Milesight

# Industrial Router Lite Series UR32L

User Guide



# Preface

Milesight

Thanks for choosing Milesight UR32L industrial cellular router. The UR32L industrial cellular router delivers tenacious connection over network with full-featured design such as automated failover/failback, extended operating temperature, dual SIM cards, hardware watchdog, VPN, Fast Ethernet and beyond.

This guide describes how to configure and operate the UR32L industrial cellular router. You can refer to it for detailed functionality and router configuration.

# Readers

This guide is mainly intended for the following users:

- Network Planners
- On-site technical support and maintenance personnel
- Network administrators responsible for network configuration and maintenance

#### © 2011-2024 Xiamen Milesight IoT Co., Ltd.

#### All rights reserved.

All information in this user guide is protected by copyright law. Whereby, no organization or individual shall copy or reproduce the whole or part of this user guide by any means without written authorization from Xiamen Milesight lot Co., Ltd.

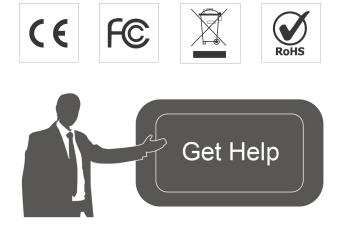
# **Safety Precautions**

Milesight will not shoulder responsibility for any loss or damage resulting from not following the instructions of this operating guide.

- The device must not be disassembled or remodeled in any way.
- To avoid risk of fire and electric shock, do keep the product away from rain and moisture before installation.
- Do not place the device where the temperature or humidity is below/above the operating range.
- The device must never be subjected to drops, shocks or impacts.
- Make sure the device is firmly fixed when installing.
- Make sure the plug is firmly inserted into the power socket.
- Do not pull the antenna or power supply cable, detach them by holding the connectors.

# **Declaration of Conformity**

UR32L is in conformity with the essential requirements and other relevant provisions of the CE, FCC, and RoHS.



For assistance, please contact Milesight technical support: Email: iot.support@milesight.com Support Portal: support.milesight-iot.com Tel: 86-592-5085280 Fax: 86-592-5023065 Address: Building C09, Software Park III, Xiamen 361024, China

# **Revision History**

Milesight

Date	Doc Version	Description
Mar. 23, 2021	V 1.0	Initial version
Sept. 17, 2021	V 1.1	<ol> <li>Cellular and ping detection support IPv6</li> <li>Add WAN connection type: DHCPv6 client, DS-Lite</li> <li>Add DHCPv6 Server feature</li> <li>Add IPv6 static routing feature</li> <li>Add Expert Option box in IPsec settings</li> <li>Support SMS inbox and outbox record clear</li> </ol>
June 30, 2023	V 1.2	<ol> <li>Add high priority link revert feature;</li> <li>Add MQTT and TR069 feature;</li> <li>Support customized cellular MTU and IMS;</li> <li>Support to import openVPN file configurations, add tls-crypt mode and authentication mode;</li> <li>Support to configure L2TP hostname.</li> </ol>
July 5, 2024	V 2.3	<ol> <li>Add WireGuard VPN feature;</li> <li>Add cellular band selection and subnet mask customization;</li> <li>Support to sync time with cellular operator;</li> <li>Support to show Ethernet port connection status and configure PoE settings;</li> <li>Update default secondary ICMP and DNS server address;</li> <li>IPsec setting web GUI optimization.</li> </ol>

# Contents

Chapter 1 Product Introduction	7
1.1 Overview	
1.2 Advantages	7
1.3 Specifications	8
1.4 Dimensions (mm)	9
Chapter 2 Access to Web GUI	10
Chapter 3 Web Configuration	
3.1 Status	11
3.1.1 Overview	11
3.1.2 Cellular	13
3.1.3 Network	14
3.1.4 VPN	15
3.1.5 Routing	
3.1.6 Host List	17
3.2 Network	17
3.2.1 Interface	17
3.2.1.1 Link Failover	17
3.2.1.2 Cellular	19
3.2.1.3 Port	
3.2.1.4 WAN	24
3.2.1.5 Bridge	29
3.2.1.6 Switch	
3.2.1.7 Loopback	31
3.2.2 DHCP	
3.2.2.1 DHCP Server/DHCPv6 Server	
3.2.2.2 DHCP Relay	
3.2.3 Firewall	
3.2.3.1 Security	34
3.2.3.2 ACL	35
3.2.3.3 Port Mapping (DNAT)	37
3.2.3.4 DMZ	
3.2.3.5 MAC Binding	38
3.2.3.6 Custom Rules	39
3.2.3.7 SPI	39
3.2.4 QoS	
3.2.5 VPN	41
3.2.5.1 DMVPN	41
3.2.5.2 IPSec Server	43
3.2.5.3 IPSec	46
3.2.5.4 GRE	

	3.2.5.5 L2TP	50
	3.2.5.6 PPTP	53
	3.2.5.7 OpenVPN Client	54
	3.2.5.8 OpenVPN Server	57
	3.2.5.9 Certifications	60
	3.2.5.10 WireGuard	61
	3.2.6 IP Passthrough	63
	3.2.7 Routing	64
	3.2.7.1 Static Routing	64
	3.2.7.2 RIP	65
	3.2.7.3 OSPF	68
	3.2.7.4 Routing Filtering	74
	3.2.8 VRRP	74
	3.2.9 DDNS	76
3.3	3 System	
	3.3.1 General Settings	
	3.3.1.1 General	
	3.3.1.2 System Time	
	3.3.1.3 Email	79
	3.3.2 Phone&SMS	81
	3.3.2.1 Phone	81
	3.3.2.2 SMS	82
	3.3.3 User Management	84
	3.3.3.1 Account	
	3.3.3.2 User Management	
	3.3.4 AAA	
	3.3.4.1 Radius	86
	3.3.4.2 TACACS+	86
	3.3.4.3 LDAP	
	3.3.4.4 Authentication	88
	3.3.5 Device Management	
	3.3.5.1 DeviceHub	
	3.3.5.2 Milesight VPN	
	3.3.6 Events	
	3.3.6.1 Events	
	3.3.6.2 Events Settings	
3.4	Service	
	3.4.1 MQTT	
	3.4.2 SNMP	
	3.4.2.1 SNMP	
	3.4.2.2 MIB View	
	3.4.2.3 VACM	
	3.4.2.4 Trap	
	3.4.2.5 MIB	

3.4.3 TR069	100
3.5 Maintenance	102
3.5.1 Tools	
3.5.1.1 Ping	102
3.5.1.2 Traceroute	102
3.5.1.3 Packet Analyzer	102
3.5.1.4 Qxdmlog	103
3.5.2 Debugger	103
3.5.2.1 Cellular Debugger	
3.5.2.2 Firewall Debugger	104
3.5.3 Log	105
3.5.3.1 System Log	
3.5.3.2 Log Download	106
3.5.3.3 Log Settings	107
3.5.4 Upgrade	108
3.5.5 Backup and Restore	
3.5.6 Reboot	109
Chapter 4 Application Examples	110
4.1 Network Connection	110
4.1.1 Cellular Connection	110
4.1.2 Ethernet WAN Connection	111
4.2 OpenVPN Client Application Example	112
4.3 NAT Application Example	114
4.4 Restore Factory Defaults	115
4.5 Firmware Upgrade	117
4.6 SNMP Application Example	
4.7 VRRP Application Example	120
4.8 QoS Application Example	123

# **Chapter 1 Product Introduction**

## 1.1 Overview

UR32L is an industrial cellular router with embedded intelligent software features that are designed for multifarious M2M/IoT applications. Supporting global WCDMA and 4G LTE, UR32L provides drop-in connectivity for operators and makes a giant leap in maximizing uptime.

Adopting high-performance and low-power consumption industrial grade CPU and wireless module, the UR32L is capable of providing wire-speed network with low power consumption and ultra-small package to ensure the extremely safe and reliable connection to the wireless network.

UR32L is particularly ideal for smart grid, digital media installations, industrial automation, telemetry equipment, medical device, digital factory, finance, payment device, environment protection, water conservancy and so on.

For details of hardware and installation, please check UR32L Quick Start Guide.

## 1.2 Advantages

#### Benefits

- Built-in industrial strong NXP CPU, big memory
- Fast Ethernet for fast data transmission
- Rugged enclosure, optimized for DIN rail or shelf mounting
- 3-year warranty included

#### Security & Reliability

- Automated failover/failback between Ethernet and Cellular
- Enable unit with security frameworks like IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN/WireGuard
- Embed hardware watchdog, automatically recovering from various failure, and ensuring highest level of availability
- Establish a secured mechanism on centralized authentication and authorization of device access by supporting AAA (TACACS+, Radius, LDAP, local authentication) and multiple levels of user authority

#### **Easy Maintenance**

- Milesight DeviceHub provides easy setup, mass configuration, and centralized management of remote devices
- The user-friendly web interface design and more than one option of upgrade help administrator to manage the device as easy as pie
- Web GUI and CLI enable the admin to achieve simple management and quick configuration among a large quantity of devices

- Efficiently manage the remote routers on the existing platform through the industrial standard SNMP and TR069

# Capabilities

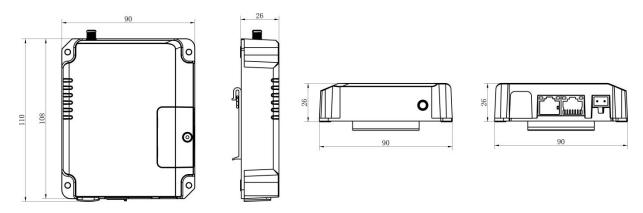
- Link remote devices in an environment where communication technologies are constantly changing
- Industrial 32-bit ARM Cortex-A7 processor, high-performance operating up to 528MHz and 128
   MB memory available to support more applications
- Support rich protocols like SNMP, TR069, MQTT, RIP, OSPF
- Support wide operating temperature ranging from -40°C to 70°C/-40°F to 158°F

Hardware System	
CPU	528MHz, 32-bit ARM Cortex-A7
Memory	128 MB Flash, 128 MB DDR3 RAM
Cellular Interfaces	
Connectors	$1 \times 50 \Omega$ SMA (Center pin: SMA Female)
SIM Slots	1 (Mini SIM-2FF)
Ethernet	
Ports	2 × RJ-45 (PoE PSE Optional)
Physical Layer	10/100 Base-T (IEEE 802.3)
Data Rate	10/100 Mbps (auto-sensing)
Interface	Auto MDI/MDIX
Mode	Full or half duplex (auto-sensing)
Software	
Network Protocols	IPv4/IPv6, PPP, PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, RIPv1/v2, OSPF, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, QoS, SNTP, Telnet, VLAN, SSH, MQTT, MQTTS, TR069, etc.
VPN Tunnel	DMVPN/IPsec/OpenVPN/PPTP/L2TP/GRE/WireGuard
Firewall	ACL/DMZ/Port Mapping/MAC Binding/SPI/DoS&DDoS Protection /IP Passthrough
Management	Web, CLI, SMS, On-demand dial up, DeviceHub
AAA	Radius, TACACS+, LDAP, Local Authentication
Multilevel Authority	Multiple levels of user authority

# **1.3 Specifications**

Reliability	VRRP, WAN Failover
Power Supply and Consu	mption
Connector	2-pin with 5.08 mm terminal block
Input Voltage	9-48 VDC
Power Consumption	Typical 1.8 W, Max 2.2 W (In Non-PoE mode)
Power Output (Optional)	2 × 802.3 af/at PoE output
Physical Characteristics	
Ingress Protection	IP30
Housing & Weight	Metal, 212 g
Dimensions	108 x 90 x 26 mm (4.25 x 3.54 x 1.02 in)
Mounting	Desktop, wall or DIN rail mounting
Others	
Reset Button	1 × RESET
LED Indicators	1 × POWER, 1 × SYSTEM, 1 × SIM, 3 × Signal strength
Built-in	Watchdog, Timer
Environmental	
	-40°C to +70°C (-40°F to +158°F)
Operating Temperature	Reduced cellular performance above 60°C
Storage Temperature	-40°C to +85°C (-40°F to +185°F)
Ethernet Isolation	1.5 kV RMS
Relative Humidity	0% to 95% (non-condensing) at 25°C/77°F

# 1.4 Dimensions (mm)



# **Chapter 2 Access to Web GUI**

This chapter explains how to access to Web GUI of the UR32L router. Connect PC to LAN port of UR32L router directly. The following steps are based on Windows 10 operating system for your reference.

Username: **admin** Password: **password** IP Address: **192.168.1.1** 

1. Go to "Control Panel"  $\rightarrow$  "Network and Internet"  $\rightarrow$  "Network and Sharing Center", then click "Ethernet" (May have different names).

Network and Sharing Center		- 0	>
> 👻 🛧 😫 « Network	and Internet > Network and Sharing Center	✓ ♂ Search Control Panel	۶
Control Panel Home	View your basic network information	n and set up connections	
Change adapter settings	View your active networks		
Change advanced sharing settings	Yeastar5G Private network	Access type: Internet HomeGroup: Ready to create Connections: Wi-Fi (Yeastar5G)	
	ldentifying	Access type: No network access Connections: U Ethernet	
	Change your networking settings		
	Set up a new connection or network Set up a broadband, dial-up, or VPN c	Ethernet	
	Troubleshoot problems Diagnose and repair network problem	is, or get troubleshooting information.	
See also			
HomeGroup			
Infrared			
Internet Options			
Windows Firewall			

2. Go to "Properties"  $\rightarrow$  "Internet Protocol Version 4(TCP/IPv4)", select "Obtain an IP address automatically" or "Use the following IP address", then assign a static IP manually within the same subnet of the device.

nternet Protocol Version 4 (TCP/	IPv4) Properties X	Internet Protocol Version 4 (TCP/IPv4) Properties	
General Alternate Configuration		General	-
	automatically if your network supports ed to ask your network administrator	You can get IP settings assigned 192.168. for the appropriate IP settings. 255.255.	Provide a second s
Obtain an IP address autom	atically	Obtain an IP address autom 192.168.	1.1
O Use the following IP address	:	Use the following IP address:	
IP address:		IP address: 192 . 168 .	1 , 20
Subnet mask:		Subnet mask: 255 . 255 . 2	55. 0
Default gateway:		Default gateway: 192 . 168 .	1.1
Obtain DNS server address a	automatically	Obtain DNS server address automatically	
Use the following DNS serve	r addresses:	Use the following DNS server addresses:	
Preferred DNS server:	a	Preferred DNS server: 192 . 168 .	1.1
Alternate DNS server:		Alternate DNS server:	•
Validate settings upon exit	Advanced	Validate settings upon exit 192.168.	1.1
	OK Cancel	OK	Cancel

3. Open a Web browser on your PC (Chrome is recommended), type in the IP address 192.168.1.1, and press Enter on your keyboard.

4. Enter the username, password, and click "Login".

- Arrest	Language English v
	Je i
2 A	

If you enter the username or password incorrectly more than 5 times, the login page will be locked for 10 minutes.

5. When you login with the default username and password, you will be asked to modify the password. It's suggested that you change the password for the sake of security. Click "Cancel" button if you want to modify it later.

Old Password	
Old Password	
New Password	
Confirm New Password	

6. After you login the Web GUI, you can view system information and perform configuration on the router.

# **Chapter 3 Web Configuration**

# 3.1 Status

#### 3.1.1 Overview

You can view the system information of the router on this page.

Milesight

Connected Devices

Overview	Cellular	Network	VPN	Routing	Host List	
System Informa	ation				System Status	
Model		UR32L-L04EU			Local Time	2021-09-17 08:27:58 Friday
Serial Number		6224B2227522			Uptime	00:01:38
Firmware Version	1	32.3.0.2			CPU Load	17%
Hardware Version	n	V3.0			RAM (Available/Capacity)	48MB/128MB(37.5%)
					Flash (Available/Capacity)	90MB/128MB(70.31%)
Cellular 🕒 Lini	k in use				WAN	
Status		Ready, TDD LTE	Tul		Status	Offline
IPv4		10.15.114.165/30	)		IPv4	192.168.22.212
IPv6		fe80::c4c:e5ff.fe5	3:3776/64		IPv6	fe80::26e1:24ff.fef1:f741/64
Connection Durat	tion	0 days, 00:00:16			MAC	24:e1:24:f1:f7:43
Data Usage Mont	thly	0.2 MiB			Connection Duration	0 days, 00:00:00
LAN						
IPv4		192.168.1.1				
IPv6		7171::1/64				

# Figure 3-1-1-1

System Information		
Item	Description	
Model	Show the model name of router.	
Serial Number	Show the serial number of router.	
Firmware Version	Show the currently firmware version of router.	
Hardware Version	Show the currently hardware version of router.	
	Table 3-1-1-1 System Information	

System Status				
ltem	Description			
Local Time	Show the currently local time of system.			
Uptime	Show the information on how long the router has been running.			
CPU Load	Show the current CPU utilization of the router.			
CPU Temperature	Show current CPU temperature.			
RAM (Available/Capacity)	Show the RAM capacity and the available RAM memory.			
Flash (Available/Capacity)	Show the Flash capacity and the available Flash memory.			

Table 3-1-1-2 System Status

Cellular				
Item	Description			
Status	Show the real-time status of the currently SIM card			
Current SIM	Show the SIM card currently used for the data connection.			
IPv4/IPv6	Show the IPv4/IPv6 address obtained from the mobile carrier.			

<b>Connection Duration</b>	Show the connection duration of the currently SIM card.			
Data Usage Monthly	Show the monthly data usage statistics of currently used SIM card.			
Table 3-1-1-3 Cellular Status				
WAN				
Item	Description			
Status	Show the currently status of WAN port.			
IPv4/IPv6	The IPv4/IPv6 address configured WAN port.			
MAC	The MAC address of the Ethernet port.			
<b>Connection Duration</b>	Show the connection duration of the WAN port.			
	Table 3-1-1-4 WAN Status			

LAN	
ltem	Description
IP4/IPv6	Show the IP4/IPv6 address of the LAN port.
Connected Devices	Number of devices that connected to the router's LAN.

Table 3-1-1-5 LAN Status

# 3.1.2 Cellular

You can view the cellular network status of router on this page.

Overview	Cellular	Network	VPN	Routing	Host List	
Modem					Network	
Model		EC25			Status	Connected
Version		EC25EUXGA	R08A05M1G		IPv4 Address	10.142.57.34/30
Signal Level		23asu (-67dB	m)		IPv4 Gateway	10.142.57.33
Register Status		Registered (H	lome network)		IPv4 DNS	211.136.17.107
IMEI		86250604370	7416		IPv6 Address	fe80::cca3:25ff:fed2:908/64
IMSI		46008137050	7437		IPv6 Gateway	=
ICCID		89860493262	190157437		IPv6 DNS	
ISP		CHINA MOBI	LE		Connection Duration	0 days, 00:00:04
Network Type		TDD LTE			Data Usage Monthly	
PLMN ID		46000				0.0.117
LAC		592f			RX	0.0 MIB
Cell ID		ceb972a			ТХ	0.0 MiB
					ALL	0.0 MiB

#### Figure 3-1-2-1

Modem Information			
Item	Description		
Status	Show corresponding detection status of module and SIM card.		
Version	Show the cellular module firmware version.		
Signal Level	Show the cellular signal level.		
Register Status	Show the registration status of SIM card.		

IMEI	Show the IMEI of the module.
IMSI	Show IMSI of the SIM card.
ICCID	Show ICCID of the SIM card.
ISP	Show the network provider which the SIM card registers on.
Network Type	Show the connected network type, such as LTE, 3G, etc.
PLMN ID	Show the current PLMN ID, including MCC, MNC, LAC and Cell ID.
LAC	Show the location area code of the SIM card.
Cell ID	Show the Cell ID of the SIM card location.

Table 3-1-2-1 Modem Information

Network			
Item	Description		
Status	Show the connection status of cellular network.		
IPv4/IPv6 Address	Show the IPv4/IPv6 address and netmask of cellular network.		
IPv4/IPv6 Gateway	Show the IPv4/IPv6 gateway and netmask of cellular network.		
IPv4/IPv6 DNS	Show the IPv4/IPv6 DNS of cellular network.		
Connection Duration	Show information on how long the cellular network has been connected.		

Table 3-1-2-2 Network Status

Data Usage Monthly		
ltem	Description	
RX	Show the monthly rx data usage statistics of SIM.	
ТХ	Show the monthly tx data usage statistics of SIM.	
ALL	Show the monthly all data usage statistics of SIM.	

Table 3-1-2-3 Data Usage Information

# 3.1.3 Network

On this page you can check the WAN and LAN status of the router.

