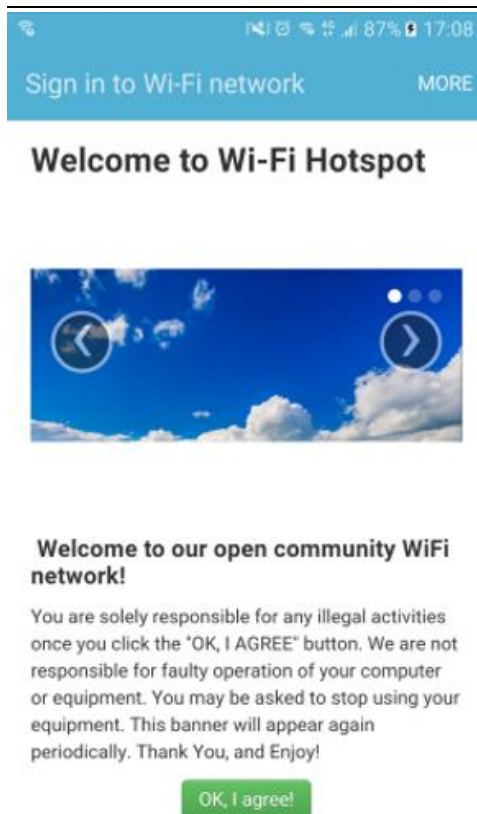
<div id="myCarousel" class="carousel slide marketing">
  <ol class="carousel-indicators">
    <li data-target="#myCarousel" data-slide-to="0" class="active"></li>
    <li data-target="#myCarousel" data-slide-to="1"></li>
    <li data-target="#myCarousel" data-slide-to="2"></li>
  </ol>

  <div class="carousel-inner">
    <div class="item active">
      
    </div>
    <div class="item">
      
    </div>
    <div class="item">
      
    </div>
  </div>
  <a class="left carousel-control" href="#myCarousel" data-slide="prev">&lsaquo;</a>
  <a class="right carousel-control" href="#myCarousel" data-slide="next">&rsaquo;</a>
</div>

<!-- <hr> -->

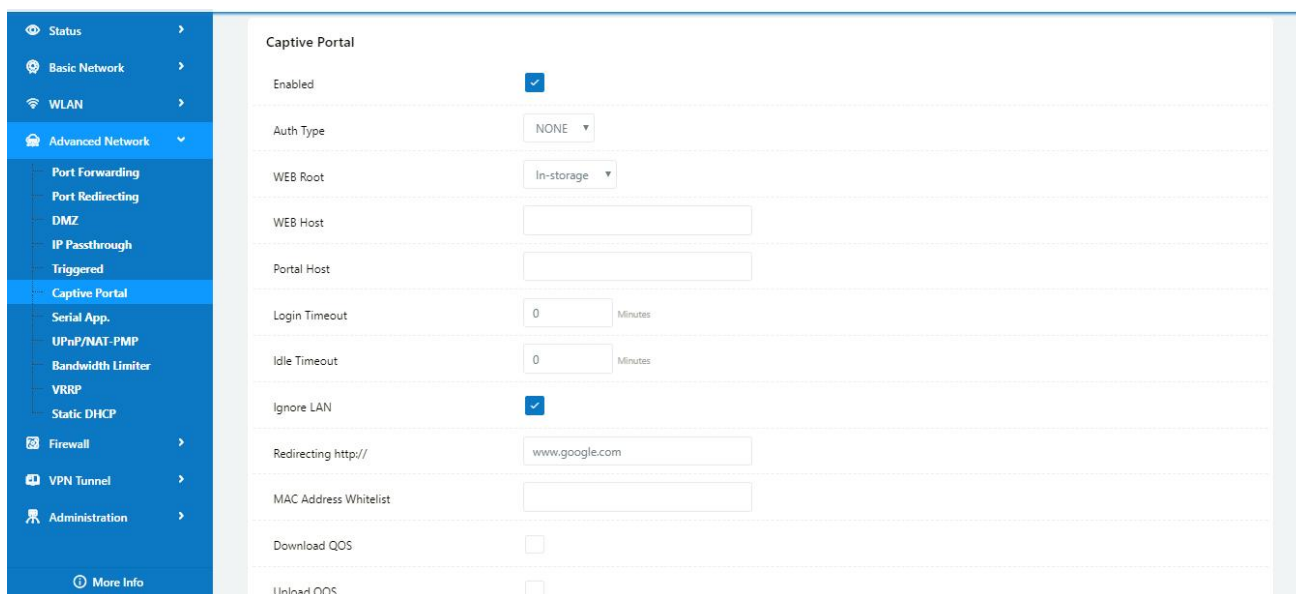
```

Finally, we can see the results by connect to router WIFI



2) Modify portal file storage path

Modify portal file storage for In-storage as below.



---End

4.7 GPS Settings

Please click "Advanced Network> GPS" to view or modify the relevant parameter.

You haven't changed the default password for this router. To change router password [click here](#).

GPS

GPS Mode: Client

Data Format: M2M_FMT

Server IP/Port: 192.168.1.2 : 40002

Heart-Beat Content:

Heart-Beat Interval: 5 (seconds)

Save ✓ Cancel ✕

Table 4-6 "GPS" Instruction

parameter	Instruction
GPS Mode	Enable/Disable
GPS Format	NMEA and M2M_FMT(WLINK)
Server IP/Port	GPS server IP and port
Heart-Beat	If choose M2M_FMT format, heart-beat ID will be packed into GPS data.
Interval	GPS data transmit as the interval time.

Step 1 Please click "save" to finis

Step 2 Connect the GPS antenna to router GPS interface

Step 3 Check GPS Status

You haven't changed the default password for this router. To change router password [click here](#).

