

# 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 $\sim$ 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
1.1 Product overview4
1.2 Model introduction4
1.3 Product Appearance
1.4 Typical Application Diagram
1.5 Features6
2 Hardware Installation
2.1 Panel
2.2 LED Status
2.3 Dimension
2.4 How to Install
3 Router Configuration
3.1 Local Configure
3.2 Basic Configuration12
3.3 Advanced Network Setting17
3.4 Firewall
3.5 VPN Tunnel
3.6 Administration
3.7 Debugging Setting45



	3.8 "RST" Button for Restore Factory Setting	48
4 C	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

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.

#### Shenzhen Wlink Technology Co., LTD 深圳市徳传物联技术有限公司

#### **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 2100/1900/850/900MHzz	1xLAN 1xRS-232	No	Yes	100M	50M
WL-R100H	1	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	1	HSPA+ 900/2100 or 850/1900MHz	1xLAN 1xRS-232	No	No	21M	5.76M
WL-R100E	1	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		A Contraction	VI	
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.

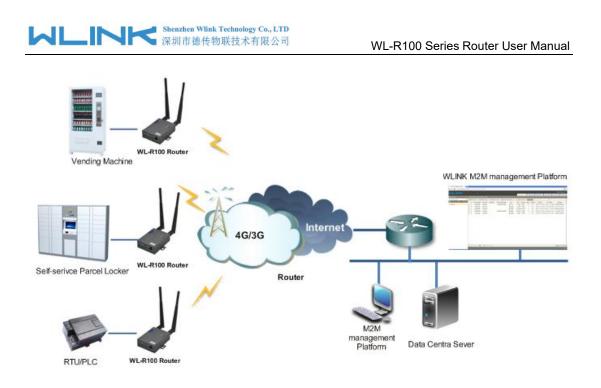


Figure 1-1 Network Topology

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

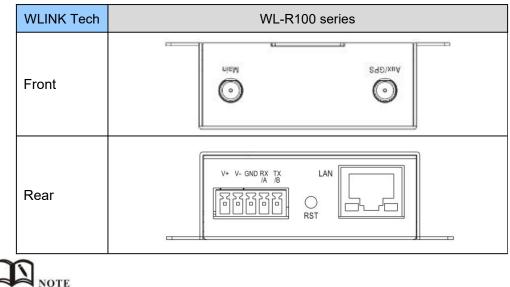
6



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





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

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



Port	Instruction	Remark
Aux/GPS	4G Aux Antenna or GPS Antenna, SMA connector, 50 $\Omega$	Optional
LAN	10/100Base-TX, MDI/MDIX self-adaption,	
RST	Reset button, (press on button 5 seconds)	
PWR	Power connector	7.5 $\sim$ 32V DC
СОМ	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		
	Green		Strong Signal		
	Orange		Normal Signal		
NET	Red		Weak Signal		
		Solid light	Connected 4G successfully		
		Blinking quickly(0.5s)	Dialing		
Green		Solid light	Connected		
LAN	Green	Blinking	Data Sending		
	Green	Dark	Not connected		
PWR	Green	Solid light	Router OS is running.		



Table 2-2 Router LED indictor Status

## 2.3 Dimension

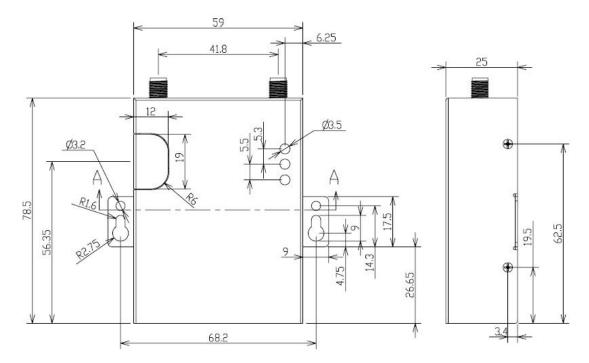


Figure 2-2 WL-R100 Series Router Dimension Figure

## 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.

# CAUTION

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

# CAUTION

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:  $+7.5V \sim +32VDC$ , 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.

# CAUTION

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 "<u>http://192.168.1.1/</u>", to enter identify page.

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

Connect to 1	92.168.8.1	? 🛛
<u>U</u> ser name:	😰 admin	
<u>P</u> assword:	Remember my	ny password
	ОК	K Cancel

Figure 3-4 User Identify Interface

----END

## 3.2 Basic Configuration

## A 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	System Status		Route
Overview			
LAN	Router Name	Router	
Device List	Hardware Verion		
Basic Network	Firmware Version	Router-4.2.2.3	
Advanced Network	Provide a secondaria		
īrewall	Router Time	Tue, 29 Mar 2016 20:40:06 +0800 Clock Sync.	
/PN Tunnel	Uptime	00:01:36	
dministration	Total / Free Memory	60.08 MB / 53.55 MB (89.14%)	
Debugging			
ogout	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.

Status	Cellular Settings	Route
Basic Network		
Cellular	Cellular Network	MU709S:WCDMA/HSPA+
LAN	Туре	n.
DDNS	ICMP Check	8
Routing		
Advanced Network	Cellular Traffic Check	
Firewall	Connect Mode	Keep Alive(Auto-Online) 🔻
VPN Tunnel	CIMI Send to	
Administration		
Debugging	SMS Code	
Logout	PIN Code	
Logout	Operator Lock	ex:46001
	Dial Number	*99#
	Mode	Auto 🔻
	APN	3GNET
	User	CARD
	Password	****
	rassword	
	Auth Type	Auto 🔻
	Local IP Address	
+		
		Save Cancel

Figure 3-1 Cellular Settings GUI

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> <li>Keep alive (Auto-online). The router will automatically connect 3G/4G network and keep online.</li> </ul>		
	<ul> <li>Connect On Demand. Idle offline if no data from LAN to 3G/4G within defined time.</li> </ul>		

Table 3-1 Cellular Setting Parameter Instruction

13

#### Shenzhen Wlink Technology Co., LTD 深圳市徳传物联技术有限公司

WL-R100 Series Router User Manual

Parameter	Instruction
	<ul> <li>Schedule, Define online and offline time. This function need to enable NTP function,</li> </ul>
	Call/SMS Triggered. Call/SMS trigger router online.
	<ul> <li>Manually. Connect 3G/4G network by manual.</li> </ul>
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		
Check IP	8.8.8.8	
Check IP (Optional)	4.4.4.4	
Interval	60	(seconds)
Retries	3	(Times)
Fail Action	Reboo	t 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

MLINK Shenzhen Wlink 深圳市徳传教	WL-R100 Series Router User Manual	
or reboot.		
Cellular Traffic Check		
Check Mode	Rx	•
Check Interval	10	(minutes)Range: 1 ~ 1440
Fail Action	Cellular R	econnect 🔻

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

Status	LAN	Router
Basic Network		
Cellular	Router IP Address	192.168.1.1
LAN	Subnet Mask	255.255.255.0
DDNS		
Routing	DHCP Server	
Advanced Network	IP Pool	192.168.1.2 - 192.168.1.53 (52)
Firewall	Lease	1440 (minutes)
VPN Tunnel		
Administration		
Debugging		
Logout		
		Save Cancel

Figure 3-2 LAN Setting GUI

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	

Table 3-2 LAN Setting Instruction

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.

Status	Dynamic DNS		Router
Basic Network			
Cellular	IP Address	Use WAN IP Address 10.232.200.48 (recommended) 🔻	
LAN	Auto sofrash arraw		
DDNS	Auto refresh every	5 minutes (0 = Disabled)	
Routing			
Advanced Network	Dynamic DNS 1		
Firewall			
VPN Tunnel	Service	None	
Administration	Jervice	HOLE	
Debugging			
Logout	Dynamic DNS 2		
	Service	None	
			Save Cancel

#### Figure 3-3 Dynamic DNS Setting

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.

				able	Current Routing T	Status
						Basic Network
	c Interface		Subnet Mask	ateway / Next Hop	New Oracle Concession and American	Celiular
	ppp0 (WAN)		255. 255. 255. 255		10.64.64.64 * 192.168.1.0 *	LAN
	br0 (LAN) lo		255. 255. 255. 0 255. 0. 0. 0		192.168.1.0 * 127.0.0.0 *	DDNS
	ppp0 (WAN)		0.0.0.0	1. 64. 64. 64		222232
	ррро (лин)	°	0.0.0.0		deraurt	Routing
						Advanced Network
				le	Static Routing Tab	īrewall
Description	Totorfoco	Matric	Subnet Mask	ateway	Destination G	/PN Tunnel
bescription		metric	Sublet mask	icenay	bescination G	dministration
	•					Debugging
					Miscellaneous	Logout
					HISCHARCOUS	
				Gateway 🔻	Mode	
				Disabled 🔻	RIPv1 & v2	
					Efficient Multicast Forwarding	
				-	BUILD B	
					DHCP Routes	

Save Cancel

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.