WAN-IPv4						
Port	Status	Туре	IPv4	Gateway	DNS	Connection Duration
LAN1/WAN	up	Static	192.168.22.210/24	192.168.22.1	114.114.114.114	08h 32m 53s
WAN-IPv6						
Port	Status	Туре	IPv6	Gateway	DNS	Connection Duration
LAN1/WAN	up	Static	fe80::26e1:24ff:fef1:2fea/64		100	08h 32m 53s



WAN Status		
ltem	Description	
Port	Show the name of WAN port.	
Status	Show the status of WAN port. "up" refers to a status that WAN is enabled and Ethernet cable is connected. "down" means Ethernet cable is disconnected or WAN function is disabled.	
Туре	Show the dial-up connection type of WAN port.	

IPv4/IPv6	Show the IPv4 address with netmask or IPv6 address with prefix-length of WAN port.
Gateway	Show the gateway of WAN port.
DNS	Show the DNS of WAN port.
Connection Duration	Show the information on how long the Ethernet cable has been connected on WAN port when WAN function is enabled. Once WAN function is disabled or Ethernet connection is disconnected, the duration will stop.

#### Table 3-1-3-1 WAN Status

Bridge				
Name	STP	IPv4	IPv6	Members
Bridge0	Disabled	192.168.219.1/24	7878::1/64	vlan 1,WLAN

#### Figure 3-1-3-2

Bridge					
ltem	Description				
Name	Show the name of the bridge interface.				
STP	Show if STP is enabled.				
IPv4/IPv6	Show the IPv4/IPv6 address and netmask of the bridge interface.				
Netmask	Show the Netmask of the bridge interface.				
Members	Show the members of the bridge interface.				

Table 3-1-3-2 Bridge Status

## 3.1.4 VPN

You can check VPN status on this page, including PPTP, L2TP, IPsec, OpenVPN and DMVPN.

Clients				
	Name	Status	Local IP	Remote IP
Server				
	Name			Status
	OpenVPN Server			Disabled
	Ipsec Server			Disabled
Connected List				
Server Type			Client IP	Duration



VPN Status	
Item	Description
Clients	
Name	Show the name of the enabled VPN clients.

Show the status of client. "Connected" refers to a status that client is connected to the server. "Disconnected" means client is disconnected to the server.
Show the local IP address of the tunnel.
Show the real remote IP address of the tunnel.
Show the name of the enabled VPN Server.
Show the status of Server.
Show the type of the server.
Show the IP address of the client which connected to the server.
Show the information about how long the client has been connected to this server when the server is enabled. Once the server is disabled or connection is disconnected, the duration will stop counting.

Table 3-1-4-1 VPN Status

# 3.1.5 Routing

You can check routing status on this page, including the routing table and ARP cache.

Routing Table					
	Destination	Netmask/Prefix Length	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.40.1	LAN1/WAN	1
	8.8.8	255.255.255.255	192.168.40.1	LAN1/WAN	1
	114.114.114.114	255.255.255.255	192.168.40.1	LAN1/WAN	1
	127.0.0.0	255.0.0.0	-	Loopback	-
	192.168.2.0	255.255.255.0	5-	vlan2	-
	192.168.3.0	255.255.255.0	-	vlan3	-
	192.168.10.0	255.255.255.0	1-	Bridge0	<i>w</i>
	192.168.40.0	255.255.255.0	-	LAN1/WAN	-
	::1	128	6 <u>.</u>	Loopback	1900 - 1900 - 1900 - 1900 - 1900 - 1900 - 1900 - 1900 - 1900 - 1900 - 1900 - 1900 - 1900 - 1900 - 1900 - 1900 -
ARP Cache					
	IP		MAC		nterface
	192.168.10.101	00:0	0:00:00:00:00		Bridge0
	192.168.40.201	24:	e1:24:f6:64:2f	L	AN1/WAN
	192.168.40.9	08:0	0:27:0a:1a:21	L	AN1/WAN
	192.168.40.35	58:	11:22:92:f8:c4	L	AN1/WAN
	8.8.8.8	00:0	0:00:00:00:00	L	AN1/WAN
	192.168.40.41	50:	eb:f6:9f:aa:60	L	AN1/WAN Manual Refresh V

Figure 3-1-5-1

lik e ne	Description	
ltem	Description	

Routing Table	
Destination	Show the IP address of destination host or destination network.
Netmask/Prefix Length	Show the netmask or prefix length of destination host or destination network.
Gateway	Show the IP address of the gateway.
Interface	Show the outbound interface of the route.
Metric	Show the metric of the route.
ARP Cache	
IP	Show the IP address of ARP pool.
MAC	Show the IP address's corresponding MAC address.
Interface	Show the binding interface of ARP.

Table 3-1-5-1 Routing Information

# 3.1.6 Host List

You can view the host information on this page.

DHCP Leases					
	IP		MAC/DUID	Lease Remaining Time	
	192.168.1.113		c8:5b:76:b2:56:1f	23h 07m 24s	
	2004::200		00:01:00:01:27:cc:cf:61:c8:5b:76:b2:56:1f	23h 09m 22s	
MAC Binding					
		lb		MAC/DUID	

Figure 3-1-6-1

Host List				
Description				
Show IP address of DHCP client				
Show MAC address of DHCPv4 client or DUID of DHCPv6 client.				
Show the remaining lease time of DHCP client.				
MAC Binding				
Show the IP address and MAC address set in the Static IP list of DHCP service.				

Table 3-1-6-1 Host List Description

# 3.2 Network

## 3.2.1 Interface

# 3.2.1.1 Link Failover

This section describes how to configure link failover strategies, their priority and the ping settings, each rule owns its own ping rules by default. Router will follow the priority to choose the next available interface to access the internet, make sure you have enable the full interface that you need to use here. If priority 1 can only use IPv4, UR32L will select a second link which IPv6 works as main IPv6 link and vice versa.

Link Failo	over	Cellular	Port	WAN	Bridge	Switch	Loopback		
Link Priori	ity								
Prio	ority	Enable Rule	Link in use		Interface	Connection	on Type	IP	Operation
1	1				WAN	Stat	tic	192.168.22.212	
2	2		•	(	Cellular-SIM1	DHC	CP	-	
Settings									
Revert Inter	rval		30		S				
Emergency	/ Reboot								
Save									

Figure 3-2-1-1

Link Failover					
ltem	Description				
Link Priority					
Priority	Display the priority of each interface, you can modify it by the operation's up and down button.				
Enable Rule	If enabled, the router will put this interface into its switching rule. For the Cellular interface, if it's not enabled here, the interface will be disabled as well.				
Link In Use	Mark whether this interface is in use with Green color				
Interface	Display the name of the interface.				
Connection type	Display how to obtain the IP address in this interface, like static IP or DHCP.				
IP	Display the IP address of the interface.				
Operation	You can change the priority of the rules and configure the ping detection rules here.				
Settings					
Revert to High	When the connection of high priority link returns back, reverting				
Priority Link	back to high priority link.				
Revert Interval	Specify the number of seconds to waiting for switching to the link with higher priority, 0 means disable the function.				
<b>Emergency Reboot</b>	Enable to reboot the device if no link is available.				

Table 3-2-1-1 Link Failover Parameters

Enable			
IPv4 Primary Server	8.8.8.8		
IPv4 Secondary Server	223.5.5.5		
IPv6 Primary Server	2001:4860:4860::8888		
IPv6 Secondary Server	2400:3200::1		
Interval	300	s	
Retry Interval	5	s	
Timeout	3	s	
Max Ping Retries	3		

Figure 3-2-1-2

Ping Detection					
ltem	Description				
Enable	If enabled, the router will periodically detect the connection status of the link.				
IPv4/IPv6 Primary Server	The router will send ICMP packet to the IPv4/IPv6 address or hostname to determine whether the Internet connection is still available or not.				
IPv4/IPv6 Secondary Server	The router will try to ping the secondary server name if primary server is not available.				
Interval	Time interval (in seconds) between two Pings.				
Retry Interval	Set the ping retry interval. When ping failed, the router will ping again in every retry interval.				
Timeout	The maximum amount of time the router will wait for a response to a ping request. If it does not receive a response for the amount of time defined in this field, the ping request will be considered to have failed.				
Max Ping Retries	The retry times of the router sending ping request until determining that the connection has failed.				

Table 3-2-1-2 Ping Detection Parameters

## 3.2.1.2 Cellular

This section explains how to set the related parameters for the cellular network.

Protocol Type	IPv4 🗸
APN	
Username	
Password	ø
PIN Code	ø
Access Number	
Authentication Type	None 🗸
Network Type	Auto 🗸
Cellular Frequency Band	B1, B2, B3, B4, B5, B7, B8, B28, B40
PPP Preferred	
IMS Enable	
SMS Center	
Enable NAT	
Roaming	
IPv4 Subnet Mask	
Customize MTU	
МТО	1500
Data Limit	110 MB
Billing Day	Day 1 🗸 of The Month



Cellular Settings						
Item	Description					
Protocol Type	Select from "IPv4", "IPv6" and "IPv4/IPv6".					
APN	Enter the Access Point Name for the cellular dial-up connection provided by the local ISP.					
Username	Enter the username for the cellular dial-up connection provided by the local ISP.					
Password	Enter the password for the cellular dial-up connection provided by the local ISP.					
PIN Code	Enter a 4-8 characters PIN code to unlock the SIM.					
Access Number	Enter the dial-up center NO. For cellular dial-up connection provided by local ISP.					
Authentication Type	Select from "None", "PAP", or "CHAP".					
Network Type	Select from "Auto", "4G Only", "3G Only", and "2G Only". Auto: connect to the network with the strongest signal automatically.					

	4G Only: connect to 4G network only.
	And so on.
Cellular Frequency	Select the cellular bands used to register the cellular network. It can be
Band	used to optimize cellular speeds by selecting specific bands.
PPP Preferred	The PPP dial-up method is preferred.
IMS Enable	Enable or disable IMS function.
SMS Center	Enter the local SMS center number for storing, forwarding, converting
SIVIS Certiter	and delivering SMS message.
Enable NAT	Enable or disable NAT function.
Roaming	Enable or disable roaming.
IPv4 Subnet Mask	Customize the cellular subnet mask. If blank, the device will use the
IF V4 SUDITEL IVIASK	subnet mask provided by the cellular base station.
Customize MTU	Enable or disable to customize the maximum transmission units. When
Customize wito	disabled, the device will use the operator's MTU settings.
MTU	Customize the maximum transmission units.
	When you reach the specified data usage limit, the data connection of
Data Limit	the currently used SIM card will be disabled. 0 means disable the
	function.
Pilling Dov	Choose the billing day of the SIM card, the router will reset the data used
Billing Day	to 0.

Table 3-2-1-3 Cellular Parameters

Connection Setting	
Connection Mode	Connect on Demand 🗸
Re-dial Interval(s)	5
Max Idle Time(s)	60
Triggered by Call	
Call Group	~
Triggered by SMS	
SMS Group	~
SMS Text	

Figure 3-2-1-4

Connection Setting					
Item	Description				
Connection Mode	Select "Always Online" and "Connect on Demand".				
Re-dial Interval(s)	Set the interval to dial into ISP when it loses connection, the default value is 5s.				
Max Idle Times	Set the maximum duration of the router when the current link is under idle status. Range: 10-3600				

Triggered by Call	The router will switch from offline mode to cellular network mode automatically when it receives a call from a specific phone number.
Call Group	Select a call group for the call trigger. Go to <b>System &gt; Phone&amp;SMS &gt; Phone</b> to set up phone group.
Triggered by SMS	The router will switch from offline mode to cellular network mode automatically when it receives a specific SMS from the specific mobile phone.
SMS Group	Select an SMS group for the trigger. Go to <b>System &gt; Phone&amp;SMS &gt; SMS</b> to set up an SMS group.
SMS Text	Fill in the SMS content for triggering.

Table 3-2-1-4 Cellular Parameters

## **Related Topics**

Milesight

<u>Cellular Network Connection</u> <u>Phone Group</u>

## 3.2.1.3 Port

This section describes how to configure the Ethernet port parameters. UR32L cellular router supports 2 Fast Ethernet ports.

Port Setting									
Port	Connection Status	Status		Property		Speed		Duplex	
LAN1/WAN	Connected	up 🗸		wan	~	auto	~	auto	~
LAN2	Connected	up	~	lan	~	auto	~	auto	~

Figure 3-2-1-5

Port Setting					
ltem	Description				
Port	Users can define the Ethernet ports according to their needs.				
Connection Status	Show the connection status of this Ethernet port.				
Status	Set the status of the Ethernet port; select "up" to enable and "down" to disable.				
Property	Show the Ethernet port's type, as a WAN port or a LAN port.				
Speed	Set the Ethernet port's speed. The options are "auto", "100 Mbps", and "10 Mbps".				
Duplex	Set the Ethernet port's mode. The options are "auto", "full", and "half".				

Table 3-2-1-5 Port Parameters

# Note:

• Only the PoE version (model name included "-P") supports the below settings.

- These settings only work when this router is powered by 48V.
- Only the devices with hardware version 4.0 and later support these features.
- Only when the port property of LAN1/WAN is set to LAN port, the PoE setting will work.

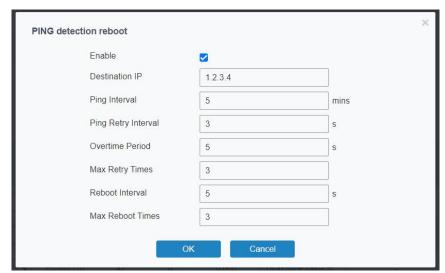
#### PoE

Port	PoE	Power Supply	Voltage (V)	Current (mA)	Power (W)	Describe	PING detection IP	Operation
LAN1	Enable 🗸	Power On	47	79	3.745		1.2.3.4	
LAN2	Enable V	Power On	47	120	5.688		1.2.3.4	



PoE Setting						
Item	Description					
Port	Users can define the Ethernet ports according to their needs.					
PoE	Enable or disable this Ethernet port to supply power.					
Power Supply	Show the power supply status of this Ethernet port.					
Voltage	Show the current output voltage of this Ethernet port.					
Current	Show the current output current of this Ethernet port.					
Power	Show the current output power of this Ethernet port.					
Describe	Add the description of this Ethernet port.					
Ping Detection	Show the IP address to send ICMP packet to detect the connection					
IP	status.					
Operation	You can change the power supply priority of the ports and configure the ping detection rules here.					







Ping Detection reboot	
Item	Description
Enable	If enabled, the router will periodically detect the connection status of the port. If detection fails, the router will reboot this port.

Destination IP	The router will send an ICMP packet to the IPv4 address to determine whether the connection is still available or not.
Interval	Time interval (in seconds) between two Pings.
Ping Retry Interval	Set the ping retry interval. When ping fails, the router will ping again in every retry interval.
Overtime Period	The maximum amount of time the router will wait for a response to a ping request. If it does not receive a response for the amount of time defined in this field, the ping request will be considered to have failed.
Max Ping Retries	The retry times of the router sending ping request until determining that the connection has failed.
Reboot Interval	The power-off interval of this Ethernet port.
Max Reboot Times	The retry times of the router rebooting this port. 0 means no limits.

Table 3-2-1-7 Ping Detection Parameters

## 3.2.1.4 WAN

The WAN port can be connected with an Ethernet cable to get Internet access.

N Settings	
- WAN_1	
Enable	
Port	LAN1/WAN
Connection Type	Static IP
IPv4 Address	192.168.40.166
Netmask	255.255.255.0
IPv4 Gateway	192.168.40.1
IPv6 Address	fe80::26e1:24ff:fe0b:6443
Prefix Length	64
IPv6 Gateway	
MTU	1500
IPv4 Primary DNS	8.8.8.8
IPv4 Secondary DNS	
IPv6 Primary DNS	
IPv6 Secondary DNS	
Enable NAT	

Figure 3-2-1-8

WAN Setting			
Item	Description	Default	
Enable	Enable WAN function.	Enable	
Port	The port that is currently set as WAN port.	WAN	
	Select connection type as required.		
	Static IP: assign a static IP address, netmask and		
	gateway for Ethernet WAN interface.		
	DHCP Client: configure Ethernet WAN interface as		
	DHCP Client to obtain IP address automatically.		
	<b>PPPoE</b> : configure Ethernet WAN interface as		
Connection Type	PPPoE Client.	Static IP	
	-DHCPv6 Client: configure Ethernet WAN interface		
	as DHCP Client to obtain IPv6 address		
	automatically.		
	Dual-Stack Lite: use IPv4-in-IPv6 tunneling to send		
	terminal device's IPv4 packet through a tunnel on		
	the IPv6 access network to the ISP.		
MTU	Set the maximum transmission unit.	1500	
IPv4 Primary DNS	Set the primary IPv4 DNS server.	8.8.8.8	
IPv4 Secondary DNS	Set the secondary IPv4 DNS server.		
IPv6 Primary DNS	Set the primary IPv6 DNS server.		
IPv6 Secondary DNS	Set the secondary IPv6 DNS server.		
Enable NAT	Enable or disable NAT function. When enabled, a private IP can be translated to a public IP.	Enable	

Table 3-2-1-8 WAN Parameters

# 1. Static IP Configuration

If the external network assigns a fixed IP for the WAN interface, select Static IP mode.

Enable	
Port	LAN1/WAN
Connection Type	Static IP 🗸
IPv4 Address	192.168.45.194
Netmask	255.255.255.0
IPv4 Gateway	192.168.45.1
IPv6 Address	fe80::26e1:24ff:fef0:ef7f
Prefix Length	64
IPv6 Gateway	
MTU	1500
IPv4 Primary DNS	8.8.8.8
IPv4 Secondary DNS	223.5.5.5
IPv6 Primary DNS	
IPv6 Secondary DNS	
Enable NAT	
Multiple IP Address	
IP A	ddress

Figure 3-2-1-9

Static IP			
ltem	Description	Default	
IPv4 Address	Set the IPv4 address of the WAN port.	192.168.0.1	
Netmask	Set the Netmask for WAN port.	255.255.255.0	
IPv4 Gateway	Set the gateway for WAN port's IPv4 address.	192.168.0.2	
IPv6 Address	Set the IPv6 address which can access the Internet.	Generated from Mac address	
Prefix-length	Set the IPv6 prefix length to identify how many bits of a Global Unicast IPv6 address are there in the network part. For example, in 2001:0DB8:0000:000b::/64, the number 64 is used to identify that the first 64 bits are in network part.	64	
IPv6 Gateway	Set the gateway for WAN port's IPv6 address. E.g.2001:DB8:ACAD:4::2.		
Multiple IP Address	Set the multiple IP addresses for WAN port.	Null	

Table 3-2-1-9 Static Parameters

# 2. DHCP Client/DHCPv6 Client

If the external network has DHCP server enabled and has assigned IP addresses to the Ethernet WAN interface, select DHCP/DHCPv6 client mode to obtain IP address automatically.

Enable	
Port	LAN1/WAN
Connection Type	DHCP Client 🗸
MTU	1500
Use Peer DNS	
IPv4 Primary DNS	8.8.8.8
IPv4 Secondary DNS	223.5.5.5
Enable NAT	



Enable		
Port	LAN1/WAN	
Connection Type	DHCPv6 Client	~
Request IPv6-address	None	~
Request IPv6-prefix of length	0-64	
MTU	1500	
IPv6 Primary DNS		
IPv6 Secondary DNS		
Enable NAT		



DHCP Client	
ltem	Description
Use Peer DNS	Obtain peer DNS automatically during PPP dialing. DNS is necessary when visiting domain name.
DHCPv6 Client	
Request IPv6-address	Choose the ways to obtain the IPv6 address from the DHCP Server. Select from try, force, none. Try: The DHCP Server will assign specific address in priority. Force: The DHCP Server assigns specific address only. None: The DHCP Server will randomly assign address.The specific address is relevant to the prefix length of IPv6 address you set.
Request prefix length of IPv6	Set the prefix length of IPv6 address which router is expected to obtain from DHCP Server.

Table 3-2-1-10 DHCP Client Parameters

# 3. PPPoE

PPPoE refers to a point to point protocol over Ethernet. User has to install a PPPoE client on the basis

of the original connection way. With PPPoE, remote access devices can get control of each user.

