



User Manual

---Apply to WL-R100 Series Industrial 4G/3G Router

V2.4

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

Feb, 2022



Copyright © Shenzhen WLINK Technology Company Limited 2012 ~ 2022

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.

Caution

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.

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 Product Introduction	4
1.1 Product overview	4
1.2 Model introduction	4
1.3 Product Appearance	5
1.4 Typical Application Diagram	5
1.5 Features	6
2 Hardware Installation	7
2.1 Panel	7
2.2 LED Status	8
2.3 Dimension	9
2.4 How to Install	9
3 Router Configuration	11
3.1 Local Configure	11
3.2 Basic Configuration	12
3.3 Advanced Network Setting	17
3.4 Firewall	26
3.5 VPN Tunnel	28
3.6 Administration	37
3.7 Debugging Setting	45

3.8 “RST” Button for Restore Factory Setting	48
4 Configuration Instance	48
4.1 Port Forwarding	49
4.2 IP Passthrough	50
4.3 GPS Settings	52
4.4 Firewall	55
4.5 VPN Tunnel	57

1

Product Introduction

1.1 Product overview

WLINK industrial Router is based on industrial grade design, built-in high-powered 32bit MIPS processor, and multi-band 4G/3G communication module, support WCDMA, HSPA+, 4G FDD/TDD etc., provide quick and convenient internet access or private network transmission to customer, provide wire-line network or wireless WLAN share high speed access, meanwhile, customized high security VPN (Open VPN、IPSec、SSL), to construct safe channel, widely used in financial, electric power, environment, oil, transportation, security, etc..

WLINK industrial series router provide GUI, optional CLI configuration interface, customer can configure by IE explore or Telnet/SSH, various configuration method, concise and friendly interface make configuring and managing of all router terminal easier ,meanwhile, WLINK provide M2M terminal management platform to manage all router terminal with remote management. User can monitor all terminals which connected to platform successfully by this platform, provide long-distance control, parameter configuration, and long-distance upgrade service.





1.2 Model introduction

WLINK industrial grade router series have single module / single SIM card, single module / double SIM card, double module / double SIM card design, support multi-band frequency WCDMA, HSPA+, 4G FDD/TDD etc., and downward compatibility to GPRS、EDGE、CDMA 1x, etc., optional GPS module Expansion positioning function, to suit different requirement and different network environment of different operators. Our Router series have many model for option, below is the product model indications in detail, for more optional models, please consult local distributors /resellers.

Partial Order Number List							
Model	4G	3G	Interface	WiFi	4G MIMO	DL	UL
WL-R10LH1	FDD 2600/2100/1900/1800/900/800MHz	HSPA+/HSPA/HSDPA 850/900/1900/2100MHz	1xLAN 1xRS-232	No	Yes	100M	50M
WL-R100L	FDD 2600/2100/1800/900/800MHz	HSPA+/HSPA/HSDPA 800/850/900/1900/2100MHz	1xLAN 1xRS-232	No	Yes	100M	50M
WL-R100LF	FDD: 1800/2100/2600MHz TDD: 1900/2300/2600MHz	HSPA+/HSPA/HSDPA 2100/1900/850/900MHz	1xLAN 1xRS-232	No	Yes	FDD:100M TDD:60M	FDD:50M TDD:60M
WL-R100LH2	FDD: 700/850/1700/1900MHz	DC-HSPA+/HSPA+/HSDPA 2100/1900/850/900MHz	1xLAN 1xRS-232	No	Yes	100M	50M
WL-R100H	/	HSPA+ 2100/1900/850MHz	1xLAN 1xRS-232	No	No	21M	5.76M
WL-R100H1	/	HSPA+ 2100/1900/900/850MHz	1xLAN 1xRS-232	No	No	21M	5.76M
WL-R100H4	/	HSPA+ 900/2100 or 850/1900MHz	1xLAN 1xRS-232	No	No	21M	5.76M
WL-R100E	/	EVDO 800MHz	1xLAN 1xRS-232	No	No	3.1M	1.8M

1.3 Product Appearance

Table 1-1 WLINK Router Appearance

Series	R100	R200	R210	R520
Appearance				
Ports	1*LAN 1*RS232	2*LAN/ 1*LAN+ 1*WAN GPS or WLAN(11n 1T1R)	2*LAN(Default) +Dual SIM GPS, WLAN Optional	1*WAN + 4*LAN + single module/dual SIM, dual module/dual SIM
Product category	Single port router	Dual-port Wi-Fi router	Multi-port Wi-Fi router	Multi-functional Wi-Fi router

1.4 Typical Application Diagram

WLINK 4G/3G Router widely used in Telecom, economic, advertisement, traffic, environment protection business area.

For example, in economic area, R100 Series Router connect server by IPSec & GRE to ensure data security, tiny design makes it could installed into ATM machine. All these technology ensured safe and reliable data transmission, and minimize the probability of network disconnection, and maximize the usability of economic business like ATM, POS .etc.

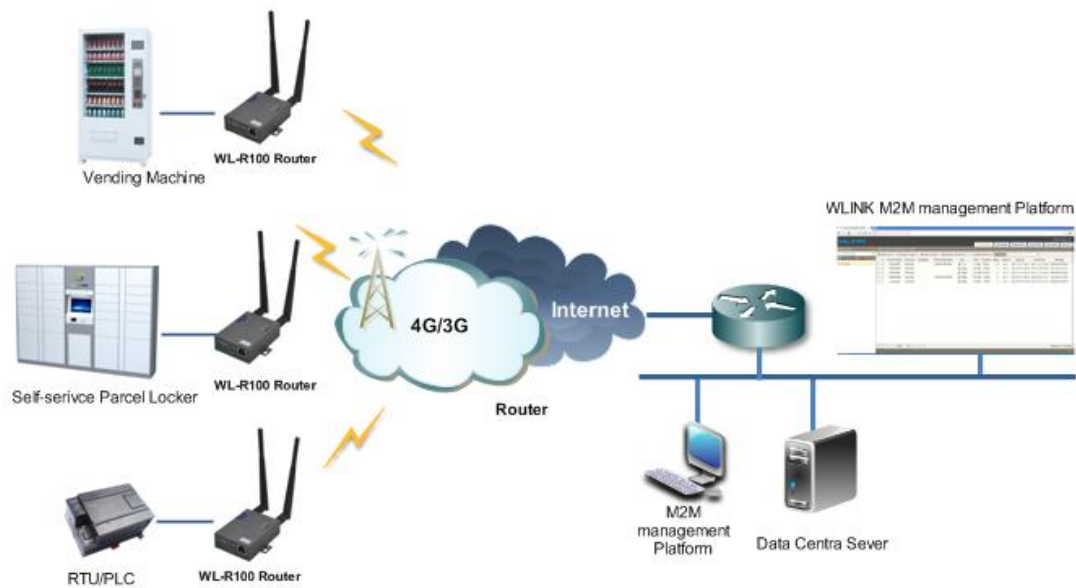


Figure 1-1 Network Topology

WLINK industrial router is based on mobile wireless public network or private network, build wireless data channel in mature network, to lower down the cost of wireless data transmission and technique.

1.5 Features


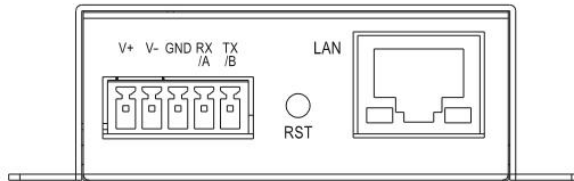
- Various cellular module optional, LTE/HSPA+/EVDO/CDMA2000 optional
- Support virtual data and private network (APN/VPDN)
- Optional support RS-232/RS-485 interface data transparent transmission and protocol conversion
- Support on-demand dialing, include timing on/off-line, voice or SMS control on/off-line, data trigger online or link idle offline
- Support TCP/IP protocol stack, support Telnet, HTTP, SNMP, PPP, PPPoE, etc., network protocol
- Support VPN Client (PPTP, L2TP), optional support Open VPN, IPSec, HTTPs, SSH, etc. advanced VPN function
- Provide friendly user interface, use normal web internet explorer to easily configure and manage, long-distance configure Telnet/SSH.
- Optional IPv6 protocol stack
- Optional support M2M terminal management platform
- WDT watchdog design, keep system stable
- Customization as customer's demand

2 Hardware Installation

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

2.1 Panel

Table 1-1 WL-R100 -Structure

WLINK Tech	WL-R100 series
Front	
Rear	



NOTE

There are some different for Antenna interface and indicator light for the expanded GPS series.

Table 2-1 Router Interface

Port	Instruction	Remark
USIM	Plug type SIM Slot, support 1.8/3V/5V automatic detection	
Main	4G/3G antenna, SMA connector, 50Ω	

Port	Instruction	Remark
Aux/GPS	4G Aux Antenna or GPS Antenna, SMA connector, 50Ω	Optional
LAN	10/100Base-TX, MDI/MDIX self-adaption,	
RST	Reset button,(press on button 5 seconds)	
PWR	Power connector	7.5 ~32V DC
COM	Three pins serial port, suitable for collection device with RS-232 or RS-485 interface, for wireless data transmission.	

2.2 LED Status

silk-screen	color	status	Indication
NET	Green		Strong Signal
	Orange		Normal Signal
	Red		Weak Signal
		Solid light	Connected 4G successfully
		Blinking quickly(0.5s)	Dialing
LAN	Green	Solid light	Connected
	Green	Blinking	Data Sending
	Green	Dark	Not connected
PWR	Green	Solid light	Router OS is running.