#### は に い に Shenzhen Wlink Technology Co., LTD 深圳市徳传物联技术有限公司

#### WL-R100 Series Router User Manual

Status	Po	rtFor	wa	rding					Rout
Basic Network				-					
Advanced Network	On	Proto		Src Address	Ext Ports	Int Port	Int Address	Description	4
Port Forwarding		VDP			1000, 2000		192.168.1.2	ex: 1000 and 2000	
Port Redirecting		Both			1000- 2000, 3000		192.168.1.2	ex: 1000 to 2000, and 3000	
DMZ		Both		1.1.1.0/24	1000-2000		192.168.1.2	ex: 1000 to 2000, restricted	×
Triggered		TCP			1000	2000	192.168.1.2	ex: different internal port	
Serial App.		TCP	•						
UPnP/NAT-PMP									bbA
VRRP Static DHCP Firewall	:	Ext Po Int Po entry is	orts ort ( sup	<ul> <li>The ports to be for optional) The dest ported when forward</li> </ul>	rwarded, as seen tination port insid rding to a differe	from the de the LAN nt internal	WAN. ex: "2345", " I. If blank, the destine	2.3.4 - 2.3.4.5", "1.2.3.0/24", "me.( 200,300", "200-300,400". nation port is the same as <i>Ext Ports</i> . (	
/PN Tunnel	•			ss - The destination					
Administration									
Debugging									
Logout									
								Save	Cancel

#### Figure 3-5 Port Forwarding GUI

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

Table 3-5 "Port Forwarding" Instruction

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.



tatus	Por	tRedire	ctin	g				
asic Network	On	Proto		Int Port	Dst Address	Ext Port	Description	
dvanced Network	<b>Un</b>	TCP	•		DST Address	Ext fort	Description	
Port Forwarding		ICP	•					
Port Redirecting								Add
DMZ								
Triggered								
Serial App.								
UPnP/NAT-PMP								
Bandwidth Limiter								
VRRP								
Static DHCP								
rewall								
PN Tunnel								
dministration								
ebugging								
ogout								

Save Cancel

Figure 3-6 Port Forwarding GUI

	5
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

Table 3-6 "Port Redirecting" Instruction

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.

#### Shenzhen Wlink Technology Co., LTD 深圳市徳传物联技术有限公司

#### WL-R100 Series Router User Manual

Status	DMZ		Router
Basic Network			
Advanced Network	Enable DMZ		
Port Forwarding	Internel Address	192.168.1.0	
Port Redirecting		192.100.1.0	
DMZ	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")	
Triggered		(opcome, ex initi, initio/2+, initi-222222 of melekemple.com)	
Serial App.	Leave Remote Access	(Redirect remote access ports for SSH and HTTP(s) to router)	
UPnP/NAT-PMP		(Redirect ferride access ports for 551 and 1117(3) to routery	
Bandwidth Limiter			
VRRP			
Static DHCP			
Firewall			
VPN Tunnel			
Administration			
Debugging			
Logout			
		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.

	深圳市德传	物联技术有限公司	WL-R100 Series Router User Manua
			Route
Status	IP Passthrough		
Basic Network			
WLAN	Enabled		
Advanced Network	MAC Address	34:00:09:AC:52:23	
Port Forwarding			
Port Redirecting	Gateway		
DMZ			
IP Passthrough			
Triggered			
Captive Portal			
Serial App.			
UPnP/NAT-PMP			
Bandwidth Control			
VRRP			
Static DHCP			
Firewall			
VPN Tunnel			
Administration			
Debugging			
Logout			
			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.



atus	Trig	gered P	ort Forwarding	I		Rot
sic Network	-					
Ivanced Network	Un	Protocol TCP	Trigger Ports 3000-4000	Forwarded Ports 5000-6000	Description ex: open 5000-6000 if 3000-400	20
Port Forwarding		TCP V		3000 0000	ex. open 3000 0000 11 3000 400	
ort Redirecting	۲	TCP •			1	
MZ						Add
riggered						
erial App.		(200-300).				
PnP/NAT-PMP	•	These ports a	re automatically closed a	fter a few minutes of inactivit	ty.	
ndwidth Limiter						
RRP						
atic DHCP						
vall						
Tunnel						
inistration						
ugging						
out						
						Save Canc

#### 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.

#### Khenzhen Wlink Technology Co., LTD 深圳市徳传物联技术有限公司

#### WL-R100 Series Router User Manual

Status	Serial to TCP/IP		Router
Basic Network			
Advanced Network	Serial to TCP/IPMode	Client 🔻	
Port Forwarding	Server IP/Port	8.8.8.8 : 40002	
Port Redirecting		: 40003	
DMZ			
Triggered	Socket Type	TCP 🔻	
Serial App.	Socket Timeout	500 (milliseconds)	
UPnP/NAT-PMP	Serial Timeout	500 (milliseconds)	
Bandwidth Limiter	Paket Payload	1024 (bytes)	
VRRP	T unce T uploud		
Static DHCP	Heart-Beat Content		
Firewall			
VPN Tunnel	Heart-Beat Interval	2 (seconds)	
Administration			
Debugging	Baud Rate	115200 🔻	
	Parity Bit	none 🔻	
Logout	Data Bit	8 🔻	
	Stop Bit	1 -	
	Stop Bit	1 *	

Save Cancel

#### Figure 3-10 Serial App Setting GUI

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

#### Table 3-10 "Serial App" Instruction



Serial port connection

PINs	DB9(male)
V+	
V-	
GND	 5
RX	 3
ТХ	 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.

Status Forwar	ded Ports											Router
Basic Network												
Advanced Network Ext Ports	Int Port	Internal Address	L 🔺	Protocol	Descr	iption						
Port Forwarding										Delete	AII	efresh
Port Redirecting												
DMZ Setting	s											
Triggered												
Serial App. Enable U	PnP											
UPnP/NAT-PMP Enable N												
Bandwidth Limiter												
VRRP Inactive	Rules Cleaning	1										
Static DHCP Cleanin	g Interval	600	seconds									
Firewall Cleanin	g Threshold	20	redirecti	ons								
VPN Tunnel Secure M	ode	when en	- oblad UB	D clients a	wolle or	od to od	d mannin	as only to th	hoir ID)			
Administration	ouc	when en	labieu, ori			ieu w au		js only to u	ilen ir j			
Debugging Chaw In	My Network											
Logout	My Network											
										Save	Ca	ancel

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.

Shenzhen Wlink Technology Co., LTI 深圳市德传物联技术有限公司	ML	INK	Shenzhen Wlink Technology Co., LTD 深圳市德传物联技术有限公司
---	----	-----	--

Status	Bandwidth Control					Router
Basic Network						
WLAN	Enable Control					
Advanced Network						
Port Forwarding						
Port Redirecting	IP   IP Range   MAC Address	DLRate	DLCeil	ULRate	VLCeil	Priority
DMZ						Normal 🔻
IP Passthrough						Add
Triggered						
Captive Portal	Default Class					
Serial App.						
UPnP/NAT-PMP	Enable Default Class					
Bandwidth Control						
VRRP						
Static DHCP						
Firewall						
VPN Tunnel						
Administration						
Debugging						
Logout						
					Sa	ve Cancel

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.

Status	VRRP		Rot
Basic Network			
Advanced Network	Enable VRRP		
Port Forwarding	Mode	Backup 🔻	
Port Redirecting			
DMZ	Virtual IP	192.168.1.3	
Triggered	Virtual Router ID		
Serial App.	Priority	100	
UPnP/NAT-PMP	Authentication	0	
Bandwidth Limiter	Script Type	Default 🔻	
VRRP	and the second		
Static DHCP	Check Interval	3	
irewall	Weight	10	
/PN Tunnel			
<b>Administration</b>			
Debugging			
Logout			
			Save Canc

Figure 3-13 VRRP Setting GUI

Step 2 Please click "save" to finish.