GPS Status

Current	OK
System Type	GPS
Satellites Numbers	05
Satellites Clock	190404 - 022121.00
Positioning	2234.22520N - 11356.63170E
Google Map	View



M2M_FMT Format as below.

1. GPS data structure.

Router ID, gps_date, gps_time, gps_use, gps_latitude, gps_NS, gps_longitude, gps_EW, gps_speed, gps_degrees, gps_FS, gps_HDOP, gps_MSL

2. Example

0001_R081850ac,150904,043215.0,06,2234.248130,N,11356.626179,E,0.0,91.5,1,1.2,97.5

3. GPS data description

Field No.	Name	Format	Example	Description
1	Router ID	String	0001_R081850ac	0001 customizable product ID. _R router indicator. 081850ac Last 8digits of routers MAC address.
2	gps_date	yymmdd	150904	Date in year,month,day
3	gps_time	hhmmss.ss s	043215.0	UTC Time, Time of position fix.
4	gps_use	numeric	06	Satellites Used, Range 0 to 12.
5	gps_latitude	ddmm.mm mm	2234.248130	Latitude, Degrees + minutes.
6	gps_NS	character	N	N/S Indicator,N=north or S=south.
7	gps_longitude	ddmm.mm mm	11356.626179	Longitude, Degrees + minutes.
8	gps_EW	character	E	E/W indicator, E=east or W=west.
9	gps_speed	numeric	0.0	Speed(Knots) over ground, units is kn/h.
10	gps_degrees	numeric	91.5	Course over ground, unit is degree.
11	gps_FS	digit	1	Position Fix Status Indicator,
12	gps_HDOP	numeric	1.2	HDOP, Horizontal Dilution of Precision
13	gps_MSL	numeric	97.5	MSL Altitude, units is meter.

---End

4.8 Firewall

1) IP/MAC/Port Filtering

This part used to intercept packages from router's WAN/Celluar interface to Internet.

Test case:

1.1 Only allow three devices (MAC/LAN/WLAN) can access to Internet via WAN: 110.110.10.10

1.2 Only allow three devices (MAC/LAN/WLAN) can access to the router page (192.168.1.1)

The screenshot shows the 'IP/MAC/Port Filtering' configuration page. On the left is a blue sidebar with navigation options: Status, Basic Network, WLAN, Advanced Network, Firewall (selected), IP/URL Filtering, Domain Filtering, VPN Tunnel, and Administration. The main content area has a title 'IP/MAC/Port Filtering'. It contains a table with columns: On, Src MAC, Src IP, Dst IP, Protocol, Src Port, Dst Port, Policy, and Description. There are five rows of configuration, each with a green checkmark in the 'On' column. The first row has 'any/0' for both Src IP and Dst IP, with a 'Drop' policy. The second row has '192.168.1.0/24' for Dst IP, with an 'Accept' policy. The third, fourth, and fifth rows have specific MAC addresses (50:78:9D:C3:9A:22, 60:F1:89:20:F0:9A, and 00:1E:64:DF:E8:46) for Src MAC, with 'any/0' for Src IP and an 'Accept' policy. Below the table is an 'Add +' button. Underneath is the 'Key Word Filtering' section, which is currently empty with an 'Add +' button.

2) Key Word Filtering

This part used to filter key word packages from router's WAN/Cellular interface to Internet.

The screenshot shows two configuration pages. The top page is 'URL Filtering', which has a table with columns: On, URL, and Description. It contains two rows with 'youtube' and 'facebook' in the URL column, both with green checkmarks in the 'On' column. Below the table is an 'Add +' button. The bottom page is 'Access Filtering', which has a table with columns: On, Src MAC, Src IP, Dst IP, Protocol, Src Port, Dst Port, Policy, and Description. It contains one row with a green checkmark in the 'On' column and 'NOI' in the Protocol column. Below the table is an 'Add +' button. At the bottom of the page are 'Save ✓' and 'Cancel X' buttons.

3) URL Filtering

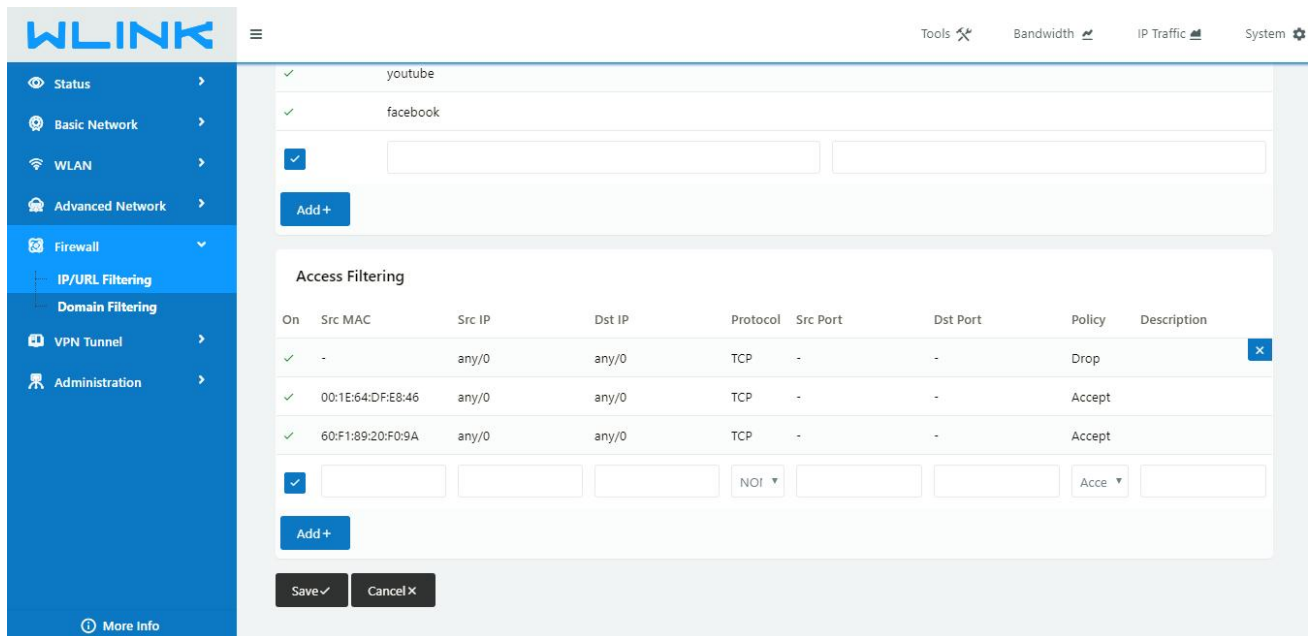
This part used to filter URL from router's WAN/Cellular interface to Internet.