Table 2-2 Router LED indicator Status

2.3 Dimension

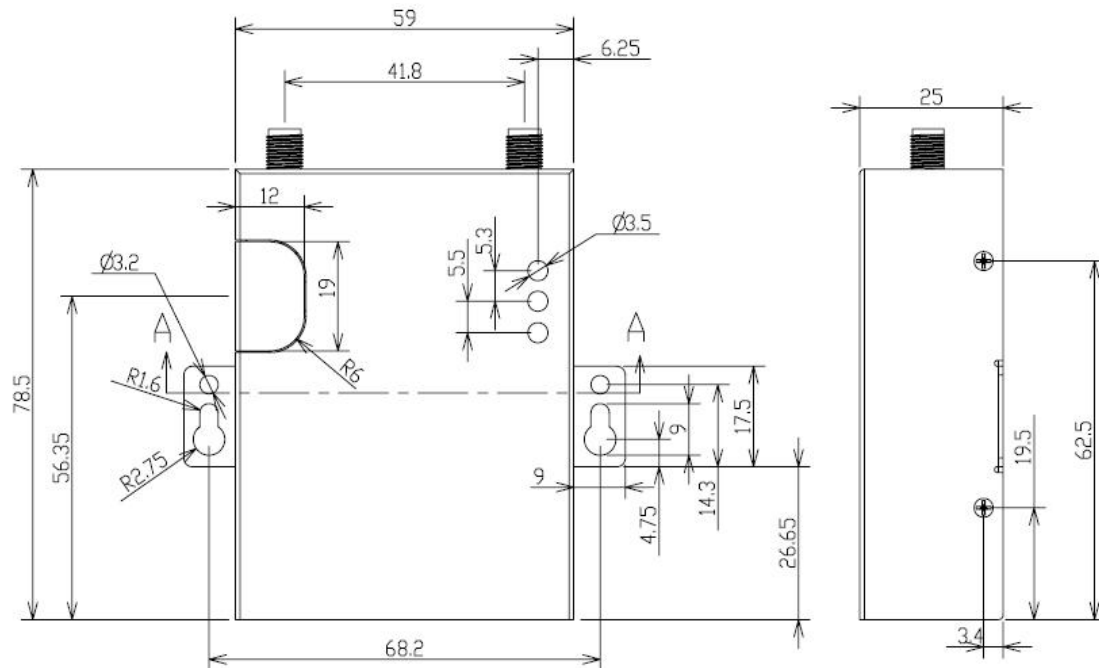


Figure 2-2 WL-R100 Series Router Dimension Figure

2.4 How to Install

2.4.1 SIM/UIM card install

If use dual SIM/UIM card router, you may need insert dual SIM before configure it. After installation, please follow below steps to connect the router.



Before connecting, please disconnect any power resource of router

2.4.2 Ethernet Cable Connection

Use the Ethernet cable to connect the cellular Router to computer directly, or transit by a switch.

2.4.3 Serial Port Connection

If you want to connect the router via serial port to laptop or other devices, you should prepare a serial port, this cable is optional. One end connect to computer serial port, the

other end connects the RX/TX and GND of the router



Before connecting, please disconnect any power resource of router

2.4.4 Power Supply

In order to get high reliability, WLINK Series Router adapt supports wide voltage input range: +7.5V~+32VDC, support hot plug and complex application environment.

2.4.5 Review

After insert the SIM/UIM card, connect Ethernet cable and necessary antenna, connect power cable.



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

Notice:

- Step 1 Check 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

This Chapter introduces the parameter configuration of the router, the router can be configured via IE, Firefox, or chrome.

3.1 Local Configure

The router supports to be configured by local Ethernet port, you could specify a static IP or DHCP get IP for your computer. The default IP address is 192.168.1.1, subnet mask is 255.255.255.0, please refer to followings:

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 3-3 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 3-4 User Identify Interface

----END

3.2 Basic Configuration



NOTE

Different software version has different web configuration interface, below take WL-R100 as example.

After access the WEB interface, you can check the current status of Router, or modify router configuration via web interface, below is the introduction for the common setting.

Status	Router
Overview	
LAN	
Device List	
Basic Network	
Advanced Network	
Firewall	
VPN Tunnel	
Administration	
Debugging	
Logout	

System Status	
Router Name	Router
Hardware Verion	
Firmware Version	Router-4.2.2.3
Router Time	Tue, 29 Mar 2016 20:40:06 +0800 Clock Sync.
Uptime	00:01:36
Total / Free Memory	60.08 MB / 53.55 MB (89.14%)

Internet Status	
Connection Type	Cellular Network
MAC Address	00:90:4C:06:50:2E
Modem IMEI	864881021779259
Modem Status	Ready
Cellular ISP	"CHN-UNICOM"
Cellular Network	"WCDMA"
USIM Status	Ready
CSQ	9
IP Address	10.232.200.48
Subnet Mask	255.255.255.255
Gateway	10.64.64.64
DNS	210.21.196.6:53, 221.5.88.88:53
Connection Status	Connected
Connection Uptime	00:00:45

Figure 3-5 Router Status GUI

3.2.1 Cellular Network Configure

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

Cellular Settings

Cellular Network Type: MU709S:WCDMA/HSPA+

ICMP Check: ☐

Cellular Traffic Check: ☐

Connect Mode: Keep Alive(Auto-Online) ▼

CIMI Send to: :

SMS Code:

PIN Code:

Operator Lock: ex:46001

Dial Number: *99#

Mode: Auto ▼

APN: 3GNET

User: CARD

Password: ****

Auth Type: Auto ▼

Local IP Address:

Save Cancel

Figure 3-1 Cellular Settings GUI

Table 3-1 Cellular Setting Parameter Instruction

Parameter	Instruction
ICMP check	To enable or disable ICMP check rules. Enable the ICMP check and setup a reachable IP address as destination IP. Once ICMP check failed, router will reconnect/reboot system as optional..
Cellular Traffic Check	There is Rx/Tx as options. Once no Rx/Tx data, router will router will reconnect/reboot system as options.
Connect Mode	<ul style="list-style-type: none"> Keep alive (Auto-online).The router will automatically connect 3G/4G network and keep online. Connect On Demand. Idle offline if no data from LAN to 3G/4G within defined time.

Parameter	Instruction
	<ul style="list-style-type: none"> ● Schedule, Define online and offline time. This function need to enable NTP function, ● Call/SMS Triggered. Call/SMS trigger router online. ● Manually. Connect 3G/4G network by manual.
CIMI Send	Send CIMI to defined IP and port by TCP protocol.
SMS Code	SMS identifying code. Router just identifies the unique code to implement SMS command.
PIN Code	Unlock the SIM PIN code.
Operator Lock	Lock operators via MCC/MNC
Service Code	The default service code as *99#.
APN	APN, provided by local ISP, usually CDMA/EVDO network do not need this parameter.
User	SIM card user name is provided by ISP
Password	SIM card password is provided by ISP
Auth Type	Support PAP/Chap/MS-Chap/MS-Chapv2
Local IP Add	Defined SIM IP from operator.



【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	<input type="text" value="8.8.8.8"/>
Check IP (Optional)	<input type="text" value="4.4.4.4"/>
Interval	<input type="text" value="60"/> (seconds)
Retries	<input type="text" value="3"/> (Times)
Fail Action	<input type="text" value="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

3.2.2 LAN Setting

Step 1 Single Click “ Basic Network>LAN” to enter below interface

Figure 3-2 LAN Setting GUI

Table 3-2 LAN Setting Instruction

Parameter	Instruction
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 Address Range	IP address range within LAN
Lease	The valid time

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

----End

3.2.3 Dynamic DNS Setting

Step 1 Single click “Basic Network->DDNS to enter the DDNS setting GUI.

Figure 3-3 Dynamic DNS Setting

Table 3-3 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

3.2.4 Routing Setting

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

Status

Basic Network

Cellular

LAN

DDNS

Routing

Advanced Network

Firewall

VPN Tunnel

Administration

Debugging

Logout

Router

Current Routing Table

Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
10.64.64.64	*	255.255.255.255	0	ppp0 (WAN)
192.168.1.0	*	255.255.255.0	0	br0 (LAN)
127.0.0.0	*	255.0.0.0	0	lo
default	10.64.64.64	0.0.0.0	0	ppp0 (WAN)

Static Routing Table

Destination	Gateway	Subnet Mask	Metric	Interface	Description
<input style="width: 100%;" type="text"/>				<div style="border: 1px solid #ccc; padding: 2px;">▼</div>	

Miscellaneous

Mode Gateway ▼

RIPv1 & v2 Disabled ▼

Efficient Multicast Forwarding ☐

DHCP Routes ☒

Spanning-Tree Protocol ☐

Figure 3-4 Routing Setting

Table 3-4 Routing Setting Instruction

Parameter	Instruction
Destination	Router can reach the destination IP address.
Gateway	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 gateway.
Description	Describe this routing name.

Step 2 Please Click “ Save “ to finish.

3.3 Advanced Network Setting

3.3.1 Port Forwarding

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

Status

Basic Network

Advanced Network

Port Forwarding

Port Redirecting

DMZ

Triggered

Serial App.

UPnP/NAT-PMP

Bandwidth Limiter

VRRP

Static DHCP

Firewall

VPN Tunnel

Administration

Debugging

Logout

PortForwarding

On	Proto	Src Address	Ext Ports	Int Port	Int Address	Description
	UDP		1000, 2000		192.168.1.2	ex: 1000 and 2000
	Both		1000-2000, 3000		192.168.1.2	ex: 1000 to 2000, and 3000
	Both	1.1.1.0/24	1000-2000		192.168.1.2	ex: 1000 to 2000, restricted
	TCP		1000	2000	192.168.1.2	ex: different internal port
<input checked="" type="checkbox"/>	TCP ▼					

- Src Address** (optional) - Forward only if from this address. ex: "1.2.3.4", "1.2.3.4 - 2.3.4.5", "1.2.3.0/24", "me.example.com".
- Ext Ports** - The ports to be forwarded, as seen from the WAN. ex: "2345", "200,300", "200-300,400".
- Int Port** (optional) - The destination port inside the LAN. If blank, the destination port is the same as *Ext Ports*. Only one port per entry is supported when forwarding to a different internal port..
- Int Address** -The destination address inside the LAN.