Enable		
Port	LAN1/WAN	
Connection Type	PPPoE	~
Username		
Password		
Link Detection Interval(s)	60	
Max Retries	0	
MTU	1500	
Use Peer DNS		
IPv4 Primary DNS	8.8.8.8	
IPv4 Secondary DNS	223.5.5.5	
Enable NAT		



PPPoE	
ltem	Description
Username	Enter the username provided by your Internet Service Provider (ISP).
Password	Enter the password provided by your Internet Service Provider (ISP).
Link Detection Interval (s)	Set the heartbeat interval for link detection. Range: 1-600.
Max Retries	Set the maximum retry times after it fails to dial up. Range: 0-9.
Use Peer DNS	Obtain peer DNS automatically during PPP dialing. DNS is necessary when visiting domain name.

Table 3-2-1-11 PPPoE Parameters

#### 4. Dual-Stack Lite

Dual-Stack Lite (DS-Lite) uses IPv4-in-IPv6 tunneling to send a subscriber's IPv4 packet through a tunnel on the IPv6 access network to the ISP. The IPv6 packet is decapsulated to recover the subscriber's IPv4 packet and is then sent to the Internet after NAT address and port translation and other LSN related processing. The response packets traverse through the same path to the subscriber.

Enable		
Port	LAN1/WAN	
Connection Type	Dual-Stack Lite	~
IPv6 Gateway		
DS-Lite AFTR Address		
Local IPv6 Address		
MTU	1500	
IPv4 Primary DNS	8.8.8.8	
IPv4 Secondary DNS	223.5.5.5	
IPv6 Primary DNS		
IPv6 Secondary DNS		
Enable NAT		

#### Figure 3-2-1-13

Dual-Stack Lite			
Item	Description		
IPv6 Gateway	Set the gateway for WAN port's IPv6 address.		
DS-Lite AFTR Address	Set the DS-Lite AFTR server address.		
Local IPv6 Address	Set the WAN port IPv6 address which use the same subnet as IPv6 gateway.		

Table 3-2-1-12 Dual-Stack Lite Parameters

# **Related Configuration Example**

Ethernet WAN Connection

## 3.2.1.5 Bridge

Bridge setting is used for managing local area network devices which are connected to LAN ports of the UR32L, allowing each of them to access the Internet.

Milesight

lame	Bridge0		
STP			
PAddress	192.168.1.1		
Netmask	255.255.255.0		
Pv6 Address	2004::1/64		
MTU	1500		
Multiple IP Address			
	IP Address	Netmask	Operation

Figure 3-2-1-14

Bridge		
Item	Description	Default
Name	Show the name of bridge. "Bridge0" is set by default and cannot be changed.	Bridge0
STP	Enable/disable STP.	Disable
IP Address	Set the IP address for bridge.	192.168.1.1
Netmask	Set the Netmask for bridge.	255.255.255. 0
IPv6 Address	Set the IPv6 address for bridge.	2004::1/64
MTU	Set the maximum transmission unit. Range: 68-1500.	1500
Multiple IP Address	Set the multiple IP addresses for bridge.	Null

Table 3-2-1-13 Bridge Settings

# 3.2.1.6 Switch

VLAN is a kind of new data exchange technology that realizes virtual work groups by logically dividing the LAN device into network segments.

LAN Settings								
Name	VLAN ID	IP Ad	idress	Netmasl	C I	MTU		Operation
								Ð
LAN Settings								
VLAN ID	LAN 1	LAN 2	LAN 3		LAN 4	CPU		Operation
1	Untagged V	Intagged 🗸 🗸	Untagged	✓ Untag	ged 🗸	Tagged	~	×
								Ŧ
		Fi	gure 3-2-1-1	5				
Switch								
ltem	Description	1						

BO

LAN Settings			
Name	Set interface name of VLAN.		
VLAN ID	Select VLAN ID of the interface.		
IP Address	Set IP address of LAN port.		
Netmask	Set Netmask of LAN port.		
MTU	Set the maximum transmission unit of LAN port. Range: 68-1500.		
VLAN Settings	VLAN Settings		
VLAN ID	Set the label ID of the VLAN. Range: 1-4094.		
LAN 1/2/3/4	Make the VLAN bind with the corresponding ports and select status		
LAN 1/2/3/4	from "Tagged", "Untagged" and "Close" for Ethernet frame on trunk link.		
CPU	Control communication between VLAN and other networks.		

Table 3-2-1-14 VLAN Trunk Parameters

## 3.2.1.7 Loopback

Loopback interface is used for replacing router's ID as long as it is activated. When the interface is DOWN, the ID of the router has to be selected again which leads to long convergence time of OSPF. Therefore, Loopback interface is generally recommended as the ID of the router.

Loopback interface is a logic and virtual interface on router. Under default conditions, there's no loopback interface on router, but it can be created as required.

Loopback Address			
IP Address	127.0.0.1		
Netmask	255.0.0.0		
Multiple IP Addresses			
1	P Address	Netmask	Operation
			Ð
Save			

Figure 3-2-1-16

Loopback			
ltem	Description	Default	
IP Address	Unalterable	127.0.0.1	
Netmask	Unalterable	255.0.0.0	
Multiple IP Addresses	Apart from the IP above, user can configure other IP addresses.	Null	

Table 3-2-1-15 Loopback Parameters

#### 3.2.2 DHCP

DHCP adopts Client/Server communication mode. The Client sends configuration request to the Server which feeds back corresponding configuration information and distributes IP address to the

Client so as to achieve the dynamic configuration of IP address and other information.

#### 3.2.2.1 DHCP Server/DHCPv6 Server

UR32L can be set as a DHCP server or DHCPv6 server to distribute IP address when a host logs on and ensures each host is supplied with different IP addresses. DHCP Server has simplified some previous network management tasks requiring manual operations to the largest extent. UR32L only supports stateful DHCPv6 when working as DHCPv6 server.

DHCP Server_1			
Enable			
Interface	Bridge0 ~		
Start Address	192.168.1.113		
End Address	192.168.1.126		
Netmask	255.255.255.0		
Lease Time(Min)	1440		
Primary DNS Server	8.8.8		
Secondary DNS Server	114.114.114		
Windows Name Server			
Static IP			
M	AC Address	IP Address	Op



CP Server	DHCPv6 Server	DHCP Relay		
DHCPv6 Server_	1			
Enable		0		
Interface		Bridge0 ~		
Start Address		2004:0:0:0:0:0:0:100		
End Address		2004:0:0:0:0:0:0:200		
Prefix Length		64		
Lease Time(Min)		1440		
Primary DNS Ser	ver	2001:D0B0:3000:3001::1		
Secondary DNS	Server	2001:4860:4860::8888		
Static IP				
	DUID		IPv6 Address	Operatio



DHCP/DHCPv6 Server		
Item	Description	Default

Milesight

Enable	Enable or disable DHCP server.	Enable
Interface	Select interface.	Bridge0
Start Address	Define the beginning of the pool of IP addresses which will be leased to DHCP clients.	192.168.1.0 0
End Address	Define the end of the pool of IP addresses which will be leased to DHCP clients.	192.168.1.9 9
Netmask	Define the subnet mask of IPv4 address obtained by DHCP clients from DHCP server.	255.255.255 .0
Prefix Length	Set the IPv6 prefix length of IPv6 address obtained by DHCP clients from DHCP server.	64
Lease Time (Min)	Set the lease time on which the client can use the IP address obtained from DHCP server. Range: 1-10080.	1440
Primary DNS Server	Set the primary DNS server.	192.168.1.1
Secondary DNS Server	Set the secondary DNS server.	Null
Windows Name Server	Define the Windows Internet Naming Service obtained by DHCP clients from DHCP sever. Generally you can leave it blank.	Null
Static IP		
MAC Address	Set a static and specific MAC address for the DHCP client (it should be different from other MACs so as to avoid conflict).	Null
DUID	Set a static and specific DUID for the DHCPv6 client (it should be different from other DUID so as to avoid conflict).	Null
IP Address	Set a static and specific IP address for the DHCP client (it should be outside of the DHCP range).	Null
		1

Table 3-2-2-1 DHCP Server Parameters

# 3.2.2.2 DHCP Relay

UR32L can be set as DHCP Relay to provide a relay tunnel to solve the problem that DHCP Client and DHCP Server are not in the same subnet.

DHCP Server	DHCPv6 Server	DHCP Relay
DHCP Relay		
Enable DHCP Server		
Save		

Figure 3-2-2-3

DHCP Relay		
Item	Description	
Enable	Enable or disable DHCP relay.	
DHCP Server	Set DHCP server, up to 10 servers can be configured; separate them by blank space or ",".	

Table 3-2-2-2 DHCP Relay Parameters

# 3.2.3 Firewall

This section describes how to set the firewall parameters, including security, ACL, DMZ, Port Mapping, MAC Binding and SPI.

The firewall implements corresponding control of data flow at entry direction (from Internet to local area network) and exit direction (from local area network to Internet) according to the content features of packets, such as protocol style, source/destination IP address, etc. It ensures that the router operate in a safe environment and host in local area network.

## 3.2.3.1 Security

Prevent Attack			
DoS/DDoS Protection			
Access Service Control			
Service	Port	Local	Remote
HTTP	80	Ø	۲
HTTPS	443	×.	×
TELNET	23	Ø	2
SSH	22		۲
FTP	21		۲
Website Blocking			
URL Blocking	http://		
Keyword Blocking			
L		•	
		·o 2-2-2-1	

Figure 3-2-3-1

Item	Description	Default
Prevent Attack		

DoS/DDoS Protection	Enable/disable Prevent DoS/DDoS Attack. Disable		
Access Service Contro			
Port	Set port number of the services. Range: 1-65535.		
Local	Access the router locally.	Enable	
Remote	Access the router remotely.	Disable	
НТТР	Users can log in the device locally via HTTP to access and control it through Web after the option is checked.	80	
HTTPS	Users can log in the device locally and remotely via HTTPS to access and control it through Web after option is checked.	443	
TELNET	Users can log in the device locally and remotely via Telnet after the option is checked.	23	
SSH	Users can log in the device locally and remotely via SSH after the option is checked.	22	
FTP	Users can log in the device locally and remotely via FTP after the option is checked.	21	
Website Blocking			
URL Blocking	Enter the HTTP address which you want to block.		
Keyword Blocking	yword Blocking You can block specific website by entering keyword. The maximum number of character allowed is 64.		
	Table 3-2-3-1 Security Parameters		

Table 3-2-3-1 Security Parameters

# 3.2.3.2 ACL

Access control list, also called ACL, implements permission or prohibition of access for specified network traffic (such as the source IP address) by configuring a series of matching rules so as to filter the network interface traffic. When router receives packet, the field will be analyzed according to the ACL rule applied to the current interface. After the special packet is identified, the permission or prohibition of corresponding packet will be implemented according to preset strategy.

The data package matching rules defined by ACL can also be used by other functions requiring flow distinction.

Security	ACL	Port Mappi	ng DN	MZ MAC Binding	g Custom F	Rules SF	PI
ACL Setting							
Default Filter P	olicy	Accept	•				
Access Contr	ol List						
ID	Action	Protocol	Source IP	Destination IP	More Detail	Description	Operation
							Ð
Interface List							
	Interface		h	n ACL	Out A	CL	Operation
							(H
Save							



Туре	extended	~
ID		
Action	permit	~
Protocol	tcp	~
Source IP		
Source Wildcard Mask	0.0.0.0	
Source Port Type	any	~
Destination IP		
Destination Wildcard Mask	0.0.0.0	
Destination Port Type	any	~
Description		

Figure 3-2-3-3

ltem	Description		
ACL Setting			
Default Filter Policy	Select from "Accept" and "Deny". The packets which are not included in the access control list		
	will be processed by the default filter policy.		
Access Control List			
Туре	Select type from "Extended" and "Standard".		
ID	User-defined ACL number. Range: 1-199.		
Action	Select from "Permit" and "Deny".		
Protocol	Select protocol from "ip", "icmp", "tcp", "udp", and "1-255".		
Source IP	Source network address (leaving it blank means all).		
Source Wildcard Mask	Wildcard mask of the source network address.		

Destination IP	Destination network address (0.0.0.0 means all).
Destination Wildcard Mask	Wildcard mask of destination address.
Description	Fill in a description for the groups with the same ID.
ICMP Type	Enter the type of ICMP packet. Range: 0-255.
ICMP Code	Enter the code of ICMP packet. Range: 0-255.
Source Port Type	Select source port type, such as specified port, port range, etc.
Source Port	Set source port number. Range: 1-65535.
Start Source Port	Set start source port number. Range: 1-65535.
End Source Port	Set end source port number. Range: 1-65535.
Destination Port Type	Select destination port type, such as specified port, port range, etc.
Destination Port	Set destination port number. Range: 1-65535.
Start Destination Port	Set start destination port number. Range: 1-65535.
End Destination Port	Set end destination port number. Range: 1-65535.
More Details	Show information of the port.
Interface List	
Interface	Select network interface for access control.
In ACL	Select a rule for incoming traffic from ACL ID.
Out ACL	Select a rule for outgoing traffic from ACL ID.
	Table 3-2-3-2 ACL Parameters

Table 3-2-3-2 ACL Parameters

## 3.2.3.3 Port Mapping (DNAT)

When external services are needed internally (for example, when a website is published externally), th e external address initiates an active connection. And, the router or the gateway on the firewall receiv es the connection. Then it will convert the connection into the an internal connection. This conversion is called DNAT, which is mainly used for external and internal services.

Port Mapping					
Source IP	Source Port	Destination IP	Destination Port Protocol	Description	Operation
0.0.0/0			TCP ~		
					•

Figure 3-2-3-3

Port Mapping		
Item	Description	
Source IP	Specify the host or network which can access local IP address. 0.0.0.0/0 means all.	
Source Port	Enter the TCP or UDP port from which incoming packets are forwarded. Range: 1-65535.	
Destination IP	Enter the IP address that packets are forwarded to after being received on the incoming interface.	
Destination Port	Enter the TCP or UDP port that packets are forwarded to after	

	being received on the incoming port(s). Range: 1-65535.	
Protocol	Select from "TCP" and "UDP" as your application required.	
Description	The description of this rule.	

Table 3-2-3-3 Port Mapping Parameters

## **Related Configuration Example**

NAT Application Example

## 3.2.3.4 DMZ

DMZ is a host within the internal network that has all ports exposed, except those forwarded ports in port mapping.

Enable	
DMZ Host	
Source Address	

#### Figure 3-2-3-4

DMZ	
ltem	Description
Enable	Enable or disable DMZ.
DMZ Host	Enter the IP address of the DMZ host on the internal network.
Source Address	Set the source IP address which can access to DMZ host. "0.0.0/0" means any address.

Table 3-2-3-4 DMZ Parameters

### 3.2.3.5 MAC Binding

MAC Binding is used for specifying hosts by matching MAC addresses and IP addresses that are in the list of allowed outer network access.

MAC	Binding List			
	MAC	IP	Description	Operation
				Ð
	Save			
		Figure 3-2-3-5		
	MAC Binding List			

MAC Binding List	
Item	Description

MAC Address	Set the binding MAC address.
IP Address	Set the binding IP address.
Description	Fill in a description for convenience of recording the meaning of the binding rule for each piece of MAC-IP.
	Table 3-2-3-5 MAC Binding Parameters

### 3.2.3.6 Custom Rules

In this page, you can configure your own custom firewall iptables rules.

	Rule	Description	Operation
Eg	: -t filter -l INPUT -s 192.168.3.240 -j DROP		×

Figure 3-2-3-6

<b>Custom Rules</b>	
ltem	Description
	Specify an iptables rule like the example shows.
Rule	Tips: You must reboot the device to take effect after modifying or
	deleting the iptables rules.
Description	Enter the description of the rule.

Table 3-2-3-6 Custom Rules Parameters

### 3.2.3.7 SPI

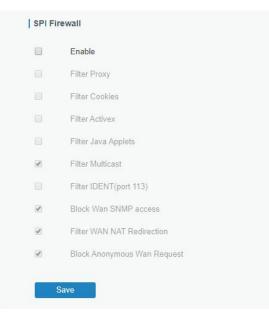


Figure 3-2-3-7

**SPI Firewall** 

ltem	Description
Enable	Enable/disable SPI firewall.
Filter Proxy	Blocks HTTP requests containing the "Host": string.
Filter Cookies	Identifies HTTP requests that contain "Cookie": String and mangle
FILLEI COOKIES	the cookie. Attempts to stop cookies from being used.
Filter ActiveX	Blocks HTTP requests of the URL that ends in ".ocx" or ".cab".
Filter Java Applets	Blocks HTTP requests of the URL that ends in ".js" or ".class".
Filter Multicast	Prevent multicast packets from reaching the LAN.
Filter IDENT(port 113)	Prevent WAN access to Port 113.
Block WAN SNMP access	Block SNMP requests from the WAN.
	Prevent hosts on LAN from using WAN address of router to
Filter WAN NAT Redirection	connect servers on the LAN (which have been configured using port redirection).
Block Anonymous WAN Requests	Stop the router from responding to "pings" from the WAN.

Table 3-2-3-7 SPI Parameters

## 3.2.4 QoS

Quality of service (QoS) refers to traffic prioritization and resource reservation control mechanisms rather than the achieved service quality. QoS is engineered to provide different priority for different applications, users, data flows, or to guarantee a certain level of performance to a data flow.

QoS(Download)	QoS(Upload)							
Download Bandwidt	h							
Enable								
Default Category		Ŧ						
Download Bandwidth	0		kbits/s					
Capacity								
Service Category								
Name		Percent(%)		Max BW(	kbps)	Min BW(	kbps)	Operatio
								Ð
Service Category Ru	iles							
Name	Source IP	Source Port		Destination IP	Destination Port	Protocol	Service Category	Operatio
								8
Save								



QoS	
Item	Description
Download/Upload	
Enable	Enable or disable QoS.
Default Category	Select the default category from Service Category list.

Download/Upload	The download/upload bandwidth capacity of the network that the	
Bandwidth Capacity	router is connected with, in kbps. Range: 1-8000000.	
Service Category		
Name	You can use characters such digits, letters and "-".	
Percent (%)	Set percent for the service category. Range: 0-100.	
Max BW(kbps)	The maximum bandwidth that this category is allowed to consume, in kbps. The value should be less than the "Download/Upload Bandwidth Capacity" when the traffic is blocked.	
Min BW(kbps)	The minimum bandwidth that can be guaranteed for the category, in kbps.The value should be less than the "MAX BW" value.	
Service Category Rules		
Item	Description	
Item Name	Description           Give the rule a descriptive name.	
Name	Give the rule a descriptive name.	
Name Source IP	Give the rule a descriptive name. Source address of flow control (leaving it blank means any). Source port of flow control. Range: 0-65535 (leaving it blank means	
Name Source IP Source Port	Give the rule a descriptive name. Source address of flow control (leaving it blank means any). Source port of flow control. Range: 0-65535 (leaving it blank means any).	
Name Source IP Source Port Destination IP	Give the rule a descriptive name. Source address of flow control (leaving it blank means any). Source port of flow control. Range: 0-65535 (leaving it blank means any). Destination address of flow control (leaving it blank means any). Destination port of flow control. Range: 0-65535 (leaving it blank	
Name Source IP Source Port Destination IP Destination Port	Give the rule a descriptive name. Source address of flow control (leaving it blank means any). Source port of flow control. Range: 0-65535 (leaving it blank means any). Destination address of flow control (leaving it blank means any). Destination port of flow control. Range: 0-65535 (leaving it blank means any).	

Table 3-2-4-1 QoS (Download/Upload) Parameters

## **Related Configuration Example**

**QoS Application Example** 

### 3.2.5 VPN

Virtual Private Networks, also called VPNs, are used to securely connect two private networks together so that devices can connect from one network to the other network via secure channels. The UR32L supports DMVPN, IPsec, GRE, L2TP, PPTP, OpenVPN, as well as GRE over IPsec and L2TP over IPsec.

### 3.2.5.1 DMVPN

A dynamic multi-point virtual private network (DMVPN), combining mGRE and IPsec, is a secure network that exchanges data between sites without passing traffic through an organization's headquarter VPN server or router.