4) Access Filtering

This part used to filter packages from Internet to router's WAN/Celluar interface.

Test case:

- 4.1) Intercept all TCP packets accessing the router's WAN/Celluar(110.110.10.10).
- 4.2) Only two devices (MAC/LAN/WLAN) are allowed to be accessed from Internet packets.

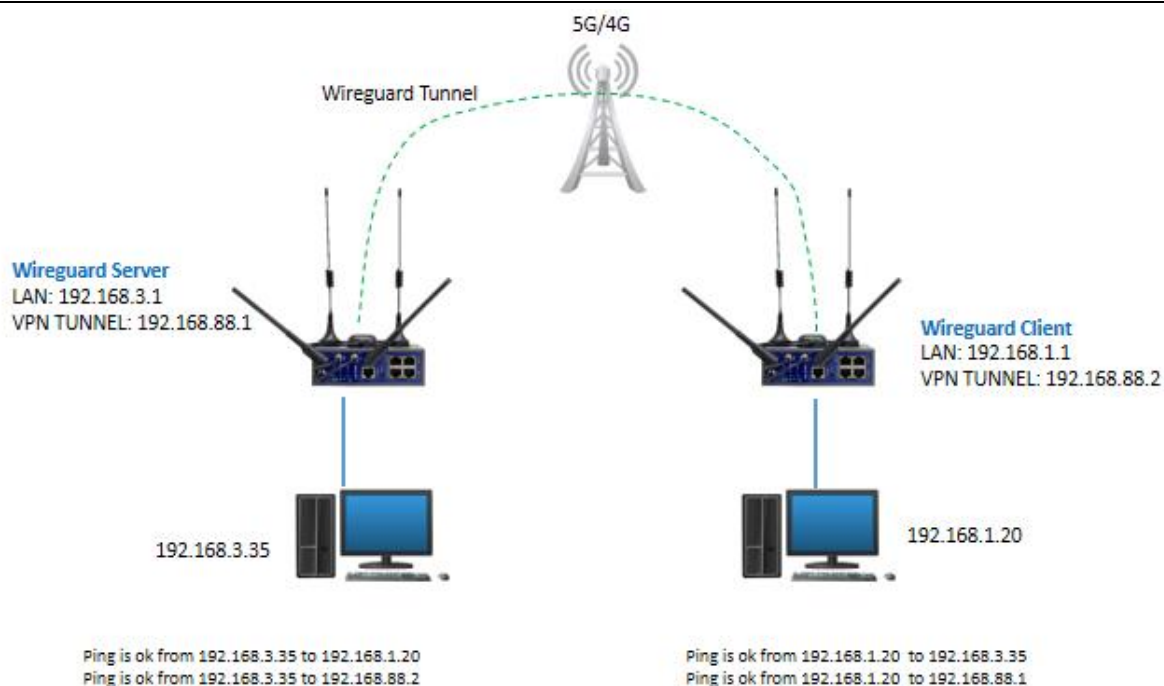


---End

4.9 VPN Tunnel

4.9.1 Wireguard VPN

Wireguard VPN between two WL-Rxx Routers



1) Wireguard VPN Client Setting

Configure Wireguard Client as Server requested. Especially, the public Key and private key is generated by server or third party. Configure server public key in the peer key table and client private key in the local key table.

Wireguard	
Enabled	<input checked="" type="checkbox"/>
Mode	Client
Peer IP/Port	113.87.81.122 : 51821
Local Key	qFfPQ7MQL6G7mohLP3NYtvS5Zer05tDDdAFaFieJgUE=
Local IP/Mask	192.168.88.4/24 ex. 192.168.88.5/24
Peer Key	9VDgAnfn5xsNaKJ+Z6VKNCi5GSCpA+dkoscbXGKmkw=
Preshared Key	
Peer Subnet IP/Mask	192.168.3.0/24 ex. 192.168.88.0/24
<input type="button" value="Save ✓"/> <input type="button" value="Cancel ✕"/>	

2) Wireguard Routing

There are two routings when Wireguard established.

Current Routing Table				
Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
default	192.168.10.1	0.0.0.0	0	wan
127.0.0.0	*	255.0.0.0	0	lo
192.168.1.0	*	255.255.255.0	0	lan
192.168.3.0	*	255.255.255.0	0	wg0
192.168.10.0	*	255.255.255.0	0	wan
192.168.10.1	*	255.255.255.255	0	wan
192.168.88.0	*	255.255.255.0	0	wg0

3) Wireguard Connection Check

Check VPN connection via Ping testing.