Figure 3-5 Port Forwarding GUI

Table 3-5 "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 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

----End

3.3.2 Port Redirecting

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

The screenshot shows the 'PortRedirecting' configuration page. On the left, a blue sidebar contains a menu with items like 'Status', 'Basic Network', 'Advanced Network', 'Port Forwarding', 'Port Redirecting' (selected), 'DMZ', 'Triggered', 'Serial App.', 'UPnP/NAT-PMP', 'Bandwidth Limiter', 'VRRP', 'Static DHCP', 'Firewall', 'VPN Tunnel', 'Administration', 'Debugging', and 'Logout'. The main content area has a title bar 'PortRedirecting' and a table with the following structure:

On	Proto	Int Port	Dst Address	Ext Port	Description
<input checked="" type="checkbox"/>	TCP				

Below the table is an 'Add' button. At the bottom right of the page are 'Save' and 'Cancel' buttons.

Figure 3-6 Port Forwarding GUI

Table 3-6 "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

----End

3.3.3 DMZ Setting

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

DMZ

Router

Enable DMZ ☐

Internal Address

Source Address Restriction

(optional; ex: "1.1.1.1", "1.1.1.0/24", "1.1.1.1 - 2.2.2.2" or "me.example.com")

Leave Remote Access ☒ (Redirect remote access ports for SSH and HTTP(s) to router)

Save Cancel

Figure 3-7 Port Redirecting GUI

Table 3-7 "DMZ" Instruction

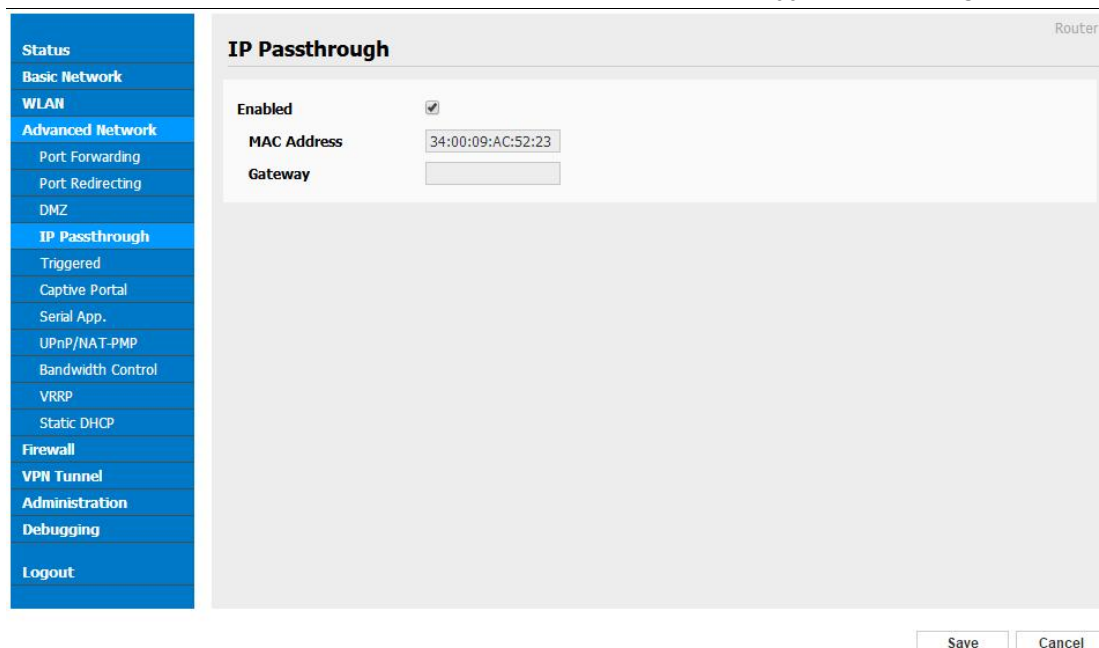
parameter	Instruction
Destination Address	The destination address inside the LAN.
Source Address Restriction	If no IP address inside, it will allow all IP address to access. If define IP address, it will just allow the defined IP address to access.
Leave Remote Access	

Step 2 Please click "save" to finish

----End

3.3.4 IP Passthrough Setting

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



IP Passthrough

Router

Enabled ☒

MAC Address 34:00:09:AC:52:23

Gateway

Save Cancel

Figure 3-8 IP Passthrough GUI

Table 3-8 “IP Passthrough” Instruction

	Instruction
Enable	Enable IP Passthrough
MAC Address	Enable DHCP of device. Configure device Mac. Device will be assigned SIM IP.
Gateway	If WL-R100 connect to multiple device, input other device gateway. The device might access to router GUI.

Step 2 Please click “save” to finish

----End

3.3.5 Triggered Setting

Step 1 Please click “Advanced Network> Triggered” to check or modify the relevant parameter.

Router

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

Add

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

Save Cancel

Figure 3-9 Triggered GUI

Table 3-9 "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

3.3.6 Serial App. Setting

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

Serial to TCP/IP

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)

Baud Rate: 115200

Parity Bit: none

Data Bit: 8

Stop Bit: 1

Save Cancel

Figure 3-10 Serial App Setting GUI

Table 3-10 “Serial App” Instruction

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



Serial port connection

PINs		DB9(male)
V+		
V-		
GND	----	5
RX	----	3
TX	----	2

Step 2 Please click "save" to finish.

---End

3.3.7 UPnp/NAT-PMP Setting

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

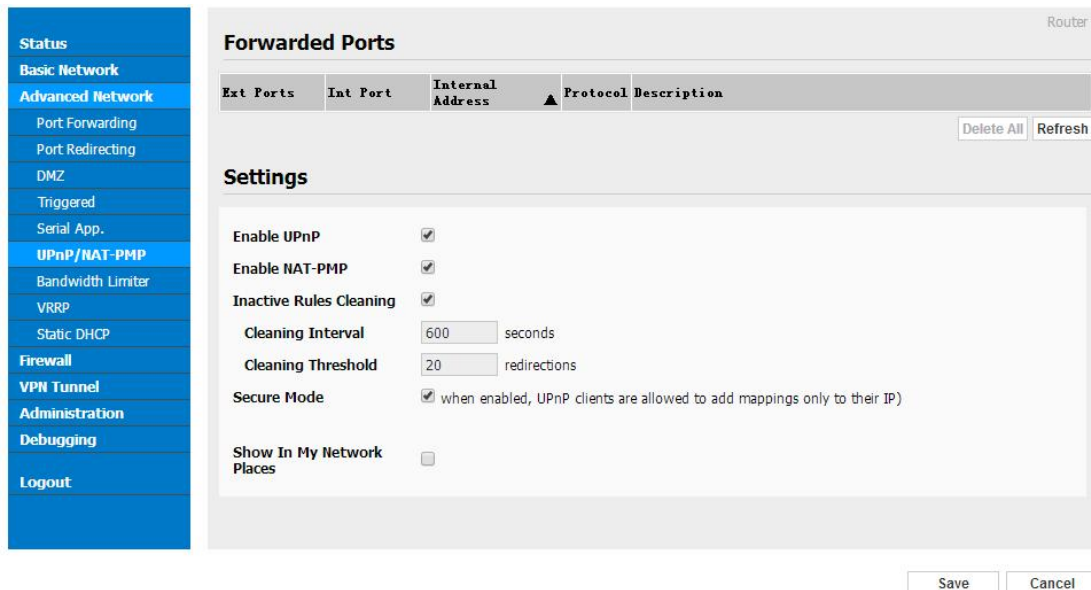


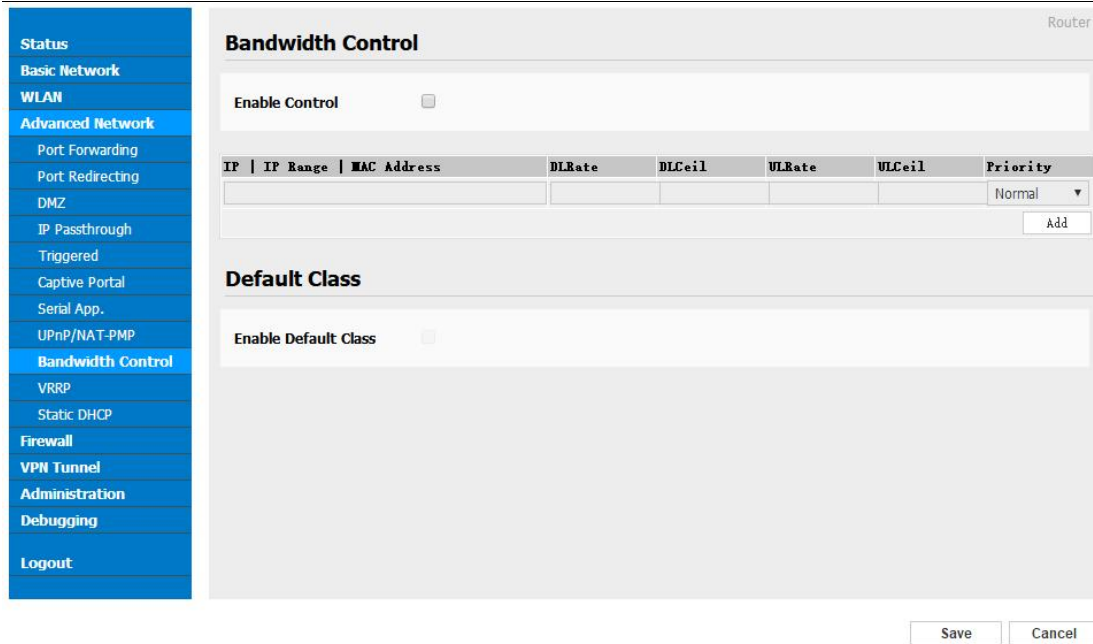
Figure 3-11 UPnp/NAT-PMP Setting GUI

Step 2 Please click "save" to finish.