#### 3.3.10 Static DHCP Setting

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

		1			
Advanced Network	MAC Address	IP Address	Hostname	٨	Description
Port Forwarding	00:00:00:00:00:00 00:00:00:00:00	192.168.1.2			
Port Redirecting	00:00:00:00:00				
DMZ					Add
Triggered					
Serial App.					
UPnP/NAT-PMP					
Bandwidth Limiter					
VRRP					
Static DHCP					
Firewall					
Firewall					
VPN Tunnel					
VPN Tunnel Administration					
VPN Tunnel Administration Debugging Logout					

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	IP,	MAC/Port	incerning						
lasic Network		Src MAC	Src IP	Dst IP	n., 1	Src Port	Dst Port	p.1'	Description
VLAN		SPC MRL	216 11	DEL TL		SFC FOFT	DEL LOLL		Description
dvanced Network					NONE ¥			Acc∈ ▼	
rewall									Add
IP/URL Filtering									
Domain Filtering	Ke	y Word Filt	ering						
N Tunnel	0	n Key Vord			Descrip				
ministration					Dezcrip	1101			
bugging		e							
									Add
		A							
	2								
									Add
	Act	cess Filteri		Ret TP	Protocol	Ste Port	Bet Port	Palian	
	Ac		ng Sre IP	Dst IP		Src Port	Dst Port	Policy	Add Description
	Act	cess Filteri		Dst IP	Protocol NONE ¥	Sre Port	Dst Port	Policy Acce V	

#### 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.



Status	Domain Filteri	ng		Router
Basic Network				
Advanced Network	On			
Firewall	Default Policy	Black List 🔻		
IP/URL Filtering	Delault Folicy	DIACK LISC .		
Domain Filtering				
VPN Tunnel	On Domain		Description	
Administration				
Debugging				bbA
Logout				
				Save Cancel

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.

	200	E Tui	(11) (11) (11)										
Basic Network	0.5	TB7 A	Tunnal	Advarr	Tunna	l Source	Tannal	Destination	Kaanaliwa	Internal	Patriar	Decar	
VLAN	I IIII		Tumer	Aut ess	rume.	L SULLUE	Tumer	Destination	Teebariie	Intervat	Aetries	Desci	IPLION
dvanced Network	۲												
irewall													Add
/PN Tunnel													
GRE	GR	E Ro	ute										
OpenVPN Client	On	Tunne	l Index		<b>A</b> 1	Destination	Addres	22	Desc	ription			
PPTP/L2TP Client		1			Ŧ								
IPSec													Add
dministration	-												Aud
Debugging													

Save Cancel



Figure 3-16 GRE Setting GUI

	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	

Table 3-13 "GRE" Instruction

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.

Status	OpenVPN Client					Router
Basic Network						
WLAN		Client 2				
Advanced Network	Basic	Advanced	Keys	Status		
Firewall	Start with WAN					
VPN Tunnel		_				
GRE	Interface Type	TUN V				
OpenVPN Client	Protocol	UDP V				
PPTP/L2TP Client	Server Address/Port				1194	
IPSec	Firewall	Automatic V				
Administration	Authorization Mode	TLS				
Debugging		TLS •				
Logout	Username/Password Authentication					
	HMAC authorization	Disabled	•			
	Create NAT on tunnel					
	Start Now					
						Save Cancel



Figure 3-17 OpenVPN Setting GUI

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.		

Table 3-14 "OpenVPN" Instruction

Status	OpenVPN Client				Router
Basic Network					
WLAN	Client 1 Basic	Client 2 Advanced	Keys	Status	
Advanced Network	Dasic	Advanced	NC/3	Jacus	
Firewall	Poll Interval	0	(in minutes, 0 to a	disable)	
VPN Tunnel	Redirect Internet				
GRE	traffic	0			
OpenVPN Client	Accept DNS configuration	Disabled	*		
PPTP/L2TP Client	Encryption cipher	Use Defau	ilt v		
IPSec	a second and a second second second				
Administration	Compression	Adaptive			
Debugging	TLS Renegotiation Time	-1	(in seconds, -1 f	or default)	
Logout	Connection retry	30	(in seconds; -1 f	or infinite)	
	Verify server certificate (tls- remote)				
	Custom Configuration Start Now				<i>b</i>

Save Cancel

30

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 time1 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.

Status	OpenVPN Client	Router
	openven chenc	
Basic Network	Client 1 Client 2	
WLAN	Basic Advanced Keys Status	
Advanced Network	For help generating keys, refer to the OpenVPN HOWTO.	
Firewall		
VPN Tunnel		13
GRE		
OpenVPN Client		
PPTP/L2TP Client	Certificate Authority	
IPSec		
Administration		
Debugging		
Logout	Client Certificate	
	Client Key	4
	Start Now	

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	OpenVPN Cli	ont				Router
	Openvri ch	CIIL				
Basic Network	Client 1	Client 2				
WLAN	Basic	Advanced	Keys	Status		
Advanced Network						
Firewall	Client is not running	or status could not b	e read.			
VPN Tunnel	<b>2 1 1 1</b>					Refresh Status
GRE	Start Now					
OpenVPN Client						
PPTP/L2TP Client						
IPSec						
Administration						
Debugging						
Logout						
					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.

itatus	LLI	P/PPTP	Dasic										
Basic Network		_									Default		
WLAN	On 🛦	Protocol	Hane	Server			Usern	ame P	assword	Firewall	Route	Local	. IP
Advanced Network		L2TP T											
īrewall													Add
/PN Tunnel													
GRE	1.21	P Advand	ced										
OpenVPN Client		i natan											
PPTP/L2TP Client	0n 🛦	Hane	Accept DHS	TU	IRU	Tunnel	Auth	Tunnel	Password	Custon	Options		
IPSec			NO	2 I.									
Administration													Add
ogout	-	rP Advan	ccu										
ogout					TOIL	WDDF	WDD		1 6	0			
Logout	0n 🛦	Hame	Accept DHS		<b>R</b> RV	MPPE	TPP	E Statef	ul Custon	Options			
Logout			Accept DWS	TTU	IRV		TPP)		ul Custon	o Options			
Logout	0n 🛦		Accept DHS		IRU		TPP)		ul Custo	0ptions			Add
logout	On A	Name	Accept DHS		TRU		TPP)		ul Custo	0ptions			Add
logout:	On A		Accept DHS		TRU		TPP		ul Custon	0 Options			bbA
logout:		Name	Accept DHS		<b>NRU</b>				ul Custon	0ptions			Add
Logout:	on▲ ♥ SCł	Wame HEDULE	Accept DWS	•					ul Custon	0 Options			Add



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.	

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

Status	IPSEC			Router
Basic Network	IPSEC 1 IP	SEC 2		
WLAN		Basic Setup Advanced Setup		
Advanced Network	Group Setup	Auvanced Setup		
Firewall	Enable IPSec			
VPN Tunnel	TRC E-ti			
GRE	IPSec Extensions	Normal <b>*</b>		
VPN Client	Local Security Gateway Interface	3G Cellular 🔻		
IPSec				
Administration	Local Security Group Subnet/Netmask	192.168.1.0/24	ex. 192.168.1.0/24	
Debugging	Local Security			
Logout	Firewalling			
	Remote Security Gateway IP/Domain			
	Remote Security Group Subnet/Netmask	10.0.0/24	ex. 192.168.88.0/24	
	Remote Security Firewalling	80		
				Save Cancel

#### 3.5.3.1 IPSec Group Setup

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

#### Shenzhen Wlink Technology Co., LTD 深圳市徳传物联技术有限公司

#### WL-R100 Series Router User Manual

Status	IPSEC				Router
Basic Network					
WLAN		SEC 2			
Advanced Network	Group Setup B	asic Setup	Advanced Setup		
Firewall	Enable IPSec				
VPN Tunnel	IPSec Extensions	Normal	*		
GRE		Normal			
VPN Client	Local Security Gateway Interface	3G Cellular	•		
IPSec					
Administration	Local Security Group Subnet/Netmask	192.168.1.0	)/24	ex. 192.168.1.0/24	
Debugging	Local Security				
Logout	Firewalling	196			
Logon	Remote Security Gateway IP/Domain				
	Remote Security Group Subnet/Netmask	10.0.0/24		ex. 192.168.88.0/24	
	Remote Security Firewalling	20			

Save Cancel

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.

# 

#### WL-R100 Series Router User Manual

Status	IPSEC		Router
Basic Network	TROCOL		
WLAN		SEC 2 asic Setup Advanced Setup	
Advanced Network	Group Setup	Advanceu Setup	
Firewall	Keying Mode	IKE with Preshared Key 🔻	
VPN Tunnel	Phase 1 DH Group	Group 2 - modp1024 V	
GRE			
VPN Client	Phase 1 Encryption	3DES (168-bit) 🔻	
IPSec	Phase 1 Authentication	MD5 HMAC (96-bit)	
Administration	Phase 1 SA Life Time	28800 seconds	
Debugging			
Logout	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		

Save Cancel

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.