```

wg0      Link encap:Ethernet HWaddr 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
        inet addr:192.168.88.2 P-t-P:192.168.88.2 Mask:255.255.255.0
        UP POINTOPOINT RUNNING NOARP MTU:1420 Metric:1
        RX packets:7 errors:0 dropped:0 overruns:0 frame:0
        TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:764 (764.0 B) TX bytes:820 (820.0 B)

root@Router:/tmp/home/root# ping 192.168.88.1
PING 192.168.88.1 (192.168.88.1): 56 data bytes
64 bytes from 192.168.88.1: seq=0 ttl=64 time=1.388 ms
64 bytes from 192.168.88.1: seq=1 ttl=64 time=1.181 ms
64 bytes from 192.168.88.1: seq=2 ttl=64 time=1.557 ms
64 bytes from 192.168.88.1: seq=3 ttl=64 time=1.246 ms
^C
--- 192.168.88.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.181/1.343/1.557 ms

root@Router:/tmp/home/root# ping 192.168.3.1
PING 192.168.3.1 (192.168.3.1): 56 data bytes
64 bytes from 192.168.3.1: seq=0 ttl=64 time=1.375 ms
64 bytes from 192.168.3.1: seq=1 ttl=64 time=1.061 ms
64 bytes from 192.168.3.1: seq=2 ttl=64 time=1.141 ms
64 bytes from 192.168.3.1: seq=3 ttl=64 time=1.141 ms
^C
--- 192.168.3.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.061/1.179/1.375 ms

root@Router:/tmp/home/root# ping 192.168.3.35
PING 192.168.3.35 (192.168.3.35): 56 data bytes
64 bytes from 192.168.3.35: seq=0 ttl=63 time=2.570 ms
64 bytes from 192.168.3.35: seq=1 ttl=63 time=1.875 ms
64 bytes from 192.168.3.35: seq=2 ttl=63 time=2.015 ms
64 bytes from 192.168.3.35: seq=3 ttl=63 time=2.251 ms
^C
--- 192.168.3.35 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.875/2.177/2.570 ms

```

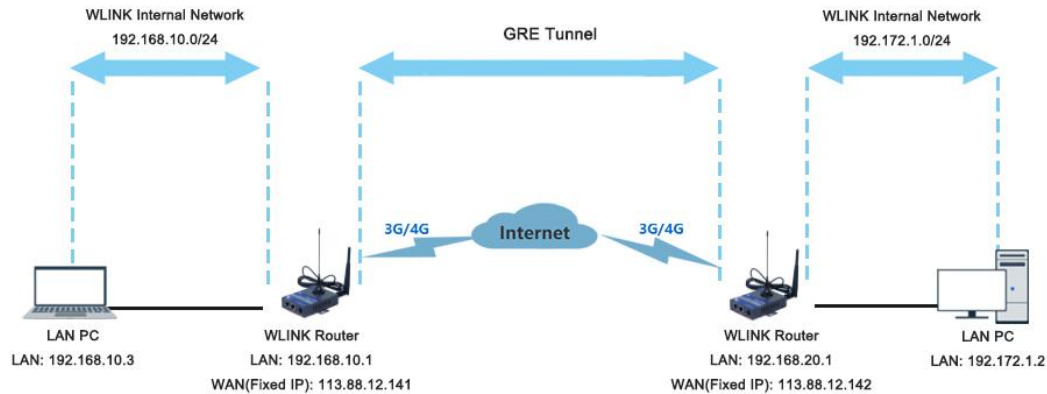
Wireguard Peer Virtual IP

WG Server Gateway IP

WG Server LAN Host IP

4.9.2 GRE

GRE Tunnel between two WL-Rxx Routers



1) WL-R200(A) Config

Navigate to **Basic Network > LAN**

You haven't changed the default password for this router. To change router password [click here](#).

LAN

Bridge ^	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)
br0	192.168.10.1	255.255.255.0	✓	192.168.10.2 - 51	1440

1

[Add +](#)

[Save ✓](#) [Cancel ✕](#)

Navigate to **VPN Tunnel > GRE**

Status

Basic Network

WLAN

Advanced Network

Firewall

VPN Tunnel

GRE

OpenVPN Client

PPTP/L2TP Client

IPSec

Administration

More Info

GRE Tunnel

On	Idx ^	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Description
<input checked="" type="checkbox"/>	1	192.168.10.10	113.113.11.11	113.111.10.10	<input checked="" type="checkbox"/>	10	5	A

☒

☐

Add +

GRE Route

On	Tunnel Index ^	Destination Address	Description
<input checked="" type="checkbox"/>	1	192.172.1.0/24	A

☒

1

Add +

Save ✓

Cancel ✕

2) WL-R200(B) Config

Navigate to **Basic Network > LAN**

Status

Basic Network

WAN

Cellular

LAN

VLAN

Schedule

DDNS

Routing

WLAN

Advanced Network

Firewall

VPN Tunnel

Administration

More Info

You haven't changed the default password for this router. To change router password [click here.](#)

LAN

Bridge ^	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)
br0	192.172.1.1	255.255.255.0	<input checked="" type="checkbox"/>	192.172.1.2 - 51	1440

1

☐

Add +

Save ✓

Cancel ✕

Navigate to **VPN Tunnel > GRE**

Status

Basic Network

WLAN

Advanced Network

Firewall

VPN Tunnel

GRE

OpenVPN Client

PPTP/L2TP Client

IPSec

Administration

More Info

GRE Tunnel

On	Idx	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Description
<input checked="" type="checkbox"/>	1	192.172.1.10	113.111.10.101	113.113.11.11	<input checked="" type="checkbox"/>	10	5	B

☒

☐

Add +

GRE Route

On	Tunnel Index	Destination Address	Description
<input checked="" type="checkbox"/>	1	192.168.10.0/24	B

☒

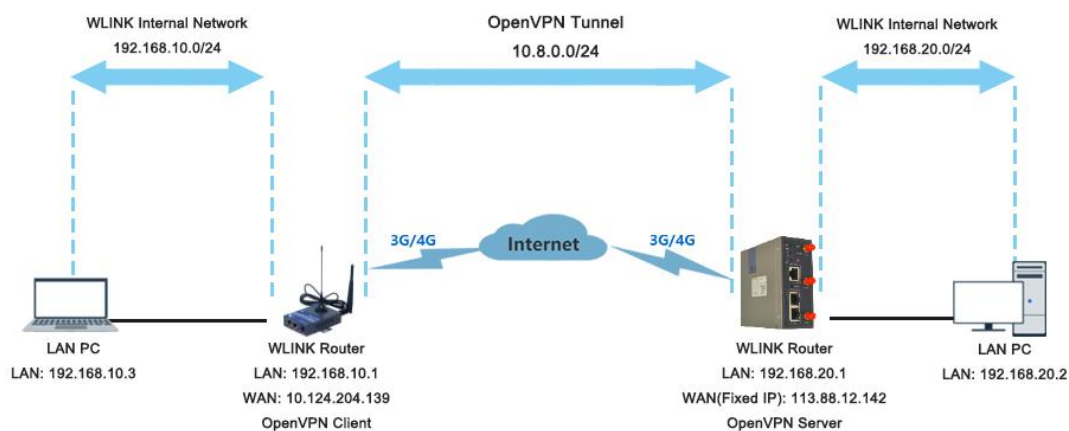
1

Add +

Save

Cancel

4.9.3 OpenVPN



OpenVPN between WL-Rxx client and Server

Please click "VPN Tunnel> OpenVPN Client" to check or modify the relevant parameter.