---End

3.3.8 Bandwidth Control Setting

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



The screenshot shows the 'Bandwidth Control' configuration page. On the left is a blue sidebar menu with options: Status, Basic Network, WLAN, Advanced Network (highlighted), Port Forwarding, Port Redirecting, DMZ, IP Passthrough, Triggered, Captive Portal, Serial App., UPnP/NAT-PMP, Bandwidth Control, VRRP, Static DHCP, Firewall, VPN Tunnel, Administration, Debugging, and Logout. The main content area is titled 'Bandwidth Control' and includes an 'Enable Control' checkbox. Below it is a table with columns: IP, IP Range, MAC Address, DLRate, DLCeil, ULRate, ULCeil, and Priority. The Priority column has a dropdown menu set to 'Normal' and an 'Add' button. Below the table is a 'Default Class' section with an 'Enable Default Class' checkbox. At the bottom right are 'Save' and 'Cancel' buttons.

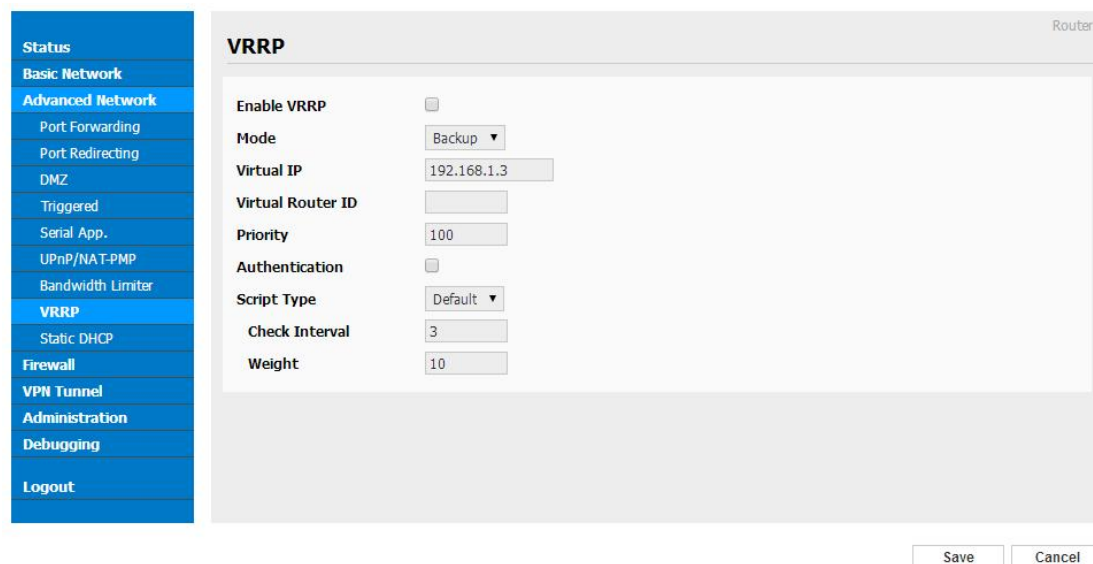
Figure 3-12 Bandwidth Control Setting GUI

Step 2 Please click "save" to finish.

---End

3.3.9 VRRP Setting

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



The screenshot shows the 'VRRP' configuration page. The left sidebar menu is the same as in Figure 3-12, with 'VRRP' highlighted. The main content area is titled 'VRRP' and includes an 'Enable VRRP' checkbox. Below it are several settings: 'Mode' (Backup), 'Virtual IP' (192.168.1.3), 'Virtual Router ID' (empty), 'Priority' (100), 'Authentication' (checkbox), 'Script Type' (Default), 'Check Interval' (3), and 'Weight' (10). At the bottom right are 'Save' and 'Cancel' buttons.

Figure 3-13 VRRP Setting GUI

Step 2 Please click "save" to finish.

---End

3.3.10 Static DHCP Setting

Step 1 Please click “Advanced Network> Static DHCP” to check or modify the relevant parameter.

MAC Address	IP Address	Hostname	Description
00:00:00:00:00:00	192.168.1.2		
00:00:00:00:00:00			

Figure 3-14 Static DHCP Setting GUI

Step 2 Please click “save” to finish.

---End

3.4 Firewall

3.4.1 IP/URL Filtering

Step 1 Please click “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

Debugging

Logout

Router

IP/MAC/Port Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
<input checked="" type="checkbox"/>				NONE ▼			Acce ▼	
<input type="button" value="Add"/>								

Key Word Filtering

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

URL Filtering

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

Access Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
<input checked="" type="checkbox"/>				NONE ▼			Acce ▼	
<input type="button" value="Add"/>								

Table 3-11 "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.

Step 2 Please click "save" to finish.

---End

3.4.2 Domain Filtering

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

Figure 3-15 Domain Filtering Setting GUI

Table 3-12 “GRE” 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

3.5 VPN Tunnel

3.5.1 GRE Setting

Step 1 Please click “VPN Tunnel> GRE” to check or modify the relevant parameter.

Figure 3-16 GRE Setting GUI

Table 3-13 “GRE” Instruction

	Instruction
IDE	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 2 Please click "save" to finish.

----End

3.5.2 OpenVPN Client Setting

Step 1 Please click “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 like Status, Basic Network, WLAN, Advanced Network, Firewall, VPN Tunnel, GRE, OpenVPN Client (highlighted), PPTP/L2TP Client, IPSec, Administration, Debugging, and Logout. The main panel is titled 'OpenVPN Client' and features tabs for 'Client 1', 'Client 2', 'Basic', 'Advanced', 'Keys', and 'Status'. The 'Basic' tab is selected, showing various configuration options: 'Start with WAN' (unchecked), 'Interface Type' (TUN), 'Protocol' (UDP), 'Server Address/Port' (a text field containing '1194'), 'Firewall' (Automatic), 'Authorization Mode' (TLS), 'Username/Password Authentication' (unchecked), 'HMAC authorization' (Disabled), and 'Create NAT on tunnel' (checked). A 'Start Now' button is located at the bottom left of the configuration area. At the bottom right of the entire window, there are 'Save' and 'Cancel' buttons.

Figure 3-17 OpenVPN Setting GUI

Table 3-14 "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.
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.

Parameter	Instruction
Poll Interval	Openvpn client check router's status as interval time.
Redirect Internet Traffic	Configure Openvpn as default routing.

Parameter	Instruction
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.

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

Status

Basic Network

WLAN

Advanced Network

Firewall

VPN Tunnel

GRE

OpenVPN Client

PPTP/L2TP Client

IPSec

Administration

Debugging

Logout

Router

OpenVPN Client

Client 1
Client 2

Basic
Advanced
Keys
Status

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.

Step 2 Please click "save" to finish.

----End

3.5.3 VPN Client Setting

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

Status

Basic Network

WLAN

Advanced Network

Firewall

VPN Tunnel

GRE

OpenVPN Client

PPTP/L2TP Client

IPSec

Administration

Debugging

Logout

Router

L2TP/PPTP Basic

On	Protocol	Name	Server	Username	Password	Firewall	Default Route	Local IP
<input checked="" type="checkbox"/>	L2TP					<input type="checkbox"/>	<input type="checkbox"/>	

[Add](#)

L2TP Advanced

On	Name	Accept DNS	MTU	MRU	Tunnel Auth	Tunnel Password	Custom Options
<input checked="" type="checkbox"/>		NO			<input type="checkbox"/>		

[Add](#)

PPTP Advanced

On	Name	Accept DNS	MTU	MRU	MPPE	MPPE Stateful	Custom Options
<input checked="" type="checkbox"/>		NO			<input type="checkbox"/>	<input type="checkbox"/>	

[Add](#)

SCHEDULE

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

[Add](#)

Save
Cancel

Table 3-15 "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 3-16 "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 3-17 "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 3-18 "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.

---End

3.5.4 IPSec Setting

3.5.3.1 IPsec Group Setup

Step 1 Please click "IPsec> Group Setup" to check or modify the relevant parameter.

Table 3-1 “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
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.

3.5.3.2 IPSec Basic Setup

Step 1 Please click “IPSec >Basic Setup ” to check or modify the relevant parameter.

Table 3-2 “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
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.

3.5.3.3 IPSec Advanced Setup

Step 1 Please click “IPSec >Advanced Setup ” to check or modify the relevant parameter.

Table 3-3 “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.

----End

3.6 Administration

3.6.1 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.

The screenshot displays the 'Router Identification' configuration page. On the left is a vertical menu with various system settings. The main content area has a title bar 'Router Identification' and a sub-header 'Router'. Below this, there are three text input fields: 'Router Name' with the value 'Router', 'Hostname' with the value 'Router', and 'Domain Name' which is empty. At the bottom right of the main area, there are two buttons labeled 'Save' and 'Cancel'.

Figure 3-1 Router Identification GUI

Table 3-1 “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

3.6.2 Time Setting

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

Figure 3-1 System Configuration GUI



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

Step 2 Please click “save to finish.

----End

3.6.3 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.

The screenshot shows the 'WebAccess' configuration page. On the left is a blue sidebar menu with options: Status, Basic Network, Advanced Network, Firewall, VPN Tunnel, Administration, Identification, Time, Admin Access (highlighted), Scheduler Reboot, SNMP, M2M Settings, Configuration, Logging, Upgrade, Reboot..., Debugging, and Logout. The main content area has a title bar 'WebAccess' with a 'Router' label on the right. Below the title bar, the 'Local Access' section includes a dropdown for 'Local Access' set to 'HTTP', a text field for 'HTTP Access Port' with '80', a dropdown for 'Remote Access' set to 'Disabled', and a checked checkbox for 'Allow Wireless Access'. The 'Open Menus' section lists seven menu items, each with an unchecked checkbox: Status, Basic Network, Firewall, VPN Tunnel, Advanced Network, Administration, and Debugging. The 'Password' section at the bottom has two password input fields, the first labeled 'Password' and the second labeled '(re-enter to confirm)', both showing masked characters.

Figure 3-1 Admin Setting GUI

Step 2 Please click save icon to finish the setting

----End

3.6.4 Schedule Reboot Setting

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

The screenshot displays the 'Scheduler Reboot' configuration page. On the left, a blue sidebar menu lists various system functions, with 'Scheduler Reboot' currently selected. The main content area has a light gray background and is titled 'Scheduler Reboot'. It includes three primary settings: an 'Enabled' checkbox, a 'Time' dropdown menu showing '1:00 AM', and a 'Days' section with checkboxes for each day of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat) and an 'Everyday' option. All checkboxes are currently checked. At the bottom right of the main area, there are two buttons: 'Save' and 'Cancel'.