IPSEC		
TIPETO 1	IDCCC 2	
Group Setup	Basic Setup Advanced Setup	
Aggressive Mode		
Compress(IP Payload Compression)		
Detection(DPD)		
ICMP Check		
IPSec Custom Options 1		
IPSec Custom Options 2		
IPSec Custom Options 3		
IPSec Custom Options 4		
	IPSEC 1         Group Setup         Aggressive Mode         Compress(IP Payload         Compress(IP Dayload         Dead Peer         Detection(DPD)         ICMP Check         IPSec Custom Options         1         IPSec Custom Options         2         IPSec Custom Options         3	IPSEC 1       IPSEC 2         Group Setup       Basic Setup       Advanced Setup         Aggressive Mode

Save Cancel

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.

	enzhen Wlink Technology Co., LTD 圳市德传物联技术有限公司
--	--

Status	Router Identifi	ication
Basic Network		
Advanced Network	Router Name	Router
Firewall	Hostname	Router
VPN Tunnel		Norce
Administration	Domain Name	
Identification		
Time		
Admin Access		
Scheduler Reboot		
SNMP		
M2M Settings		
Configuration		
Logging		
Upgrade		
Reboot		
Debugging		
Logout		

Save Cancel

Router

Figure 3-1 Router Identification GUI

Table 3-1	"Router	Identification"	Instruction
	rtoutor	achanoadori	moulon

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



# **3.6.2** Time Setting

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

Status	Time		Route
Basic Network			
Advanced Network	Router Time	Sat, 01 Jan 2000 09:03:52 +0800 Clock Sync.	
Firewall	Kouter fille	Sat 01 Jan 2000 09.05.52 +0800 Clock Sync.	
VPN Tunnel	Time Zone	UTC+08:00 China, Hong Kong, Western Australia, Singapore, Taiwan 🔻	
Administration		o ic+oc.oo china, Hong Kong, Western Australia, Singapore, Taiwan 🔹	
Identification	Auto Daylight Savings Time	2	
Time			
Admin Access	Auto Update Time	Every 4 Hours 🔻	
Scheduler Reboot	Physics of the second second second		
SNMP	Trigger Connect On Demand		
M2M Settings	NTP Time Server	Asia 🔻	
Configuration	NTP Time Server		
Logging		0.asia.pool.ntp.org, 1.asia.pool.ntp.org 2.asia.pool.ntp.org	
Upgrade			
Reboot			
ebugging			
.ogout			
			Save Cancel
			Save
		Figure 3-1 System Configuration GUI	

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

Step 2 Please click "save to finish.



# 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.

Status	WebAccess	Router
Basic Network		
Advanced Network	Local Access	НТТР 🔻
Firewall		
VPN Tunnel	HTTP Access Port	80
Administration	Remote Access	Disabled <b>•</b>
Identification	Allow Wireless Access	
Time		
Admin Access	Open Menus	
Scheduler Reboot	Status	
SNMP	Basic Network	
M2M Settings	Firewall	
Configuration		—
Logging	VPN Tunnel	
Upgrade	Advanced Network	
Reboot	Administration	0
Debugging	Debugging	
Logout		
	Password	
	Password	********
	(re-enter to confirm)	••••••

Figure 3-1 Admin Setting GUI

Step 2 Please click save iron to finish the setting



# 3.6.4 Schedule Reboot Setting

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

Status	Scheduler Re	boot	Router
Basic Network			
Advanced Network	Enabled		
Firewall	Time	1:00 AM	
/PN Tunnel			
Administration	Days	🖉 Sun 🦉 Mon 🖉 Tue 🦉 Wed 🧭 Thu 🦿 Fri 🖉 Sat 🖉 Everyday	
Identification			
Time			
Admin Access			
Scheduler Reboot			
SNMP			
M2M Settings			
Configuration			
Logging			
Jpgrade			
Reboot			
ebugging			
ogout			
		Save	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.



Status	SNMP Settings		Router
Basic Network			
Advanced Network	Enable SNMP		
Firewall			
VPN Tunnel	Port	161	
Administration			
Identification	Remote Access		
Time	Allowed Remote IP Address		
Admin Access	IP Address	(optional; ex: "1.1.1.1", "1.1.1.0/24", "1.1.1.1 - 2.2.2.2" ")	
Scheduler Reboot	Location	router	
SNMP	Location		
M2M Settings	Contact	admin@router	
Configuration	RO Community	rocommunity	
Logging			
Upgrade			
Reboot			
Debugging			
Logout			

Save Cancel

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.

Status	m2m	F	Router
Basic Network			
Advanced Network	M2M Enabled		
Firewall	Fail Action	Restart M2M	
VPN Tunnel		Restart MZM	
Administration	Device ID		
Identification			
Time	M2M Server/Port		
Admin Access	Heartbeat Intval	10 (seconds)	
Scheduler Reboot	Heartbeat Retry	10 (Range:10-1000)	
SNMP			
M2M Settings			
Configuration			
Logging			
Upgrade			
Reboot			
Debugging			
Logout			
		Save	ncel



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

		outer
Status	Backup Configuration	
Basic Network	Router_Router-4223_m06502d .cfg Backup	
Advanced Network	Link	
Firewall		
VPN Tunnel		
Administration	Restore Configuration	
Identification		
Time	Select the configuration file to restore: 选择文件 未选择任何文件 Restore	
Admin Access	<u>这件文件</u> 小这件证例文件 Restore	
Scheduler Reboot		
SNMP	Destant Default Configuration	
M2M Settings	Restore Default Configuration	
Configuration	Select V Save	
Logging		
Upgrade		
Reboot		
Debugging	Total / Free NVRAM: 32.00 KB / 14.11 KB (44.10%)	
Logout		

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.



# 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).

Status	Syslog		Router
Basic Network			
Advanced Network	Log Internally	2	
Firewall	Log To Remote System		
VPN Tunnel			
Administration	Generate Marker	Every 1 Hour	
Identification	Limit	60 (messages per minute / 0 for unlimited)	
Time			
Admin Access			
Scheduler Reboot			
SNMP			
M2M Settings			
Configuration			
Logging			
Upgrade			
Reboot			
Debugging			
Logout			
		Save Ca	ancel

Figure 3-1 System log Setting GUI

Step 2 After configure, please click "Save" to finish.



# **3.6.9 Firmware upgrade**

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

Status	Upgrade Firmware	Route
Basic Network	Select the file to use:	
Advanced Network	Select the ne to use: 选择文件 未选择任何文件 Upgrade	
Firewall		
VPN Tunnel	After flashing, erase all data in NVRAM memory	
Administration	Current Version: Router-4.2.2.3-160329-114644	
Identification	Free Memory: 53.52 MB (aprox. size that can be buffered completely in RAM)	
Time		
Admin Access		
Scheduler Reboot		
SNMP		
M2M Settings		
Configuration		
Logging		
Upgrade		
Reboot		
Debugging		
Logout		

Figure 3-1 Firmware Upgrade GUI



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.



Status	Router
Basic Network	View
Advanced Network	A REAL PROPERTY AND
Firewall	Download Log File
VPN Tunnel	Find
Administration	
Debugging	» Logging Configuration
Logs	
Ping	
Trace Route	
Logout	

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.

							Router
Status	Ping						
Basic Network							
Advanced Network	IP Address	baidu.co	om	Ping			
Firewall	Ping Count	10					
VPN Tunnel	1						
Administration	Packet Size	56	(bytes)				
Debugging							
Logs							
Ping	Seq Address			RX Bytes	TTL	RTT (ms)	+/- (ms)
Trace Route							
Logout							

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.

Status	Trace Route							Ro	outer
Basic Network									
Advanced Network	IP Address			Trace					
Firewall	Maximum Hops	20							
VPN Tunnel			-						
Administration	Maximum Wait Time	3	(seconds per hop)						
Debugging									
Logs									
Ping	Hop Address				min (ms)	max (ms)	avg (ms)	+/-	(ns)
Trace Route									Common Common (
Logout									



Figure 3-1 Trace GUI

Step 2 After configure, please click "Save" to finish.