Save

Milesight

DMVPN Settings		
Enable		
Hub Address		
Local IP Address		
GRE HUB IP Address		
GRE Local IP Address		
GRE Mask	255.255.255.0	
GRE Key		
Negotiation Mode	Main	Ŧ
Authentication Algorithm	DES	v.
Encryption Algorithm	MD5	Ŧ
DH Group	MODP768-1	Ψ.
Көу		
Local ID Type	Default	Ŧ
IKE Life Time(s)	10800	
SA Algorithm	DES-MD5	Ψ.
PFS Group	NULL	Ŧ
Life Time(s)	3600	
DPD Time Interval(s)	30	
DPD Timeout(s)	150	
Cisco Secret		
NHRP Holdtime(s)	7200	

## Figure 3-2-5-1

DMVPN			
ltem	Description		
Enable	Enable or disable DMVPN.		
Hub Address	The IP address or domain name of DMVPN Hub.		
Local IP address	DMVPN local tunnel IP address.		
GRE Hub IP Address	GRE Hub tunnel IP address.		
GRE Local IP Address	GRE local tunnel IP address.		
GRE Netmask	GRE local tunnel netmask.		
GRE Key	GRE tunnel key.		
Negotiation Mode	Select from "Main" and "Aggressive".		
Authentication	Select from "DES", "3DES", "AES128", "AES192" and		
Algorithm	"AES256".		
<b>Encryption Algorithm</b>	Select from "MD5" and "SHA1".		
DH Group	Select from "MODP768_1", "MODP1024_2" and		
	"MODP1536_5".		
Key	Enter the preshared key.		
Local ID Type	Select from "Default", "ID", "FQDN", and "User FQDN"		
IKE Life Time (s)	Set the lifetime in IKE negotiation. Range: 60-86400.		
	Select from "DES_MD5", "DES_SHA1", "3DES_MD5",		
SA Algorithm	"3DES_SHA1", "AES128_MD5", "AES128_SHA1",		
SA Algontinin	"AES192_MD5", "AES192_SHA1", "AES256_MD5" and		
	"AES256_SHA1".		
PFS Group	Select from "NULL", "MODP768_1", "MODP1024_2" and		
	"MODP1536-5".		

Life Time (s)	Set the lifetime of IPsec SA. Range: 60-86400.
DPD Interval Time (s)	Set DPD interval time
DPD Timeout (s)	Set DPD timeout.
Cisco Secret	Cisco Nhrp key.
NHRP Holdtime (s)	The holdtime of NHRP protocol.
NHRP Holdtime (s)	The holdtime of NHRP protocol.

Table 3-2-5-1 DMVPN Parameters

### 3.2.5.2 IPSec Server

IPsec is especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers.

IPsec provides three choices of security service: Authentication Header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE). AH essentially allows authentication of the senders' data. ESP supports both authentication of the sender and data encryption. IKE is used for cipher code exchange. All of them can protect one and more data flows between hosts, between host and gateway, and between gateways.

IPsec Server		
Enable		
IPsec Mode	Tunnel	~
IPsec Protocol	ESP	~
Local Subnet		
Local Subnet Mask		
Local ID Type	Default	~
Remote Subnet		
Remote Subnet Mask		
Remote ID Type	Default	~



IPsec Server			
Item	Description		
Enable	Enable or disable IPsec server mode.		
IPsec Mode	Select Tunnel or Transport.		
IPsec Protocol	Select from ESP or AH.		
Local Subnet	Enter the local LAN subnet IP address on the IPsec tunnel.		
Local Subnet Netmask	Enter the local LAN netmask on the IPsec tunnel.		
	Select the identifier type, and send it to remote peer.		
Local ID Type	Default: None		

<b>ID:</b> use local subnet IP address as ID			
	FQDN: fully qualified domain name, example: test.user.com		
	User FQDN: fully qualified username string with email address		
	format, example: test@user.com		
Remote Subnet	Set the remote LAN subnet on the IPsec tunnel.		
Remote Subnet Mask	Enter the remote LAN netmask on the IPsec tunnel.		
	Select the identifier type that is the same as remote peer local		
	ID.		
	Default: None		
Remote ID type	ID: use remote subnet IP address as ID		
	FQDN: fully qualified domain name, example: test.user.com		
	User FQDN: fully qualified username string with email address		
	format, example: test@user.com		

Table 3-2-5-2 IPsec Server Parameters

IKE Parameter	➢ Collapse	
IKE Version	IKEv1	~
Negotiation Mode	Main	~
Encryption Algorithm	DES	~
Authentication Algorithm	MD5	~
DH Group	MODP768-1	~
Local Authentication	PSK	~
XAUTH		
Lifetime(s)	12000	
PSK List		
	Selector	
	Selector	

Figure 3-2-5-3

SA Parameter	S Collapse	
SA Encryption Algorithm	DES	~
SA Authentication Algorithm	MD5	~
PFS Group	NULL	
Lifetime(s)	3600	
DPD Time Interval(s)	30	
DPD Timeout(s)	150	
IPsec Advanced		
Enable Compression		
Margintime(s)	100	
VPN Over IPsec Type	NONE	~
Expert Options		

Figure 3-2-5-4

IKE Parameter				
ltem	Description			
IKE Version	Select the method of key exchange from IKEv1 and IKEv2.			
Negotiation Mode	When using IKEv1, select Main or Aggressive.			
Encryption Algorithm	Select DES, 3DES, AES128, AES192 or AES256.			
Authentication Algorithm	Select MD5, SHA1 or SHA2-256.			
DH Group	Select MODP768-1, MODP1024-2, MODP1536-5, MODP2048-14 or MODP3072-15.			
	Select PSK or CA.			
	<b>PSK:</b> use pre-shared key to complete the authentication.			
Local Authentication	CA: use certificate to complete the authentication. After selecting, go			
	to Network > VPN > > Certifications page to import CA certificate, local			
	certificate and private key to corresponding fields.			
	When using IKEv2, select PSK or CA.			
	<b>PSK:</b> use pre-shared key to complete the authentication.			
Remote Authentication	CA: use certificate to complete the authentication. After selecting, go			
	to Network > VPN > > Certifications page to import remote certificate			
	to corresponding fields.			
XAUTH	When using IKEv1, define XAUTH username and password after			
	XAUTH is enabled.			
Lifetime (s)	Set the lifetime in IKE negotiation. Range: 60-86400.			
XAUTH List				
Username	Enter the username used for the xauth authentication.			
Password	Enter the password used for the xauth authentication.			
PSK List				

Selector	Enter the corresponding identification number for PSK authentication.	
PSK	Enter the pre-shared key.	
SA Parameter		
SA Encryption Algorithm	Select DES, 3DES, AES128, AES192 or AES256.	
SA Authentication Algorithm	Select MD5, SHA1 or SHA2-256.	
PFS Group	Select NULL, MODP768-1 , MODP1024-2 or MODP1536-5.	
Lifetime (s)	Set the lifetime of IPsec SA. Range: 60-86400 s.	
DPD Time Interval(s)	Set DPD retry interval to send DPD requests. Range: 1-86400 s	
DPD Timeout(s)	Set DPD timeout to detect the remote side fails. Range: 10-86400 s.	
IPsec Advanced		
Enable Compression	The head of IP packet will be compressed after it's enabled.	
Margintime	Set advanced time before the lifetime expires to begin the re-negotiation.	
VPN Over IPsec Type	Select from NONE, GRE and L2TP.	
Expert Options User can enter some other initialization strings in this field and separate the strings with semicolon.		

Table 3-2-5-3 IPsec Server Parameters

### 3.2.5.3 IPSec

UR32L supports running at most 3 IPsec clients at the same time.

IPsec_1		
Enable		
IPsec Gateway Address		
IPsec Mode	Tunnel	~
IPsec Protocol	ESP	~
Local Subnet		
Local Subnet Mask		
Local ID Type	Default	Ŷ
Remote Subnet		
Remote Subnet Mask		
Remote ID Type	Default	~
IKE Parameter	>> Expand	
SA Parameter	>> Expand	
IPsec Advanced	» Expand	
Expert Options		

Figure 3-2-5-5

Milesight

IPsec		
Item	Description	
Frable	Enable or disable IPsec client mode. A maximum of 3 tunnels	
Enable	is allowed.	
IP Gateway Address	Enter the remote IPsec server address.	
IPsec Mode	Select Tunnel or Transport.	
IPsec Protocol	Select from ESP or AH.	
Local Subnet	Enter the local LAN subnet IP address on the IPsec tunnel.	
Local Subnet Netmask	Enter the local LAN netmask on the IPsec tunnel.	
	Select the identifier type, and send it to remote peer.	
	Default: None	
	ID: use local subnet IP address as ID	
Local ID Type	FQDN: fully qualified domain name, example: test.user.com	
	User FQDN: fully qualified username string with email address	
	format, example: test@user.com	
Remote Subnet	Set the remote LAN subnet on the IPsec tunnel.	
Remote Subnet Mask	Enter the remote LAN netmask on the IPsec tunnel.	
	Select the identifier type that is the same as remote peer local	
	ID.	
	Default: None	
Remote ID type	ID: use remote subnet IP address as ID	
	FQDN: fully qualified domain name, example: test.user.com	
	User FQDN: fully qualified username string with email address	
	format, example: test@user.com	

Table 3-2-5-4 IPsec Parameters

IKE Parameter	Collapse	
IKE Version	IKEv1	~
Negotiation Mode	Main	~
Encryption Algorithm	DES	~
Authentication Algorithm	MD5	~
DH Group	MODP768-1	~
Local Authentication	PSK	~
Local Secrets		Þ
XAUTH		
Lifetime(s)	10800	
SA Parameter		
SA Encryption Algorithm	DES	~
SA Authentication Algorithm	MD5	~
PFS Group	NULL	~
Lifetime(s)	3600	
DPD Time Interval(s)	30	
DPD Timeout(s) 150		
IPsec Advanced		
Enable Compression		
Margintime(s)	100	
VPN Over IPsec Type	NONE	~
Expert Options		

Figure 3-2-5-6

IKE Parameter		
Item	Description	
IKE Version	Select the method of key exchange from IKEv1 and IKEv2.	
Negotiation Mode	When using IKEv1, select Main or Aggressive.	
Encryption Algorithm	Select DES, 3DES, AES128, AES192 or AES256.	
Authentication Algorithm	Select MD5, SHA1 or SHA2-256.	
DLL On sure	Select MODP768-1, MODP1024-2, MODP1536-5, MODP2048-14 or	
DH Group	MODP3072-15.	
	Select PSK or CA.	
	<b>PSK:</b> use pre-shared key to complete the authentication.	
Local Authentication	CA: use certificate to complete the authentication. After selecting, go	
	to Network > VPN > > Certifications page to import CA certificate, local	
	certificate and private key to corresponding fields.	
Local Secrets	Enter the pre-shared key which is defined on serer side.	
Remote Authentication	When using IKEv2, select PSK or CA.	

	PSK: use pre-shared key to complete the authentication.	
	CA: use certificate to complete the authentication. After selecting, go	
	to Network > VPN > > Certifications page to import remote certificate	
	to corresponding fields.	
Remote Secrets	Enter the pre-shared key which is defined on server side.	
XAUTH	Enter XAUTH username and password which is defined on server side.	
Lifetime (s)	Set the lifetime in IKE negotiation. Range: 60-86400.	
SA Parameter		
SA Encryption Algorithm	Select DES, 3DES, AES128, AES192 or AES256.	
SA Authentication	Select MD5, SHA1 or SHA2-256.	
Algorithm		
PFS Group	Select NULL, MODP768-1, MODP1024-2 or MODP1536-5.	
Lifetime (s)	Set the lifetime of IPsec SA. Range: 60-86400 s.	
DPD Time Interval(s)	Set DPD retry interval to send DPD requests. Range: 1-86400 s	
DPD Timeout(s)	Set DPD timeout to detect the remote side fails. Range: 10-86400 s.	
IPsec Advanced		
Enable Compression	The head of IP packet will be compressed after it's enabled.	
Morgintimo	Set advanced time before the lifetime expires to begin the	
Margintime	re-negotiation.	
VPN Over IPsec Type	Select from NONE, GRE and L2TP.	
Export Options	User can enter some other initialization strings in this field and	
Expert Options	separate the strings with semicolon.	
	Table 2-2-5-5 IDeec Parameters	

Table 3-2-5-5 IPsec Parameters

## 3.2.5.4 GRE

Generic Routing Encapsulation (GRE) is a protocol that encapsulates packets in order to route other protocols over IP networks. It's a tunneling technology that provides a channel through which encapsulated data message could be transmitted and encapsulation and decapsulation could be realized at both ends.

In the following circumstances the GRE tunnel transmission can be applied:

- GRE tunnel could transmit multicast data packets as if it were a true network interface. Single use of IPSec cannot achieve the encryption of multicast.
- A certain protocol adopted cannot be routed.
- A network of different IP addresses shall be required to connect other two similar networks.

GRE Settings	
- GRE_1	
Enable	
Remote IP Address	
Local IP Address	
Local Virtual IP Address	
Netmask	255.255.255.0
Peer Virtual IP Address	
Global Traffic Forwarding	
Remote Subnet	
Remote Netmask	
MTU	1500
Key	
Enable NAT	2
+ GRE_2	
+ GRE_3	

Figure 3-2-5-7

GRE		
ltem	Description	
Enable	Check to enable GRE function.	
Remote IP Address	Enter the real remote IP address of GRE tunnel.	
Local IP Address	Set the local IP address.	
Local Virtual IP Address	Set the local tunnel IP address of GRE tunnel.	
Netmask	Set the local netmask.	
Peer Virtual IP Address	Enter remote tunnel IP address of GRE tunnel.	
Global Traffic	All the data traffic will be sent out via GRE tunnel when this	
Forwarding	function is enabled.	
Remote Subnet	Enter the remote subnet IP address of GRE tunnel.	
Remote Netmask	Enter the remote netmask of GRE tunnel.	
MTU	Enter the maximum transmission unit. Range: 64-1500.	
Key	Set GRE tunnel key.	
Enable NAT	Enable NAT traversal function.	

Table 3-2-5-6 GRE Parameters

### 3.2.5.5 L2TP

Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet service provider (ISP) to enable the operation of a virtual private network (VPN) over the Internet.

L2TP Settings				
— L2TP_1				
Enable		۵		
Remote IP A	Address			
Hostname				
Username				
Password				
Authenticati	on	Auto	~	
Global Traff	ic Forwarding			
Remote Sub	onet			
Remote Sub	onet Mask			
Key				
Advanced S	ettings	$\mathbf{\Sigma}$		
+ L2TP_2				
+ L2TP_3				

Figure 3-2-5-8

L2TP		
Item	Description	
Enable	Check to enable L2TP function.	
Remote IP Address	Enter the public IP address or domain name of L2TP server.	
Hostname	Enter the hostname to verify with L2TP server.	
Username	Enter the username that L2TP server provides.	
Password	Enter the password that L2TP server provides.	
Authentication Select from "Auto", "PAP", "CHAP", "MS-CHAPv1" and "MS-CHAPv2".		
Global Traffic	All of the data traffic will be sent out via L2TP tunnel after	
Forwarding	this function is enabled.	
Remote Subnet	Enter the remote IP address that L2TP protects.	
Remote Subnet Mask	Enter the remote netmask that L2TP protects.	
Кеу	Enter the password of L2TP tunnel.	

Table 3-2-5-7 L2TP Parameters

Advanced Settings	
Local IP Address	
Peer IP Address	
Enable NAT	
Enable MPPE	Image: A start of the start
Address/Control Compression	
Protocol Field Compression	
Asyncmap Value	fffffff
MRU	1500
MTU	1500
Link Detection Interval(s)	60
Max Retries	0
Expert Options	

Figure 3-2-5-9

Advanced Settings		
ltem	Description	
Local IP Address	Set tunnel IP address of L2TP client. Client will obtain tunnel IP address automatically from the server when it's null.	
Peer IP Address	Enter tunnel IP address of L2TP server.	
Enable NAT	Enable NAT traversal function.	
Enable MPPE	Enable MPPE encryption.	
Address/Control Compression	For PPP initialization. User can keep the default option.	
Protocol Field Compression	For PPP initialization. User can keep the default option.	
Asyncmap Value	One of the PPP protocol initialization strings. User can keep the default value. Range: 0-ffffffff.	
MRU	Set the maximum receive unit. Range: 64-1500.	
MTU	Set the maximum transmission unit. Range: 64-1500	
Link Detection Interval (s)	Set the link detection interval time to ensure tunnel connection. Range: 0-600.	
Max Retries	Set the maximum times of retry to detect the L2TP connection failure. Range: 0-10.	
Expert Options	User can enter some other PPP initialization strings in this field and separate the strings with blank space.	

Table 3-2-5-8 L2TP Parameters

### 3.2.5.6 PPTP

Point-to-Point Tunneling Protocol (PPTP) is a protocol that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network.

PPTP Settings	
- PPTP_1	
Enable	
Remote IP Address	
Username	
Password	
Authentication	Auto
Global Traffic Forwarding	
Remote Subnet	
Remote Subnet Mask	
Advanced Settings	$\Sigma$
+ PPTP_2	
+ PPTP_3	
(hourse)	

Figure 3-2-5-10

PPTP	
ltem	Description
Enable	Enable PPTP client. A maximum of 3 tunnels is allowed.
Remote IP Address	Enter the public IP address or domain name of PPTP server.
Username	Enter the username that PPTP server provides.
Password	Enter the password that PPTP server provides.
Authentication	Select from "Auto", "PAP", "CHAP", "MS-CHAPv1", and "MS-CHAPv2".
Global Traffic	All of the data traffic will be sent out via PPTP tunnel once
Forwarding	enable this function.
Remote Subnet	Set the peer subnet of PPTP.
Remote Subnet Mask	Set the netmask of peer PPTP server.

Table 3-2-5-9 PPTP Parameters

Milesight

Local IP Address	
Peer IP Address	
Enable NAT	
Enable MPPE	
Address/Control Compression	
Protocol Field Compression	
Asyncmap Value	fffffff
MRU	1500
MTU	1500
Link Detection Interval(s)	60
Max Retries	0
Expert Options	

Figure 3-2-5-11

Description
Set IP address of PPTP client.
Enter tunnel IP address of PPTP server.
Enable the NAT faction of PPTP.
Enable MPPE encryption.
For PPP initialization. User can keep the default option.
For PPP initialization. User can keep the default option.
One of the PPP protocol initialization strings. User can keep the default value. Range: 0-ffffffff.
Enter the maximum receive unit. Range: 0-1500.
Enter the maximum transmission unit. Range: 0-1500.
Set the link detection interval time to ensure tunnel connection. Range: 0-600.
Set the maximum times of retrying to detect the PPTP connection failure. Range: 0-10.
User can enter some other PPP initialization strings in this field and separate the strings with blank space.

Table 3-2-5-10 PPTP Parameters

## 3.2.5.7 OpenVPN Client

OpenVPN is an open source virtual private network (VPN) product that offers a simplified security

framework, modular network design, and cross-platform portability. The default OpenVPN version of UR32L is 2.4.9.

UR32L supports running at most 3 OpenVPN clients at the same time. You can import the ovpn file directly or configure the parameters on this page to set clients.

OpenVPN Client Settings	
- OpenVPN Client_1	
Enable Configuration Method Configuration File	File Configuration  pervpn_1-custom.conf Browse Import Export Delete
+ OpenVPN Client_2 + OpenVPN Client 3	

Figure 3-2-5-12

OpenVPN Client - File Configuration			
ltem	Description		
Browse	Click to browse the client configuration ovpn format file including the settings and certificate contents. Please refer to the client configuration file according to sample: client.conf		
Edit	Click to edit the imported file.		
Export	Export the server configuration file.		
Delete	Click to delete the configuration file.		