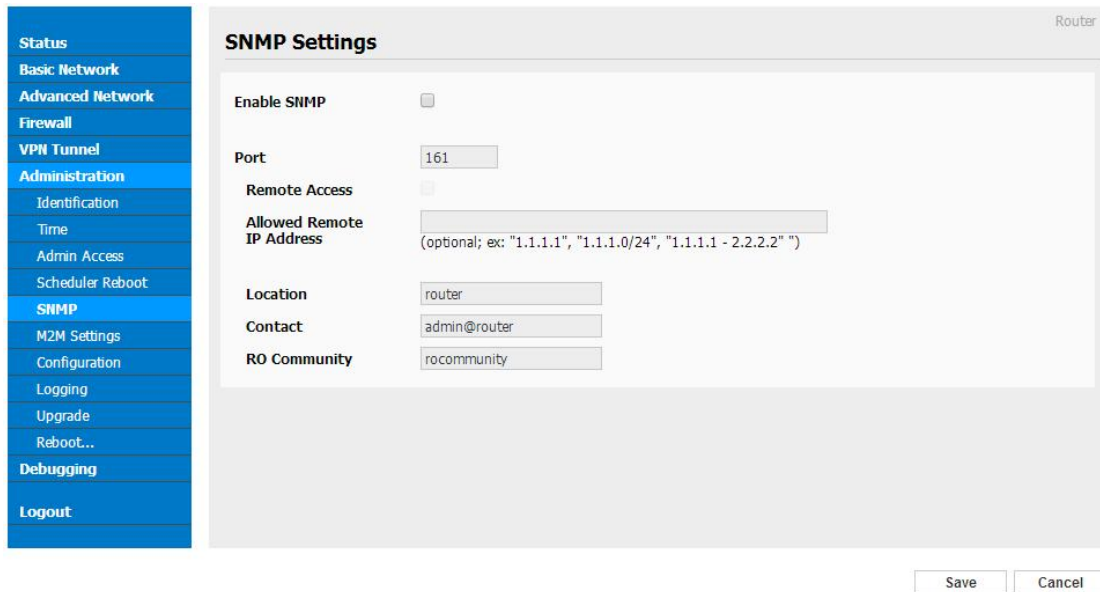
Figure 3-1 Scheduler Reboot Setting GUI

Step 2 Please click save iron to finish the setting

----End

3.6.5 SNMP Setting

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



The image shows the 'SNMP Settings' configuration page in the router's web interface. On the left is a blue sidebar menu with options: Status, Basic Network, Advanced Network, Firewall, VPN Tunnel, Administration (highlighted), Identification, Time, Admin Access, Scheduler Reboot, SNMP (highlighted), M2M Settings, Configuration, Logging, Upgrade, Reboot..., Debugging, and Logout. The main content area is titled 'SNMP Settings' and contains the following fields: 'Enable SNMP' (checkbox, unchecked), 'Port' (text box with '161'), 'Remote Access' (checkbox, unchecked), 'Allowed Remote IP Address' (text box with '(optional; ex: "1.1.1.1", "1.1.1.0/24", "1.1.1.1 - 2.2.2.2")'), 'Location' (text box with 'router'), 'Contact' (text box with 'admin@router'), and 'RO Community' (text box with 'rocommunity'). At the bottom right of the main area are 'Save' and 'Cancel' buttons.

Figure 3-1 SNMP Setting GUI

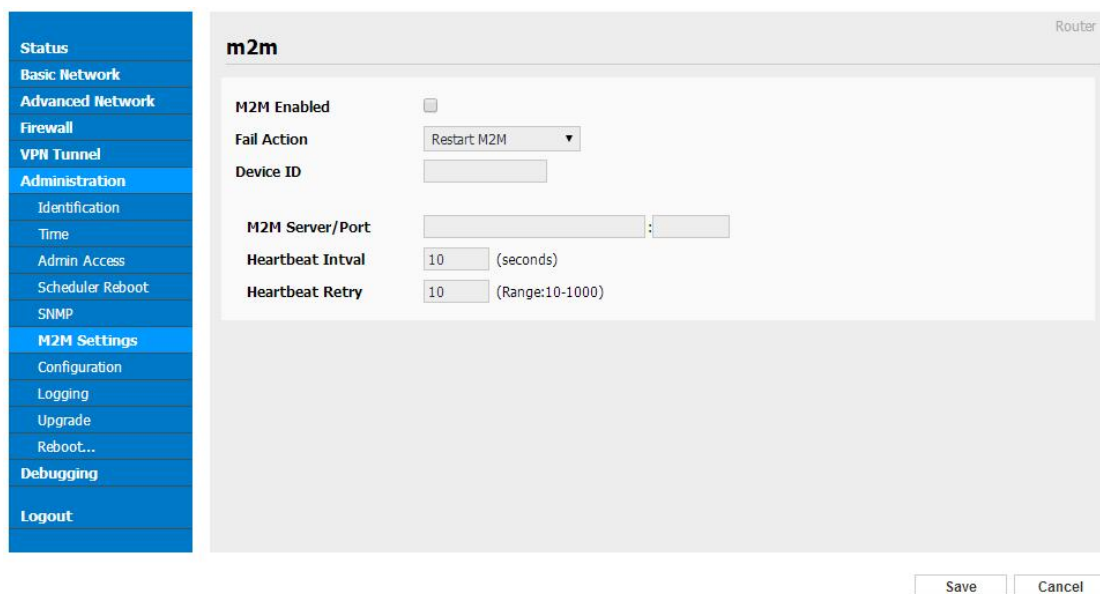
Step 2 Please click save iron to finish the setting

----End

3.6.6 M2M Access Setting

(Apply to M2M management platform installation application only)

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



The image shows the 'm2m' configuration page in the router's web interface. The left sidebar menu is the same as in the previous figure, but 'M2M Settings' is highlighted. The main content area is titled 'm2m' and contains the following fields: 'M2M Enabled' (checkbox, unchecked), 'Fail Action' (dropdown menu showing 'Restart M2M'), 'Device ID' (text box), 'M2M Server/Port' (text box with a port separator), 'Heartbeat Intval' (text box with '10' and '(seconds)'), and 'Heartbeat Retry' (text box with '10' and '(Range:10-1000)'). At the bottom right of the main area are 'Save' and 'Cancel' buttons.

Figure 3-1 M2M Access Setting GUI

Step 2 Please click save iron to finish the setting

----End

3.6.7 Configuration Setting

Step 1 Please click “ Administration> Configuration ” to do the backup setting

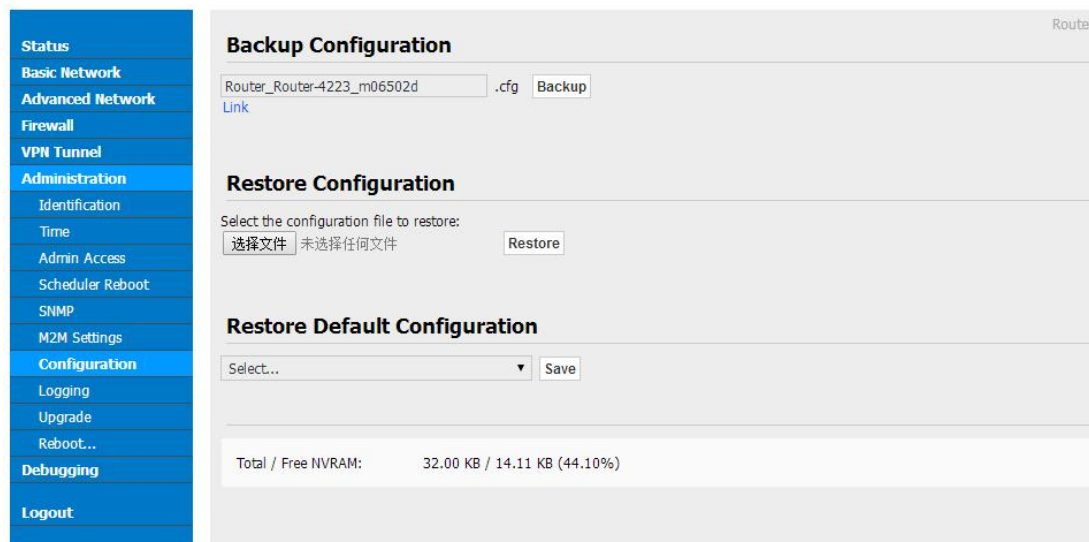


Figure 3-1 Backup and Restore Configuration GUI



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

Step 2 After setting the backup and restore configuration. The system will reboot automatically.

----End

3.6.8 Logging Setting

Step 1 Please click “Administrator> Logging” to start the configuration, you can set the file path to save the log (Local or remote sever).

The screenshot displays the 'Syslog' configuration interface. On the left, a vertical menu lists various system functions, with 'Logging' selected under the 'Administration' category. The main configuration area includes the following options:

- Log Internally:** A checked checkbox.
- Log To Remote System:** An unchecked checkbox.
- Generate Marker:** A dropdown menu currently set to 'Every 1 Hour'.
- Limit:** A text input field containing '60', with a note '(messages per minute / 0 for unlimited)'.

At the bottom right of the configuration area, there are two buttons: 'Save' and 'Cancel'.

Figure 3-1 System log Setting GUI

Step 2 After configure, please click “Save” to finish.

----End

3.6.9 Firmware upgrade

Step 1 Please click “Administrator>firmware upgrade” to open upgrade firmware tab.



Figure 3-1 Firmware Upgrade GUI



NOTE

When upgrading, please don't cut off the power.

3.6.10 System Reboot

Step 2 Please click “Administrator>Reboot” to restart the router. System will popup dialog to remind “Yes” or “NO” before the next step.

Step 3 If choose “yes”, the system will restart, all relevant update configuration will be effective after reboot.