# 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 or 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.

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

#### Table 3-1 System Default Instruction



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



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

Status	System Status			
Overview				
VPN	Router Name	Router		
LAN	Hardware Version	C11-D20		
Device List	Firmware Version	Router-4.3.4.1		
Basic Network	Router Time	Thu, 22 Jun 2017 14:33:33 +0800 Clo	ck Sync.	
WLAN	Uptime	00:24:56		
Advanced Network	Total / Free Memory	60.05 мв / 48.55 мв (80.84%)	Network Connection Deta	ails 🗙 🗙
Firewall			Network Connection Details	
VPN Tunnel	Internet Status		Property	Value
Administration	Internet Status		Connection-specific DN	
Debugging	Connection Type MAC Address Modem Type Modem IMEI Modem Status Cellular ISP Cellular Network USIM Status CSQ IP Address Subnet Mask Gateway	Cellular Network 00:00:4C:4C:4B:02 3G-MC2716:CDMA 1x/CDMA 2000 0x8044E8E3 Ready EVDO Ready 30	Description Physical Address DHCP Enabled IPv4 Address IPv4 Subnet Mask Lease Obtained Lease Expires IPv4 Default Gateway IPv4 DHCP Server IPv4 DHCP Server IPv4 UHCP Server IPv4 UHCP Server IPv4 WINS Server NetBIOS over Topip En Link-local IPv6 Address IPv6 Default Gateway IPv6 DNS Server	Intel(R) Ethemet Connection (3) I218-V 50-78-9D-C3-9A-22 Yes 192.168.1.36 255.255.255.0 22 June 2017 14:11:07 23 June 2017 14:11:07 192.168.1.1 192.168.1.1 192.168.1.1 Yes fe80::4dc:db8c:21dd:4323%14
	DNS Connection Status Connection Uptime	202.96.128.86:53, 202.96.134.133:53 Connected 00:23:55		Close

#### 3) Configuration

Status	Po	rtForm	arding					
Basic Network	0.0	Protocol	Src Address	Ext Ports	Int Port	Int Address	Description	
WLAN		TCP	Sic Address	443	443	192,168,1,36	test	
Advanced Network	On	TCP		554	554	192.168.1.36	test	
Port Forwarding	On	TCP		88	88	192.168.1.36	test	×
Port Redirecting	On	TCP		81	81	192.168.1.36	test	
DMZ		TCP	•					
IP Passthrough								Add
	1.1.1							
Triggered Captive Portal Serial App. UPnP/NAT-PMP		Ext Port Int Port	s - The ports to be f	orwarded, as seen estination port insi	from the Wide the LAN.	AN. ex: "2345", "2 If blank, the desti	.2.3.4 - 2.3.4.5", "1.2.3.0/24 200,300", "200-300,400". nation port is the same as <i>Ext</i>	
Captive Portal Serial App.	:	Ext Port Int Port entry is s	s - The ports to be f (optional) The de	orwarded, as seen estination port insi rarding to a differe	from the W ide the LAN. ent internal p	AN. ex: "2345", "2 If blank, the desti	200,300", "200-300,400".	
Captive Portal Serial App. UPnP/NAT-PMP Bandwidth Control	:	Ext Port Int Port entry is s	<ul> <li>The ports to be f (optional) The de upported when forw</li> </ul>	orwarded, as seen estination port insi rarding to a differe	from the W ide the LAN. ent internal p	AN. ex: "2345", "2 If blank, the desti	200,300", "200-300,400".	
Captive Portal Serial App. UPnP/NAT-PMP Bandwidth Control VRRP Static DHCP	:	Ext Port Int Port entry is s	<ul> <li>The ports to be f (optional) The de upported when forw</li> </ul>	orwarded, as seen estination port insi rarding to a differe	from the W ide the LAN. ent internal p	AN. ex: "2345", "2 If blank, the desti	200,300", "200-300,400".	
Captive Portal Serial App, UPnP/NAT-PMP Bandwidth Control VRRP Static DHCP Firewall	:	Ext Port Int Port entry is s	<ul> <li>The ports to be f (optional) The de upported when forw</li> </ul>	orwarded, as seen estination port insi rarding to a differe	from the W ide the LAN. ent internal p	AN. ex: "2345", "2 If blank, the desti	200,300", "200-300,400".	
Captive Portal Serial App. UPnP/NAT-PMP Bandwidth Control VRRP Static DHCP Firewall VPN Tunnel	:	Ext Port Int Port entry is s	<ul> <li>The ports to be f (optional) The de upported when forw</li> </ul>	orwarded, as seen estination port insi rarding to a differe	from the W ide the LAN. ent internal p	AN. ex: "2345", "2 If blank, the desti	200,300", "200-300,400".	
Captive Portal Serial App. UPnP/NAT-PMP Bandwidth Control VRRP	:	Ext Port Int Port entry is s	<ul> <li>The ports to be f (optional) The de upported when forw</li> </ul>	orwarded, as seen estination port insi rarding to a differe	from the W ide the LAN. ent internal p	AN. ex: "2345", "2 If blank, the desti	200,300", "200-300,400".	

Save Cancel

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



# 4.2 IP Passthrough

1) The router online

	Custom Chatra	,	Router
Status	System Status		
Overview	a harmonia and		
VPN	Router Name	Router	
LAN	Hardware Version		
Device List	Firmware Version	Router-4.3.4.4	
Basic Network	Router Time	Thu, 24 Jan 2019 14:48:02 +0800 Clock Sync.	
WLAN	Uptime	00:02:24	
Advanced Network	Total / Free Memory	60.05 MB / 48.04 MB (79.99%)	
Firewall			
VPN Tunnel	Internet Status		
Administration	Connection Turns	Cellular Network	
Debugging	Connection Type Modem Type	EC25:LTE/WCDMA	
	Modem IMEI	861107038587730	
Logout	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	120.80.80:53, 221.5.88.88:53	
	Connection Uptime	00:00:00	
	Connection Status Connection Uptime	Connected 00:00:00	

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

Status	IP Passthroug	h	🖗 Ethernet Status		>
Basic Network	Enabled		General		
WAN			Connection		
Cellular	MAC Address	50:7B:9D:C3:9A:22	IPv4 Connectivity:		Internet
LAN	Gateway		IPv6 Connectivity:	Nor	network access
DDNS					
Routing			Network Connection Deta	ails	>
WLAN			Network Connection Details		
Advanced Network					
Port Forwarding			Property	Value	
Port Redirecting			Connection-specific DN		
DMZ			Description Physical Address	Intel(R) Ethemet Con 50-7B-9D-C3-9A-22	nection (3) I218-V
IP Passthrough			DHCP Enabled	No	1
Triggered			IPv4 Address	192.168.10.110	
Captive Portal			IPv4 Subnet Mask	255.255.255.0	
GPS			IPv4 Default Gateway	192.168.10.1	
UPnP/NAT-PMP			IPv4 DNS Server	192.168.10.1	
Bandwidth Control			IPv4 WINS Server NetBIOS over Tcpip En	No	
VRRP			Link-local IPv6 Address	fe80::69ca:9764:1fe	1.cbh1%20
			IPv6 Default Gateway		
Static DHCP			IPv6 DNS Server		
Firewall					
VPN Tunnel					
Administration					
Debugging					
Logout					Close

3) Set the PC to DHCP



Ethernet Status	Ethernet Properties	Internet Protocol Version 4 (TCP/IPv4) Properties
General	Networking Sharing	General Alternate Configuration
Connection IPv4 Connectivity: Internet IPv6 Connectivity: No network access	Connect using:	You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Media State: Enabled Duration: 05:11:32 Speed: 100.0 Mbps Details	Co This connection uses the following items:	Sybnet mask:
Activity Sent Received	Microsoft Network Adapter Multiplexor Protoco     Microsoft LLDP Protocol Driver     Microsoft LLDP Protocol Version 6 (TCP/IPv6)     <	Olyge the following DNS server addresses:
Bytes:         39,134,796         630,257,094           Properties         Disable         Diagnose	Install Uninstall Pro Description Transmission Control Protocol/Internet Protocol. The wide area network protocol that provides communica across diverse interconnected networks.	Preferred DNS server:
Close	OK	OK Cancel

#### 4) Check the Ethernet status and ping test

Ethernet Status	Network Connection Deta	iils	Command Prompt
ieneral	Network Connection Details		Microsoft Windows [Version 10.0.16299.547] (c) 2017 Microsoft Corporation. All rights reserved.
Connection IPv4 Connectivity: Internet IPv5 Connectivity: No network access Media State: Enablee Duration: 00:00:4 Speed: 1.0 Gbps Details	Description Physical Address DHCP Enabled IPv4 Address		C:\Users\Root>ping 8.8.8.8 <sup>2</sup> pinging 8.8.8.8 with 32 bytes of data: Reply from 8.8.8.8.8.1 bytes=32 time=121ms TTL=247 Reply from 8.8.8.8.8 bytes=32 time=591ms TTL=247 Reply from 8.8.8.8.8 bytes=32 time=591ms TTL=247 Reply from 8.8.8.8.8 bytes=32 time=297ms TTL=247 Ping statistics for 8.8.8.8: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 121ms, Maximum = 591ms, Average = 336ms
Sent — Received Bytes: 32,938,948   14,187,797 @Properties @Diagnose	IPv4 WINS Server NetBIOS over Topip En	120.80.80.80	C:\Users\Root>ping 8.8.4.4 Pinging 8.8.4.4 with 32 bytes of data: Reply from 8.8.4.4: bytes=32 time=57ms TTL=247 Reply from 8.8.4.4: bytes=32 time=82ms TTL=248 Reply from 8.8.4.4: bytes=32 time=152ms TTL=247 Reply from 8.8.4.4: bytes=32 time=152ms TTL=248
Clos	2	с	<sup>b</sup> Ping statistics for 8.8.4.4: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 57ms, Maximum = 152ms, Average = 107ms

