

MLINK

User Manual

---Apply to WL-G930 Series Industrial 5G Router

V1.0 http://www.wlink-tech.com June, 2020

Contents

1.1	1
<i>1</i> Hardware Installation	4
1.1 Panel	4
1.2 LED Status	5
1.3 Dimension	6
1.4 How to Install	6
2 Router Configuration	
2.1 Local Configure	8
2.2 Status	9
2.3 Tool Column	11
2.4 Basic Network	
2.5 WLAN Setting	22
2.6 Advanced Network Setting	25
2.7 Firewall	
2.8 VPN Tunnel	
2.9 Administration	
2.10 "Reset" Button for Restore Factory Setting	
3 Configuration Instance	
3.1 Port Forwarding	
3.2 IP Passthrough	63

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

3.3 Captive Portal	65
3.4 GPS Settings	68



1 Hardware Installation

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

1.1 Panel

WLINK Tech. G930 series \bigcirc 5G Wi-Fi 5G Wi-Fi 2.4G Wi-Fi 2.4G Wi-Fi \bigcirc \bigcirc \bigcirc \bigcirc ()Front 0 0 0 0 0 0 0 0 0 0 0 4 3 2 1 0 NET1 NET2 WLAN PWR WTD 10 70 \bigcirc \bigcirc SIM1 SIM2 \bigcirc 5G-5 5G-4 5G-3 5G-2 5G-1 5G-6 GPS \bigcirc \bigcirc \bigcirc Back USB LANO LAN1 LAN2 LAN3 LAN4 V+ v-DC \bigcirc \bigcirc

Table 1-1 WL-G930 Structure

NOTE

There are some difference on Antenna interface and indicator light for the device with extended Wi-Fi, GPS features.

Port	Instruction	Remark
USIM	Plug type SIM Slot, support 1.8/3V/5V automatic detection.	
Main	5G-1~5G-6 antenna, SMA connector, 50Ω .	
GPS	GPS antenna, SMA connector, 50Ω.	Optional

Table 1-2 Router Interface



WL-G930 Series Router User Manual

Port	Instruction	Remark
Wi-Fi	2.4G Wi-Fi, 5G Wi-Fi. dual-band antennas, RP-SMA connector	
LAN0~LAN4	10/100/1000Base-TX, MDI/MDIX self-adaption.	
Reset	Reset button, (press on button at least 5 seconds)	
PWR	Power connector	7.5~32VDC
Power Interface	1xDC, 1x 4Pins	
Terminal Block	2xD1, 1xDO, 1xRS232,1xRS485	
USB	USB Host Port	

1.2 LED Status

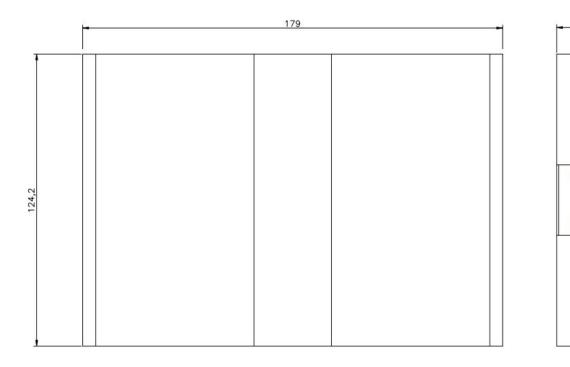
|--|

silk-screen	Indicator		Note			
	Color	Green	Good Signal			
	COIOI	Red	Poor Signal			
NET		Quick Blinking (0.5s)	Offline			
	Status	Slow Blinking (1.5s)	5G Dialing			
		Solid light	5G online			
PWR	Constant Light		System power operation.			
	Constant li	ght	WLAN enable, but no data communication.			
WLAN	Blinking qu	ickly	Data in transmitting			
	Light off		WLAN disable			
WTD	Slow Blinking(1s)		Serial port and IO indication			
Green		Constant light	Connected.			
LAN	Green Blinking		Data in transmitting.			
	Green	Light off	Disconnection.			



43

1.3 Dimension





1.4 How to Install

1.4.1 SIM/UIM card install

Please insert the dual SIM cards before configure the router.



O CAUTION Before connecting, please disconnect any power resource of router



1.4.2 Ethernet Cable Connection

Connect the router with a computer by an Ethernet cable for GUI configuration, or transit by a switch.

1.4.3 5G and Wi-Fi Antenna Plug

Connect the two magnetic 5G antennas to 5G-1 to 5G-6 interfaces, and the four paddle shape Wi-Fi antennas to Wi-Fi interfaces.

NOTE

Wi-Fi antenna supports dual-band 2.4G and 5G band.

1.4.6 Power Supply

Voltage input range: +7.5~32VDC. (Extended models: 7.5~ 48VDC)

1.4.7 Review

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

CAUTION

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

Notice:

Step 1 Check the antenna connection.

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

----END





WL-G930 Series routers support GUI and CLI configuration. This chapter introduce GUI configuration via Ethernet port, if need CLI configuration guide, please contact our technical support department by email: support@wlink-tech.com.

2.1 Local Configure

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

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



Figure 2-1 Network Connection

- Step 2 Obtain a IP address automatically or set up IP address,192.168.1.xxx(XXX can be any number between 2~254)
- Step 3 Run an Internet Explorer and visit "<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 19	2.168.8.1 ? 🔀
R	GR
<u>U</u> ser name: <u>P</u> assword:	🖸 admin 🔛
	Remember my password

Figure 2-2 User Identify Interface

----END

2.2 Status

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

You haven't changed the default password for this router. To change router password click here.

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

Already changed login password successfully.

2.2.1 Overview

The overview GUI will be display router system information, Ethernet ports status, VPN connection status, LAN information, 5G connection information and WLAN information,

Status Overview	~	System				~	Cellular		¢	~
Traffic Stats.		Router Name	R	louter			Connection Type	ECM/QMI		
Device List		Hardware Version	c	C11-D20			Modem IMEI	864284040039005		
Basic Network	3	Firmware Version	G	59.0.1.5			Modem Status	Ready		
P Basic Network		Router Sn	1	120G9220081	40005		Cellular ISP	"CHINA MOBILE"		
8 WLAN	2	Chipset	N	/ediaTek MT7	521 SoC		Cellular Network	(5G NR/NG)		
Advanced Network							USIM Status	Ready		
		Router Time	F	ri, 14 Aug 202	0 16:40:55 +08	00	CSQ	291		
Firewall		Uptime	0	0:05:23			IP Address	10.32.208.202		
VPN Tunnel	>	Memory Usage	2	5.69 MB / 503.	36 MB (5.10%)		Subnet Mask	255.255.255.252		
		NVRAM Usage	1	9.22 KB / 64.00	кв (30.04%)		Gateway	10.32.208.201		
Administration	*						DNS	120.196.165.7 221.179.38.7		
							Connection Statu	is Connected		
							Connection Uptir	me 00:03:41		
		Ethernet Ports St	tatus			~				
		LAN0	LAN1	LAN2	LAN3	LAN4	LAN		\$	~
			1	1	1	1	LAN		Ŷ	^
(i) More Info		UP U	Inplugged	Unplugged	Unplugged	Unplugged	Wireless (5 Gł	Hz)	\$	~

Figure 2-3 Router Status GUI

2.2.2 Traffic Stats.

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

Status	~		Already changed login password	d successfully.
Overview			, , , , , ,	
Traffic Stats.		Traffic Stats.		
Device List				
Basic Network	•	Interface	Transmit Data	R
ବି WLAN	•	Cellular(usb0)	95.67 KB	1
Advanced Network	•			
3 Firewall	\$ 0			
VPN Tunnel				
Administration				



2.2.3 Device List

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

Status	~			Already cl	nanged login	password succe	ssfully.			
Overview Traffic Stats.		Device Lis	t							
Device List										
Basic Network	•	Interface	MAC Address	IP Address 个	Name	RSSI	Quality	TX/RX Rate	Lease	
常 WLAN	•	br0	54:E1:AD:C3:99:8B	192.168.1.2			ā.			
Advanced Net	work									
🔞 Firewall	•							~	3 seconds	
💷 VPN Tunnel	2									
R Administration	n 🔶									



Figure 2-5 Device List GUI

2.3 Tool Column

Tools 🛠	Bandwidth 👱	IP Traffic 📶	System 🏚		
		Figure 2-6 Too	ol Column GUI		

2.3.2 **Tools**

2.3.2.1 Ping

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

	OL 🖿 Log 🔒 🤇	Capture					
Ping							
IP Address	8.8.8.8		Ping				
Ping Count	5						
Packet Size	56	(bytes)					
Seq Address				RX Bytes	TTL	RTT (ms)	+/- (ms)

2.3.2.2 Trace

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

IP Address		Trace	
Maximum Hops	20		
Maximum Wait Time	3	(seconds per hop)	

2.3.2.3 WOL



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

Ø [®] Ping Ø [∧] Trace ^I [™] ₂₀ WOL ^I	🖿 Log 🔒 Capture		
Wake On Lan			
MAC Address	IP Address	Status	Name 🔨
54:E1:AD:C3:99:8B	192.168.1.2	Active (In ARP)	
Click to wake up MAC Address List			
Wake Up 🔨			Refresh C

2.3.2.4 Log

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

🔊 Ping	n Trace	🔛 WOL	Log	Capture		
Logs View						
View						
Download	d Log File					
				FindQ		
» Logging) Configuration	on				

2.3.2.5 Capture

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

🔊 Ping	n Trace	😨 WOL	Log	Captur	e
Capture					
Time1			15	minutes 🔻	Start
Network			LA	N .	