WLINK Tools Bandwidth IP Traffic System

VPN Tunnel

- GRE
- OpenVPN Client**
- PPTP/L2TP Client
- IPSec

OpenVPN Client

Client 1 Client 2

Basic Advanced Keys Status

VPN Client #1 (Stopped)

Start with WAN ☒

Interface Type TUN

Protocol UDP

Server Address wlink-tech.com 1194

Firewall Automatic

Authorization Mode TLS

Username/Password Authentication ☐

HMAC authorization Disabled

Create NAT on tunnel ☒

Start Now

Parameter	Instruction
Start with WAN	Enable the Openvpn feature for 4G/3G/WAN port.
Interface Type	Tap and Tun type are optional. Tap is for bridge mode and Tunnel is for routing mode.
Protocol	UDP and TCP optional.
Server Address	The Openvpn server public IP address and port.
Firewall	Auto, External only and Custom are optional
Authorization Mode	TLS, Static key and Custom are optional.
User name/Password Authentication	As the configuration requested.
HMAC authorization	As the configuration requested.
Create NAT on tunnel	Configure NAT in Openvpn tunnel.

The screenshot displays the 'OpenVPN Client' configuration page. On the left is a navigation menu with options like Status, Basic Network, WLAN, Advanced Network, Firewall, VPN Tunnel, GRE, OpenVPN Client, PPTP/L2TP Client, IPSec, and Administration. The main area is titled 'OpenVPN Client' and has tabs for 'Client 1' and 'Client 2'. Below these are sub-tabs: 'Basic', 'Advanced', 'Keys', and 'Status'. The 'Advanced' tab is active, showing settings for 'VPN Client #1 (Stopped)'. The settings include: Poll Interval (0 minutes), Redirect Internet traffic (checkbox), Accept DNS configuration (Disabled), Encryption cipher (Use Default), Compression (Adaptive), TLS Renegotiation Time (-1 seconds), Connection retry (30 seconds), Verify server certificate (checkbox), and a Custom Configuration text area.

Parameter	Instruction
Poll Interval	Openvpn client check router's status as interval time.
Redirect Internet Traffic	Configure Openvpn as default routing.
Access DNS	As the configuration requested.
Encryption	As the configuration requested.
Compression	As the configuration requested.
TLS Renegotiation Time	TLS negotiation time. -1 as default for 60s.
Connection Retry Time	Openvpn retry to connection interval.
Verify server certificate	As the configuration requested.
Custom Configuration	As the configuration requested.

You haven't changed the default password for this router. To change router password [click here](#).

OpenVPN Client

Client 1 Client 2

Basic Advanced **Keys** Status

VPN Client #1 (Stopped)

For help generating keys, refer to the OpenVPN HOWTO.

Certificate Authority

Client Certificate

Client Key

Start Now

Save ✓ Cancel ✕

Parameter	Instruction
Certificate Authority	Keep certificate same as the server
Client Certificate	Keep client certificate same as the server
Client Key	Keep client key same as the server

You haven't changed the default password for this router. To change router password [click here](#).

OpenVPN Client

Client 1 Client 2

Basic Advanced Keys **Status**

VPN Client #1 (Stopped)

Client is not running or status could not be read.

Refresh Status

Start Now

Save ✓ Cancel ✕

Parameter	Instruction
Status	Check OpenVPN status and data statistics.

Click “save” and “start now” to enable OpenVPN when you have done all the client config.