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

#### Shenzhen Wlink Technology Co., LTD 深圳市徳传物联技术有限公司

#### WL-R100 Series Router User Manual

tworking Sharing			General			
Connect using:	et Connection (3) 1218-1	/	You can get IP settings assigned automatically if your network s this capability. Otherwise, you need to ask your network admini for the appropriate IP settings.			
		Configure	O <u>O</u> btain an IP address auto	matically		
	the following items:		O     Use the following IP addre	ss:		
Client for Mi	crosoft Networks iter Sharing for Microsof	Networks	IP address:	192,168,1,2		
QoS Packet Scheduler     Internet Protocol Version 4 (TCP/IPv4)     Microsoft Network Adapter Multiplexor Protocol			Subnet mask: 255 . 255 . 255 . 0			
			Default gateway:	·····		
	DP Protocol Driver tocol Version 6 (TCP/IP	v6) 🗸	O Obtain DNS server address	s automatically		
<		>	• Use the following DNS serv	ver addresses:		
Install	Uninstall	Properties	Preferred DNS server:	· · · ·		
Description			Alternate DNS server:			
wide area network	rol Protocol/Internet Pro protocol that provides o pronnected networks.		Validate settings upon exi	it Advanced		

# 4.3 GPS Settings

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

# 

#### WL-R100 Series Router User Manual

Status	GPS		Router
Basic Network			
Advanced Network	GPS Mode	Client 🔻	
Port Forwarding	Data Format	M2M_FMT •	
Port Redirecting			: 40002
DMZ	Server IP/Port	192.168.1.2	: 40002
Triggered			
Serial App.	Heart-Beat Content		
GPS	Heart-Beat Interval	5 (seconds)	
UPnP/NAT-PMP			
Bandwidth Limiter			
VRRP			
Static DHCP			
Firewall			
VPN Tunnel			
Administration			
Debugging			
Logout			

Save Cancel

### 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





### Step 3 Check GPS Status

Overview     Current     OK       VPN     Current     OK       LAN     System Type     GPS       GPS Status     Satellites Numbers     07       GPS Status     Satellites Clock     180321 - 092040.00       Device List     Positioning     2234,22737N - 11356.62888E       Basic Network     Google Map     View	
Content     System Type     GPS       LAN     System Type     GPS       Satellites Numbers     07	
LAN         Satellites Numbers         07           GPS Status         Satellites Clock         180321 - 092040.00           Device List         Positioning         2234.22737N - 11356.62888E	
GP5 Status         Satellites Clock         180321 - 092040.00           Device List         Positioning         2234.22737N - 11356.62888E           Genole Man         View	
Google Man View	
asic Network Google Map View	
/LAN	
dvanced Network	
rewall	
PN Tunnel	
dministration	
ebugging	
ogout	



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,0.0,91.5,1,1.2,9 7.5

3. GPS data description

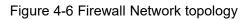
WLINK	Shenzhen Wlink Technology Co., LTD 深圳市德传物联技术有限公司
-------	--

		ī德传物联技术有限	公司 WI	L-R100 Series Router User Manual
Field No.	Name	Format	Example	Description
1	Router ID	String	0001_R081850 ac	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





### 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)

Basic Network										
	On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description	
VLAN	On	-	any/0	any/0	<ul> <li>output</li> </ul>	package	-	Drop		
dvanced Network	On	-	any/0	192.168.1.0/24	- input p	ackage	-	Accept		
irewall	On	50:7B:9D:C3:9A:22	any/0	any/0	-	-	-	Accept		
IP/URL Filtering	On	60:F1:89:20:F0:9A	any/0	any/0	-	-	-	Accept		
Domain Filtering	On	00:1E:64:DF:E8:46	any/0	any/0	-	-		Accept		
/PN Tunnel					NONE V			Acc 🔻		
									4	Add
Administration										
Debugging		Sector Contractory Contractory								
	Key	y Word Filteri	ng							
ogout										
	01				Descriptio	on				

## 2) Key Word Filtering

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

Description
Description
Description

### 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.

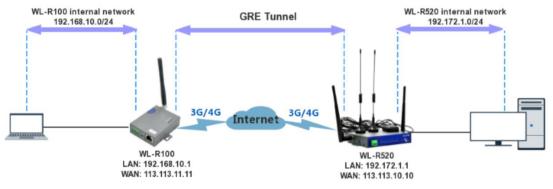


c Network	- Aller	menoso zwale su da na							
	On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
N	On	-	any/0	any/0	-	-	-	Drop	
nced Network	On	-	any/0	192.168.1.0/24	-	-	-	Accept	
vall	On	50:7B:9D:C3:9A:22	any/0	any/0	-	-	-	Accept	
/URL Filtering	On	60:F1:89:20:F0:9A	any/0	any/0	-	-	-	Accept	
main Filtering	On	00:1E:64:DF:E8:46	any/0	any/0	-	-	-	Accept	
Tunnel					NONE V			Acc 🔻	
nistration									
	Or @	CH REPORT A CONSTRUCTION			Descriptio	on			
	×.				Descriptio	on			
	■ UR	L Filtering							
	×.	L Filtering			Descriptio				
	UR Or	L Filtering							
		L Filtering URL URL CESS Filtering Src MAC	Src IP any/0 any/0	Dst IP any/0 any/0			Dst Port -	Policy Drop Accept	

## 4.5 VPN Tunnel

## 4.5.1 GRE

#### GRE Tunnel between WL-R100 and WL-R520





## 1) WL-R100 Config

1.1) Navigate to Basic Network > LAN



Status	LAN		Router
Basic Network			
WAN	Router IP Address	192.168.10.1	
Cellular	Subnet Mask	255.255.255.0	
LAN	DHCP Server	2	
DDNS	IP Pool	192.168.10.2 - 192.168.10.53 (52)	
Routing	Lease	1440 (minutes)	
WLAN	Use internal DNS	<ul> <li>✓</li> <li>✓</li> </ul>	
Advanced Network	ose internal ons		
Firewall			
VPN Tunnel			
Administration			
Debugging			
Logout			

Save Cancel

## 1.2) Navigate to **VPN Tunnel > GRE**

Status	GR	E Tu	innel							Router
Basic Network	On	IDX	▲ Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Descript	tion
WLAN	On		192.168.10.10	113.113.11.11	113.111.10.10	On	10	5	test	
Advanced Network						0				
Firewall										Add
VPN Tunnel	CD	<b>F D</b>								
GRE	GR	ER	oute							
OpenVPN Client	On	Tunn	el Index 🔹	Destination Address		Description				
PPTP/L2TP Client	On	1	•	192.172.1.0/24		test				
IPSec										Add
Administration										
Debugging										
Logout										

Save Cancel

## 2) WL-520 Config

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

Status	LAN		Router
Basic Network			
WAN	Router IP Address 1	192.172.1.1	
Cellular	Subnet Mask 1	255.255.255.0	
LAN	Router IP Address 2	0.0.0.0	
DDNS	Subnet Mask 2	0.0.0.0	
Routing	Router IP Address 3	0.0.0.0	
/LAN	Subnet Mask 3	0.0.0.0	
dvanced Network	Router IP Address 4	0.0.0.0	
rewall	Subnet Mask 4	0.0.0.0	
PN Tunnel	DHCP Server	e.e.e.e	
dministration			
ebugging	IP Pool	192.172.1.2 - 192.172.1.51 (50)	
ogout	Lease	1440 (minutes)	
oyour	Use internal DNS	8	
			Save Cancel

2.2) Navigate to VPN Tunnel > GRE



Basic Network	On	IDX	A Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Descri	otion
VLAN	On	1	192.172.1.10	113.111.10.101	113.113.11.11	On	10	5	test	
dvanced Network										
irewall										Add
'PN Tunnel		1000000000	and the second							
GRE	GR	E R	oute							
OpenVPN Client	On	Tunn	el Index	Destination Address		Description				
PPTP/L2TP Client	On Ø	1		192.168.10.0/24		test				
IPSec		1	*							Add
dministration										
Debugging										
ogout										

# 4.5.2 OpenVPN

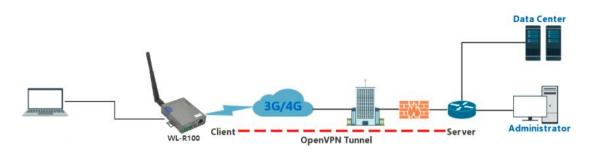


Figure 4-7-2 OpenVPN Network topology

## 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	OpenVPN Client					
Basic Network	Client 1	Client 2				
WLAN	Basic	Advanced	Keys	Status		
Advanced Network						
Firewall	Start with WAN					
/PN Tunnel	Interface Type	TUN ¥				
GRE	Protocol	UDP T				
OpenVPN Client	Server Address/Port				1194	
PPTP/L2TP Client	Firewall	Automatic V			1.525.0	
IPSec	Authorization Mode	TLS V				
dministration		11.5				
ebugging	Username/Password Authentication	0				
ogout	HMAC authorization	Disabled	¥			
n Seacour	Create NAT on tunnel	Routes must b	e configured manually.			
	Start Now					
					Save	Cance



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	<b>OpenVPN</b> Client		Router
Basic Network	Client 1 Cli	ient 2	
WLAN		Advanced Keys Status	
Advanced Network			
Firewall	Poll Interval	0 (in minutes, 0 to disable)	
VPN Tunnel	Redirect Internet traffic	8	
GRE	Accept DNS	Disabled <b>T</b>	
OpenVPN Client	configuration	Disabled	
PPTP/L2TP Client	Encryption cipher	Use Default	
IPSec	Compression	Adaptive 🔻	
Administration	TLS Renegotiation Time	-1 (in seconds, -1 for default)	
Debugging	Connection retry	30 (in seconds; -1 for infinite)	
Logout	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.