2.3.3 Bandwidth

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



eal Time Bandw	idth (
Cellular (usb0)	LAN (br0)	LAN (eth0)	LAN (vlan) WAN (vlan2)	Wi-Fi/2.4G (eth1)	Wi-Fi/5G (eth2)	n 05:03 pm / 12942.27 mbit/s (16	17.78 MB/c)
^12885.00 mbit/s 咢	(1610.63 MB/s)					TVU	10000 pm7 1294227 mbl95 [10	17.76 WID/S
 (v) 12885.00 mbit/s 12885.00 mbit/s 8590.00 mbit/s 4295.00 mbit/s 	(1073.75 MB/s)				Π			
4295.00 mbit/s ((536.88 MB/s)							
10 minute windov	v, 2 second inte	erval)						
RX + 14.24 kbit (1.74 KB/s				54 mbit/s 5 MB/s)	Peak	17179.21 mbit/s (2047.92 MB/s)	Total	8,192.2 MB
10.85 kbit (1.32 KB/s				53 mbit/s i5 MB/s)	Peak	17179.39 mbit/s (2047.94 MB/s)	Total	8,192. MB

2.3.4 System

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

Reboot 🗘	Hardware Reboot ୯
	Logout 🔂

2.4 Basic Network

2.4.1 WAN Setting

Step 1 Basic Network>WAN to enter below interface.

۲	Status	>
Ø	Basic Network	
	WAN	
	Cellular	
	LAN VLAN	
	Schedule	
	DDNS Routing	
\$	WLAN	
A	Advanced Network	
2	Firewall	
۹	VPN Tunnel	
Я	Administration	



Table 2-1 WAN Setting Instruction

Parameter	Instruction
Туре	Support DHCP, PPPoE, Static IP address

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

----End

2.4.2 Cellular Setting

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

Status	Cellular Settings	
😟 Basic Network 🛛 🛩		_
WAN	Enable Modem	
Cellular		
LAN	Basic Settings SIM 1 SIM 2	
VLAN Schedule	Use PPP	
DDNS		
Routing	ICMP Check	
ŵ WLAN →	Cellular Traffic Check	
Advanced Network >	CIMI Send to	:
Ø Firewall →	SMS Code	
VPN Tunnel Administration	Operator Lock	ex:46001
	DualSim Mode	Fail Over 💌
	Save ✓ Cancel ×	
 More Info 		
Basic Settings SIM 1	SIM 2	
SIM 1 Mode	Auto	π
SIM 1 PIN Code		
SIM 1 APN	3GNET	
SIM 1 User	CARD	
SIM 1 Password		
SIM 1 Dial Number	*99#	
CIA 1 April 7	Auto	*
SIM 1 Auth Type	Auto	
SIM 1 Local IP Address		



Table 2-	2 WAN Setting Instruction
Parameter	Instruction
Enable Modem	Enable/Disable 5G mode.
Use PPP	ECM dialup as default. PPP optional.
ICMP check	If enable ICMP check and setup a reachable IP address as destination IP, the router will reconnect/reboot once ICMP check failed.
Cellular Traffic Check	The router will reconnect/reboot once there's no Rx/Tx data.
CIMI Send to	Send CIMI to a defined IP and port by TCP protocol.
SMS Code	Remote control the router by SMS. Only the configured SMS code will work.
Operator Lock	Lock a specified operator for the router by MCC/MNC code.
Dual SIM Mode	【Fail Over】Two SIM cards mutual backup. Once SIM1 failed, it'll switch to SIM2 and work on SIM2, and vice versa.
	【SIM1 Only】Only SIM1 works.
	【SIM2 Only】Only SIM2 works.
	【Backup】 SIM1 is the primary SIM. Once SIM1 failed, it'll switch
	to SIM2 and work on SIM2 for a specified period of time, then it
	switches back to SIM1.
Connect Mode	【Auto】The router will automatically connect to 3G/5G networks and give priority to 5G.
	[LTE] Router will connect to 5G only.
	[3G] Router will connect to 3G only.
Pin Code	Some SIM cards are locked with a Personal Identification Number (PIN) code in case they are lost or stolen.
APN	APN is provided by local ISP, usually CDMA/EVDO networks do not need this parameter.
User	SIM card user name is provided by ISP
Password	SIM card password is provided by ISP
Auth. Type	Auto/PAP/Chap/MS-Chap/MS-Chapv2 authentication optional.
SIM Local IP Address	Fix SIM IP. The feature is available if carrier can provide this service.

NOTE ICMP Check and Cellular Traffic Check are alternative.



[ICMP Check]

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

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

ICMP Check		
Check IP	8.8.8.8	
Check IP (Optional)	4.4.4.4	
Interval	60	(seconds)
Retries	3	(Times)
Fail Action	Reboot	: System 🔻

【Cellular Traffic Check】

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

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

Cellular Traffic Check	×	
Check Mode	Rx v	
Check Interval	10	(minutes)Range: 1 ~ 1440
Fail Action	Cellular Reco	nnect 🔻

Step 2 After Setting, please click "save" icon.

----End

2.4.3 LAN Setting

Step 1 Basic Network>LAN to enter below interface

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

WL-G930 Series Router User Manual

	•		Alrea	ay changed login pus.	sword successfully		
Basic Network	*						
WAN		LAN					
Cellular		Bridge ^	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minute
LAN		br0	192.168.1.1	255.255.255.0	~	192.168.1.2 - 51	1440
VLAN Schedule							
DDNS		1	T				
Routing							
F WLAN	•	Add+					
Advanced Network	•						
Firewall	>	Save ✓ Cancel ×					
VPN Tunnel	3 5						
Administration	,						
O More Info LAN							
 More Info 		IP Address	Subnet Mask	DHCP	Server	IP Pool	Lease(minu
O More Info LAN		IP Address 192.168.1.1	Subnet Mask 255.255.255.0		Server /	IP Pool 192.168.1.2 - 51	Lease(minu 1440
() More Info LAN Bridge 4		192.168.1.1			/		

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

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

----End

2.4.4 **VLAN**

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

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

1	~	Tagged ×	LAN 2	Tagged ×	LAN 3	Tagged ×	LAN 4	Tagged	WAN	Tagged ×	Bridge br0
2	×	×	×	×	×	×	×	×	×	×	WAN
		_									
v											none

Table 2-4 LAN Setting Instruction

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

Step 2 Please Click "Save" to finish.

----End

2.4.5 Schedule

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

Status	>	Enabled Link	s								1
Basic Network	~	Link Name			Link	Туре			Description		
WAN Cellular		modem			ECM/	/QMI					
LAN											
VLAN		ICMP Check									3
Schedule							9 mg			-	
DDNS		On Link		Des	tination	li	iterval	Ret	ries	Description	
Routing		Image: A state of the state									
ଚ୍ଚି WLAN	>										
Advanced Network	6 ×	Add+									
3 Firewall	>										
VPN Tunnel	•	Schedule									
R Administration	•)	On L	.ink 1		Link 2		Policy		Description		
			modem	٣	modem	٣	FAILOVER	*			
 More Info 		Add+									

Parameters	Instruction
modem	The router dial-up to network via modem



	深圳市德传物联技术有限公司	WL-G930 Series Router User Manual
wan	The router dial-up to network via \	WAN (DHCP, PPPOE, Static IP) port.
ICMP Check	When the ICMP Check fails, the	switching action between Link1 and
	Link2 will be triggered.	
Link1	The Primary link	
Link2	The Secondary link	
BACKUP		ink1 is the primary link. Once Link1 is ork on Link2. Once Link1 recovers, it
FAILOVER	Link1 is the primary link, Link2 is t	the backup link. Once Link1 is failed, it
	will switch to Link2 and work on Li	ink2.

Link Name	Link Type		Description		
modem	ECM/QMI				
wan	WAN(STATIC)				
ICMP Check					~
On Link	Destination	Interval	Retries	Description	
✓ wan	8.8.8.8	10	5		
Add +					
Schedule					~
On Link 1	Link 2	Policy	Description		
wan	• modem	▼ FAILOVER	• wan as primary and m	nodem as secondary	
Add +					



The VLAN should be configured with WAN and 5G backup together. Please define WAN port as bridge WAN interface in the VLAN GUI as below.

ML		Shenzhen Wlink Technology Co., LTD 深圳市德传物联技术有限公司						WL-G930 Series Router User Ma						
Status	•					Already	changed loo	gin password	d successful	ly.				
Basic Network	*	VLAN												~
Cellular		VID /	A LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge	
VLAN		1	~	×	~	×	~	×	~	×	×	×	br0	_
Schedule DDNS		2	×	×	×	×	×	×	×	×	~	×	WAN	
Routing		0	•										none	٣
WLAN	•	Add +												
Advanced Network	•		-											
🐻 Firewall	•	Save√	Cancel ×											
VPN Tunnel	•													
R Administration	•													

Step 2 Please Click "Save" to finish.