OpenVPN Keys Guide

The following steps are for server running on Windows 7/8/10

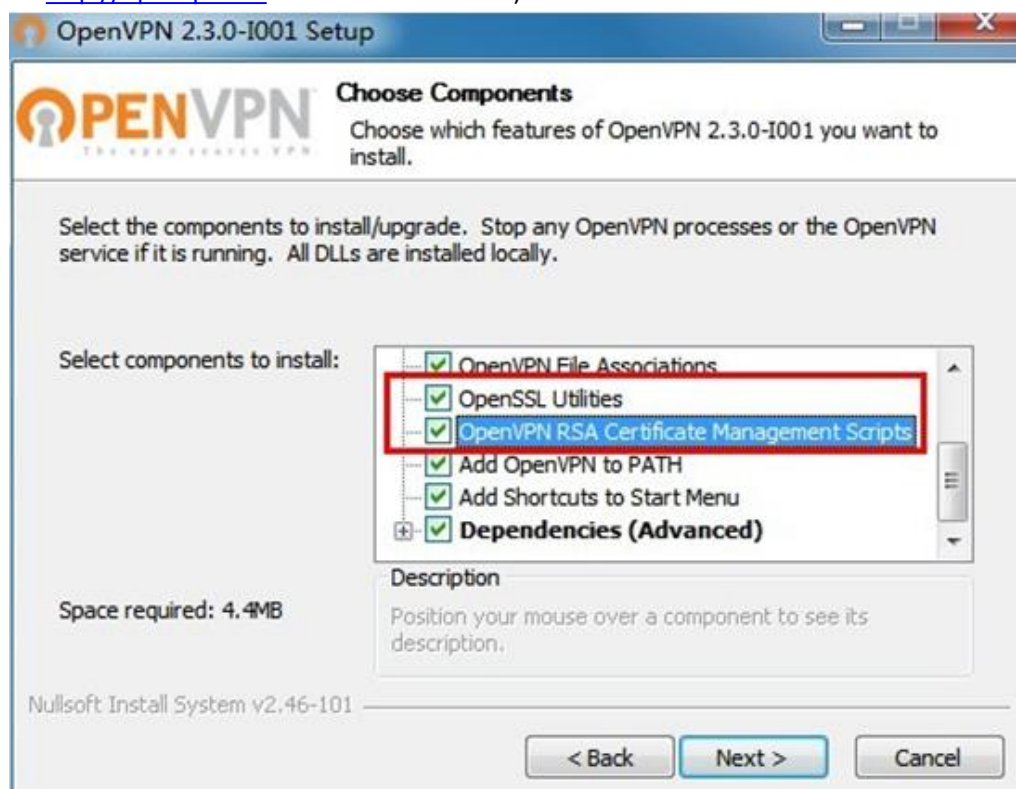
Access to (<http://openvpn.net/release/>) and download the file “openvpn-2.3.0-install.exe” (or higher)



Index of /release

Name	Last modified	Size	Description
Parent Directory	-		
lzo-1.08-3.0.el2.dag.i386.rpm	21-Feb-2012 00:50	55K	
lzo-1.08-3.0.rh7.dag.i386.rpm	21-Feb-2012 00:50	54K	
lzo-1.08-3.0.rh8.dag.i386.rpm	21-Feb-2012 00:50	58K	
lzo-1.08-4.0.rh9.rf.i386.rpm	21-Feb-2012 00:50	59K	
lzo-1.08-4.1.el3.rf.i386.rpm	21-Feb-2012 00:50	58K	
lzo-1.08-4.1.el3.rf.x86_64.rpm	21-Feb-2012 00:50	55K	
lzo-1.08-4.1.fc1.rf.i386.rpm	21-Feb-2012 00:50	58K	

After installing OpenVPN, please find the OpenVPN folder to generate the certificate of server and client.
(Access to <http://openvpn.net> for more information)



PC > Newdisk (D:) > OpenVPN >

Name	Date modified	Type	Size
bin	2019-01-10 11:42	File folder	
config	2019-01-10 14:10	File folder	
doc	2019-01-10 11:42	File folder	
easy-rsa	2019-01-10 11:54	File folder	
log	2019-01-10 14:10	File folder	
sample-config	2019-01-10 11:41	File folder	
icon.ico	2015-02-18 17:56	Icon	22 KB
Uninstall.exe	2019-01-10 11:42	Application	117 KB

Configure "vas.bat.sample" to complete the initialization step and keys

This PC > Newdisk (D:) > OpenVPN > easy-rsa >

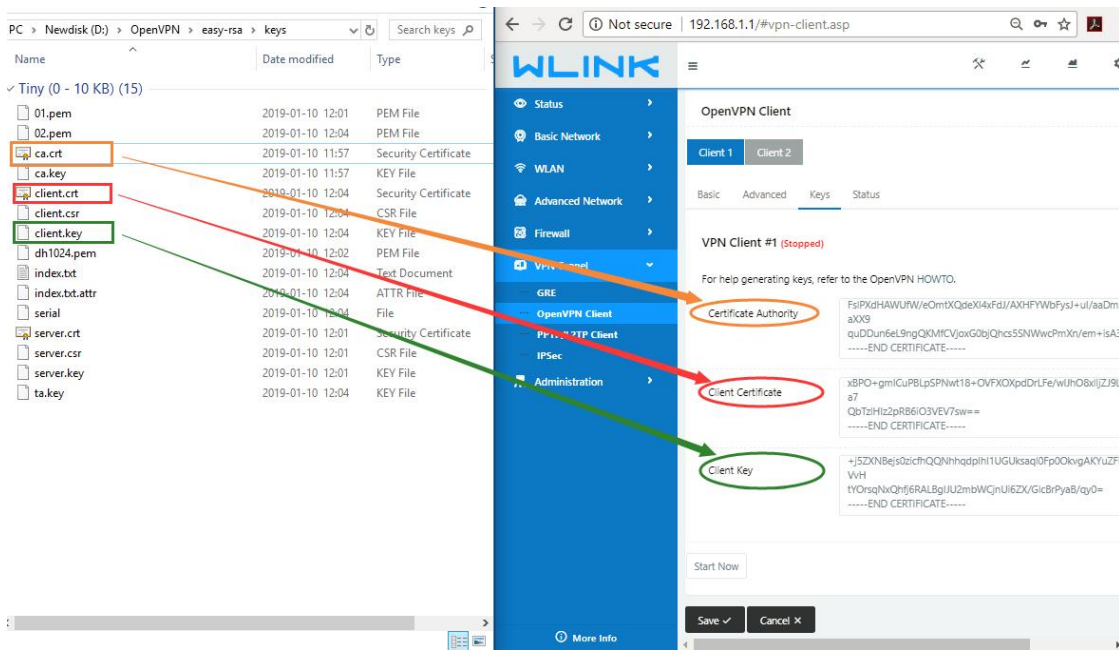
Name	Date modified	Type	Size
keys	2019-01-10 12:04	File folder	
.rnd	2019-01-10 12:04	RND File	1 KB