#### Table 3-2-5-11 OpenVPN Client Parameters

Enable		
Configuration Method	Page Configuration	~
Protocol	UDP	~
Remote IP Address		
Port	1194	
Interface	tun	~
Authentication	None	~
Local Tunnel IP		
Remote Tunnel IP		
Enable NAT		
Compression	LZO	~
Link Detection Interval(s)	60	
Link Detection Timeout(s)	300	
Cipher	None	~
Authentication Mode	None	~
MTU	1500	
Max Frame Size	1500	
Verbose Level	ERROR	~
Expert Options		
Local Route		
Subne	t	

Figure 3-2-5-13

ltom	Description				
Item	Description				
Protocol	Select a transport protocol used by connecting UDP and TCP.				
Remote IP Address	Enter remote OpenVPN server's IP address or domain name.				
Port	Enter the TCP/UCP service number of remote OpenVPN server. Range:				
	1-65535.				
	Select virtual VPN network interface type from TUN and TAP. TUN				
Interface	devices encapsulate IPv4 or IPv6 (OSI Layer 3) while TAP devices				
	encapsulate Ethernet 802.3 (OSI Layer 2).				
	Select authentication type used to secure data sessions.				
	Pre-shared: use the same secret key as server to complete the				
	authentication. After selecting, go to <b>Network &gt; VPN &gt; Certifications</b> page				
	to import a static.key to <b>PSK</b> field.				
	Username/Password: use username/password which is preset in server				
Authentication Type	side to complete the authentication.				
	<b>X.509 cert:</b> use X.509 type certificate to complete the authentication.				
	After selecting, go to <b>Network &gt; VPN &gt; Certifications</b> page to import CA				
	certificate, client certificate and client private key to corresponding fields.				
	X.509 cert + use both username/password and X.509 cert				
	authentication type.				
Local Virtual IP	Set local tunnel address when authentication type is <b>None</b> or <b>Pre-shared</b> .				
Remote Virtual IP	Set remote tunnel address when authentication type is <b>None</b> or				
	Pre-shared.				
Global Traffic	All the data traffic will be sent out via OpenVPN tunnel when this function				
Forwarding	is enabled.				
Enable TLS	Select from None, TLS Auth and TLS Crypt. When selecting TLS Auth or				
Authentication	TLS Crypt, go to <b>Network &gt; VPN &gt; Certifications</b> page to import a ta.key.				
Compression	Select to enable or disable LZO to compress data.				
Link Detection Interval	Set link detection interval time to ensure tunnel connection. If this is set				
(s)	on both server and client, the value pushed from server will override the				
	client local values. Range: 10-1800 s.				
Link Detection	OpenVPN will be reestablished after timeout. If this is set on both server				
Timeout (s)	and client, the value pushed from server will override the client local				
	values. Range: 60-3600 s.				
Cipher	Select from NONE, BF-CBC, DES-CBC, DES-EDE3-CBC, AES-128-CBC, AES-192-CBC and AES-256-CBC.				
Authoptication Made					
Authentication Mode	Select from NONE, MD5, SHA1, SHA256, and SHA512.				
MTU May Frama Siza	Enter the maximum transmission unit. Range: 128-1500.				
Max Frame Size	Set the maximum frame size. Range: 128-1500.				
Verbose Level	Select from ERROR, WARING, NOTICE and DEBUG.				
Furnant O. I	User can enter some initialization strings in this field and separate the				
Expert Options	strings with semicolon.				
	Example: ncp-ciphers AES-128-GCM; key direction 1				

Subnet	Set the local route's IP address.	
Subnet Mask	Set the local route's netmask.	

Table 3-2-5-12 OpenVPN Client Parameters

### **Related Topic**

OpenVPN Client Application Example

### 3.2.5.8 OpenVPN Server

The UR32L supports OpenVPN server to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. You can import the ovpn file directly or configure the parameters on this page to set this server. UR32L supports at most 20 openVPN clients connections.

OpenVPN Server Settings	
Enable	
Configuration Method	File Configuration 🗸
Configuration File	Browse Import Export Delete



OpenVPN Server - File Configuration			
ltem	Description		
Browse	Click to browse the server configuration ovpn format file including the settings and certificate contents. Please refer to the server configuration file according to sample: <u>server.conf</u>		
Edit	Click to edit the imported file.		
Export	Export the server configuration file.		
Delete	Click to delete the configuration file.		

Table 3-2-5-13 OpenVPN Server Parameters

.

Enable		
Configuration Method	Page Configuration	~
Protocol	UDP	~
Port	1194	
Listening IP		
Interface	tun	~
Authentication	None	~
Local Virtual IP		
Remote Virtual IP		
Enable NAT		
Compression	LZO	~
Link Detection Interval	60	
Link Detection Timeout	150	
Cipher	None	~
Authentication Mode	None	~
мти	1500	
Max Frame Size	1500	
Verbose Level	ERROR	~
Expert Options		



Account				
	Username		Password	Operation
				8
Local Route				
	Subnet		Netmask	Operation
				E
Client Subnet				
	Name	Subnet	Netmask	Operation

Figure 3-2-5-16

OpenVPN Server - Page Configuration				
Item Description				
Protocol Select a transport protocol used by connection from UDP and TCP.				
Listening IP	Enter the local hostname or IP address for bind. If left blank, OpenVPN server will bind to all interfaces.			
Port	Enter the TCP/UCP service number for OpenVPN client connection. Range: 1-65535.			

Milesight

Select virtual VPN network interface type from TUN and TAP. TUN devices encapsulate IPv4 or IPv6 (OSI Layer 3) while TAP devices
encapsulate Ethernet 802.3 (OSI Layer 2).
Select authentication type used to secure data sessions.
Pre-shared: use the same secret key as server to complete the
authentication. After select, go to <b>Network &gt; VPN &gt; Certifications</b> page to
import a static.key to <b>PSK</b> field.
Username/Password: use username/password which is preset in server
side to complete the authentication.
<b>X.509 cert:</b> use X.509 type certificate to complete the authentication.
After select, go to Network > VPN > Certifications page to import CA
certificate, client certificate and client private key to corresponding fields.
X.509 cert + user: use both username/password and X.509 cert
authentication type.
Set local tunnel address when authentication type is None or Pre-shared.
Set remote tunnel address when authentication type is None or
Pre-shared.
Define an IP address pool for openVPN client.
Set the client subnet netmask to limit the IP address range.
Renegotiate data channel key after this interval. 0 means disable.
Limit server to a maximum of concurrent clients, range: 1-20.
<b>Note:</b> please adjust log severity to Info if you need to connect many
clients.
Enable or disable CRL verify.
When enabled, openVPN clients can communicate with each other.
Allow multiple clients to connect with the same common name or
certification.
Select from None, TLS Auth and TLS Crypt. When selecting TLS Auth or
TLS Crypt, go to <b>Network &gt; VPN &gt; Certifications</b> page to import a ta.key.
Select to enable or disable LZO to compress data.
Set link detection interval time to ensure tunnel connection. If this is set
on both server and client, the value pushed from server will override the
client local values. Range: 10-1800 s.
OpenVPN will be reestablished after timeout. If this is set on both server
and client, the value pushed from server will override the client local
values. Range: 60-3600 s.
Select from NONE, BF-CBC, DES-CBC, DES-EDE3-CBC, AES-128-CBC,
AES-192-CBC and AES-256-CBC.
Select from NONE, MD5, SHA1, SHA256, and SHA512.
Enter the maximum transmission unit. Range: 64-1500.
Set the maximum frame size. Range: 64-1500.
Select from ERROR, WARING, NOTICE and DEBUG.
User can enter some initialization strings in this field and separate the

Example: ncp-ciphers AES-128-GCM; key direction 1				
Account				
	Set username and password for OpenVPN client when authentication type			
Username & Password	is username/password.			
Local Route				
Subnet	Subnet Set the local route's IP address.			
Subnet Mask Set the local route's netmask.				
Client Subnet				
Name	Set the name as OpenVPN client certificate common name.			
Subnet Set the subnet of OpenVPN client.				
Subnet Mask	Set the subnet netmask of OpenVPN client.			

Table 3-2-5-14 OpenVPN Server Parameters

## 3.2.5.9 Certifications

User can import/export certificate and key files for OpenVPN and IPsec on this page.

OpenVPN Client	
- OpenVPN Client_1	
CA	Browse Import Export Delete
Public Certificate	Browse Import Export Delete
Private Key	Browse Import Export Delete
TA	Browse Import Export Delete
TLS Crypt	Browse Import Export Delete
Preshared Key	Browse Import Export Delete
PKCS12	Browse Import Export Delete
+ OpenVPN Client_2	
+ OpenVPN Client_3	

Figure 3-2-5-17

MAKE SENSING MATTER

Milesight

- OpenVPN Server					
CA	Browse	Import	Export	Delete	
Public Certificate	Browse	Import	Export	Delete	
Private Key	Browse	Import	Export	Delete	
DH	Browse	Import	Export	Delete	
TA	Browse	Import	Export	Delete	
TLS Crypt	Browse	Import	Export	Delete	
CRL	Browse	Import	Export	Delete	
Preshared Key	Browse	Import	Export	Delete	



IPs	ec						
13	- IPsec_1						
	СА		Browse	Import	Export	Delete	
	Local Certificate		Browse	Import	Export	Delete	
	Remote Certificate		Browse	Import	Export	Delete	
	Private Key		Browse	Import	Export	Delete	
	CRL		Browse	Import	Export	Delete	
+	- IPsec_2						
+	- IPsec_3						
		Figure 3-2-5-19	I				
IP	sec Server						
1	- IPsec Server						

CA	Browse Import Export Delete
Local Certificate	Browse Import Export Delete
Private Key	Browse Import Export Delete
CRL	Browse Import Export Delete



#### 3.2.5.10 WireGuard

WireGuard is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography.

# WireGuard passes traffic over UDP protocol.

<ul> <li>WireGuard_1</li> </ul>				
Enable				
Interface	wg0			
Customized Private Key				
Private Key	<i>i</i> ¢			
Public Key	F8xRHUqMQ0fgJTw4V4M7gvm			
IP Address				
Listening Port				
DNS				
MTU				
Peer	Public Key	Allowed IP	Endpoint Address	Operation
				_
				+

Figure 3-2-5-21

WireGuard					
ltem	Description				
Enable	Enable WireGuard interface. A maximum of 3 WireGaurd interfaces is allowed.				
Interface	Show the WireGuard interface name.				
Customized Private Key	Enable or disable to customize the private key of this WireGuard interface. If disabled, the client will use the private key generated by this router.				
Public Key	Show the public key generated by the private key.				
IP Address	Set the local virtual IP address and netmask. Example: 10.8.0.2/24				
Listening Port	Set the port to send or receive WireGuard packets. The port numbers of different WireGuard interfaces should be different.				
DNS	Set the DNS server address of this WireGuard interface. If left blank, the router will use DNS server address of common network interfaces (WAN, cellular, etc.).				
MTU	Set the maximum transmission unit of this WireGuard interface. If left blank, the router will use MTU of common network interfaces (WAN, cellular, etc.).				
Peer Table	Click "+" to add WireGuard peers of this WireGuard interface. One WireGuard interface can add 20 peers at most.				

Table 3-2-5-15 WireGuard Parameters

Milesight

Edit			
	Peer		
	Public Key		
	Allowed IP		×
			Ð
	Route Allowed IP		
	Preshared Key	ø	
	Endpoint Address		
	Endpoint Port		
	Keepalive Interval	25	
		Save	

Figure 3-2-5-22

WireGuard-Peer					
ltem	Description				
Peer	Set a WireGuard peer name. This name should be unique in this WireGuard client.				
Public Key	Set the public key of WireGuard peer server/client.				
Allowed IP	Set the real IP address and netmask of WireGuard peer's LAN network. Example: 192.168.1.0/24 One WireGuard peer supports to add 8 allowed IP addresses.				
Route Allowed IP Enable or disable to add static routings of allowed IP addr					
Preshared Key	Set the presahred key and both this interface and peer interface should set the same key value.				
Endpoint Address	Set IP address or domain name of WireGuard peer server/client.				
Endpoint Port	Set the destination port of WireGuard peer server/client.				
Keepalive Interval	After the connection is established, this WireGuard interface will send heartbeat packet regularly to keep alive. 0 means disabled.				

Table 3-2-5-16 WireGuard-Peer Parameters

## 3.2.6 IP Passthrough

IP Passthrough mode shares or "passes" the Internet providers assigned IP address to a single LAN client device connected to the router.

IP Passthrough		
Enable		
Passthrough Mode	DHCPS-Fixed	Ŧ
MAC		

Figure 3-2-6-1

IP Passthrough		
Item	Description	
Enable	Enable or disable IP Passthrough.	
Passthrough Mode	Select passthrough mode from DHCPS-Fixed and DHCPS-Dynamic.	
MAC	Set MAC address when mode is DHCPS-Fixed.	

Table 3-2-6-1 IP Passthrough Parameters

## 3.2.7 Routing

### 3.2.7.1 Static Routing

A static routing is a manually configured routing entry. Information about the routing is manually entered rather than obtained from dynamic routing traffic. After setting static routing, the package for the specified destination will be forwarded to the path designated by user.

Static Routing	RIP	OSPF	Routing Filtering				
Static Routing							
	Destination		Netmask/Prefix Length	Interface	Gateway	Distance	Operation
114.	114.114.114		255.255.255.255	LAN1/WAN 🗸	192.168.5.1	1	×
8.8.8	3.8		255.255.255	LAN1/WAN 🗸	192.168.5.1	1	×
0.0.0	0.0		0.0.0.0	LAN1/WAN 🗸	192.168.5.1	1	×
							•



Static Routing		
ltem	Description	
Destination	Enter the destination IP address.	
Netmask/Prefix Length	Enter the subnet mask or prefix length of destination address.	
Interface	The interface through which the data can reach the destination address.	

Gateway	IP address of the next router that will be passed by before the input data reaches the destination address.	
Distance	Priority, smaller value refers to higher priority. Range: 1-255.	
Table 3-2-7-1 Static Routing Parameters		

#### 3.2.7.2 RIP

RIP is mainly designed for small networks. RIP uses Hop Count to measure the distance to the destination address, which is called Metric. In RIP, the hop count from the router to its directly connected network is 0 and the hop count of network to be reached through a router is 1 and so on. In order to limit the convergence time, the specified metric of RIP is an integer in the range of 0 - 15 and the hop count larger than or equal to 16 is defined as infinity, which means that the destination network or host is unreachable. Because of this limitation, the RIP is not suitable for large-scale networks. To improve performance and prevent routing loops, RIP supports split horizon function. RIP also introduces routing obtained by other routing protocols.

Each router that runs RIP manages a routing database, which contains routing entries to reach all reachable destinations.

Static Routing	RIP	OSPF	Rou	ting Filtering
RIP Settings				
Enable	•			
Update Timer	30			s
Timeout Timer	180			s
Garbage Collection Timer	120			s
Version	v2		•	
Show Advanced Options				
Default Information Originate	e 🔲			
Default Metric	1			
Redistribute Connected				
Redistribute Static				
Redistribute OSPF				

Figure 3-2-7-2

RIP	
Item	Description

Milesight

Enable	Enable or disable RIP.
Update Timer	It defines the interval to send routing updates. Range: 5-2147483647, in seconds.
Timeout Timer	It defines the routing aging time. If no update package on a routing is received within the aging time, the routing's Routing Cost in the routing table will be set to 16. Range: 5-2147483647, in seconds.
Garbage Collection Timer	It defines the period from the routing cost of a routing becomes 16 to it is deleted from the routing table. In the time of Garbage-Collection, RIP uses 16 as the routing cost for sending routing updates. If Garbage Collection times out and the routing still has not been updated, the routing will be completely removed from the routing table. Range: 5-2147483647, in seconds.
Version	RIP version. The options are v1 and v2.
Advanced Settings	
Default Information Originate	Default information will be released when this function is enabled.
Default Metric	The default cost for the router to reach destination. Range: 0-16
Redistribute Connected	Check to enable.
Metric	Set metric after "Redistribute Connected" is enabled. Range: 0-16.
Redistribute Static	Check to enable.
Metric	Set metric after "Redistribute Static" is enabled. Range: 0-16.
Redistribute OSPF	Check to enable.
Metric	Set metric after "Redistribute OSPF" is enabled. Range: 0-16.

Table 3-2-7-2 RIP Parameters

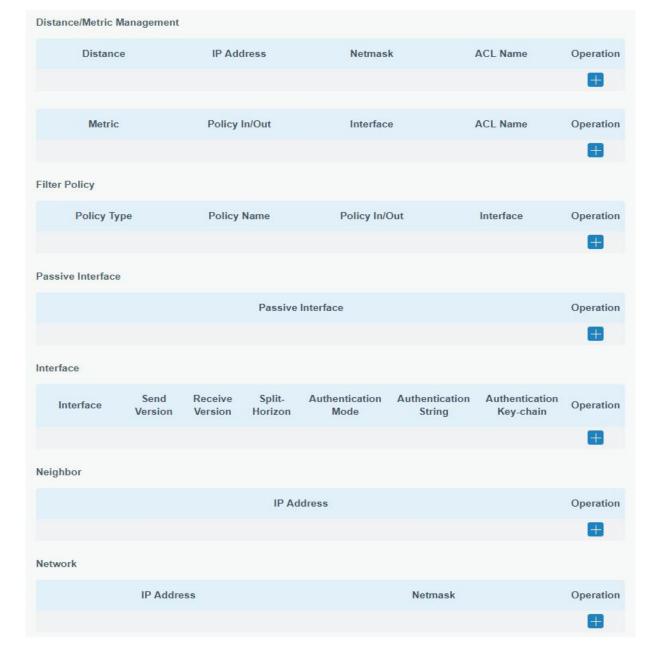


Figure 3-2-7-3

Item	Description	
Distance/Metric Mana	Distance/Metric Management	
Distance	Set the administrative distance that a RIP route learns. Range: 1-255.	
IP Address	Set the IP address of RIP route.	
Netmask	Set the netmask of RIP route.	
ACL Name	Set ACL name of RIP route.	
Metric	The metric of received route or sent route from the interface. Range: 0-16.	
Policy in/out	Select from "in" and "out".	

Interface	Select interface of the route.
ACL Name	Access control list name of the route strategy.
Filter Policy	
Policy Type	Select from "access-list" and "prefix-list".
Policy Name	User-defined prefix-list name.
Policy in/out	Select from "in" and "out".
Interface	Select interface from "cellular0", "LAN1/WAN" and "Bridge0".
Passive Interface	
Passive Interface	Select interface from "cellular0" and "LAN1/WAN", "Bridge0".
Interface	
Interface	Select interface from "cellular0", "LAN1/WAN" and "Bridge0".
Send Version	Select from "default", "v1" and "v2".
Receive Version	Select from "default", "v1" and "v2".
Split-Horizon	Select from "enable" and "disable".
Authentication Mode	Select from "text" and "md5".
Authentication String	The authentication key for package interaction in RIPV2.
Authentication Key-chain	The authentication key-chain for package interaction in RIPV2.
Neighbor	
IP Address	Set RIP neighbor's IP address manually.
Network	
IP Address	The IP address of interface for RIP publishing.
Netmask	The netmask of interface for RIP publishing.

Table 3-2-7-3

## 3.2.7.3 OSPF

OSPF, short for Open Shortest Path First, is a link status based on interior gateway protocol developed by IETF.

If a router wants to run the OSPF protocol, there should be a Router ID that can be manually configured. If no Router ID configured, the system will automatically select an IP address of interface as the Router ID. The selection order is as follows:

- If a Loopback interface address is configured, then the last configured IP address of Loopback interface will be used as the Router ID;
- If no Loopback interface address is configured, the system will choose the interface with the biggest IP address as the Router ID.

## Five types of packets of OSPF:

- Hello packet

- DD packet (Database Description Packet)
- LSR packet (Link-State Request Packet)
- LSU packet (Link-State Update Packet)
- LSAck packet (Link-Sate Acknowledgment Packet)

### **Neighbor and Neighboring**

After OSPF router starts up, it will send out Hello Packets through the OSPF interface. Upon receipt of Hello packet, OSPF router will check the parameters defined in the packet. If it's consistent, a neighbor relationship will be formed. Not all matched sides in neighbor relationship can form the adjacency relationship. It is determined by the network type. Only when both sides successfully exchange DD packets and LSDB synchronization is achieved, the adjacency in the true sense can be formed. LSA describes the network topology around a router, LSDB describes entire network topology.

Enable		
Router ID		
ABR Type	cisco	Ŧ
RFC1583 Compatibility	1	
OSPF Opaque-LSA		
		ms
OSPF Opaque-LSA SPF Delay Time SPF Initial-holdtime		ms
SPF Delay Time	0	

Figure 3-2-7-4

OSPF	
ltem	Description
Enable	Enable or disable OSPF.
Router ID	Router ID (IP address) of the originating LSA.
ABR Type	Select from cisco, ibm, standard and shortcut.
RFC1583 Compatibility	Enable/Disable.
OSPF Opaque-LSA	Enable/Disable LSA: a basic communication means of the OSPF routing protocol for the Internet Protocol (IP).
SPF Delay Time	Set the delay time for OSPF SPF calculations. Range: 0-6000000, in milliseconds.

SPF Initial-holdtime	Set the initialization time of OSPF SPF.
	Range: 0-6000000, in milliseconds.
SPF Max-holdtime	Set the maximum time of OSPF SPF.
	Range: 0-6000000, in milliseconds.
Reference Bandwidth	Range: 1-4294967, in Mbit.