----End

2.4.6 **Dynamic DNS Setting**

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

C Status		Already changed login password successfully.	
Basic Network WAN	×	Dynamic DNS	~
Cellular LAN		IP Address Use WAN IP Address 0.0.0.0 (recommended)	
VLAN Schedule		Auto refresh every 28 minutes (0 = Disabled)	
DDNS			
Routing		Dynamic DNS1	~
WLAN	•)	Service None *	
Advanced Network	•		
🐼 Firewall	•		
VPN Tunnel	•	Dynamic DNS2	~
R Administration	•	Service None •	
 More Info 		Save ✓ Cancel ×	
Dynamic DNS			~
non 🕊 name deserves de la construction de			
IP Address		Use WAN IP Address 0.0.0.0 (recommended) *	
Auto refresh ever	ry	28 minutes (0 = Disabled)	
Dynamic DNS1			~
Service		None 🔻	
Dynamic DNS2			~
Service		None v	
Save 🗸 Cance	el X		



Table 2-5 DDNS Setting Instruction

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

Step 2 Please Click "Save" to finish.

----End

2.4.7 Routing Setting

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

Current Routing Table								8
Destination	Gateway,	/ Next Hop		Subnet Mask		Metric	Interface	
192.168.1.0	×			255.255.255.0		0	LAN	
127.0.0.0	*			255.0.0.0		0	lo	
Static Routing Table								
Destination	Gateway		Subnet Mask	Metric		Interface	Description	
	0.0.00			0		LAN *		
Add+								
Miscellaneous								
		Colours						
Mode								
RIPv1 & v2		Disabled *						
DHCP Routes								
Spanning-Tree Protocol								
Save 🗸 Cancel X								
Gateway / Nex	t Hop		Subnet Ma	sk	Metric	5	Interface	
*			255.255.255	5.0	0		LAN	
*			255.0.0.0		0		lo	
Gateway		Subnet Mask	Met	ric	Inter	face De	scription	
0.0.0.0			0		LAN	1 *		
Ga	atewav 🔻							
	sabled 🔻							
	Destination 192.168.1.0 127.0.00 Static Routing Table Destination Add + Miscellaneous Mode RIPv1 & v2 DHCP Routes Spanning-Tree Protocol Save ✓ Cancel × Gateway / Next *	Destination Gateway, 192.168.1.0 * 127.0.0.0 * Static Routing Table Gateway Destination Gateway Destination Gateway Mode 0.0.0.0 Add+ 0.0.0.0 Mode 0.0.0.0 Spanning-Tree Protocol 0.0.0 Save <	Destination Gateway / Next Hop 192.168.1.0 • 127.0.0.0 * Static Routing Table	Destination Gateway / Next Hop 192.168.1.0 • 127.0.00 * Static Routing Table Destination Gateway Subnet Mask Mode Gateway / Next Hop Spanning-Tree Protocol Sypanning-Tree Protocol Sateway / Next Hop Subnet Mask * 255.255.255 * 255.00.0	Destination Gateway / Next Hop Subnet Mask 192.168.1.0 * 255.255.0 127.0.0.0 * 255.0.0 Static Routing Table Destination Gateway Subnet Mask Metric 0.0.0.0 0 Add = Mode Gateway RIPv1 & v2 Disabled * DHCP Routes Spanning-Tree Protocol State Cancel x Gateway / Next Hop Subnet Mask Subnet Mask State x 255.255.255.0 * 255.00.0	Destination Gateway / Next Hop Subnet Mask 192.168.1.0 • 255.255.255.0 127.0.0.0 • 255.0.0 Static Routing Table Destination Gateway Subnet Mask Metric 0.0.0.0 0 Adde Mode Gateway * Node Gateway * DHCP Routes Spanning-Tree Protocol State X Gateway / Next Hop Subnet Mask Metric Gateway / Next Hop Subnet Mask Metric State X Gateway / Next Hop Subnet Mask Metric Subnet Mask Metric Stateway Subnet Mask Metric Subnet Mask Metric Subnet Mask Metric	Destination Gateway / Next Hop Subnet Mask Metric 127.00.0 • 255.255.00 0 127.00.0 • 255.00.0 0 Static Routing Table	Destination Gateway / Next Hop Subnet Mask Metric Interface 127.0.0.0 • 255.255.255.00 0 LAN 127.0.0.0 • 255.00.0 0 Io Static Routing Table Destination Gateway Subnet Mask Metric Interface Description Add#

Table 2-6	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.

```
----End
```

2.5 WLAN Setting

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

2.5.1 Basic Setting

Step 1 WLAN->Basic Setting to configure relative parameter

۲	Status	2	Radio Mode	2.4G + 5G *
Ø	Basic Network	\$]		
	WLAN	~	Wireless(2.4 GHz) Wireless(5 GHz)	
	Basic Settings		Enable WLAN	
	Wireless Survey		MAC Address	34:0A:92:19:51:03
۲	Advanced Network	•	MAC Address	
Ø	Firewall	•	Wireless Mode	Access Point 🔻
0	VPN Tunnel	.	Radio Band	2.4 GHz 💌
Я	Administration	•	Wireless Network Mode	Auto •
			SSID	router-wifi, 195103
			Broadcast SSID	
			Channel	7 - 2.442 GHz Y Scan Q
	 More Info 		Channel Width	40 MHz *



Wireless(2.4 GHz) Wireless(5 GHz)	
Enable WLAN	
MAC Address	34:0A:92:19:51:03
Wireless Mode	Access Point
Radio Band	2.4 GHz 🔹
Wireless Network Mode	Auto 🔻
SSID	router-wifi_195103
Broadcast SSID	
Channel	7 - 2.442 GHz 🔻 Scan Q
Channel Width	40 MHz 🔹
Control Sideband	Lower 🔻
Maximum Clients	128 (range: 1 - 255)
Security option	Disabled *



Wireless(2.4 GHz) Wireless(5 GHz)	
Enable WLAN	
MAC Address	34:0A:92:19:51:04
Wireless Mode	Access Point *
Radio Band	5 GHz 🔻
Wireless Network Mode	Auto 🔻
SSID	router-wifi_195103_5G
Broadcast SSID	
Channel	149 - 5.745 GHz 🔻 Scan ۹
Channel Width	80 MHz *
Control Sideband	Lower 🔻
Maximum Clients	128 (range: 1 - 255)
Security option	Disabled •

Table 2-7 Basic of WLAN Setting Instruction

Parameter	Instruction
Radio Mode	 2.4G+5G mode as default. Support 2.4G, 5G modes optional. 2.4G+5G model, Wi-Fi bandwidth for 683Mbps 2.4G model, Wi-Fi bandwidth for 300Mbps 5C model, Wi Fi bandwidth for 266Mbps
	5G model, Wi-Fi bandwidth for 866Mbps
Enable wireless	Enable or Disable the Wireless
Wireless mode	Support AP mode.
Wireless Network protocol	Support Auto/b/g/n optional for 2.4G. Support Auto/A/N optional for 2.4G.
SSID	The default is router, can be modified as per application.
Channel	The channel of wireless network, suggest keep the default
Channel Width	20MHz and 40MHz alternative for 2.4G. 20MHz, 40MHz and 80MHzalternative for 2.4G.
Security	Support various encryption method as requested.



Step 2 Please click "Save" to finish.

----End

2.5.2 Wireless Survey

Step 1 WLAN> Wireless Survey to check survey.

Status	>
Basic Network	
🗇 WLAN	
Basic Settings	
Wireless Survey	
Advanced Networ	
VPN Tunnel	
R Administration	
① More Info	

2.6 Advanced Network Setting

2.6.1 **Port Forwarding**

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

⊅ Status →		AI	ready changed lo	gin password	successfully.	
Basic Network	PortForwarding					
⊽ WLAN →	Ford of warding					
Advanced Network	On Proto	Src Address	Ext Ports	Int Port	Int Address	Description ^
Port Forwarding	× UDP		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
IP Passthrough	× TCP		1000	2000	192.168.1.2	ex: different internal port
Triggered	× TCP		1000	2000	192.166.1.2	ex: different internal port
Captive Portal	ТСР	×				
Serial App.						
UPnP/NAT-PMP	Add +					
Bandwidth Limiter	Src Address (antion	al) - Forward only if from t	ais address ev: "1 2 3 /" "	1234-2345" "123	0/24" "me example com"	
VRRP		is to be forwarded, as seen				
Static DHCP			e the LAN. If blank, the de	stination port is the sa	me as <i>Ext Ports</i> . Only one p	ort per entry is supported when
Firewall	forwarding to a diff Int Address - The definition of the definiti	erent internal port estination address inside th	e LAN.			
and a second state of the						
VPN Tunnel						
VPN Tunnel Administration						

Table 2-8	Port Forwarding Instructio	n
-----------	----------------------------	---

Parameter	Instruction			
Protocol	Support UDP, TCP, both UDP and TCP			
Src. Address	Source IP address. Forward only if from this address.			