1	<ul><li>ペレーII ペレー 深圳市徳</li></ul>	传物联技术有限公司 WL-R100 Series Router User Manual
	TLS Renegotiation Time	TLS negotiation time1 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

Status	OpenVPN Client	Router
Basic Network		
WLAN	Client 1 Client 2	
Advanced Network	Basic Advanced Keys Status	
Firewall	For help generating keys, refer to the OpenVPN HOWTO.	
VPN Tunnel		
GRE		
OpenVPN Client		
PPTP/L2TP Client	Certificate Authority	
IPSec		Ŧ
Administration		11
Debugging		
Logout	Client Certificate	*
	Client Key	•
	Start Now	

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



Status	OpenVPN Clie	ent				Router
Basic Network	A CONTRACTOR OF					
WLAN	Client 1 Basic	Client 2 Advanced	Keys	Status		
Advanced Network						
Firewall	Client is not running or	status could not be read.				
VPN Tunnel	Start Now					Refresh Status
GRE	Start NOW					
OpenVPN Client						
PPTP/L2TP Client						
IPSec						
Administration						
Debugging						
Logout						
					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.



#### 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)

← → C Secure | https://openvpn.net/release/

## Index of /release

Name	Last modified	Size Description
Parent Directory		-
1zo-1.08-3.0.el2.dag.i386.rpm	21-Feb-2012 00:50	55K
1zo-1.08-3.0.rh7.dag.i386.rpm	21-Feb-2012 00:50	54K
1zo-1.08-3.0.rh8.dag.i386.rpm	21-Feb-2012 00:50	58K
2 1zo-1.08-4.0.rh9.rf.i386.rpm	21-Feb-2012 00:50	59K
2 lzo-1.08-4.1.el3.rf.i386.rpm	21-Feb-2012 00:50	58K
1zo-1.08-4.1.el3.rf.x86_64.rpm	21-Feb-2012 00:50	55K
2 1zo-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 <u>http://openvpn.net</u> for more information)



PENVPIN a	hoose Components hoose which features of OpenVPN 2.3.0-I001 you want hstall.	to
Select the components to insta service if it is running. All DLLs	II/upgrade. Stop any OpenVPN processes or the OpenV are installed locally.	PN
Select components to install:	OpenVPN File Associations     OpenSSL Utilities	1 ^
	OpenVPN RSA Certificate Management Scripts     Add OpenVPN to PATH     Add Shortcuts to Start Menu	
		-
Space required: 4.4MB	Description Position your mouse over a component to see its description.	
	Soon prom	
Iulisoft Install System v2.46-101		

PC

lame	Date modified	Туре	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	lcon	22 KB
Uninstall.exe	2019-01-10 11:42	Application	117 KB
·		11	

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

#### Shenzhen Wlink Technology Co., LTD 深圳市徳传物联技术有限公司

#### WL-R100 Series Router User Manual

lame	Date modified	Туре	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/keys4.1) Client certificate (Generated on the server)

Name	Date modified	Туре	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

Name	Date modified	Туре		
Tiny (0 - 10 KB) (15)				
01.pem	2019-01-10 12:01	PEM File		
02.pem	2019-01-10 12:04	PEM File	us OpenVPN	Client
🙀 ca.crt	2019-01-10 11:57	Security Certificate	c Network Client 1	Client 2
a.key	2019-01-10 11:57	KEY File	anced Network Basic	Advanced Keys Status
🗔 client.crt	2019-01 10 12:04	Security Certificate	wall	
] client.csr	2019-01-10 12:04	COR File	Tunnel For help generating ke	eys, refer to the OpenVPN HOWTO.
] client.key	2019-01-10 12:04	KEY File	RE	BEGIN CERTIFICATE
dh1024.pem	2019-01-10 12:02	PEM File	penvi	MIIDsjCCAxugAwIBAgIJAIa+M9jXuMF6MA0GCSqGSIb3DQEBB
index.txt	2019-01-10 12:04	Text Document	TP/L2TP Client	VQQGEwJDTjELMAkGA1UECBMCR0QxCzAJBgNVBAcTAlNaMRM UGxheWVyMQ4wDAYDVQQLEwVhZG1pbjETMBEGA1UEAxQKT
index.txt.attr	2019-01-10 12:04	ATTRACT	Sec	A1UEKRMKQ29kZVBsYXllcjEgMB4GCSqGSIb3DQEJARYRYWRta b20wHhcNMTkwMTEwMDM1NzM1WhcNMjkwMTA3MDM1NzM1
📄 serial	2019-01-10 12:04	File	inistration	Q04xCzAJBqNVBAqTAkdEMQswCQYDVQQHEwJTWjETMBEGA1
🙀 server.crt	2019-01-10 12-01	Security Certificate	ing	CIEDMAWGA1UECXMFYWRtaW4xEzARBgNVBAMUCk9wZW5WL
server.csr	2019-01-10 12:01	SR File		Certificate: Data:
server.key	2019-01-10 12:01	KEY FILL	xut	Version: 3 (0x2)
ta.key	2019-01-10 12:04	KEY File	Client Certifica	Issuer: C=CN, ST=GD, L=SZ, O=CodePlayer, OU=admir
				CN=OpenVPN_CA/name=CodePlayer/emailAddress=admin@3 Validity
				BEGIN PRIVATE KEY MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwggJdAgEAAoGB
			Client Key	JATHshtMULVml/g9WZC4InKIImitBGID232mrHbBOKBDSMmhNl fqoIGYxoXSITsaZqdIZfyzc80qZq1jcbStHbBVK0orGjEbIIKR9Rw Ju0Nsty/f31++zKIHSPdSarXmylbAgMBAAECgYEAgrukQ3Vorye
				V081UR2yRzpqvNu39nd8ruxA10MiHILUvM/ZBLMhxPedJZRK bTq6uRT90wkCrV1xK27/zTTKzjSymZBAiOPbw18ItDScaarA49Q UyexLQAHP1IqML3oeECQQDgMuCb61qV/12xh7TV67UbP0264
			Start Now	



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

Status	OpenVPN Client		
Basic Network Advanced Network Firewall VPN Tunnel	Client 1 Client 2 Basic Advanced Data current as of Thu Jan 10 15:07:1	Keys Status	
GRE	General Statistics		an Telnet 192.168.1.1
Oper/VPN Client PPTP/U2TP Client IPSec Administration Debugging Logout	Stop Now	Name         Value           TUN/TAP with bytes         0           TUN/TAP with bytes         0106166           TCP/UDP read bytes         106186           TCP/UDP read bytes         37999           Auth read bytes         57636           pre-compress bytes         0           pre-decompress bytes         0           pre-decompress bytes         16638           post-decompress bytes         19330	64 bytes from 10.0.8.1: seq=79 tt1=126 time=492.024 ms 64 bytes from 10.0.8.1: seq=80 tt1=126 time=52.058 ms 64 bytes from 10.0.8.1: seq=81 tt1=126 time=386.797 ms 64 bytes from 10.0.8.1: seq=82 tt1=126 time=471.722 ms 64 bytes from 10.0.8.1: seq=83 tt1=126 time=511.801 ms 64 bytes from 10.0.8.1: seq=84 tt1=126 time=511.801 ms 64 bytes from 10.0.8.1: seq=86 tt1=126 time=76.989 ms 64 bytes from 10.0.8.1: seq=88 tt1=126 time=761.989 ms 64 bytes from 10.0.8.1: seq=88 tt1=126 time=491.682 ms 64 bytes from 10.0.8.1: seq=81 tt1=126 time=491.682 ms 64 bytes from 10.0.8.1: seq=81 tt1=126 time=39.470 ms 64 bytes from 10.0.8.1: seq=91 tt1=126 time=517.1811 ms 64 bytes from 10.0.8.1: seq=92 tt1=126 time=517.1811 ms 64 bytes from 10.0.8.1: seq=91 tt1=126 time=517.1811 ms