Table 3-2-7-4 OSPF Parameters

Interface							
Inte	rface	Hello Interval(s)	Dead Inte	erval(s)	Retransmit Interval(s)	Transmit Delay(s)	Operation
Bridge0	۲	10	40	5		] [1	×
Interface Adva	anced Options						Ð
Interface	Network	Cost	Priority	Authenticat ion	Key ID	Кеу	Operation
Bridge 🔻	broad 🔻	10 1					×
							<b>H</b>

Figure 3-2-7-5

ltem	Description			
Interface				
Interface	Select interface from "cellular0","WAN" and "Bridge0".			
Hello Interval (s)	Send interval of Hello packet. If the Hello time between two adjacent routers is different, the neighbour relationship cannot be established. Range: 1-65535.			
Dead Interval (s)	Dead Time. If no Hello packet is received from the neighbours within the dead time, then the neighbour is considered failed. If dead times of two adjacent routers are different, the neighbour relationship cannot be established.			
Retransmit Interval (s)	When the router notifies an LSA to its neighbour, it is required to make acknowledgement. If no acknowledgement packet is received within the retransmission interval, this LSA will be retransmitted to the neighbour. Range: 3-65535.			
Transmit Delay (s)	It will take time to transmit OSPF packets on the link. So a certain delay time should be increased before transmission the aging time of LSA. This configuration needs to be further considered on the low-speed link. Range: 1-65535.			
Interface Advanced Options				
Interface	Select interface.			
Network	Select OSPF network type.			
Cost	Set the cost of running OSPF on an interface. Range: 1-65535.			
Priority	Set the OSPF priority of interface. Range: 0-255.			
Authentication	Set the authentication mode that will be used by the OSPF area.			

	Simple: a simple authentication password should be configured and confirmed again. MD5: MD5 key & password should be configured and confirmed again.
Key ID	It only takes effect when MD5 is selected. Range 1-255.
Кеу	The authentication key for OSPF packet interaction.

#### Table 3-2-7-5 OSPF Parameters

Passive Interface				
	Passi	ve Interface		Operation
				8
Network				
IP Address	N	etmask	Area ID	Operatior
				•
Neighbor				
IP Address	F	Priority	Poll	Operation
				Ð
Area				
Area ID	Area	No Summary	Authentication	Operation
				Ð

### Figure 3-2-7-6

Item	Description		
Passive Interface			
Passive Interface	Select interface from "cellular0", "LAN1/WAN" and "Bridge0".		
Network			
IP Address	The IP address of local network.		
Netmask	The netmask of local network.		
Area ID	The area ID of original LSA's router.		
Area			
Area ID	Set the ID of the OSPF area (IP address).		
Area	Select from "Stub" and "NSSA".		
	The backbone area (area ID 0.0.0.0) cannot be set as "Stub" or "NSSA".		
No Summary	Forbid route summarization.		
Authentication	Select authentication from "simple" and "md5".		

Table 3-2--7-6 OSPF Parameters



Figure 3-2-7-7

Area Advanced Options			
ltem	Description		
Area Range			
Area ID	The area ID of the interface when it runs OSPF (IP address).		
IP Address	Set the IP address.		
Netmask	Set the netmask.		
No Advertise	Forbid the route information to be advertised among different areas.		
Cost	Range: 0-16777215		
Area Filter			
Area ID	Select an Area ID for Area Filter.		
Filter Type	Select from "import", "export", "filter-in", and "filter-out".		
ACL Name	Enter an ACL name which is set on "Routing > Routing Filtering" webpage.		
Area Virtual Link			
Area ID	Set the ID number of OSPF area.		
ABR Address	ABR is the router connected to multiple outer areas.		
Authentication	Select from "simple" and "md5".		
Key ID	It only takes effect when MD5 is selected. Range 1-15.		
Key	The authentication key for OSPF packet interaction.		
Hello Interval	Set the interval time for sending Hello packets through the interface. Range: 1-65535.		
Dead Interval	The dead interval time for sending Hello packets through the interface. Range: 1-65535.		
Retransmit Interval	The retransmission interval time for re-sending LSA. Range: 1-65535.		
Transmit Delay	The delay time for LSA transmission. Range: 1-65535.		

Table 3-2-7-7 OSPF Parameters



Redistribution					
Redistribution Type	Metric	Met	ric Type	Route Map	Operation
connected •		1	•		×
					<b>H</b>
Redistribution Advanced Options	•				
Always Redistribute Default Route					
Redistribute Default Route Metric	0				
Redistribute Default Route Metric Type	1	•			
Distance Management					
Агеа Тур	е		Distance		Operation
					<b>H</b>

Figure 3-2-7-8

Item	Description
Redistribution	
Redistribution Type	Select from "connected", "static" and "rip".
Metric	The metric of redistribution router. Range: 0-16777214.
Metric Type	Select Metric type from "1" and "2".
Route Map	Mainly used to manage route for redistribution.
Redistribution Advance	ed Options
Always Redistribute Default Route	Send redistribution default route after starting up.
Redistribute Default Route Metric	Send redistribution default route metric. Range: 0-16777214.
Redistribute Default Route Metric Type	Select from "0", "1" and "2".
Distance Management	
Area Type	Select from "intra-area", "inter-area" and "external".
Distance	Set the OSPF routing distance for area learning. Range: 1-255.

Table 3-2-7-8 OSPF Parameters

### 3.2.7.4 Routing Filtering

Name	Acti	on	Match Any	IP Ad	dress	Netr	nask	Operation
	deny	¥					]	×
								•
Prefix-List								
Name	Sequence Number	Action	Match Any	IP Address	Netmask	GE Length	LE Length	Operation
		deny 🔻						×

Figure 3-2-7-9

<b>Routing Filterin</b>	ng
ltem	Description
Access Contro	List
Name	User-defined name, need to start with a letter. Only letters, digits and underline (_) are allowed.
Action	Select from "permit" and "deny".
Match Any	No need to set IP address and subnet mask.
IP Address	User-defined.
Netmask	User-defined.
IP Prefix-List	
Name	User-defined name, need to start with a letter. Only letters, digits and underline (_) are allowed.
Sequence Number	A prefix name list can be matched with multiple rules. One rule is matched with one sequence number. Range: 1-4294967295.
Action	Select from "permit" and "deny".
Match Any	No need to set IP address, subnet mask, FE Length, and LE Length.
IP Address	User-defined.
Netmask	User-defined.
FE Length	Specify the minimum number of mask bits that must be matched. Range: 0-32.
LE Length	Specify the maximum number of mask bits that must be matched. Range: 0-32.

Table 3-2-7-9 Routing Filtering Parameters

#### 3.2.8 VRRP

The Virtual Router Redundancy Protocol (VRRP) is a computer networking protocol that provides automatic assignment of available Internet Protocol (IP) routers for participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections in an IP sub-network.

Increasing the number of exit gateway is a common method for improving system reliability. VRRP

adds a group of routers that undertake gateway function into a backup group so as to form a virtual router. The election mechanism of VRRP will decide which router undertakes the forwarding task, and the host in LAN is only required to configure the default gateway for the virtual router.

In VRRP, routers need to be aware of failures in the virtual master router. To achieve this, the virtual master router sends out multicast "alive" announcements to the virtual backup routers in the same VRRP group.

The VRRP router who has the highest number will become the virtual master router. The VRRP router number ranges from 1 to 255 and usually we use 255 for the highest priority and 100 for backup.

If the current virtual master router receives an announcement from a group member (Router ID) with a higher priority, then the latter will pre-empt and become the virtual master router.

VRRP has the following characteristics:

- The virtual router with an IP address is known as the Virtual IP address. For the host in LAN, it is only required to know the IP address of virtual router, and set it as the address of the next hop of the default route.
- The network Host communicates with the external network through this virtual router.
- A router will be selected from the set of routers based on its priority to undertake the gateway function. Other routers will be used as backup routers to perform the duties of gateway for the gateway router in the case of any malfunction, so as to guarantee uninterrupted communication between the host and external network.

When interface connected with the uplink is at the state of Down or Removed, the router actively lowers its priority so that priority of other routers in the backup group will be higher. Thus the router with the highest priority becomes the gateway for the transmission task.

Status	DISABLE		
	DIGIDEL		
VRRP Settings			
Enable			
Interface	Bridge0	۳	
Virtual Router ID	1		
Virtual IP			
Priority	100		
Advertisement Interval (s)	1		
Preemption Mode			
IPV4 Primary Server	8.8.8		
IPV4 Secondary Server	114.114.114.114		
Interval	300		s
Retry Interval	5		s
Timeout	3		s
Max Ping Retries	3		



VRRP		
ltem	Description	Default

Enable	Enable or disable VRRP.	Disable
Interface	Select the interface of Virtual Router.	None
Virtual Router ID	User-defined Virtual Router ID. Range: 1-255.	None
Virtual IP	Set the IP address of Virtual Router.	None
Priority	The VRRP priority range is 1-254 (a bigger number indicates a higher priority). The router with higher priority will be more likely to become the gateway router.	100
Advertisement Interval (s)	Heartbeat package transmission time interval between routers in the virtual ip group. Range: 1-255.	1
Preemption Mode	If the router works in the preemption mode, once it finds that its own priority is higher than that of the current gateway router, it will send VRRP notification package, resulting in re-election of gateway router and eventually replacing the original gateway router. Accordingly, the original gateway router will become a Backup router.	Disable
IPV4 Primary Server	The router will send ICMP packet to the IP address or hostn ame to determine whether the Internet connection is still av ailable or not.	8.8.8.8
IPV4 Secondary Server	The router will try to ping the secondary server name if prim ary server is not available.	223.5.5.5
Interval	Time interval (in seconds) between two Pings.	300
Retry Interval	Set the ping retry interval. When ping failed, the router will ping again every retry interval.	5
Timeout	The maximum amount of time the router will wait for a resp onse to a ping request. If it does not receive a response for the amount of time defined in this field, the ping request will be considered as failure.	3
Max Ping Retries	The retry times of the router sending ping request until dete rmining that the connection has failed.	3

Table 3-2-8-1 VRRP Parameters

### **Related Configuration Example**

VRRP Application Example

### 3.2.9 DDNS

Dynamic DNS (DDNS) is a method that automatically updates a name server in the Domain Name System, which allows user to alias a dynamic IP address to a static domain name.

DDNS serves as a client tool and needs to coordinate with DDNS server. Before starting configuration, user shall register on a website of proper domain name provider and apply for a domain name.

DDNS Status	
Status	2
DDNS Method List	
Enable	
Name	
Service Type	DynDNS 🗸
Username	
User ID	
Password	
Server	
Server Path	L
Hostname	
Append IP	
Use HTTPS	

Figure 3-2-9-1

DDNS	
ltem	Description
Enable	Enable/disable DDNS.
Name	Give the DDNS a descriptive name.
Interface	Set interface bundled with the DDNS.
Service Type	Select the DDNS service provider.
Username	Enter the username for DDNS register.
User ID	Enter User ID of the custom DDNS server.
Password	Enter the password for DDNS register.
Server	Enter the name of DDNS server.
Server Path	By default the hostname is appended to the path.
Hostname	Enter the hostname for DDNS.
Append IP	Append your current IP to the DDNS server update path.
Use HTTPS	Enable HTTPS for some DDNS providers.

Table 3-2-9-1 DDNS Parameters

# 3.3 System

Milesight

#### 3.3.1 General Settings

### 3.3.1.1 General

General settings include system info and HTTPS certificates.

Hostname		ROU	JTER			
Web Login Tin	neout(s)	1800	)			
Encrypting Cle	eartext Passwords					
HTTPS Certif	ficates https.crt		Browse	Import	Export	Delete

Figure 3-3-1-1

General		
Item	Description	Default
System		
Hostname	User-defined router name, needs to start with a letter.	ROUTER
Web Login Timeout (s)	You need to log in again if it times out. Range: 100-3600.	1800
Encrypting Cleartext Passwords	This function will encrypt all of cleartext passwords into ciphertext passwords.	Enable
HTTPS Certificates		
Certificate	Click "Browse" button, choose certificate file on the PC, and then click "Import" button to upload the file into router. Click "Export" button will export the file to the PC. Click "Delete" button will delete the file.	
Кеу	Click "Browse" button, choose key file on the PC, and then click "Import" button to upload the file into router. Click "Export" button will export file to the PC. Click "Delete" button will delete the file.	

Table 3-3-1-1 General Setting Parameters

#### 3.3.1.2 System Time

This section explains how to set the system time including time zone and time synchronization type. Note: to ensure that the router runs with the correct time, it's recommended that you set the system

#### time when configuring the router.

**M**ilesight

Current Time	2020-04-30 17:58:27 Thu	r
Time Zone	8 China (Beijing)	٠
Sync Type	Sync with NTP Server	٠
Primary NTP Server	1.cn.pool.ntp.org	
Secondary NTP Server		-
TP Server		
nable NTP Server		

Figure 3-3-1-2

System Time				
ltem	Description			
Current Time	Show the current system time.			
Time Zone	Click the drop down list to select the time zone you are in.			
	Click the drop down list to select the time synchronization type.			
	Sync with Browser: Synchronize time with browser.			
Suno Tuno	Sync with NTP Server: Synchronize time with NTP Server.			
Sync Type	Set up Manually: configure the time manually.			
	Sync with Cellular Operator: Synchronize time with cellular operator.			
	This only works when the device has registered to cellular network.			
Sync with Browser	Synchronize time with browser.			
Browser Time	Show the current time of browser.			
Set up Manually	Manually configure the system time.			
Primary NTP Server	Enter primary NTP Server's IP address or domain name.			
Secondary NTP Server	Enter secondary NTP Server's IP address or domain name.			
NTP Server				
Enable NTP Server	NTP client on the network can achieve time synchronization with router			
LIIADIE NIF SEIVEI	after this option is checked.			

Table 3-3-1-2 System Time Parameters

### 3.3.1.3 Email

SMTP, short for Simple Mail Transfer Protocol, is a TCP/IP protocol used in sending and receiving e-mail. This section describes how to configure email settings and add email groups for alarms and events.

Enable		
Ema <mark>il A</mark> ddress		
Password		
SMTP Server Add	Iress	
Port	25	
Encryption	STARTTLS	•

Figure 3-3-1-3

SMTP Client Settings				
ltem	Description			
Enable	Enable or disable SMTP client function.			
Email Address	Enter the sender's email account.			
Password	Enter the sender's email password.			
SMTP Server Address	Enter SMTP server's domain name.			
Port	Enter SMTP server port. Range: 1-65535.			
	Select from: None, TLS/SSL, STARTTLS.			
	None: No encryption. The default port is 25.			
	STARTTLS: STARTTLS is a way to take an existing insecure			
	connection and upgrade it to a secure connection by using			
	SSL/TLS. The default port is 587.			
Encryption	TLS/SSL: SSL and TLS both provide a way to encrypt a			
	communication channel between two computers (e.g. your			
	computer and our server). TLS is the successor to SSL and			
	the terms SSL and TLS are used interchangeably unless			
	you're referring to a specific version of the protocol.The			
	default port is 465.			

Table 3-3-1-3 SMTP Setting

Milesight

Email List						
Em	ail Address			Description		Operation
						×
						(E)
Email Group List						
	Group ID					
	Description					
	List			Selected		
					*	
		_				
		Save	Cancel			

Figure 3-3-1-4

ltem	Description
Email List	
Email Address	Enter the Email address.
Description	The description of the Email address.
Email Group List	
Group ID	Set number for email group. Range: 1-100.
Description	The description of the Email group.
List	Show the Email address list.
Selected	Show the selected Email address.

Table 3-3-1-4 Email Settings

# **Related Topics**

Events Setting

## 3.3.2 Phone&SMS

#### 3.3.2.1 Phone

Phone settings involve in call/SMS trigger, SMS control and SMS alarm for events.

Phone	SMS						
Phone Numb	ber List						
	Nu	nber		I	Description		Operation
							×
							<b>H</b>
Phone Grou	p List						
		Group ID					
		Description	[				
		List			Selected		
			* D			*	

Figure 3-3-2-1

Phone				
Item	Description			
Phone Number List				
Number	Enter the telephone number. Digits, "+" and "-" are allowed.			
Description	The description of the telephone number.			
Phone Group List				
Group ID	Set number for phone group. Range: 1-100.			
Description	The description of the phone group.			
List	Show the phone list.			
Selected	Show the selected phone number.			

Table 3-3-2-1 Phone Settings

## **Related Topic**

Connect on Demand

## 3.3.2.2 SMS

SMS settings involve in remote SMS control, sending SMS and SMS receiving and sending status. Ensure the SMS center number is typed on **Network > Interface > Cellular** page before using SMS features.

Milesight

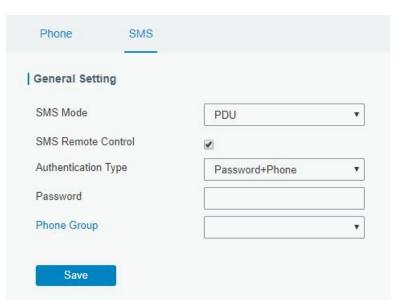


Figure 3-3-2-2

SMS Settings				
ltem	Description			
SMS Mode	<ul> <li>Select SMS mode:</li> <li>Text: Pure text mode, mainly used in Europe and America. Technicall y, it can also be used to send Short Messages in Chinese. When CLI commands will be sent to control the router, Text mode is recommen ded to choose.</li> <li>PDU: It;s the default encoding Mode for mobile phones, which confor m to all mobile phones SMS format and can use any character.</li> </ul>			
SMS Remote Control	Enable/disable SMS Remote Control to send SMS to control the router.			
Authentication Type	You can choose "phone number" or "password + phone number". Phone number: only the phone numbers on phone groups support remote control. Password + phone number: only the phone numbers on phone groups support remote control; besides, control SMS should be sent as format password+";"+command content.			
Password	Set password for authentication.			
Phone Group	Select the Phone group which used for remote control. User can click the Phone Group and set phone number.			

Table 3-3-2-2 SMS Remote Control Parameters

Send SMS				
Phone Number				
Content				
Send				
Inbox				
From	То	Sender	Search Clear All	
	Sender	Time	(	Content
< 1 > 10 v	Go to:			
Outbox				
From	То	Recipient	Search Clear All	l
	Recipient T	ime	Content	Status

Figure 3-3-2-3

SMS		
Item Description		
Send SMS		
Phone Number	Enter the number to receive the SMS.	
Content	SMS content.	
Inbox/Outbox		
Sender	SMS sender from outside.	
Recipient	SMS recipient which UR32L send to.	
From	Select the start date.	
То	Select the end date.	
Search	Search for SMS record.	
Clear All	Clear all SMS records in web GUI.	
	Table 2.2.2.2 CMC Cattings	

Table 3-3-2-3 SMS Settings

## 3.3.3 User Management

#### 3.3.3.1 Account

Here you can change the login username and password of the administrator. Note: it is strongly recommended that you modify them for the sake of security.

Change Account Info		
Username	admin	
Old Password		
New Password		
Confirm New Password		

Figure 3-3-3-1

Account	
ltem	Description
Username	Enter a new username. You can use characters such as a-z, 0-9, "_", "-". The first character can't be a digit.
Old Password	Enter the old password.
New Password	Enter a new password. You can use any ASCII characters except blank.
Confirm New Password	Enter the new password again.

Table 3-3-3-1 Account Settings

### 3.3.3.2 User Management

This section describes how to create common user accounts. The common user permission includes Read-Only and Read-Write.

Account	User Management			
User List				
	Username	Password	Permission	Operation
			Read-Only 🗸	×
				œ

Figure 3-3-3-2

User Management		
ltem	Description	
Username	Enter a new username. You can use characters such as a-z, 0-9, "_", "-". The first character can't be a digit.	
Password	Set password. You can use any ASCII characters except blank.	
Permission	Select user permission from "Read-Only" and "Read-Write". <b>Read-Only:</b> users can only view the configuration of router in this level. <b>Read-Write:</b> users can view and set the configuration of router in this level.	

Table 3-3-3-2 User Management

# 3.3.4 AAA

AAA access control is used for visitors control and the available corresponding services once access is allowed. It adopts the same method to configure three independent safety functions. It provides modularization methods for following services:

- Authentication: verify if the user is qualified to access to the network.
- Authorization: authorize related services available for the user.
- Charging: record the utilization of network resources.

### 3.3.4.1 Radius

Using UDP for its transport, Radius is generally applied in various network environments with higher requirements of security and permission of remote user access.