build-ca.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-dh.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-key.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-key-pass.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-key-pkcs12.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-key-server.bat	2016-01-04 20:41	Windows Batch File	1 KB
clean-all.bat	2016-01-04 20:41	Windows Batch File	1 KB
index.txt.start	2016-01-04 20:41	START File	0 KB
init-config.bat	2016-01-04 20:41	Windows Batch File	1 KB
openssl-1.0.0.cnf	2016-01-04 20:41	CNF File	9 KB
README.txt	2016-01-04 20:41	Text Document	2 KB
revoke-full.bat	2016-01-04 20:41	Windows Batch File	1 KB
serial.start	2016-01-04 20:41	START File	1 KB
vars.bat	2019-01-10 11:43	Windows Batch File	1 KB
vars.bat.sample	2019-01-10 11:43	SAMPLE File	1 KB

Configure the client keys to WLINK OpenVPN client GUI when you create the server and client certificate in the path OpenVPN/easy-rsa/keys

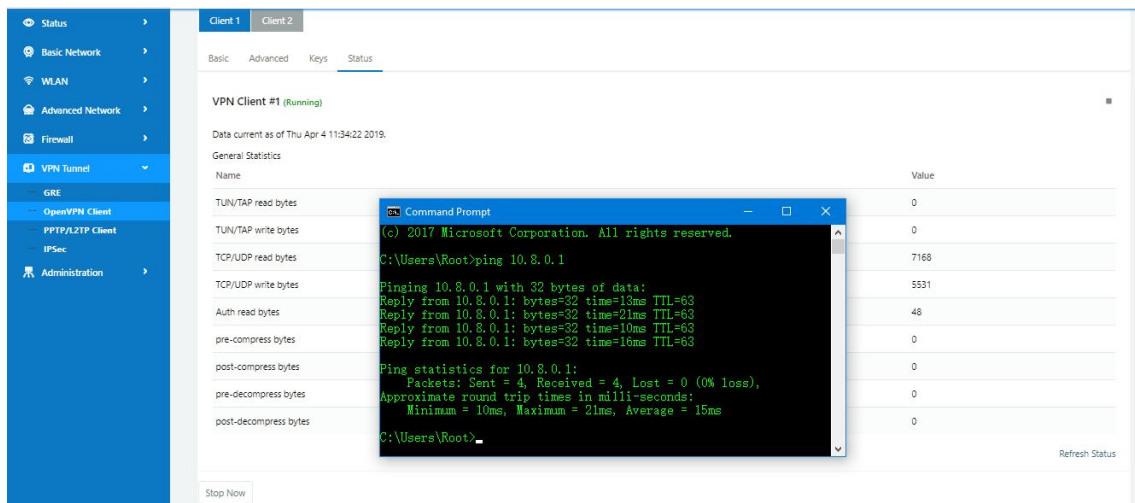
Client certificate (Generated on the server)

Name	Date modified	Type	Size
ca.crt	2019-01-10 11:57	Security Certificate	2 KB
client.crt	2019-01-10 12:04	Security Certificate	4 KB
client.key	2019-01-10 12:04	KEY File	1 KB
client.ovpn	2019-01-10 14:08	OpenVPN Config ...	4 KB
ta.key	2019-01-10 12:04	KEY File	1 KB

OpenVPN>easy-rsa>keys



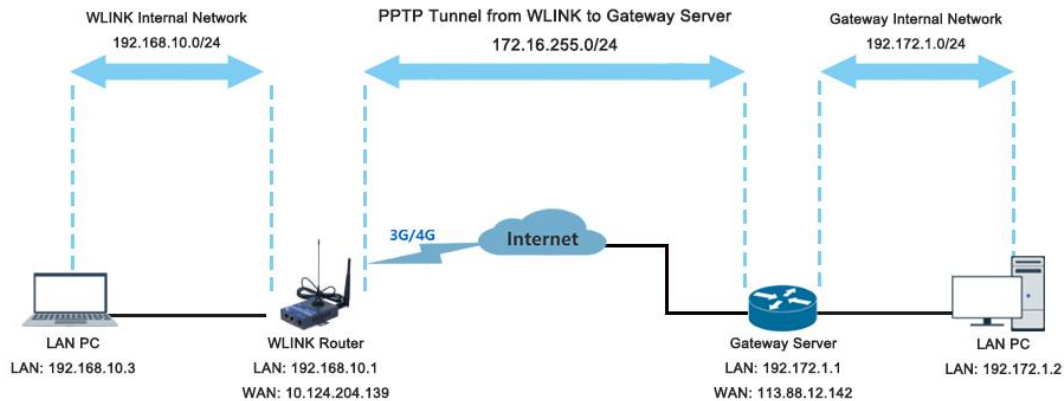
Ping test to your server when the tunnel is established



---End

4.9.4 L2TP/PPTP

Please click “VPN Tunnel>PPTP/L2TP Client” to view or modify the relevant parameter.