Parameter	Instruction			
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

2.6.2 Port Redirecting

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

Status >		Already	changed login passwo	ord successfully.	
Basic Network			5 5 1		
WLAN >	PortRedirecting				
Advanced Network	On Proto	Int Port	Dst Address	Ext Port	Description
Port Forwarding	тср 🔻				
Port Redirecting					
DMZ	Add +				
IP Passthrough Triggered					
Captive Portal					
Serial App.	Save ✓ Cancel ×				
UPnP/NAT-PMP					
Bandwidth Limiter					
VRRP					
Static DHCP					
Firewall					
VPN Tunnel >					
Administration >					
① More Info	•				

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
```



2.6.3 DMZ Setting

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

👁 Status 🔹 🗘		Already changed login password successfully.
Basic Network		, , ,
🕏 WLAN 🔹 🔸	DMZ	
Advanced Network	Enable DMZ	
Port Forwarding	Internel Address	192.168.1.0
Port Redirecting		
DMZ	Source Address	
IP Passthrough	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		(opuonal, existanti, tatal/24, tatal-22222 of melexample.com)
Captive Portal		
Serial App.	Leave CLI Remote Access	 (Redirect remote access ports for CLI to router)
UPnP/NAT-PMP	Leave WEB Remote Access	(Redirect remote access ports for HTTP(s) to router)
Bandwidth Limiter	Leave WEB Remote Access	
VRRP		
Static DHCP	Save ✓ Cancel ×	
3 Firewall		
D VPN Tunnel >		
Administration		
① More Info		

Table 2-10 DMZ Instruction

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

Step 2 Please click "save" to finish

----End

2.6.4 **IP Passthrough Setting**

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

	Shenzhen Wlink Techn 深圳市德传物联技	ology Co., LTD 反术有限公司	WL-G930 Series Router User Manual
● Status >		Already changed login pa	ssword successfully.
Basic Network S WLAN	IP Passthrough		
Advanced Network	Enabled		
Port Forwarding Port Redirecting	MAC Address		
DMZ	Gateway		
IP Passthrough Triggered			
Captive Portal Serial App.	Save ✓ Cancel ×		
UPnP/NAT-PMP			
Bandwidth Limiter VRRP			
Static DHCP			
Firewall			
R Administration			
 More Info 			

Table 2-11 IP Passthrough Instruction

parameter	Instruction		
Enable	Enable IP Passthrough		
MAC Address	Enable DHCP of device. Configure device Mac. Device will be assigned SIM IP.		
Gateway	If WL-G930 connect to multiple device, input other device gateway. The device might access to router GUI.		

Step 2 Please click "save" to finish

----End

2.6.5 Triggered Setting

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

👁 Status 🔹 🔶			Already changed login	password successfully
Basic Network				
ŵ WLAN →	Triggered Port Forwar	ding		
Advanced Network	On Protocol	Trigger Ports	Forwarded Ports	Description A
Port Forwarding	× TCP	3000-4000	5000-6000	ex: open 5000-6000 if 3000-4000
Port Redirecting	ТСР			
DMZ	TCP			
IP Passthrough	Add +			
Triggered				
Captive Portal	• (200-300).			
Serial App.		tomatically closed after a	few minutes of inactivity.	
UPnP/NAT-PMP				
Bandwidth Limiter	Save ✓ Cancel ×			
VRRP	Javeo Cancerx			
VINNP				
Static DHCP				
Static DHCP				
Static DHCP				



Table 2-12 mggered 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

2.6.6 Captive Portal

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

👁 Status 🔹 🕯	Captive Portal		
Basic Network >	Enabled		
≌ WLAN →	Auth Type	NONE *	
Advanced letwork 🛩	WEB Root	Default	Y
Port Forwarding Port Redirecting	WEB Host		
DMZ	Portal Host		
IP Passthrough Triggered	Login Timeout	0	Minutes
Captive Portal	Idle Timeout	0	Minutes
Serial App. UPnP/NAT-PMP	Ignore LAN		
Bandwidth Limiter	Redirecting http://	www.googl	e.com
VRRP Static DHCP	MAC Address Whitelist		
Firewall >	Download QOS		
🕽 VPN Tunnel 🔸 🖕	Upload OOS		



Parameter	Instruction
Enable	Enable Captive portal feature.
Auth Type	Reserved.
Web Root	Choose captive portal file storage path.
	Default: Captive portal file is in the firmware as default.
	In-storage: Captive portal file is in router's Flash.
	Ex-storage: Captive portal file is in extended storage such as SD card.



Parameter	Instruction
Web Host	Configure domain name for the captive portal access. For example, Configure as wlink.tech.com, we might directly access to captive portal page in the website as wlink.tech.com
Portal Host	Reserved.
Logged Timeout	Maximum time user has connectivity. User need to re-login Captive Portal page after defined time.
Idle Timeout	Maximum time user has connectivity if no network activity from Wi-Fi User.If User need to re-login Captive page to surf internet.
Ignore LAN	If enabled, LAN devices will bypass the Captive Portal page.
Redirecting	Router will redirect to the defined link after accepting the terms and conditions on the Captive Portal page.
MAC Whitelist	No captive portal page for Wi-Fi device.
Download QoS	Enable to apply the Download and Upload per user limits.
Upload Qos	Maximum download speed available to each user.

Step 2 Please click "save" to finish.

----End

2.6.7 Serial App. Setting

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

		Already changed login password successfully.
Basic Network > The second s	Serial to TCP/IP	
😪 Advanced	IPoC Mode	Serial *
Network 👻 Port Forwarding	Serial to TCP/IPMode	Disabled *
Port Redirecting		
DMZ IP Passthrough		
Triggered	Save ✓ Cancel ×	
Captive Portal		
Serial App. UPnP/NAT-PMP		
Bandwidth Limiter		
VRRP Static DHCP		
Ø Firewall >		
VPN Tunnel >		



Serial to TCP/IP	
IPoC Mode	Serial 💌
Serial to TCP/IPMode	Client •
Server IP/Port	8.8.8.8 : 40002
Socket Type	тср т
Socket Timeout	500 (milliseconds)
Serial Timeout	500 (milliseconds)
Packet Payload	1024 (bytes)
Heart-Beat Content	
Heart-Beat Interval	2 (seconds)
Port Type	RS485/RS232 *
Cache Enable	
Debug Enable	
Baud Rate	57600 *
Parity Bit	none 🔻
Data Bit	8 🔻
Stop Bit	1 .
Save ✓ Cancel ×	

Table 2-14 Serial App Instruction

Parameter	Instruction
Serial to TC/IP 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



WL-G930 Series Router User Manual

Parameter	Instruction
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
ТХ	 2
DI-1	
DI-2	
DO	

Step 2 Please click "save" to finish.

----End

2.6.8 UPnp/NAT-PMP Setting

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

Status			Already changed login	password successfully.	
Basic Network					
🕆 WLAN	Forwarded Ports				
Advanced Network	Ext Ports	Int Port	Internal Address	Protocol	Description
Port Forwarding					Delete All × C Refresh
Port Redirecting					
DMZ					
IP Passthrough	Settings				
Triggered	Enable UPnP				
Captive Portal					
Serial App.	Enable NAT-PMP				
UPnP/NAT-PMP					
Bandwidth Limiter	Inactive Rules Cleaning		1. A A A A A A A A A A A A A A A A A A A		
VRRP			when enabled, UPnP clients are allowed	d to be defined and the state the second	
Static DHCP	Secure Mode		when enabled, OPHP clients are allowed	to add mappings only to their IP)	
🛛 Firewall					
VPN Tunnel	Show In My Network Places	1			
R Administration					
More Info	Save ✓ Cancel ×				

Step 2 Please click "save" to finish.

----End



2.6.9 Bandwidth Control Setting

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

Status	,		Already c	hanged login passwo	ord successfully.		
Basic Network							
ক WLAN		Bandwidth Control					
Advanced Network		Enable Control					
Port Forwarding							
Port Redirecting		IP IP Range MAC Address	DLRate	DLCeil	ULRate	ULCeil	Priority
DMZ							
IP Passthrough							Normal 🔻
Triggered		Add +					
Captive Portal							
Serial App.							
UPnP/NAT-PMP		Default Class					
Bandwidth Limiter							
VRRP		Enable Default Class					
- Static DHCP							
Firewall		Save ✓ Cancel ×					
VPN Tunnel							
R Administration							
 More Info 							

Table 2-15 Bandwidth Control Instruction

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

Step 2 Please click "save" to finish.

----End

2.6.10 VRRP Setting

Step 1 Advanced Network> VRRP 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

Status	>		Already changed login password successfully.
Basic Network		VRRP	
🕈 WLAN			
Advanced Network		Enable VRRP	
Port Forwarding		Mode	backup 🔻
Port Redirecting DMZ		Virtual IP	192.168.1.3
- IP Passthrough		Virtual Router ID	
Triggered			
Captive Portal Serial App.		Priority	100
UPnP/NAT-PMP		Authentication	
Bandwidth Limiter			
VRRP		Script Type	Default 🔻
Static DHCP		Check Interval	3
🔯 Firewall			
VPN Tunnel		Weight	10
R Administration			
① More Info		Save ✓ Cancel ×	

Step 2 Please click "save" to finish.