Radius	Tacacs+	LDAP	Authentication
Radius Settin	gs		
Enable			
Server IP Addr	ess		
Server Port		1812	
Shared Secret			
-			
Save			

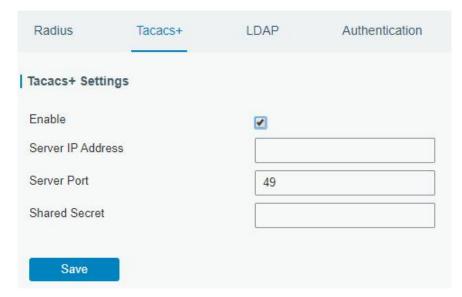
Figure 3-3-4-1

Radius	
Item	Description
Enable	Enable or disable Radius.
Server IP Address	Fill in the Radius server IP address/domain name.
Server Port	Fill in the Radius server port. Range: 1-65535.
Кеу	Fill in the key consistent with that of Radius server in order to get connected with Radius server.

Table 3-3-4-1 Radius Parameters

### 3.3.4.2 TACACS+

Using TCP for its transport, TACACS+ is mainly used for authentication, authorization and charging of the access users and terminal users by adopting PPP and VPDN.





on disable TACACS+.
disable TACACS+.
TACACS+ server IP address/domain name.
TACACS+ server port. Range: 1-65535.
key consistent with that of TACACS+ server in et connected with TACACS+ server.
ļ

Table 3-3-4-2 TACACS+ Parameters

#### 3.3.4.3 LDAP

Milesight

A common usage of LDAP is to provide a central place to store usernames and passwords. This allows many different applications and services to connect the LDAP server to validate users.

LDAP is based on a simpler subset of the standards contained within the X.500 standard. Because of this relationship, LDAP is sometimes called X.500-lite as well.

Radius	Tacacs+	LDAP	Authentication
LDAP Setting	IS		
Enable			
Server IP Addr	ess		
Server Port		389	
Base DN			
Security		None	•
Username			
Password			

Figure 3-3-4-3

LDAP	
Item	Description
Enable	Enable or Disable LDAP.
Server IP Address	Fill in the LDAP server's IP address/domain name. The
Server IF Address	maximum count is 10.
Server Port	Fill in the LDAP server's port. Range: 1-65535
Base DN	The top of LDAP directory tree.
Security	Select secure method from "None", "StartTLS" and "SSL".
Username	Enter the username to access the server.
Password	Enter the password to access the server.
	Table 3-3-5-3 I DAP Parameters

Table 3-3-5-3 LDAP Parameters

### 3.3.4.4 Authentication

AAA supports the following authentication ways:

- None: uses no authentication, generally not recommended.
- Local: uses the local username database for authentication.
  - > Advantages: rapidness, cost reduction.
  - > Disadvantages: storage capacity limited by hardware.
- Remote: has user's information stored on authentication server. Radius, TACACS+ and LDAP supported for remote authentication.

When radius, TACACS+, and local are configured at the same time, the priority level is: 1 >2 >3.

thenticatio	on Settings							
Se	rvice	1			2		3	
Сог	nsole	None	T	No	ne	¥	None	٣
V	Veb	None	•	No	ne		None	
Те	elnet	None	•	No	ne	v	None	٣
S	SH	None	¥	No	ne	*	None	· •

Figure 3-3-4-4

Authentication		
ltem	Description	
Console	Select authentication for Console access.	
Web	Select authentication for Web access.	
Telnet	Select authentication for Telnet access.	
SSH	Select authentication for SSH access.	

Table 3-3-4-4 Authentication Parameters

### 3.3.5 Device Management

#### 3.3.5.1 DeviceHub

You can connect the device to the Milesight DeviceHub on this page so as to manage the router centrally and remotely. For more details please refer to **DeviceHub User Guide**.

Device Management	Milesight VPN
Device Management	
Status	Disconnected
Server Address	
Activation Method	By Authentication Code 🗸
Authentication Code	
Connect	
Connect	

Figure 3-3-5-1

DeviceHub	
ltem	Description
Status	Show the connection status between the router and the DeviceHub.
Disconnected	Click this button to disconnect the router from the DeviceHub.
Server Address	IP address or domain of the device management server.
Activation Method	Select activation method to connect the router to the DeviceHub server, options are "By Authentication Code" and "By Account name".
Authentication Code	Fill in the authentication code generated from the DeviceHub.
Account name	Fill in the registered DeviceHub account (email) and personard
Password	Fill in the registered DeviceHub account (email) and password.

Table 3-3-5-1

## 3.3.5.2 Milesight VPN

You can connect the device to the Milesight VPN on this page so as to manage the router and connected devices centrally and remotely. For more details please refer to *MilesightVPN User Guide*.

Device Management	Milesight VPN	
Milesight VPN Setting		
Server		
Port	18443	
Authorization Code		
Device Name		
Connect		
Milesight VPN Status		
Status	Disconnected	
Local IP	-	
Remote IP	-	
Duration		

Figure 3-3-5-2

Milesight VPN				
Item	Description			
Milesight VPN Settin	gs			
Server	Enter the IP address or domain name of Milesight VPN.			
Port	Enter the HTTPS port number.			
Authorization code Enter the authorization code which generated by Milesight VPN.				
Device Name	Enter the name of the device.			
Milesight VPN Status	;			
Status	Show the connection information about whether the router is			
Status	connected to the Milesight VPN.			
Local IP	Show the virtual IP of the router.			
Remote IP	Show the virtual IP of the Milesight VPN.			
Duration	Show the information on how long the router has been			
Duration	connected to the Milesight VPN.			

Table 3-3-5-2

### 3.3.6 Events

Event feature is capable of sending alerts by Email when certain system events occur.

#### 3.3.6.1 Events

You can view alarm messages on this page.

Events	Events Settings			
Mark as Read	Delete	Mark All as Read	Delete All Alarms	
Sta	itus	Туре	Time	Message
< > 10 •	Go to:	GO		

Figure 3-3-6-1

Events				
ltem	Description			
Mark as Read	Mark the selected event alarm as read.			
Delete	Delete the selected event alarm.			
Mark All as Read	Mark all event alarms as read.			
Delete All Alarms	Delete all event alarms.			
Status	Show the reading status of the event alarms, such as "Read" and "Unread".			

Туре	Show the event type that should be alarmed.	
Time	Show the alarm time.	
Message	Show the alarm content.	

Table 3-3-6-1 Events Parameters

## 3.3.6.2 Events Settings

In this section, you can decide what events to record and whether you want to receive email and SMS notifications when any change occurs.

Events Settings				
Enable  Phone Group List Email Group List	• •			
Events	Record	Email 🗐 Email Group List	SMS 📮 Phone Group List	SNMP
System Startup				
System Reboot				
System Time Update				
VPN Up				
VPN Down				
WAN Up				
WAN Down				
Link switch				
Weak Signal				
Cellular Up				
	_	re 3-3-6-2	U.	
Collision Down				

Cellular Down	4		
Cellular Data Stats Clear			
Cellular Data Traffic is running out			
Cellular Data Traffic Overflow			

Figure 3-3-6-3

Event Settings			
Item	Description		
Enable	Check to enable "Events Settings".		
Phone Group List	Select phone group to receive SMS alarm.		
Email Group List	Select email group to receive alarm.		

Record	The relevant content of event alarm will be recorded on "Event" page if this option is checked.
Email	The relevant content of event alarm will be sent out via email if this option is checked.
Email Setting	Click and you will be redirected to the page "Email" to configure email group list.
SMS	The relevant content of event alarm will be sent out via SMS if this option is checked.
SMS Setting	Click and you will be redirected to the page of "Phone" to configure phone group list.
VPN Up	VPN is connected.
VPN Down	VPN is disconnected.
WAN Up	Ethernet cable is connected to WAN port.
WAN Down	Ethernet cable is disconnected to WAN port.
Link Switch	Switch to use other interface for Internet access.
Weak Signal	The signal level of cellular is low (RSSI < 11 or $\ge$ 99).
Cellular Up	Cellular network is connected.
Cellular Down	Cellular network is disconnected.
Cellular Data Stats Clear	Zero out the data usage of the main SIM card.
Cellular Data Traffic is running out	The main SIM card is reaching the data usage limit.
Cellular Data Traffic Over Flow	The main SIM card has exceeded the data usage plan.

**Related Topics** 

Email Setting

### 3.4 Service

### 3.4.1 MQTT

UR32L supports to work as MQTT client to forward data and router information to MQTT broker in two ways:

Table 3-3-6-2 Events Parameters

- 1. Users send requests to the router to enquire the router information;
- 2. The router publishes the data automatically.

MQTT					
Connections					
	ID	Name	Address	Status	Operation
	1	mqtttest1	192.168.44.54:1883	Connected	<pre> « X </pre>
	2	555	666:1883	Disconnected	2 ×
					Đ



MQTT	
Status	
Status	Disable
General	
Name	
Enable	
Broker Address	
Broker Port	1883
Client ID	24:e1:24:f2:63:10_linyptjr
Connection Timeout(s)	30
Keep Alive Interval(s)	60
Auto Reconnect	
Reconnect Period	4
Clean Session	
User Credentials	
Enable	
Username	
Password	
TLS	
Enable	۵
Mode	CA signed server certificate 🗸

Figure 3-4-1-2

Awill
QoS 0 🗸
{     "will":"offlinetest"     }

#### Request and Response Topic

Milesight

Data Type	Торіс	Retain	QoS	
Status Request	/status/request		QoS 0	~
Status Response	/status/response		QoS 0	~

| System Status Publish Topic

Data Type	Торіс	Publish Interval(s)	Retain	QoS
System Info	/systeminfo	60		QoS 0
System Status	/systemstatus	60		QoS 0
Cellular	/cellular	60		QoS 0
Ethernet	/ethernet	60		QoS 0

#### Figure 3-4-1-3

MQTT Settings	MQTT Settings		
ltem	Description		
Status	Show connection status between router and MQTT broker.		
General			
Name	Customize a unique connection name. It is not allowed to change after save.		
Enable	Enable or disable this MQTT connection.		
Broker Address	MQTT broker address to receive data.		
Broker Port	MQTT broker port to receive data.		
Client ID	Client ID is the unique identity of the client to the server. It must be unique when all clients are connected to the same server, and it is the key to handle messages at QoS 1 and 2.		
Connection Timeout/s	If the client does not get a response after the connection timeout, the connection will be considered as broken. The Range: 1-65535.		
Keep Alive	After the client is connected to the server, the client will send heartbeat		
Interval/s	packet to the server regularly to keep alive. Range: 1-65535.		
Auto Reconnect	When connection is broken, try to reconnect the server automatically.		

Reconnect	When connection is broken, the period to reconnect the server
Period	periodically.
Clean Session	When enabled, the connection will create a temporary session and all information will lose when the client is disconnected from broker; when disabled, the connection will create a persistent session that will remain and save offline messages until the session logs out overtime.
User Credentials	
Enable	Enable user credentials.
Username	The username used for connecting to the MQTT broker.
Password	The password used for connecting to the MQTT broker.
TLS	
Enable	Enable the TLS encryption in MQTT communication.
	Select from Self signed certificates, CA signed server certificate.
	CA signed server certificate: verify with the certificate issued by
Mode	Certificate Authority (CA) that pre-loaded on the device.
	Self signed certificates: upload the custom CA certificates, client
	certificates and secret key for verification.
Last Will and Tes	stament
	Last will message is automatically sent when the MQTT client is
Enable	abnormally disconnected. It is usually used to send device status
Ellable	information or inform other devices or proxy servers of the device's offline
	status.
Last-Will Topic	Customize the topic to receive last will messages.
Last-Will QoS	QoS0, QoS1 or QoS2 are optional.
Last-Will Retain	Enable to set last will message as retain message.
Last-Will	Customize the last will message contents.
Payload	ouotomize the last will message contents.
Request and Res	ponse Topic
	The router supports to send requests to enquire router information.
	Status Request: users is able to send requests to this topic to enquire
	router information. Request format:
	{
	"id":"1",
Торіс	"status":"systeminfo",
	"sn": "64E1213132456",
	"need_response":1 //1 means need response
	}
	The id is a random value, and the status can be set as 4 types: systeminfo,
	systemstatus, cellular, ethernet.
Datain	<b>Status Response:</b> users is able to subscribe this topic to get the replies.
Retain	Enable to set the latest message of this topic as retain message.
QoS System Status P	QoS0, QoS1 or QoS2 are optional.
System Status P	
Data Type	Data type sent to MQTT broker automatically.

Торіс	Topic name of the data type used for publishing.
Publish Interval (s)	The interval to publish data to MQTT broker automatically.
Retain	Enable to set the latest message of this topic as retain message.
QoS	QoS0, QoS1 or QoS2 are optional.

Table 3-4-1-1 MQTT Parameters

### 3.4.2 SNMP

SNMP is widely used in network management for network monitoring. SNMP exposes management data with variables form in managed system. The system is organized in a management information base (MIB) which describes the system status and configuration. These variables can be remotely queried by managing applications.

Configuring SNMP in networking, NMS, and a management program of SNMP should be set up at the Manager.

Configuration steps are listed as below for achieving query from NMS:

- 1. Enable SNMP setting.
- 2. Download MIB file and load it into NMS.
- 3. Configure MIB View.
- 4. Configure VCAM.

### **Related Configuration Example**

**SNMP Application Example** 

### 3.4.2.1 SNMP

UR32L supports SNMPv1, SNMPv2c and SNMPv3 version. SNMPv1 and SNMPv2c employ community name authentication. SNMPv3 employs authentication encryption by username and password.

SNMP	MIB View	VACM	Trap	MIB
SNMP Setting	gs			
Enable				
Port		161		
SNMP Version		SNMPv2		•
Location Information		225_locati		
Contact Information		225_Contact		

#### Figure 3-4-2-1

SNMP Settings			
ltem	Description		
Enable	Enable or disable SNMP function.		
Port	Set SNMP listened port. Range: 1-65535.		
FUIL	The default port is 161.		
SNMP Version	Select SNMP version; support SNMP v1/v2c/v3.		
Location Information	Fill in the location information.		
Contact Information	Fill in the contact information.		

Table 3-4-2-1 SNMP Parameters

### 3.4.2.2 MIB View

This section explains how to configure MIB view for the objects.

SNMP	MIB View	VACM	Trap	MIB	
View List					
v	iew Name		Filter	View OID	Operation
All		Included	•	1	
system		Included	•	1.3.6.1.2.1.1	
					+

Figure 3-4-2-2

MIB View	
ltem	Description
View Name	Set MIB view's name.
View Filter	Select from "Included" and "Excluded".
View OID	Enter the OID number.
Included	You can query all nodes within the specified MIB node.
Excluded	You can query all nodes except for the specified MIB node.

Table 3-4-2-2 MIB View Parameters

## 3.4.2.3 VACM

This section describes how to configure VCAM parameters.

SNMP	MIB View	VACM	Trap	MIB			
NMP v1 & v	2 User List						
Сог	nmunity	Permissio	n	MIB View		Network	Operation
private		Read-Write	•	All	▼ 0.0.0.0/0	)	×
public		Read-Write	• .	All	• 0.0.0.0/0	)	×



VACM		
ltem	Description	
SNMP v1 & v2 Us	er List	
Community	Set the community name.	
Permission	Select from "Read-Only" and "Read-Write".	
MIB View	Select an MIB view to set permissions from the MIB view list.	
Network	The IP address and bits of the external network accessing the MIB view.	
Read-Write	The permission of the specified MIB node is read and write.	
Read-Only	The permission of the specified MIB node is read only.	
SNMP v3 User Gr	oup	
Group Name	Set the name of SNMPv3 group.	
Security Level	Select from "NoAuth/NoPriv", "Auth/NoPriv", and " Auth/Priv".	
Read-Only View	Select an MIB view to set permission as "Read-only" from the MIB view list.	
Read-Write View	Select an MIB view to set permission as "Read-write" from the MIB view list.	
Inform View	Select an MIB view to set permission as "Inform" from the MIB view list.	
SNMP v3 User Lis	st	
Username	Set the name of SNMPv3 user.	
Group Name	Select a user group to be configured from the user group.	
Authentication	Select from "MD5", "SHA", and "None".	
Authentication	The password should be filled in if authentication is "MD5" and "SHA".	
Password	The password should be filled in it authentication is MDS and SHA.	
Encryption	Select from "AES", "DES", and "None".	
Encryption	The password should be filled in if encryption is "AES" and "DES".	
Password	The password should be filled in it encryption is ALS and DLS.	

Table 3-4-2-3 VACM Parameters

# 3.4.2.4 Trap

This section explains how to enable network monitoring by SNMP trap.

SNMP	MIB View	VACM	Trap	MIB
SNMP Trap				
Enable		۲		
SNMP Versior	1	SNMPv2		•
Server Addres	s			
Port				
Name				



SNMP Trap	
Item	Description
Enable	Enable or disable SNMP Trap function.
SNMP Version	Select SNMP version; support SNMP v1/v2c/v3.
Server Address	Fill in NMS's IP address or domain name.
Port	Fill in UDP port. Port range is 1-65535. The default port is 162.
Name	Fill in the group name when using SNMP v1/v2c; fill in the username when using SNMP v3.
Auth/Priv Mode	Select from "NoAuth & No Priv", "Auth & NoPriv", and "Auth & Priv".

Table 3-4-2-4 Trap Parameters

### 3.4.2.5 MIB

This section describes how to download MIB files. The last MIB file "LTE-ROUTER-MIB.txt" is for the UR32L router.

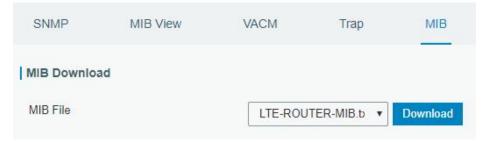


Figure 3-4-2-5

MIB		
Item	Description	
MIB File	Select the MIB file you need.	
Download	Click "Download" button to download the MIB file to PC.	

Table 3-4-2-5 MIB Download

## 3.4.3 TR069

Technical Report 069 (TR-069) is a technical specification of Broadband Forum that defines an application layer protocol for remote management and provisioning of customer-premises equipment (CPE) connected to an Internet Protocol (IP) network.

TR-069	
Enable	
Status	
Last Inform	2
ACS Setting	
URL	
ACS Username	
ACS Password	
CPE Setting	
Enable Period Inform	
Period Inform Interval(s)	300
CPE Username	
CPE Password	

Figure 3-4-3-1

TR-069	TR-069		
ltem	Description		
Enable	Enable or disable TR069 feature.		
Last Inform	The last time the router informed to TR069 ACS.		
ACS Setting			
URL	The URL of TR069 auto configuration server (ACS).		
ACS Username	The username used by ACS to authenticate the CPE when it initiates a connection request.		
ACS Password	The password used by ACS to authenticate the CPE when it initiates a connection request.		
CPE Setting			
Enable Period Inform	Enable or disable inform periodically.		
Period Inform	The interval to report information to ACS, this should be less than the timeout		
Interval (s)	of peer ACS.		
CPE Username	The username used by CPE to authenticate the ACS when it initiates a		

	connection request.
CPE Password	The password used by CPE to authenticate the ACS when it initiates a
CFE Fassword	connection request.

Table 3-4-3-1 TR069 Parameters

### 3.5 Maintenance

This section describes system maintenance tools and management.

### 3.5.1 Tools

Troubleshooting tools includes ping, traceroute, packet analyzer and qxdmlog.

### 3.5.1.1 Ping

Ping tool is engineered to ping outer network.

IP Ping		
Host	Ping	Stop

Figure 3-5-1-1

PING	
Item	Description
Host	Ping outer network from the router.
	Table 2.5-1-1 ID Ding Darameters

Table 3-5-1-1 IP Ping Parameters

### 3.5.1.2 Traceroute

Traceroute tool is used for troubleshooting network routing failures.

Host	Trace	Stop

Figure 3-5-1-2

Traceroute	
ltem	Description
Host	Address of the destination host to be detected.
	Table 3-5-1-2 Traceroute Parameters

### 3.5.1.3 Packet Analyzer

Packet Analyzer is used for capturing the packet of different interfaces.

Ethernet Interface	Any	۲
P Address		
Port		
Advanced		



Packet Analyzer		
Item	Description	
Ethernet Interface	Select the interface to capture packages.	
IP Address	Set the IP address that the router will capture.	
Port	Set the port that the router will capture.	
Advanced	Set the rules for sniffer. The format is tcpdump.	

Table 3-5-1-3 Packet Analyzer Parameters

### 3.5.1.4 Qxdmlog

This section allow collecting diagnostic logs via QXDM tool.



## 3.5.2 Debugger

### 3.5.2.1 Cellular Debugger

This section explains how to send AT commands to router and check cellular debug information.