----End

3.7 Debugging Setting

3.7.1 Logs Setting

Step 1 Please click “Debugging>Logs” to check and modify relevant parameter.

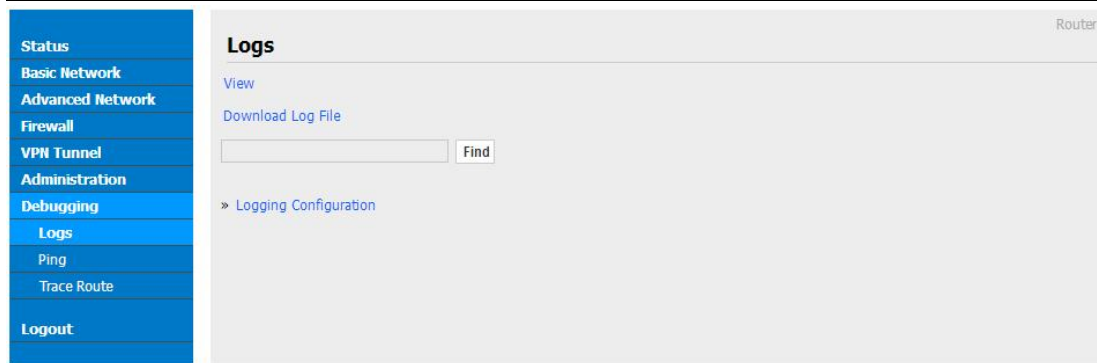


Figure 3-1 Logs GUI

Step 2 After configure, please click “Save” to finish.

----End

3.7.2 Ping Setting

Step 1 Please click “Debugging>Logs” to check and modify relevant parameter.



Figure 3-1 Ping GUI

Step 2 After configure, please click “Save” to finish.

----End

3.7.3 Trace Setting

Step 1 Please click “Debugging>Trace” to check and modify relevant parameter.

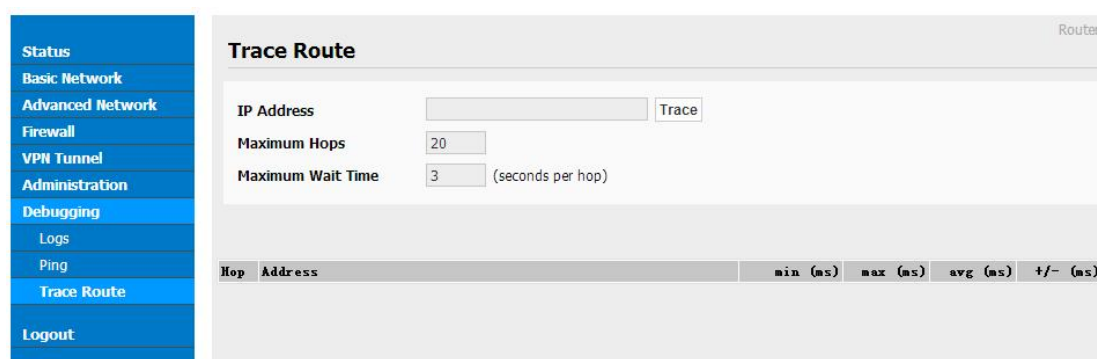


Figure 3-1 Trace GUI

Step 2 After configure, please click “Save” to finish.

----End

3.8 “RST” Button for Restore Factory Setting

If you couldn't enter web interface for other reasons, you can also use this way.
For R100 Series, “RST” button is on the left of Ethernet port, for R100 Series, the button is on the left of NET light. 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 restored to factory.

Table 3-1 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



NOTE

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 Port Forwarding

1) The router online and got a public IP address 14.27.85.41

Note: It's based on SIM card carrier

2) The PC is connected to router and got IP address 192.168.1.36

3) Configuration

4) The PC can be accessed via 14.27.85.41:443 over Internet

4.2 IP Passthrough

1) The router online

System Status

Router Name	Router
Hardware Version	
Firmware Version	Router-4.3.4.4
Router Time	Thu, 24 Jan 2019 14:48:02 +0800 Clock Sync.
Uptime	00:02:24
Total / Free Memory	60.05 MB / 48.04 MB (79.99%)

Internet Status

Connection Type	Cellular Network
Modem Type	EC25/LTE/WCDMA
Modem IMEI	861107038587730
Modem Status	Ready
Cellular ISP	"CHN-UNICOM"
Cellular Network	LTE
USIM Selected	USIM Card 1 Running...
USIM Status	Ready
CSQ	21
IP Address	10.80.50.191
Subnet Mask	255.255.255.128
Gateway	10.80.50.192
DNS	120.80.80.80:53, 221.5.88.88:53
Connection Status	Connected
Connection Uptime	00:00:00

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

IP Passthrough

Enabled ☒

MAC Address: 50:7B:9D:C3:9A:22

Gateway:

Ethernet Status

General

Connection: Internet

IPv4 Connectivity: Internet

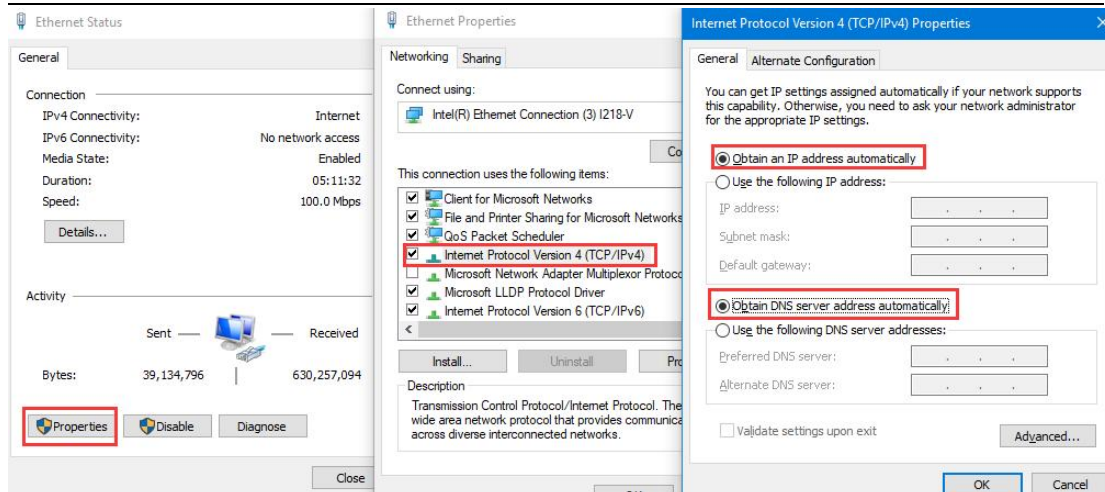
IPv6 Connectivity: No network access

Network Connection Details

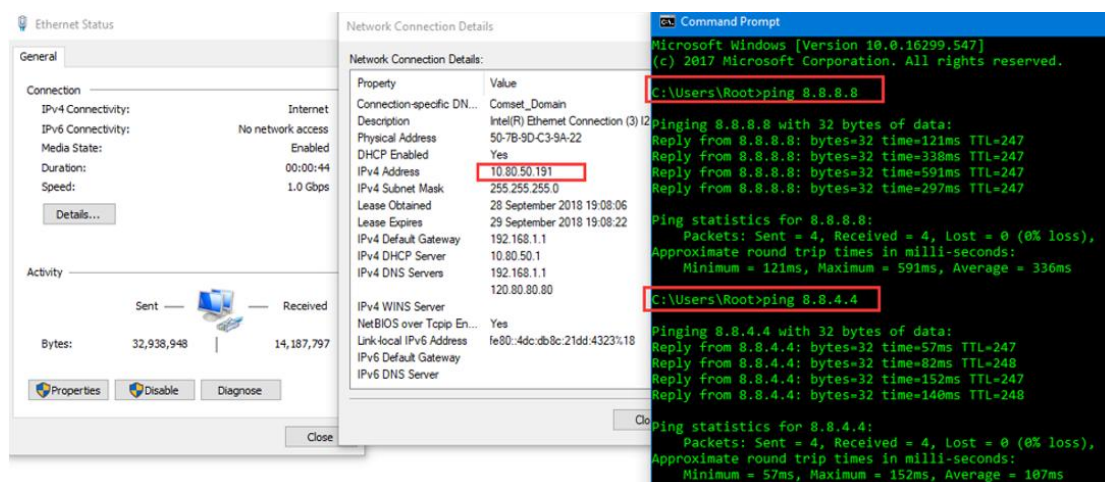
Property	Value
Connection-specific DN...	
Description	Intel(R) Ethernet Connection (3) I218-V
Physical Address	50-7B-9D-C3-9A-22
DHCP Enabled	No
IPv4 Address	192.168.10.110
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	192.168.10.1
IPv4 DNS Server	192.168.10.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	No
Link-local IPv6 Address	fe80::69ca:9764:1fe1:cbb1%20
IPv6 Default Gateway	
IPv6 DNS Server	