```
----End
```

2.6.11 Static DHCP Setting

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

• Status		Already changed login passo	word successfully.	
Basic Network	Static DHCP			
ବି WLAN 🔸	MAC Address	IP Address	Hostname 🔨	Description
Advanced Network				
Port Forwarding	00:00:00:00:00	192.168.1.2		
Port Redirecting	00:00:00:00:00			
DMZ				
IP Passthrough	Add +			
Triggered				
Captive Portal				
Serial App.	Save ✓ Cancel ×			
UPnP/NAT-PMP				
Bandwidth Limiter				
VRRP				
Static DHCP				
🛙 Firewall 🔹 🔹				
VPN Tunnel				
R Administration				
More Info				

Step 2 Please click "save" to finish.

----End

2.7 Firewall

2.7.1 IP/URL Filtering

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

	*	IP/MAC/Po	rt Filtering					
asic Network /LAN	2 3	On Src MA	C Src IP	Dst IP	Protocol	Src Port Ds	Port Polic	/ Description
ivanced Net					NON *		Acc	2] ¥
ewall	~	Add +						
P/URL Filteri								
omain Filter PN Tunnel	ing >	Key Word F						
dministratior	5	On	Key Word			Description		
		Add +						
		URL Filterin	ıg					
		On	URL	Description				
		~						
		Add +						
More In	fo							
	_							
P/MAC/Por	t Filtering							
Src MAC		Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
				NON *			Accej 🔻	
\dd +								
Key Word Fi	Itering							
	Key Word				Descript	ion		
	Key Word				Descript	ION		
vdd +								
JRL Filterin	g							
	URL				Descript	ion		
2								
vdd +								
seese Eilter	ing							
ccess Filter		C 10	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
		Src IP					1000 F000	and the second sec
Src MAC		SICIP		NON .			Accej *	

Table 2-16 IP/URL Filtering Instruction

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



Step 2 Please click "save" to finish.

---End

2.7.2 **Domain Filtering**

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

Status	Already changed login password successfully.				
Basic Network >	Domain Filtering				
�WLAN →					
Advanced Network	On				
🔞 Firewall 🗸 🗸	Default Policy White List *				
IP/URL Filtering	On Domain Description				
Domain Filtering					
VPN Tunnel					
果 Administration >	Add+				
	Save Cancel ×				

Table 2-17 Domain Filtering Instruction

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

Step 2 Please click "save" to finish.

----End

2.8 VPN Tunnel

2.8.1 **GRE Setting**

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

Status	Already changed login password successfully.						
Basic Network >	GRE Tunnel						
ବ WLAN 🔹 🔸		-					
Advanced Network>	On Idx ~ Tunnel Addr	ress Tunnel Source Tunnel Destination	Keepalive Interval Retries	Description			
🗟 Firewall >							
🗘 VPN Tunnel 🛛 👻							
GRE	Add +						
OpenVPN Client PPTP/L2TP Client IPSec	GRE Route On Tunnel Index ^	Destination Address	Description				
果 Administration →	✓ 1 Add+	•					



Table 2-18 GRE Instruction

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

Step 2 Please click "save" to finish.

```
----End
```

2.8.2 **OpenVPN Client Setting**

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

Basic Network >	c	OpenVPN Client	
🗇 WLAN 🔷			
AdvancedNetwork →		lient 1 Client 2	
🖾 Firewall 🔷	Ba	asic Advanced Keys Status	
😫 VPN Tunnel 🗸 🗸	v	/PN Client #1 (Stopped)	÷
GRE		Start with WAN	
OpenVPN Client PPTP/L2TP Client		Interface Type	TUN *
IPSec	1	Protocol	UDP Y
R Administration →		Server Address	1194
		Firewall	Automatic *
		Authorization Mode	TLS •
		Username/Password Authentication	
		HMAC authorization	Disabled •
		Create NAT on tunnel	
	Sta	art Now	

WL	INK	Shenzhen Wlink Technology Co., LTD 深圳市德传物联技术有限公司
		你列中您很104012个月的公司

asic Advanced Keys Status	
VPN Client #1 (Stopped)	
Start with WAN	
Interface Type	TUN 🔻
Protocol	UDP 🔻
Server Address	1194
Firewall	Automatic 🔻
Authorization Mode	TLS
Username/Password Authentication	
HMAC authorization	Disabled *
Create NAT on tunnel	✓

Table 2-19 Basic of OpenVPN Instruction

Parameter	Instruction	
Start with WAN	Enable the Openvpn feature for 5G/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	As the configuration requested.	



WL-G930 Series Router User Manual

Parameter	Instruction
Authentication	
HMAC authorization	As the configuration requested.
Create NAT on tunnel	Configure NAT in Openvpn tunnel.

PN Client #1 (Stopped)		
Poll Interval	0	in minutes, 0 to disable)
Redirect Internet traffic		
Accept DNS configuration	Disabled *	
ncryption cipher	Use Default	Y
Compression	Adaptive *	
LS Renegotiation Time	-1	(in seconds, -1 for default)
connection retry	30	(in seconds; -1 for infinite)
erify server certificate (tls-remote)		
ustom Configuration		

Table 2-20 Advanced of OpenVPN Instruction

Parameter	Instruction	
Poll Interval	Openvpn client check router's status as interval time.	
Redirect Internet Traffic	Configure Openvpn as default routing.	
Access DNS	As the configuration requested.	
Encryption	As the configuration requested.	
Compression	As the configuration requested.	
TLS Renegotiation Time	TLS negotiation 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.	



/PN Client #1 <mark>(Stopped)</mark>		
or help generating keys, refer to th	OpenVPN HOWTO.	
Certificate Authority		
Client Certificate		
Client Key		
		-

Table 2-21 Keys of OpenVPN Instruction

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

OpenVPN Client	
Client 1 Client 2	
Basic Advanced Keys Status	
VPN Client #1 (Stopped)	Þ
Client is not running or status could not be read.	
	Refresh Status
Start Now	

Table 2-22 Status of OpenVPN Instruction

Parameter	Instruction
Status	Check Openvpn status and data statistics.

Step 2 Please click "save" to finish.

----End

2.8.3 PPTP/L2TP Client Setting

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

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

WL-G930 Series Router User Manual

Status	*	L2TP/PPTP Basic	:						
Basic Network	•	On	Protocol ^	Name	Server	Username	Password F	irewall Default Ro	ute Local IP
WLAN	•	~	L2TP *						
Advanced twork	•	Add +							
Firewall	>								
VPN Tunnel	~	L2TP Advanced							
GRE		On	Name ^	Accept DNS	MTU	MRU	Tunnel Auth	Tunnel Password	Custom Options
OpenVPN Clie PPTP/L2TP Cli		~		NO	*				
PPTP/L2TP Cli PSec	ent	Add +							
Administratior	>	Add+							
		PPTP Advanced							
		On	Name 🔿	Accept DN	s MTU	MRU	MPPE	MPPE Statefu	Custom Options
				NO					
		Add+							
		Schedule							
		On		Name 1 ^	Name	2	Policy	Descrip	otion
		Image: A start of the start					FAILOVER	•	
More Info		Add+							

Table 2-23 PPTP/L2TP Basic Instruction

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

Table 2-24 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.
Options	

Table 2-25 PPTP Advanced Instruction

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

Table 2-26 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



2.8.4 IPSec Setting

Status		Already changed login password successfully.		
Basic Network >	IPSec	IPSec		
🗟 WLAN 🔷 🔸				
😭 Advanced	IPSec 1 IPSec 2 Schedule			
Network >	Group Setup Basic Setup Advanced 3	Setup		
🖾 Firewall 🔶		0.01		
🔹 VPN Tunnel 🛛 🛩	Enable IPSec			
GRE	IPSec Extensions	Normal		
OpenVPN Client PPTP/L2TP Client	Local Security Gateway Interface	3G Cellular 🎽		
IPSec	Local Security Group Subnet/Netmask	192.168.1.0/24 ex. 192.168.1.0/24		
R Administration >	Local Security Firewalling	2		
	Remote Security Gateway IP/Domain			
	Remote Security Group Subnet/Netmask	10.0.0./24 ex. 192.168.88.0/24		
	Remote Security Firewalling			