Configured as PPTP

The screenshot shows the web interface for configuring PPTP. The left sidebar lists various settings, with 'VPN Tunnel' selected. The main area shows the 'L2TP/PPTP Basic' configuration. A table lists the PPTP configuration:

On	Protocol	Name	Server	Username	Password	Firewall	Default Route	Local IP
<input checked="" type="checkbox"/>	PPTP	3	wlinktech.com.cn	test123	test123	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

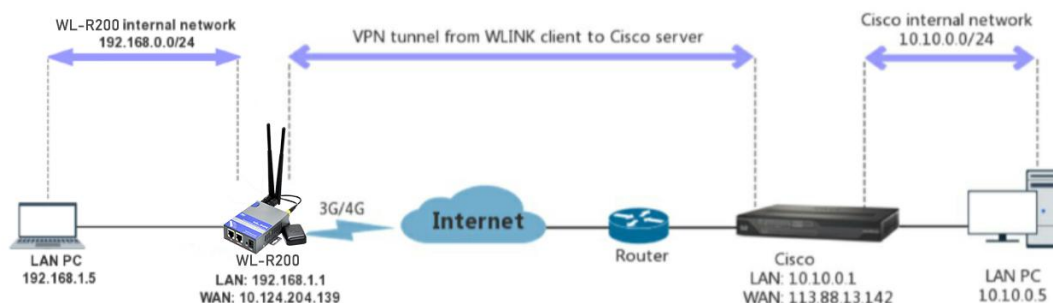
Below the table, there are sections for 'L2TP Advanced' and 'PPTP Advanced' configurations, each with an 'Add +' button.

Note: The Custom Options are based on your server

---End

4.9.5 IPSec

IPSec between WL-R200 and Cisco Router



1) Cisco Config (main mode)

!

crypto isakmp policy 10

encr 3des

hash md5

authentication pre-share

group 2

crypto isakmp key test1234 address 0.0.0.0 0.0.0.0

!

!

crypto ipsec transform-set Tran-set esp-3des esp-sha-hmac

crypto ipsec nat-transparency spi-matching

!

2) WLINK Config

Navigate to **VPN Tunnel > IPsec > Group Setup**

You haven't changed the default password for this router. To change router password [click here](#).

IPSec

IPSec 1 | IPSec 2 | Schedule

Group Setup | Basic Setup | Advanced Setup

Enable IPsec ☒

IPSec Extensions Normal

Local Security Gateway Interface 3G Cellular

Local Security Group Subnet/Netmask 192.168.1.0/24 ex. 192.168.1.0/24

Local Security Firewalling ☒

Remote Security Gateway IP/Domain 113.88.13.142

Remote Security Group Subnet/Netmask 10.10.0.0/24 ex. 192.168.88.0/24

Remote Security Firewalling ☒

Save ✓ Cancel ✕

Navigate to **VPN Tunnel > IPsec > Basic Setup**

IPSec 1 | IPSec 2 | Schedule

Group Setup | Basic Setup | Advanced Setup

Keying Mode IKE with Preshared Key

Phase 1 DH Group Group 2 - modp1024

Phase 1 Encryption 3DES (168-bit)

Phase 1 Authentication MD5 HMAC (96-bit)

Phase 1 SA Life Time 28800 seconds

Phase 2 DH Group Group 2 - modp1024

Phase 2 Encryption 3DES (168-bit)

Phase 2 Authentication SHA1 HMAC (96-bit)

Phase 2 SA Life Time 3600 seconds

Preshared Key *****

Save ✓ Cancel ✕

Navigate to **VPN Tunnel > IPsec > Advanced Setup**

Status

Basic Network

WLAN

Advanced Network

Firewall

VPN Tunnel

GRE

OpenVPN Client

PPTP/L2TP Client

IPSec

Administration

More Info

IPSec

IPSec 1 | IPSec 2 | Schedule

Group Setup | Basic Setup | Advanced Setup

Aggressive Mode

Compress(IP Payload Compression)

Dead Peer Detection(DPD)

ICMP Check

Check Period Time Interval

Check Timeout Count

Check IP

IPSec Custom Options 1

IPSec Custom Options 2

IPSec Custom Options 3

IPSec Custom Options 4

Save ✓ | Cancel ✕

Status

Overview

Traffic Stats.

GPS Status

Device List

Basic Network

WLAN

Advanced Network

Firewall

VPN Tunnel

Administration

More Info

VPN Status

Name

2

Protocol

L2TP

Connection Status

Disconnected

IP Address

0.0.0.0

Gateway

0.0.0.0

IPSec 1

Connected

Phase 1 Status

21 seconds

Phase 1 IKE

3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024

Phase 2 Status

TUNNEL

Phase 2 ESP

3DES_CBC/HMAC_SHA1_96

IPSec Recv.

84 Bytes

IPSec Send.

84 Bytes

LAN

Router MAC Address

34:0A:94:01:51:01

Router IP Addresses

br0 (LAN) - 192.168.1.1/24

DHCP

br0 (LAN) - 192.168.1.2 - 192.168.1.51

Wireless Mode

Wireless Network Mode

Interface Status

Radio

SSID

Broadcast

Security

Channel

Channel Width

Interference Level

Rate

Access Point

Auto

Up (LAN)

Enabled ✓

router-wifi_015103_5G

Enabled ✓

disabled

149 - 5.745 GHz

80 MHz

Acceptable

433 Mbps

Wireless (2.4 GHz)

MAC Address

Wireless Mode

Wireless Network Mode

Interface Status

Radio

SSID

Broadcast

Security

Channel

Channel Width

Interference Level

Rate

34:0A:94:01:51:03

Access Point

Auto

Up (LAN)

Enabled ✓

router-wifi_015103

Enabled ✓

disabled

7 - 2.442 GHz

40 MHz

Acceptable

200 Mbps

---End