Save Cancel

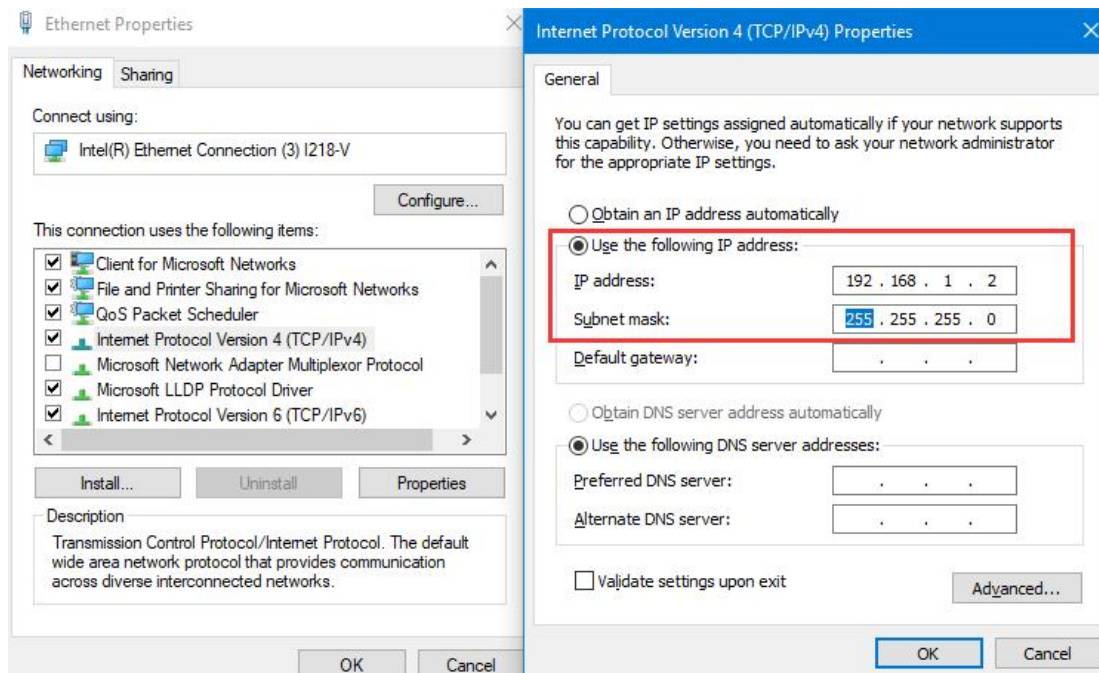
3) Set the PC to DHCP



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



4.3 GPS Settings

Step 1 Please click "Advanced Network> GPS" to view or modify the relevant parameter.

Figure 4-5 GPS GUI

Table 4-5 “GPS” Instruction

	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

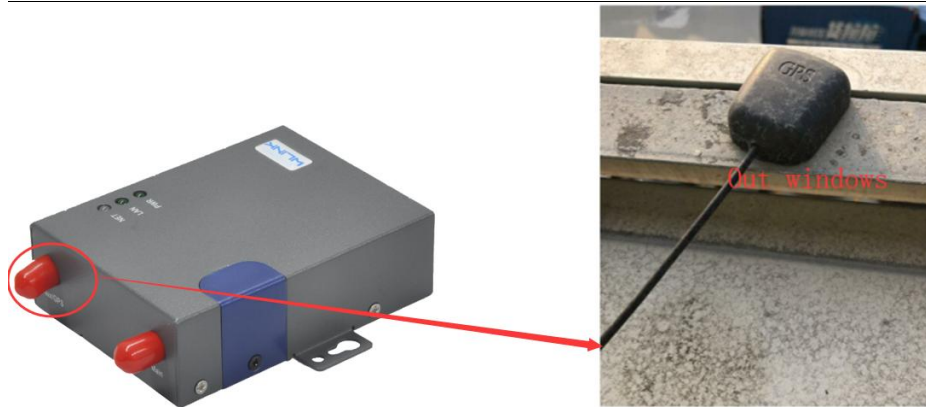
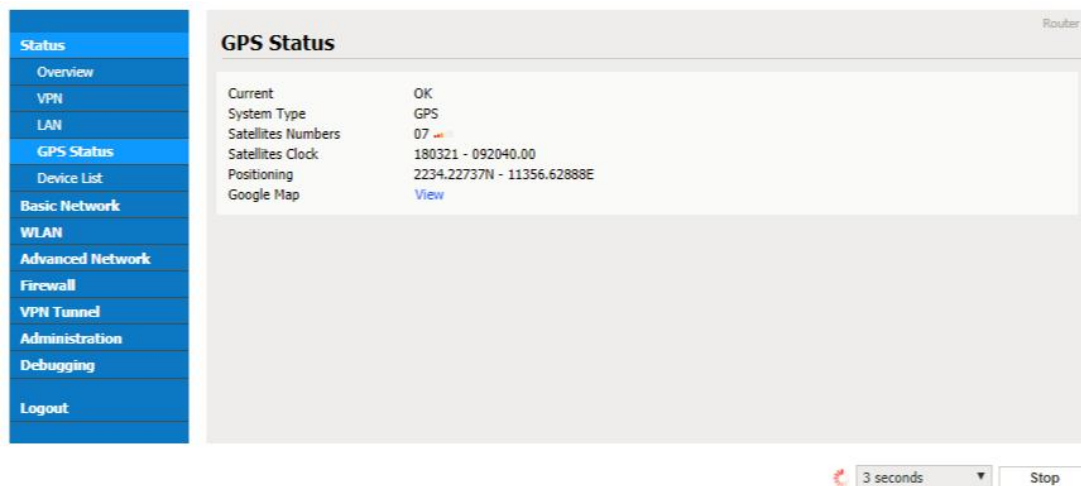


Figure 4-5 GPS Connection

Step 3 Check GPS Status



NOTE

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 over ground, units is km/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.

4.4 Firewall

Note: The WL-R100 same as WL-R100 on the firewall, but WL-R100 not support WIFI



Figure 4-6 Firewall Network topology

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)

2) Key Word Filtering

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

3) URL Filtering

This part used to filter URL from router's WAN/Celluar 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.

Status

Basic Network

WLAN

Advanced Network

Firewall

IP/URL Filtering

Domain Filtering

VPN Tunnel

Administration

Debugging

Logout

Router

IP/MAC/Port Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
On	-	any/0	any/0	-	-	-	Drop	
On	-	any/0	192.168.1.0/24	-	-	-	Accept	
On	50:7B:9D:C3:9A:22	any/0	any/0	-	-	-	Accept	
On	60:F1:89:20:F0:9A	any/0	any/0	-	-	-	Accept	
On	00:1E:64:DF:E8:46	any/0	any/0	-	-	-	Accept	
<input checked="" type="checkbox"/>				NONE ▼			Acc ▼	

[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

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
On	-	any/0	any/0	TCP	-	-	Drop	
On	00:1E:64:DF:E8:46	any/0	any/0	TCP	-	-	Accept	
On	60:F1:89:20:F0:9A	any/0	any/0	TCP	-	-	Accept	

4.5 VPN Tunnel

4.5.1 GRE

GRE Tunnel between WL-R100 and WL-R520

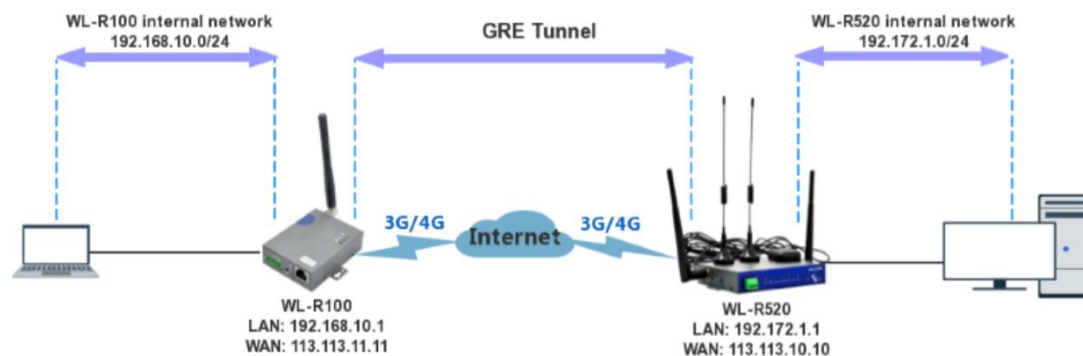


Figure 4-7-1 GRE Network topology

1) WL-R100 Config

1.1) Navigate to **Basic Network > LAN**

Status

Basic Network

WAN

Cellular

LAN

DDNS

Routing

WLAN

Advanced Network

Firewall

VPN Tunnel

Administration

Debugging

Logout

Router

LAN

Router IP Address 192.168.10.1

Subnet Mask 255.255.255.0

DHCP Server ☒

IP Pool 192.168.10.2 - 192.168.10.53 (52)

Lease 1440 (minutes)

Use internal DNS ☒

1.2) Navigate to VPN Tunnel > GRE

Status

Basic Network

WLAN

Advanced Network

Firewall

VPN Tunnel

GRE

OpenVPN Client

PPTP/L2TP Client

IPSec

Administration

Debugging

Logout

Router

GRE Tunnel

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

GRE Route

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

2) WL-520 Config

2.1) Navigate to Basic Network > LAN

Status

Basic Network

WAN

Cellular

LAN

DDNS

Routing

WLAN

Advanced Network

Firewall

VPN Tunnel

Administration

Debugging

Logout

Router

LAN

Router IP Address 1 192.172.1.1

Subnet Mask 1 255.255.255.0

Router IP Address 2 0.0.0.0

Subnet Mask 2 0.0.0.0

Router IP Address 3 0.0.0.0

Subnet Mask 3 0.0.0.0

Router IP Address 4 0.0.0.0

Subnet Mask 4 0.0.0.0

DHCP Server ☒

IP Pool 192.172.1.2 - 192.172.1.51 (50)

Lease 1440 (minutes)

Use internal DNS ☒

2.2) Navigate to VPN Tunnel > GRE

Status

Basic Network

WLAN

Advanced Network

Firewall

VPN Tunnel

GRE

OpenVPN Client

PPTP/L2TP Client

IPSec

Administration

Debugging

Logout

GRE Tunnel

On	IDX	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Description
On	1	192.172.1.10	113.111.10.101	113.113.11.11	On	10	5	test

☒ ☐

Add

GRE Route

On	Tunnel Index	Destination Address	Description
On	1	192.168.10.0/24	test

☒ ☐

Add

Save Cancel

4.5.2 OpenVPN

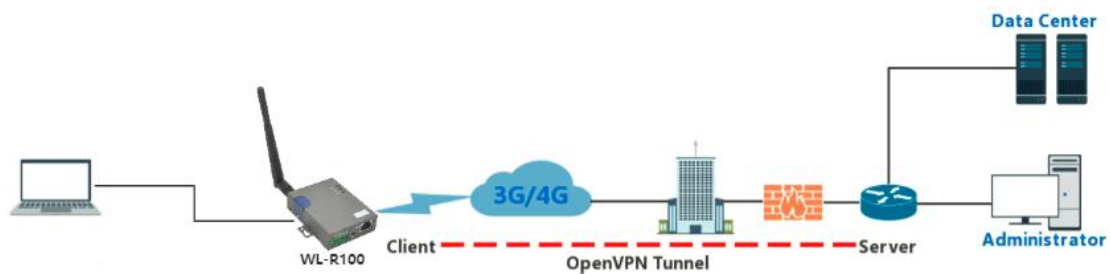


Figure 4-7-2 OpenVPN Network topology

Configured test case: OpenVPN between WL-R100 client and Server

Step 1 Please click “VPN Tunnel> OpenVPN Client” to check or modify the relevant parameter.