	Save 🗸 Cancel X			
 More Info 				

2.8.4.1 IPSec Group Setup

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

Group Setup Basic Setup Advanced S	etup	
Enable IPSec		
IPSec Extensions	Normal	
Local Security Gateway Interface	3G Cellular 🔻	
Local Security Group Subnet/Netmask	192.168.1.0/24	ex. 192.168.1.0/24
Local Security Firewalling		
Remote Security Gateway IP/Domain		
Remote Security Group Subnet/Netmask	10.0.0/24	ex. 192.168.88.0/24
Remote Security Firewalling		

Table 2-27	IPSec Group Se	tup 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



WL-G930 Series Router User Manual

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

Step 2 Please click "save" to finish.

2.8.4.2 IPSec Basic Setup

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

Group Setup Basic Setup	Advanced Setup
Keying Mode	IKE with Preshared Kev
Phase 1 DH Group	Group 2 - modp1024 🔻
Phase 1 Encryption	3DES (168-bit)
Phase 1 Authentication	MD5 HMAC (96-bit)
Phase 1 SA Life Time	28800 seconds
Phase 2 DH Group	Group 2 - modp1024 🔻
Phase 2 Encryption	3DES (168-bit)
Phase 2 Authentication	MD5 HMAC (96-bit)
Phase 2 SA Life Time	3600 seconds
Preshared Key	

Table 2-28	IPSec Basic Setup	Instruction
------------	-------------------	-------------

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



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

Step 2 Please click "save" to finish.

2.8.4.3 IPSec Advanced Setup

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

Group Setup Basic Setup	Advanced Setup
Aggressive Mode	
Compress(IP Payload Compres	iion)
Dead Peer Detection(DPD)	
ICMP Check	
IPSec Custom Options 1	
IPSec Custom Options 2	
IPSec Custom Options 3	
IPSec Custom Options 4	



WL-G930 Series Router User Manual

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

2.9 Administration

2.9.1 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.

Status	•		Already changed login password successfully.
Basic Network		Router Identification	
🕏 WLAN			D. In
Advanced		Router Name	Router
Network		Hostname	Router
S Firewall		Domain Name	
VPN Tunnel			
R Administration		Save 🗸 Cancel 🗙	
Identification			

Router Identification

Router Name	Router	
Hostname	Router	
Domain Name		

Save
√ Cancel
×

Table 2-30 Router Identification Instruction	n
--	---

Parameter	Instruction	
Router name	Default is router, can be set	maximum 32 character
Host name	Default is router, can be set	maximum 32 character



WL-G930 Series Router User Manual

Parameter	Instruction
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



2.9.2 Time Setting

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

Basic Network		
🗟 WLAN 🔹	Time	
Advanced Network	Router Time	Tue, 24 Nov 2020 14:17:02 +0800 Clock Sync.
🐼 Firewall 🔹		
VPN Tunnel	Time Zone	UTC+08:00 China, Hong Kong, Western Australia, Singapore, Taiwan 🔻
R Administration	Auto Daylight Savings Time	
Identification		
Time	Auto Update Time	Every 4 Hours 🔹
Admin Access		
Scheduled Reboot	Trigger Connect On Demand	
SNMP	NTP Time Server	Asia 🔻
Storage Settings	NTP Time server	A210 .
M2M Settings		0.asia.pool.ntp.org. 1.asia.pool.ntp.org 2.asia.pool.ntp.org
TR-069		
DI/DO Setting		
Configuration	Save ✓ Cancel ×	
Logging	Save Cancel X	
Upgrade		

CAUTION

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

Step 2 Please click "save to finish.

----End



2.9.3 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		2	WebAccess	
🤵 Basic N	letwork	•	Local Access	HTTP •
🗟 WLAN		•	HTTP Access Port	80
Advan	ced Network	>	Remote Access	Disabled V
🔯 Firewa	II (2	Nemote Access	
💷 VPN To	unnel	•	Allow Wireless Access	
界 Admin	istration	•	Block WAN Ping	
Identi	fication			
Time			SSH Enable at Startup	
	n Access Iuled Reboot		Allow Telnet Remote Access	
SNMP				
Storag	je Settings			
— M2M	Settings		Password	
TR-06				
) Setting		Password (admin)	
Loggi	guration ng		(re-enter to confirm)	
Upgra	ide			

Step 2 Please click save iron to finish the setting

----End

2.9.4 Schedule Reboot Setting

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

Status	>		Already changed login password successfully.
Basic Network	>	Scheduled Reboot	
🕏 WLAN		Scheduled Reboot	
Advanced		Enabled	
Network	>	Time	1:00 AM
S Firewall	>	Dava	Sun Mon Tue Wed Thu Fri Sat Everyda
VPN Tunnel	>	Days	
Administration		Save ✓ Cancel ×	
Identification			
Time			
Admin Access			
Scheduled Rel	oot		

Step 2 Please click save iron to finish the setting

----End

2.9.5 SNMP Setting

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

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

• Status	1	SNMP Settings		
Basic Network		Enable SNMP		
🗟 WLAN 🔷				
Advanced Network		Port	161	
🐻 Firewall 🔷		Remote Access		
VPN Tunnel		Allowed Remote		
R Administration		IP Address		(optional; ex: "1.1.1.1", "1.1.1.0/24", "1.1.1.1 - 2.2.2.2" ")
Identification		6 N	detran	
Time		System Name	Getran	
Admin Access Scheduled Reboot		Location	router	
SNMP		Contact	admin@router	
Storage Settings				
M2M Settings		RO Community	rocommunity	
TR-069				
DI/DO Setting		RW Community	rwcommunity	
Configuration				
Logging		SNMPv3 Authentication Type	NONE V	
Upgrade				
MCU Upgrade	-	SNMPv3 Privacy Type	NONE *	

Step 2 Please click save iron to finish the setting

----End

2.9.6 Storage Setting

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

Image: Setwork > Image: Setwork > Image: Setwork > Image: Setwork > Image: Setwork >	Storage settings Storage	Router V Total :16.00 MB Fn	ee:15.50 MB	v
♥ VPN Tunnel > ★ Administration Identification Time	Upload new file No file chosen	Choose File Upload		~
Admin Access Scheduled Reboot SNMP	Current file list File name	File size	File operation	~
Storage Settings M2M Settings TR-069 DI/DO Setting	sms.list	408	× 9	
DI/DO Setting Configuration Logging Upgrade	Save-/ Cancel X			

Step 2 Please click save iron to finish the setting

----End

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

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

	Shenzhen Wlink Technology Co., LTD 深圳市德传物联技术有限公司	WL-G930 Series Router	
Status		Already changed login pass	word successfully.
Basic Network >	m2m		
🕏 WLAN 🔶	M2M Enabled		
AdvancedNetwork →	Fail Action	Restart M2M	
🔯 Firewall 🔹	Device ID		
VPN Tunnel			
⊼ Administration 🐱	M2M Server/Port	: 8000	
Identification	Heartbeat Intval	60 (seconds)	
Time Admin Access	Heartbeat Retry	10 (Range:10-1000)	
Scheduled Reboot	Named-Pipe Enabled	Remote Connect *	
Storage Settings M2M Settings	Named-Pipe Server Port	8002 (Range:	1024-65535)
DI/DO Setting	Named-Pipe Status	Offline	
Configuration			
Logging	Named-Pipe Address	0.0.0.0	
Upgrade	na ny volu su na na fastanta se ze v 🖬 di kata nganjan kata se kata se s		
⑦ More Info	Save ✓ Cancel ×		

Step 2 Please click save iron to finish the setting

----End

2.9.8 TR-069 Setting

Step 3 Please click "Administrator>TR-069 Setting" to check and modify relevant parameter.

Ø	Basic Network	>		
\$	WLAN	•	TR069	
e	Advanced Network		Enabled	
0	Firewall	•	Enable Periodic Transmission	
٩	VPN Tunnel	>	Username	openacs
Я	Administration	·•		
	Identification		Password	openacs
	Time		URL	http://192.168.1.110:8080/openacs/acs
	Admin Access		UNE	(1), (1), (1), (1), (1), (1), (1), (1),
	Scheduled Reboot			
	SNMP		Save - Cancel ×	
	Storage Settings			
	M2M Settings			
	TR-069			
	DI/DO Setting			
	Configuration			
	Logging			
-	Upgrade			

Step 4 Please click save iron to finish the setting