## 4.5.3 L2TP/PPTP

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

asic Network											Default		
/LAN		Protocol	Name	Server			Usern	50005KA - 51	assword	Firewall	Route	Local IP	
dvanced Network		PPTP	3	wlinktech	h.com.cn		test12	!3 te	est123	On		_	
rewall		L2TP 1	·										
PN Tunnel													Add
GRE													
OpenVPN Client	L21	<b>FP</b> Advar	nced										
PPTP/L2TP Client	0	Name	Accept DNS	MTU	MRU	Tunnel	Auth	Tunnel Pa	anword	Custom O	ntiona		
IPSec		Name	NO NO		MRU	Tunner		Turmer Pa	ISSWOLD	Custom O	puons		
ministration	<u>e</u>		NO										
bugging													Ade
gout	PP'		Accent DNS	MTU	MRU	MPPE	MPP	F Stateful	Custom	Intions			
gout	On 4	Name	Accept DNS	MTU	MRU	MPPE	MPP	E Stateful	Custom C		iro mono 1	120	
gout.	On A	Name	NO	1440	MRU 1440	On	MPPI			Options ipdefault;requ	ire-mppe-1	128	
gout.	On 4	Name		1440			MPPI	E Stateful			ire-mppe-1	128	
gout	On A	Name	NO	1440		On	MPPI				ire-mppe-1	128	Ade
	On A On	Name	NO	1440		On	MPPI				ire-mppe-1	128	Ad
yur.	on ₄ On ℱ	Name 3 HEDULE	NO NO V	1440		On					ire-mppe-1	128	Ade
	On ▲ On SCI	Name 3	NO	Policy	1440	On					ire-mppe-1	128	Ad
yur.	on ₄ On ℱ	Name 3 HEDULE	NO NO V	1440	1440	On					ire-mppe-1	128	
	On ▲ On SCI	Name 3 HEDULE	NO NO V	Policy	1440	On					ire-mppe-1	128	Ado

Note: The Custom Options based on your server

## Configured test case: L2TP



On 🕑	L2TP	2	and the second second second			Username	rat	sword	Firewall	Route	Local IP	
	1000000000		wlinkteck	h.com.cn		test123	tes	123	On	Route		
	L2TP V		T			1			0	8		
												Ado
1.21	D Advar	cod										
121	P Auvai	lceu										
		Accept DNS	MTU	MRU			nel Pas	sword	Custom O	ptions		
	2	NO	1440	1440					debug			
		NO V										
												Add
On 🔺	Name	Accept DNS	MTU	MRU	MPPE	MPPE St	ateful	Custom	Options			
		NO T	,									
												Ado
SCI	HEDULE											
		Name 2	Deliana		Description							
0- 1		Name z	Policy		Description							
On A	- Hame I		FATLON									
On A			FAILOV	ER 🔻								Ado
		On ▲ Name On 2 PPTP Advar On ▲ Name	On         2         NO           Image: Constraint of the second se	On ▲ Name         Accept DNS         MTU           On 2         NO         1440           Image: Constraint of the second	On ▲ Name         Accept DNS         MTU         MRU           On 2         NO         1440         1440           Image: Constraint of the state of	On ▲ Name         Accept DNS         MTU         MRU         Tunnel.           On 2         NO         1440         1440         On           Image: Second	On ▲ Name         Accept DNS         MTU         MRU         Tunnel Auth         Tun           On 2         NO         1440         1440         On           Image: Second Se	On ▲ Name     Accept DNS     MTU     MRU     Tunnel Auth     Tunnel Past       On 2     NO     1440     1440     On         PPTP Advanced       On ▲ Name     Accept DNS     MTU     MRU     MPPE       MO     ▼     □     □	On ▲ Name     Accept DNS     MTU     MRU     Tunnel Auth     Tunnel Password       On 2     NO     1440     1440     On         PPTP Advanced       On ▲ Name     Accept DNS     MTU     MRU     MPPE       MO     ▼     □	On ▲ Name     Accept DNS     MTU     MRU     Tunnel Auth     Tunnel Password     Custom O       On 2     NO     1440     0n     debug       Image: State of the state	On ▲ Name     Accept DNS     MTU     MRU     Tunnel Auth     Tunnel Password     Custom Options       On 2     NO     1440     1440     On     debug         PPTP Advanced       Image: Model of the state	On ▲ Name     Accept DNS     MTU     MRU     Tunnel Auth     Tunnel Password     Custom Options       On 2     NO     1440     On     debug         Image: PPTP Advanced   On ▲ Name       Accept DNS     MTU     MRU     MPPE     MPPE Stateful     Custom Options

Note: The Custom Options based on your server

Step 2 Please click "Save" icon

#### **VPN Status**

Status	VPN Status		
Overview			
VPN	VPN Name	1	
LAN	VPN Protocol	L2TP	
Device List	Local IP	172.1.1.18	
Basic Network	Peer IP	172.1.1.1	
Advanced Network			
Firewall			
VPN Tunnel			
Administration			
Debugging			
Logout			



# 4.5.4 IPSec

IPSec between WLINK and Cisco Router

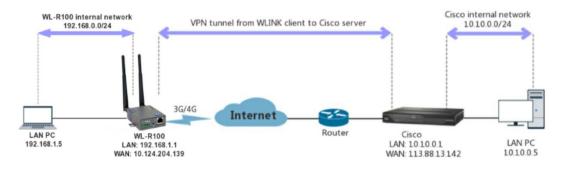


Figure 4-7-4 IPSec Network topology

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

ļ

2.1) Navigate to VPN Tunnel > IPSec > Group Setup

Status	IPSEC				Router
Basic Network	IPSEC 1	SEC 2	SCHDULE		
WLAN		Basic Setup	Advanced S	Tabia	
Advanced Network	Group Setup	sasic setup	Auvanceu 5	semb	
Firewall	Enable IPSec	•			
VPN Tunnel	IPSec Extensions	a second	*		
GRE	IPSec Extensions	Normal			
OpenVPN Client	Local Security Gateway Interface	3G Cellular	*		
PPTP/L2TP Client		1			
IPSec	Local Security Group Subnet/Netmask	192.168.1.0	/24	ex. 192.168.1.0/24	
Administration	Local Security	-			
Debugging	Firewalling	•			
Logout	Remote Security Gateway IP/Domain	113.88.13.1	42		
	Remote Security Group Subnet/Netmask	10.10.0.0/2	1	ex. 192.168.88.0/24	
	Remote Security Firewalling	2			
					Save Cancel



### 2.2) Navigate to VPN Tunnel > IPSec > Basic Setup

Status	IPSEC	Router	
Basic Network	IPSEC 1 IP	SEC.2 SCHDULE	
WLAN		asic Setup Advanced Setup	
Advanced Network	or oup occup	and Solup	
Firewall	Keying Mode	IKE with Preshared Key V	
VPN Tunnel	Phase 1 DH Group	Group 2 - modp1024 V	
GRE			
OpenVPN Client	Phase 1 Encryption	3DES (168-bit) • IKE SA	
PPTP/L2TP Client	Phase 1 Authentication	MD5 HMAC (96-bit)	
IPSec	Phase 1 SA Life Time	28800 seconds	
Administration			
Debugging	Phase 2 DH Group	Group 2 - modp1024 🔻	
Logout	Phase 2 Encryption	3DES (168-bit) 🔹	
	Phase 2 Authentication	SHA1 HMAC (96-bit)    IPSec SA	
	Phase 2 SA Life Time	3600 seconds	
	Preshared Key		

Save Cancel

2.3) Navigate to VPN Tunnel > IPSec > Advanced Setup

Status	IPSEC		Route
Basic Network	IPSEC 1	IPSEC 2	SCHDULE
WLAN	Group Setup	Basic Setup	Advanced Setup
Advanced Network	Group Setup	basic setup	Auvanceu Setup
Firewall	Aggressive Mode		
VPN Tunnel		_	
GRE	Compress(IP Payload Compression)		
OpenVPN Client	Dead Peer	_	
PPTP/L2TP Client	Detection(DPD)		
IPSec	ICMP Check	4	
Administration	Check Period Time	1	have a
Debugging	Interval	10	seconds
Logout	Check Timeout Count	3	Times
	Check IP	10.10.0.1	
	IPSec Custom Options 1	rightid=%a	sny
	IPSec Custom Options 2		
	IPSec Custom Options 3		
	IPSec Custom Options 4	1	

## 2.4) Status

VPN Status		
IPSec 1	Enable	
Phase 1 Status	73 seconds	
Phase 1 IKE	3DE5_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024	
Phase 2 Status	TUNNEL	
Phase 2 ESP	3DE5_CBC/HMAC_SHA1_96	
IPSec Recv.	420 Bytes	
IPSec Send.	680 Bytes	

--End