Basic

Status

Basic Network

WLAN

Advanced Network

Firewall

VPN Tunnel

GRE

OpenVPN Client

PPTP/L2TP Client

IPSec

Administration

Debugging

Logout

OpenVPN Client

Client 1

Client 2

Keys

Status

Basic

Start with WAN ☒

Interface Type TUN

Protocol UDP

Server Address/Port 1194

Firewall Automatic

Authorization Mode TLS

Username/Password Authentication ☐

HMAC authorization Disabled

Create NAT on tunnel ☐ Routes must be configured manually.

Start Now

Save Cancel

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.

Advanced

Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Client
PPTP/L2TP Client
IPSec
Administration
Debugging
Logout

OpenVPN Client

Client 1 Client 2

Basic Advanced Keys Status

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

Save Cancel

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.

Keys

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

Status









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.

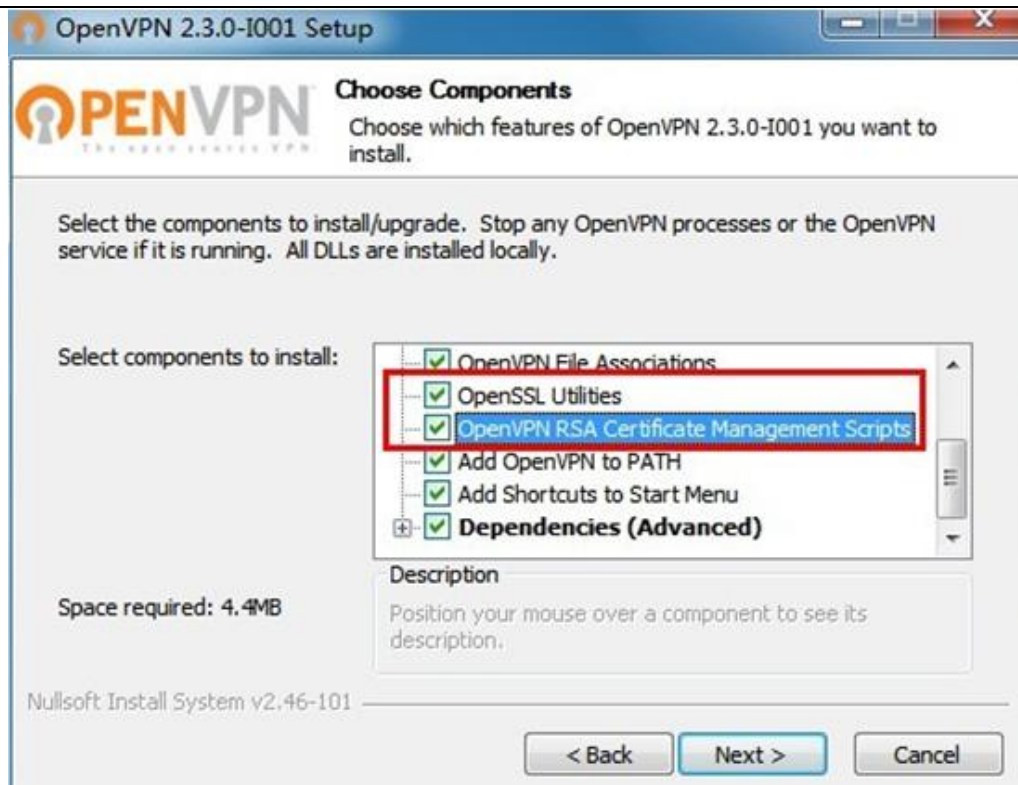
OpenVPN Keys Guide

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

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

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	

2) 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

3) 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

4) You may configure the client keys to WLINK OpenVPN client GUI when you create the server and client certificate in the path OpenVPN/easy-rsa/keys

4.1) 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

4.1) OpenVPN>easy-rsa>keys

The screenshot shows the WLINK OpenVPN Client GUI with the 'Keys' tab selected. On the left, a file explorer shows the contents of the 'OpenVPN > easy-rsa > keys' directory. Three arrows indicate the mapping of files to the GUI fields:

- Red arrow:** Points from `ca.crt` in the file explorer to the **Certificate Authority** field in the GUI.
- Orange arrow:** Points from `client.crt` in the file explorer to the **Client Certificate** field in the GUI.
- Green arrow:** Points from `client.key` in the file explorer to the **Client Key** field in the GUI.

The GUI also displays a 'Status' section on the left and a 'Start Now' button at the bottom.

5) You may do the ping test to your server when the tunnel is established

The screenshot shows the 'OpenVPN Client' status page on a router. The 'Status' tab is selected, showing 'Client 1' is connected. A 'General Statistics' table is displayed, showing various metrics like TUN/TAP read/write bytes, TCP/UDP read/write bytes, and authentication statistics. Overlaid on the right is a terminal window showing a series of ping commands to 192.168.1.1, all successful with 64 bytes and a TTL of 126.

Name	Value
TUN/TAP read bytes	0
TUN/TAP write bytes	87508
TCP/UDP read bytes	106186
TCP/UDP write bytes	3599
Auth read bytes	87636
pre-compress bytes	0
post-compress bytes	0
pre-decompress bytes	16638
post-decompress bytes	19330

4.5.3 L2TP/PPTP

Step 1 Please click "VPN Tunnel>PPTP/L2TP Client" to view or modify the relevant parameter.

The screenshot shows the 'L2TP/PPTP Basic' configuration page. The 'Basic' tab is selected, showing a table of configured clients. The 'L2TP' checkbox is checked. Below this, the 'L2TP Advanced' and 'PPTP Advanced' tabs are visible. The 'PPTP Advanced' tab is selected, showing a table of configured clients. The 'Schedule' tab is also visible at the bottom.

On	Protocol	Name	Server	Username	Password	Firewall	Default Route	Local IP
On	PPTP	3	wlinktech.com.cn	test123	test123	On		

On	Name	Accept DNS	MTU	MRU	MPPE	MPPE Stateful	Custom Options
On	3	NO	1440	1440	On		debug,noipdefault,require-mppe-128

On	Name 1	Name 2	Policy	Description
On			FAILOVER	

Note: The Custom Options based on your server

Configured test case: L2TP

Status

Basic Network

WLAN

Advanced Network

Firewall

VPN Tunnel

GRE

OpenVPN Client

PPTP/L2TP Client

IPSec

Administration

Debugging

Logout

L2TP/PPTP Basic

On	Protocol	Name	Server	Username	Password	Firewall	Default Route	Local IP
On	L2TP	2	wlinktech.com.cn	test123	test123	On		
<input checked="" type="checkbox"/>	L2TP					<input type="checkbox"/>	<input type="checkbox"/>	

Add

L2TP Advanced

On	Name	Accept DNS	MTU	MRU	Tunnel Auth	Tunnel Password	Custom Options
On	2	NO	1440	1440	On		debug
<input checked="" type="checkbox"/>		NO			<input type="checkbox"/>		

Add

PPTP Advanced

On	Name	Accept DNS	MTU	MRU	MPPE	MPPE Stateful	Custom Options
<input checked="" type="checkbox"/>		NO			<input type="checkbox"/>	<input type="checkbox"/>	

Add

SCHEDULE

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

Add

Save
Cancel

Note: The Custom Options based on your server

Step 2 Please click "Save" icon

VPN Status

Status

Overview

VPN

LAN

Device List

Basic Network

Advanced Network

Firewall

VPN Tunnel

Administration

Debugging

Logout

VPN Status

VPN Name	1
VPN Protocol	L2TP
Local IP	172.1.1.18
Peer IP	172.1.1.1

4.5.4 IPSec

IPSec between WLINK and Cisco Router

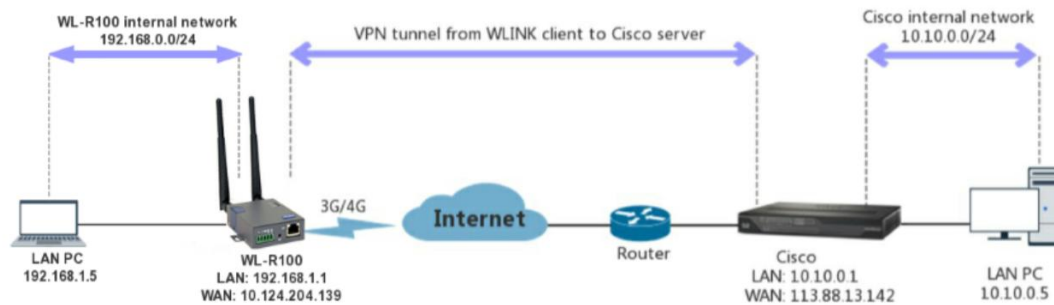


Figure 4-7-4 IPSec Network topology

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

2.1) Navigate to VPN Tunnel > IPSec > Group Setup

Status

Basic Network

WLAN

Advanced Network

Firewall

VPN Tunnel

GRE

OpenVPN Client

PPTP/L2TP Client

IPSec

Administration

Debugging

Logout

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

2.2) Navigate to VPN Tunnel > IPsec > Basic Setup

2.3) Navigate to VPN Tunnel > IPsec > Advanced Setup

2.4) Status

VPN Status	
IPSec 1	Enable
Phase 1 Status	73 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.	420 Bytes
IPSec Send.	680 Bytes

--End