```
----End
```



2.9.9 DI/DO Setting

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

Basic Network		
ବ wlan 🔸	DI Setting	
Advanced Network	Enabled	Port1 Port2
🔯 Firewall		
VPN Tunnel >		
💂 Administration 👻	DO Setting	
Identification	Enabled	
Time Admin Access	Alarm Source	DI Control SMS Control
Scheduled Reboot SNMP	Alarm Action	ON V
Storage Settings M2M Settings	Power On Status	OFF v
TR-069 DI/DO Setting	Keep On	1 (*100ms)
Configuration		
Logging Upgrade	Save√ Cancel×	

2.9.7.1 DI Configure



DI Setting		
Enabled	Port1 🔽	Port2
Port1Mode	ON	¥
Filter	1	(*100ms)
SMS Alarm		
DO Setting		
Enabled	~	
Alarm Source	DI Control	SMS Control
Alarm Action	ON T	
Power On Status	OFF 🔻	
rower on status		

Table 2-31 DI Instruction

Parameter	Instruction
Enable	Enable DI. Port1 is for I/O1 and Port2 is I/O2. Both I/O1 and I/O2 are DI ports
Mode	Selected from OFF, ON and EVENT_COUNTER modes. OFF Mode: DI from high level(3.3v~5V) to low level(0V), it will trigger alarm. ON Mode: DI from low level(0V) to high level(3.3v~5V), it will trigger alarm. EVENT COUNTER Model: Enter EVENT COUNTER mode.
Filter	Software filtering is used to control switch bounces. Input (1~100)*100ms. Under OFF and ON modes, WL-G930 detects pulse signal and compares with first pulse shape and last pulse shape. If both are the same level, WL-G930 will trigger alarm.



Parameter	Instruction
	Under EVENT_COUNTER mode, if first pulse shape and last pulse shape are not the same level, WL-G930 will trigger alarm according to Counter Action setting.
Counter Trigger	Available when DI under Event Counter mode
	Input from 0 to 100. (0=will not trigger alarm)
	It will trigger alarm when counter reaches this value. After triggering alarm, DI will keep counting but no trigger alarm again.
Counter Period	It's a reachable IP address. Once the ICMP check is failed, GRE will be established again.
Counter	it will re-count after counter trigger alarm. The value is 0~30000(*100ms).
Recover	0 means no counter.
	HI_TO_LO and LO_TO_HI is available when DI under Event Counter mode.
Counter Action	In Event Counter mode, the channel accepts limit or proximity switches and counts events according to the ON/OFF status. When LO_TO_HI is selected, the counter value increase when the attached switch is pushed. When HI_TO_LO is selected, the counter value increases when the switch is pushed and released.
Counter Start	Available when DI under EVENT_COUNTER mode. Start counting when enable this feature.
SMS Alarm	The alarm SMS will send to specified phone group.
	Each phone group include up to 2 phone numbers.
SMS Content	70 ASCII Char Max
Number 1	SMS receiver phone number.
Number 2	SMS receiver phone number.

Step 2 Please click "save" to finish.

OFF Mode

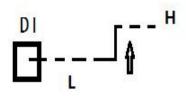
DI from high level 3.3~5V to low level 0V will be triggered.

L

ON Mode

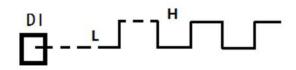
Data input from low level 0V to high level 3.3~5V will be triggered.





EVENT_COUNTER Model

The counted number of pulses will be triggered.



2.9.7.2 DO Configure

DO Setting	~
Enabled	
Alarm Source	DI Control 🧹 SMS Control 🗸
Alarm Action	ON 🔻
Power On Status	OFF •
Keep On	1. (*100ms)
SMS Trigger Content	70 ASCII Max
SMS Reply Content	70 ASCII Max
SMS admin Num1	
SMS admin Num2	Backup
Save√ Cancel×	

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



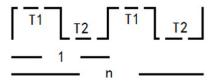
Parameter	Instruction
	receiving SMS from the number in phone book. M2M Control: it's not ready.
Alarm Action	Digital Output initiates when there is an alarm. Selected from "OFF", "ON", "Pulse". OFF: Open from GND when triggered. ON: Short contact with GND when triggered. Pulse: Generates a square wave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

Step 3 Please click "save" to finish.





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



NOTE

2.9.10 Configuration Setting

Step 1 Please click "Administrator> Configuration " to do the backup setting

0	Basic Network	•		
\$	WLAN	•	Backup Configuration	
e	Advanced Network	•	router_015_m199201	.cfg Backup 🛆
22	Firewall	•	Save As Default Configuratio	חנ
•	VPN Tunnel	•	Save	
累	Administration	•	Restore Configuration	
	Identification		Select the configuration file to resto	ore:
	Time		No file chosen	Choose File Restore
	Admin Access			
	Scheduled Reboot		Restore Default Configuratio	n
	SNMP		Select	▼ OK
	Storage Settings			
	M2M Settings		Total / Free NVRAM:	64.00 KB / 44.48 KB (69.51%)
	TR-069		Idda / The INVICANT	04,00 KB / 44,40 KB (05,51,8)
	DI/DO Setting			
	Configuration			
	Logging			
	Upgrade			

Figure 3-1 Backup and Restore Configuration GUI

CAUTION

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

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

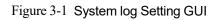
----End



2.9.11 System Log 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).

0	Basic Network	Syslog	
		Log Internally	
2	Firewall >	Log To Remote System	
٩	VPN Tunnel	Generate Marker	Every 1 Hour
黒	Administration 👻	Limit	60 (messages per minute / 0 for unlimited)
	Identification	Link	includes per innacci o to anninces
	Time		
	Admin Access	Save✓ Cancel×	
	Scheduled Reboot		
	SNMP		
	Storage Settings		
	M2M Settings		
	TR-069		
	DI/DO Setting		
	Configuration		
	Logging		
	Upgrade		



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

----End



2.9.12 Firmware upgrade

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

Basic Network		
ক WLAN	Upgrade Firmware	
	Select the file to use:	
Advanced Network	No file chosen	Choose File Upgrade
🔯 Firewall 🔹	After flashing, erase all	data in NVRAM memory
VPN Tunnel	Current Version:	G9.0.1.5-201118-144109
💂 Administration 👻	Current Version:	G9.0.1.5-201118-144109
Identification	Free Memory:	477.20 MB (aprox. size that can be buffered completely in RAM)
Time		
Admin Access		
Scheduled Reboot		
SNMP		
Storage Settings		
M2M Settings		
TR-069		
DI/DO Setting		
Configuration		
Logging		
Upgrade		

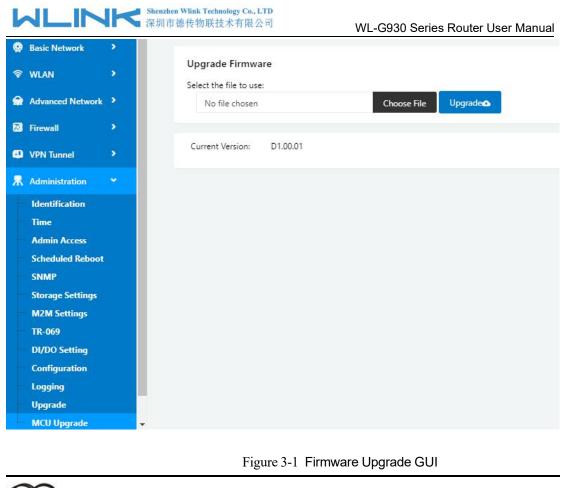
Figure 3-1 Firmware Upgrade GUI

NOTE NOTE

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

2.9.13 Firmware upgrade

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



D_{NOTE}

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

2.10 "Reset" Button for Restore Factory Setting

If you couldn't enter web interface for other reasons, you can also use this way. "Reset" button is near to Console port in WL-G930 panel, This button can be used when the router is in use or when the router is turned on.

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

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 2-33 System Default Instruction



NOTE

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



Configuration Instance

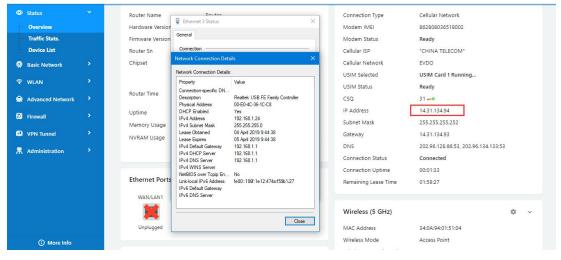
This chapter is mainly for configured test case, there would be some difference between the scheme and real object. But the difference doesn't have any influence to products performance.

3.1 Port Forwarding

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

Note: It's based on SIM card carrier

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



3) Configuration

	Status			Ye	ou haven't changed	the default passwor	d for this router. T	o change router pass	word_click here.
	Basic Network	>							
	WLAN	•	PortFo	orwarding					
	Advanced Network	~	On	Proto	Src Address	Ext Ports	Int Port	Int Address	Description ^
	Port Forwarding		~	UDP		8000	8000	192.168.1.24	
	Port Redirecting		~	TCP		433	433	192.168.1.24	
	DMZ IP Passthrough			Both		8080	8080	192.168.1.24	
	Triggered		_						
	Captive Portal		Dele	ete × Can	celØ OK✓				
	Serial App.			TCP	w l				
	UPnP/NAT-PMP Bandwidth Limiter								
	VRRP		Add	I+					
	Static DHCP				onal) - Forward only if from				
	Firewall	•	• Ir	nt Port (optional	orts to be forwarded, as see The destination port insi ifferent internal port				t per entry is supported when
9	VPN Tunnel	>			destination address inside 1	the LAN.			
	Administration								



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

3.2 IP Passthrough

1) The router online

Status		Ye	u haven't change	d the default p	assword for	this router. To change router	assword click here.		
···· Overview									
Traffic Stats.	System				~	WAN		\$	<u> </u>
Device List		Router							
Basic Network	Router Name					Connection Type	Cellular Network		
	Hardware Version	C11-D20				Modem IMEI	862808036518002		
🕆 WLAN	Firmware Version	G5.0.1.5				Modem Status	Ready		
Advanced Network	Router Sn		1904010001			Cellular ISP	"CHINA TELECOM"		
	Chipset	ARMv7 P	rocessor rev 5 (v7l)			Cellular Network	EVDO		
Firewall						USIM Selected	USIM Card 1 Running		
VPN Tunnel	Router Time	Thu, 04 A	pr 2019 09:59:42 +0800	Clock Sync.		USIM Status	Ready		
	Uptime	00:17:18				CSQ	31 🛹		
R Administration	Memory Usage		/ 122.22 MB (30.76%)			IP Address	14.31.134.94		
	0.000		64.00 KB (50.67%)			Subnet Mask	255.255.255.252		
	NVRAM Usage	32,43 K8 /	64.00 KB (50.67%)			Gateway	14.31.134.93		
						DNS	202.96.128.86:53, 202.96.134.133:53		
						Connection Status	Connected		
	Ethernet Ports Status				~	Connection Uptime	00:16:09		
						Remaining Lease Time	01:43:51		
	WAN/LAN1	LAN2	LAN3	LAN4					
			1	1		man a common		227	
	Unplugged	100M Full	Unplugged	Unplugged		Wireless (5 GHz)		\$	~
		100111101	Cripioggeo	Chiproggeo		MAC Address	34:0A:94:01:51:04		
						Wireless Mode	Access Point		
	VPN Status				¢ ~	Wireless Network Mode	Auto		
	No Active VPN					Interface Status	Up (LAN)		
③ More Info	NO ACOVE VPN					Radio	Enabled 🗸		

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

Basic Network	>	IP Passthrough		🔋 Ethernet 3 Status	5
ଟି WLAN	>			Network Connection Deta	ils X
Advanced Netwo	rk 🐣	Enabled		Network Connection Details:	
Port Forwarding Port Redirecting		MAC Address	00:E0:4C:36:1C:C8	Property Connection-specific DN Description	Value Realtek USB FE Family Controller
DMZ IP Passthrough		Gateway		Physical Address DHCP Enabled IPv4 Address	00-E0-4C-36-1C-C8 Yes 192.168.1.24
Triggered Captive Portal		Save ✓ Cancel ×		IPv4 Subnet Mask Lease Obtained Lease Expires IPv4 Default Gateway	255.255.255.0 04 April 2019 9:58:17 05 April 2019 9:58:16 192.168.1.1
Serial App. UPnP/NAT-PMF Bandwidth Limi				IPv4 DHCP Server IPv4 DNS Server IPv4 WINS Server NetBIOS over Topip En	
VRRP Static DHCP				Link-local IPv6 Address IPv6 Default Gateway IPv6 DNS Server	fe80::186f:1e12:474a;f59b%27
3 Firewall	>				Close
VPN Tunnel	>				
R Administration	>				

3) Set the PC to DHCP

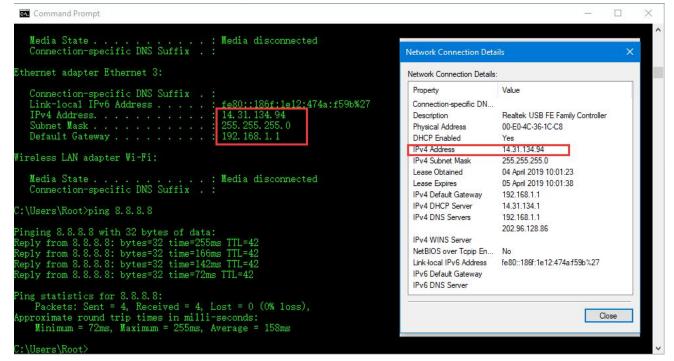


(

WL-G930 Series Router User Manual

Ethernet Status	Ethernet Properties	Internet Protocol Version 4 (TCP/IPv4) Properties
Seneral	Networking Sharing	General Alternate Configuration
Connection IPv4 Connectivity: Internet	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.
IPv6 Connectivity: No network access Media State: Enabled Duration: 05:11:32 Speed: 100.0 Mbps	Co This connection uses the following items: 	Uge the following IP address:
Activity Sent Received	Cos Packet Scheduler Cos Packet Scheduler Scheduler Microsoft Network Adapter Multiplexor Protocol Microsoft LLDP Protocol Driver Internet Protocol Version 6 (TCP/IPv6) <	Subnet mask:
Bytes: 39,134,796 630,257,094	Install Uninstall Pro	Alternate DNS server:
Properties Diagnose Diagnose	Transmission Control Protocol/Internet Protocol. The wide area network protocol that provides communica across diverse interconnected networks.	
Close	ОК	OK Cancel

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



WL-G930 Series Router User Manual

working Sharing			General		
nnect using: Intel(R) Ethernet	Connection (3) 1218-\	/		d automatically if your network supports need to ask your network administrator	
	L . C . II	Configure	O Obtain an IP address auto	matically	
is connection uses t	Constant of the states		O <u>s</u> e the following IP addre	SS:	
Client for Micr File and Prints	osoft Networks er Sharing for Microsoft	Networks	IP address:	192 . 168 . 1 . 2	
🛛 🐙 QoS Packet 🤅			Subnet mask: 255 . 255 . 0		
🗌 🔟 Microsoft Net	work Adapter Multiplex		Default gateway:		
	col Version 6 (TCP/IP	v6) 🗸	Obtain DNS server address	s automatically	
and the second se		>	• Use the following DNS serv	ver addresses:	
Install	Uninstall	Properties	Preferred DNS server:		
		tagal The default	<u>Alternate DNS server:</u>		
Description	Protocol/Internet Pro				

3.3 Captive Portal

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

Status	•	Captive Portal	
Basic Network	•	Enabled	
🕆 WLAN	•	Auth Type	NONE ¥
Advanced Network		WEB Root	Default ¥
Port Forwarding		TED NOT	
Port Redirecting DMZ		WEB Host	
 IP Passthrough Triggered 		Portal Host	
Captive Portal		Login Timeout	0 Minutes
Serial App. UPnP/NAT-PMP Bandwidth Limiter		Idle Timeout	0 Minutes
VRRP Static DHCP		Ignore LAN	
Firewall	•	Redirecting http://	www.google.com
VPN Tunnel	•	MAC Address Whitelist	
R Administration	•	Download QOS	
		Upload QOS	
More Info		Save-2 Cancel X	

1) Upload Portal file and Splash.html by local

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

Furthermore, also might upload splash with images together.

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

WL-G930 Series Router User Manual

Status	۲	Yo	ou haven't changed the default passwo	rd for this router. To change router password <u>click here.</u>	
Basic Network					
🕏 WLAN		Storage settings			~
Advanced Network		Storage	Router Total :5,632.00 KB Fr	ree:5,372.00 KB	
🔕 Firewall					
VPN Tunnel		Upload new file			~
R Administration		No file chosen Cho	pose File Upload		
- Identification - Time			_		
Admin Access		Current file list			~
Scheduled Reboot					
 SNMP Storage Settings 		File name	File size	File operation	
M2M Settings		sms.list	159	× G	
DI/DO Setting					
Configuration					
— Logging		Save ✓ Cancel ×			
Upgrade		Javey Califern			
① More Info					

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

Ø 1	Status Basic Network WLAN	> > >	Storage settings	Router V Tot	tal :5,632.00 ks Free:5,100.00 ks		~
	Advanced Network Firewall VPN Tunnel Administration	> > >	Upload new file No file chosen	Choose File Upload			v
	Identification Time Admin Access Scheduled Reboot		Current file list File name		File size	File operation	~
			0001_portal.png		23.8K	× E	
	SNMP Storage Settings M2M Settings DI/DO Setting Configuration Logging Upgrade		0001_portal.png 0002_portal.png 0003_portal.png bootstrap_portal.css jquery_portaljs splash.html		23.8K 45.3K 46.0K 124.3K 289.7K 3.4K	* 8 * 8 * 8 * 8	



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

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

ML

. IP

ৰ জাৱে ৪০% এ ৫০% এ ৫০% এ ৫০% এ ৫০% এ Sign in to Wi-Fi network MORE

Welcome to Wi-Fi Hotspot



Welcome to our open community WiFi network!

You are solely responsible for any illegal activities once you click the "OK, I AGREE" button. We are not responsible for faulty operation of your computer or equipment. You may be asked to stop using your equipment. This banner will appear again periodically. Thank You, and Enjoy!



2) Modify portal file storage path

Modify portal file storage for In-storage as below.



O Status	Captive Portal	
Basic Network	Enabled	
🗇 WLAN		
Advanced Network	Auth Type	NONE V
Port Forwarding Port Redirecting	WEB Root	In-storage 💌
DMZ	WEB Host	
IP Passthrough Triggered	Portal Host	
Captive Portal		
Serial App.	Login Timeout	0 Minutes
UPnP/NAT-PMP		
Bandwidth Limiter	Idle Timeout	0 Minutes
VRRP		
Static DHCP	Ignore LAN	
🔯 Firewall	Redirecting http://	www.google.com
VPN Tunnel		
R Administration	MAC Address Whitelist	
	Download QOS	
① More Info	Upload QOS	

3.4 GPS Settings

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

O Status	You haven't changed the default password for this router. To change router password <u>click here.</u>				
Basic Network					
ବି WLAN	GPS				
Advanced Network	GPS Mode	Client			
Port Forwarding	Data Format	M2M_FMT V			
 Port Redirecting DMZ 		192.168.1.2 : 40002			
- IP Passthrough	Server IP/Port	192.108.1.2			
Triggered	Heart-Beat Content				
Captive Portal Serial App.					
GPS	Heart-Beat Interval	5 (seconds)			
UPnP/NAT-PMP					
Bandwidth Limiter	Save ✓ Cancel ×				
Static DHCP					
Tirewall					
VPN Tunnel					
R Administration					
(i) More Info					

Figure 4-5 GPS GUI

Table 4-5 "GPS"	Instruction
-----------------	-------------

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



WL-G930 Series Router User Mar	ual
--------------------------------	-----

parameter	Instruction
Interval	GPS data transmit as the interval time.

Step 2 Please click "save" to finis

Step 3 Connect the GPS antenna to router GPS interface

Step 4 Check GPS Status

Status		You haven't	changed the default password for this router. To change router password <u>click here.</u>
Overview			이가 물건가 있는 것이가 있는 것 같아요. 정말한 것 같아요. 것 같아요. 한 것 같아요. 전 것 같아요. 물건가 있는 것 같아요. 것 같아요. 것 같아요. 것 같아요. 것 같아요. 것 같아요. 것 같아요. 물건가 있는 것이 같아요. 것 같아요. 것 같아요. 것 같아요. 것 같아요. 것 같아요. 물건가 있는 것 같아요. 가
Traffic Stats.		GPS Status	
GPS Status		Current	ОК
Device List		System Type	GPS
Basic Network	•	Satellites Numbers	05 .
🗟 WLAN	•	Satellites Clock	190404 - 022121.00
		Positioning	2234.22520N - 11356.63170E
Advanced Network	>	Google Map	View
🔯 Firewall	>		
VPN Tunnel	2		
R Administration	>		
 More Info 			



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

Field	Name	Format	Example	Description
No.				
1	Router ID	String	0001_R081850	0001 customizable product
			ac	ID.
				_R router indicator.



		市德传物联技术有限	公司 V	/L-G930 Series Router User Manual
				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	Ν	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.