Cellular Debugger	Firewall Debugger	
Cellular Debugger		
Command	Eg: AT+CGREG? Send	
View Recent Logs (lines)	20 🔻	
Result	2020-05-08 19:23:38: [SEQ2,ID2]<<< OK           2020-05-08 19:23:38: [SEQ3,ID3]>>> ATE0           2020-05-08 19:23:38: [SEQ3,ID3]<<< ATE0	Manual Refresh

Figure 3-5-2-1

Cellular Debugger		
Item	Description	
Command	Enter the AT command that you want to send to cellular modem.	
View Recent Logs (lines)	View the specified lines of the result.	
Result	Show the response result from cellular modem.	

Table 3-5-2-1 Cellular Debugger Parameters

# 3.5.2.2 Firewall Debugger

This section explains how to send commands to router and check firewall information.

Cellular Debugger	Firewall Debugger	
Firewall Debugger		
Command	Egt nat -nvL INPUT	Send
Result		
	Clear Log Download	

Figure 3-5-2-2

Firewall Debugger	
ltem	Description
Command	Enter the AT command that you want to send to firewall module.
Result	Show the response result from firewall module.

Table 3-5-2-2 Firewall Debugger Parameters

### 3.5.3 Log

The system log contains a record of informational, error and warning events that indicates how the system processes. By reviewing the data contained in the log, an administrator or user troubleshooting the system can identify the cause of a problem or whether the system processes are loading successfully. Remote log server is feasible, and router will upload all system logs to remote log server such as Syslog Watcher.

### 3.5.3.1 System Log

This section describes how to view the recent log on web.

/iew recent(lines)		20	•	
Eri May 9 10:22:22 :	2020 daaman dabua u	tysh ubus[1631]: ubus lib.c:/	129 coll command 'end'	 
		[3107]: finish yruo log.get	420 Call Command end	*
	2020 user.info : Failed			
	2020 user.info : STA			
		3107]: ==call yruo log.get		
		tysh ubus[1631]: ubus lib.c:	428 call command 'end'	10.000
Fri May 8 19:32:37	2020 user.debug httpd	[3107]: finish yruo_log.get		
Fri May 8 19:32:38	2020 daemon info dhcl	ient: No DHCPOFFERS rece	eived.	
Fri May 8 19:32:38	2020 daemon.info dhcl	ient: No working leases in pe	ersistent database - sleeping.	
Fri May 8 19:32:40	2020 user.info : Failed	to open GPS device.		
	2020 user. <mark>inf</mark> o : STA			
		[3107]: ==call yruo_log.get		
Fri May 8 19:32:42	2020 daemon.debug vi	tysh_ubus[1631]: ubus_lib.c:/	428 call command 'end'	*

#### Figure 3-5-3-1

System Log		
Item	Description	
View recent (lines)	View the specified lines of system log.	
Clear Log	Clear the current system log.	
	Table 3-5-3-1 System Log Parameter	

#### Tuble 0 0 0 1 Oystelli Eog i ul

# 3.5.3.2 Log Download

This section describes how to download log files.

System Log	Log Download	Log Settings		
Download				
				Download All
File Name	1	File Size/KB	Creation Time	Operation
vpn.log		1	2020/04/30 14:37:55	.↓
system.log	1	872	2020/05/08 19:35:03	.↓
httpd.log		645	2020/05/08 19:34:12	4
firewall.log	1	0	2020/04/30 14:37:09	↓
cellular.log	1	1619	2020/05/08 19:35:01	4

Figure 3-5-3-2

Log Download	
ltem	Description
Download All	Download all log files.

File Name	Show the name of log files.
File Size/KB	Show the size of log files.
Creation Time	Show the creation time of log files.
Operation	Click to download every log file.
	Table 3-5-3-2 System Log Parameter

Table 3-5-3-2 System Log Parameter

## 3.5.3.3 Log Settings

This section explains how to enable remote log server and local log setting.

System Log	Log Download		Log Settings	
Remote Log Server				
Enable				
Syslog Server Address			-	
Port		514		]
Local Log File				
Storage		Local	¥	]
Size		2048		KB
Log Severity		Debug	ı <b>•</b>	]
Save				

Figure 3-5-3-3

Log Settings			
ltem	Description		
Remote Log Server			
Enable	With "Remote Log Server" enabled, router will send all system logs to the remote server.		
Syslog Server Address Fill in the remote system log server address (IP/doma name).			
Port	Fill in the remote system log server port.		
Local Log File			
Storage	User can store the log file in memory.		
Size	Set the size of the log file to be stored.		
Log Severity	The list of severities follows the syslog protocol.		

Table 3-5-3-3 Log Settings Parameters

### 3.5.4 Upgrade

This section describes how to upgrade the router firmware via web. Generally you don't need to do the firmware upgrade.

**Note:** any operation on web page is not allowed during firmware upgrade, otherwise the upgrade will be interrupted, or even the device will break down.

Upgrade			
Upgrade			
Firmware Version	32.3.0.1		
Reset Configuration to Factory Default			
Upgrade Firmware	C:\fakepath\32.3.0.2.bin	Browse	Upgrade

Figure 3-5-4-1

Description	
Show the current firmware version.	
When this option is checked, the router will be reset to	
factory defaults after upgrade.	
Click "Browse" button to select the new firmware file, and	
click "Upgrade" to upgrade firmware.	

Table 3-5-4-1 Upgrade Parameters

### **Related Configuration Example**

Firmware Upgrade

### 3.5.5 Backup and Restore

This section explains how to create a complete backup of the system configurations to a file, restore the config file to the router and reset to factory defaults.

Restore Config		
Config File	Browse	Import
Backup Running-config		
Backup		
Restore Factory Defaults		
Reset		

Figure 3-5-5-1

Backup and Restore					
Item	Description				
Config File	Click "Browse" button to select configuration file, and then click "Import" button to upload the configuration file to the router.				
Backup	Click "Backup" to export the current configuration file to the PC.				
Reset	Click "Reset" button to reset factory default settings. Router will restart after reset process is done.				

Table 3-5-5-1 Backup and Restore Parameters

### **Related Configuration Example**

**Restore Factory Defaults** 

### 3.5.6 Reboot

On this page you can reboot the router immediately or regularly. We strongly recommend clicking "Save" and "Apply" button before rebooting the router so as to avoid losing the new configuration.

Reboot					
Reboot Device					
Reboot Now	Í				
Schedule					
Enable					
Enable Cycles	✓ Every Day	•	0	:	0
		¥	0	:	0

Figure 3-5-6-1

Reboot	
Item	Description
Reboot Now	Reboot the router immediately.
Schedule	
Enable	Reboot the router at a scheduled frequency.
Cycles	Select the date and time to execute the schedule.

Table 3-5-2-1 Schedule Parameters

# **Chapter 4 Application Examples**

#### 4.1 Network Connection

#### 4.1.1 Cellular Connection

- 1. Ensure the SIM card is inserted well before powering on and all cellular antennas are connected to the correct connectors.
- 2. Go to **Network > Interface > Cellular > Cellular Setting** to configure the cellular info, then click **Save** and **Apply**.

Link Failover	Cellular	Port	WAN	Bridge
Cellular Settings				
Protocol Type		IPv4/IPv6		~
APN				
Username				
Password				
PIN Code				
Access Number				
Authentication Type		Auto		~
Network Type		4G Only		~
PPP Preferred				
SMS Center				
Enable NAT				
Roaming				
Data Limit		0		MB
Billing Day		Day 1	✓ of The Month	1

 Go to Network > Interface > Link Failover to enable correspond SIM and drag buttons to change link priority.

Status	Link Failover	Cellular	Port	WAN Bridge	Switch Lo	opback	
Network 👻	Link Priority						
Interface	Priority	Enable Rule	Link in use	Interface	Connection Type	IP	Operation
DHCP	1		•	Cellular-SIM1	DHCP	10.142.57.34	
Firewall	2			WAN	Static	192.168.22.212	

4. Click do to configure ICMP ping detection information. When ping probe is enabled, the router will send ICMP packets to detection server to check if this link is valid. If no response and exceeding max retries, it will switch to the lower priority link.

**Note:** if you use private SIM card, please change a private server address or disable the ping probe.

Enable		
IPv4 Primary Server	8.8.8.8	
IPv4 Secondary Server	223.5.5.5	
IPv6 Primary Server	2001:4860:4860::8888	
IPv6 Secondary Server	2400:3200::1	
Interval	300	
Retry Interval	5	
Timeout	3	
Max Ping Retries	3	

5. Go to **Status > Cellular** to view the status of the cellular connection. If it shows Connected, the SIM has dialed up successfully.

Overview	Cellular	Network	VPN	Routing	Host List	
Modem					Network	
Model		EC25			Status	Connected
Version		EC25EUXGA	R08A05M1G		IPv4 Address	10.142.57.34/30
Signal Level		23asu ( <mark>-</mark> 67dE	im)		IPv4 Gateway	10.142.57.33
Register Status		Registered (H	lome network)		IPv4 DNS	211.136.17.107
IMEI		86250604370	)7416		IPv6 Address	fe80::cca3:25ff.fed2:908/64
IMSI		46008137050	07437		IPv6 Gateway	**
ICCID		89860493262	2190157437		IPv6 DNS	
ISP		CHINA MOBI	LE		Connection Duration	0 days, 00:23:21
Network Type		TDD LTE			Data Usage Monthly	
PLMN ID		46000				1.0.110
LAC		592f			RX	4.0 MiB
Cell ID		ceb972a			ТХ	2.8 MiB
					ALL	6.8 MiB

#### **Related Topic**

<u>Cellular Setting</u> <u>Cellular Status</u>

#### 4.1.2 Ethernet WAN Connection

UR32L supports to get Internet access via WAN port.

### **Configuration Steps**

1. Go to **Network > Interface > WAN** to select connection type and configure WAN parameters, then save all settings. The following examples of static IP type, DHCP Client type, and PPPoE type are

Status	Link Failover	Cellular	Port	WAN	Bridge	Switch
Network 🔻	— WAN_1					
Interface	Enable	Г	ø		Ĩ.	
DHCP	Port		LAN1/WAN			
Firewall	Connection <sup>-</sup>	Type	Static IP			
QoS	IPv4 Addres	s	192.168.22.225			
VPN	Netmask		255.255.255.0			
	IPv4 Gatewa		192.168.22.1			
IP Passthrough	IPv6 Addres	s	fe80::26e1:24ff.f	ef0:3192		
Routing	Prefix-length	1	64			
VRRP	IPv6 Gatewa	ау				
DDNS	МТО		1500			
DUNS	Primary DNS	3	8.8.8.8			
System 🕨	Secondary E	DNS				
	Enable NAT		•			

#### listed for your reference.

2. Go to Network > Interface > Link Failover to enable WAN and drag buttons to change link priority.

ink Failover	Cellular	Port	WAN Bridge	Switch Loopback		
nk Priority						
Priority	Enable Rule	Link in use	Interface	Connection Type	IP	Operation
1			WAN	Static	192.168.22.212	
2		•	Cellular-SIM1	DHCP	10.142.57.34	

## **Related Topic**

WAN Setting

WAN Status

### 4.2 OpenVPN Client Application Example

UR32L routers can work as OpenVPN clients or OpenVPN servers. We are about to take an example of configuring an OpenVPN client to connect to OpenVPN CloudConnexa.

#### **Configuration Steps**

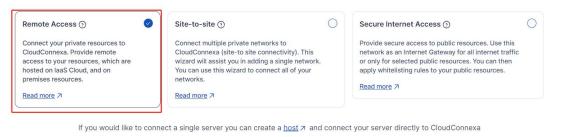
1. Ensure the UR32L has gotten access to the Internet.

2. Log in the CloudConnexa account, select the Network section and select the service depending on your requirement and follow the wizard to continue the settings.

Milesight MAKE SENSING MATTER

#### Select Network Scenarios

Please select all applicable scenarios for the network you are going to create.



Skip Wizard	Continue

3. Select the provider type as OpenWrt and download the OVPN file.

Deploy Network Connector (connector01) Connector Details	
Name connector01	Region Singapore
Each Connector must be installed and connected to CloudConnexa. Sel OpenVPN Compatible Router : OpenWrt	ect where you would like to deploy Network Connector.
Download OVPN Profile     Use .ovpn Profile	
Use .ovpn Profile on your router and connect it to CloudCon Read how to use .ovpn Profile and connect OpenWrt router to	

4. If you need to access the terminal devices under subnet, it's necessary to add the route and IP service as LAN subnet of the router.

Network Configuration Selected Scenarios: Remote Access		
Add route Routes define public and private subnets that will be routed to this Network. Routes are pushed to the routing table of User Devices and Connectors,	<ul> <li>I</li> </ul>	Define Network Deploy Network Connector
so that they can access IP Services.	Ĭ	connector01 ✓
No Route defined yet.	$\checkmark$	Add Application
Add Route	4	Add Routes and IP Services
Add IP Service	5	Configure Access Group (Optional)
IP Services are defined as access to specific IP address ranges and protocols.		
No IP Service defined yet.		

5. Go to Network > VPN > OpenVPN Client, select configuration method as File Configuration, then

#### import the OVPN file.

OpenVPN Client Settings	
- OpenVPN Client_1	
Enable	
Configuration Method	File Configuration
Configuration File	openvpn_1-custom.conf Browse Import Export Delete

#### 6. Go to **Status > VPN** page to check if the client is connected.

Overview	Cellular	Network	WLAN	VPN	Routing	Host List	GPS	
Clients								
	Nam	e	S	tatus		Local IP		Remote IP
	openvp	n_1	Cor	nnected		100.96.1.18		100.96.1.17
	ipsec	_1	Disc	onnected				-

You can also check the connection status on CloudConnexa.

Connectors 🔂				Search	Q
Connector is an unatter	nded device, which pr	ovides constant connec	ctivity to OpenVPN Cloud.		
Connection Status	Name	Region	Tunnel IP Address		Ū
<ul> <li>Online</li> </ul>	connector01	London	100.96.1.18	Deploy 🔻	0:
			fd:0:0:8101::2		

### **Related Topic**

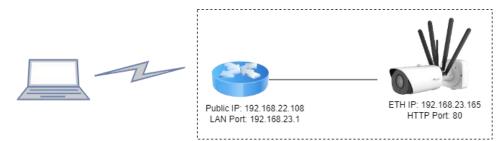
**OpenVPN Client** 

**VPN Status** 

### 4.3 NAT Application Example

#### Example

An UR32L router can access to the Internet via cellular and get a public IP address. LAN port is connected with an IP camera whose IP address is 192.168.23.165 and HTTP port is 80. This IP camera can be accessed by public IP address via the below port mapping settings.



### **Configuration Steps**

Go to **Firewall > Port Mapping** and configure port mapping parameters as below. Source IP address 0.0.0.0/0 means all external addresses are allowed to access. After that, users can use public IP: external port to access the IP camera.

atus		Security							
etwork	•	Port Mapping							
Interface		Sou	rce IP	Source Port	Destination IP	Destination Port	Protocol	Description	Operation
DHCP		0.0.0/0		45 19	2.168.23.165	80	Both 🗸 C	camera access	×
Firewall									Đ
QoS		Save							
$\leftrightarrow \rightarrow c$									
	3 (3 192.168.2	22.108:45/index.html							* 🛎
	ight Networ							English 🔹 💄 adm	n E→ Logo
Milesi	ight Networ	k Camera					_		
Milesi	ight Networ	k Camera	tion Region 🔻		1.4//0	07/2021	*_auto ▼ 🛃		
Milesi Second	ight Networ ndary Stream • Pl	k Camera		9 0 51 m <b>- 4</b> .2		07/2021			
Milesi Second	ight Networ ndary Stream • Pl	k Camera lugin-Free ▼ Hide Detec Samera		2 0. 51 <b>m - 4.7</b>		07/2021		5	
Milesi Second	ight Networ ndary Stream • Pl	k Camera lugin-Free ▼ Hide Detec Samera		90 Stu <u>m 5-4-2</u>		07/2021		5	
Milesi Second	ight Networ ndary Stream • Pl	k Camera lugin-Free ▼ Hide Detec Samera				07/2021		5	
Milesi Second	ight Networ ndary Stream • Pl	k Camera lugin-Free ▼ Hide Detec Samera		• • • • • • • • • • • • • • • • • • •					
Milesi Second	ight Networ ndary Stream • Pl	k Camera lugin-Free ▼ Hide Detec Samera		20 Stumes 4.7					
Milesi Second	ight Networ ndary Stream • Pl	k Camera lugin-Free ▼ Hide Detec Samera					13: 11: 3 6 475 2kbps 10 Rate 25hz		
Milesi Second	ight Networ ndary Stream • Pl	k Camera lugin-Free ▼ Hide Detec Samera					13: 11: 3 6 475 2kbps 10 Rate 25hz		

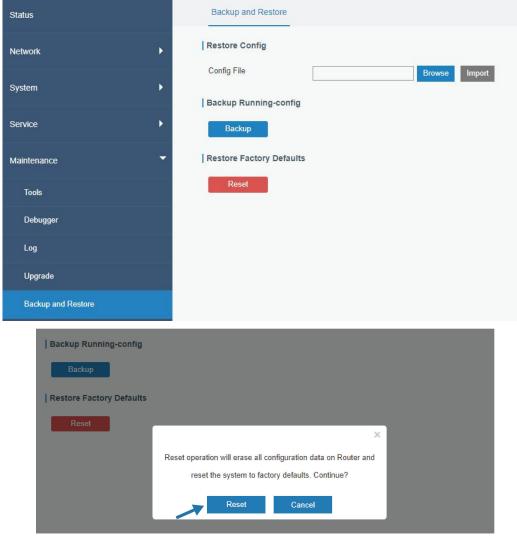
## **Related Topic**

Port Mapping

## **4.4 Restore Factory Defaults**

### Method 1:

Log in web interface, and go to **Maintenance > Backup and Restore**, click **Reset** button. You will be asked to confirm if you'd like to reset it to factory defaults. Then click **Reset** button.



Then the router will reboot and restore to factory settings immediately.

Restore Config	
Config File	Browse
Backup Running-config	
Backup	Reset, please do not power off
Restore Factory Defaults	
Reset	

Please wait till the SYSTEM LED blinks slowly and login page pops up again, which means the router has already been reset to factory defaults successfully.

### **Related Topic**

**Restore Factory Defaults** 

## Method 2:

Locate the reset button on the router, press and hold the reset button for more than 5s until the LED blinks.

## 4.5 Firmware Upgrade

It is suggested that you contact Milesight technical support first before you upgrade router firmware. After getting firmware file please refer to the following steps to complete the upgrade.

- 1. Go to **Maintenance > Upgrade**, click **Browse** and select the correct firmware file from the PC.
- 2. Click **Upgrade** and the router will check if the firmware file is correct. If it's correct, the firmware will be imported to the router, and then the router will start to upgrade.

Note: It is recommended to check the box of Reset Configuration to Factory Default before upgrade.

Upgrade			
Upgrade			
Firmware Version	32.3.0.1		
Reset Configuration to Factory Default			
Upgrade Firmware	C:\fakepath\32.3.0.2.bin	Browse	Upgrade

## **Related Topic**

<u>Upgrade</u>

## 4.6 SNMP Application Example

Before you configure SNMP parameters, please download the relevant MIB file from the UR32L's WEB GUI first, and then upload it to any software or tool which supports standard SNMP protocol. Here we take ManageEngine MibBrowser Free Tool as an example to access the router to query cellular information.

1. Go to **Service > SNMP > MIB** and download the MIB file **LTE-ROUTER-MIB.txt** to PC.

SNMP	MIB View	VACM	Trap	MIB	
MIB Download					
MIB File		LTE-ROU	TER-MIB.tx ¥	Download	

 Start ManageEngine MibBrowser Free Tool on the PC. Click File > Load MIB on the menu bar. Then select LTE-ROUTER-MIB.txt file from PC and upload it to the software.

MarageEngine MibBro Eile Edit View Operations	<u>H</u> elp	) 🔨 🖄 🛅 👋	e 🛫 🚥 😟	b 🖪 🔒 🚝	) 🧇	Download More Free Tools	×
♣ Loaded MibModules	Host	localhost	×	Port Write Community	161		~
	Set Value Device Type Device Type Id Suggested OIE	entified Not Available Ds None	~		~	C Reload	
	Object ID	ailed					
	Loading MIBs C Loading MIBs Fi	Users\Ursalink\Desktop\L					~

Click the "+" button beside LTE-ROUTER-MIB, which is under the **Loaded MibModules** menu, and find **usCellularinfo**. And then you will see the OID of cellular info is ".1.3.6.1.4.1.50234", which will be filled in the MIB View settings.

ManageEngine MibBrowser Free Tool											×
<u>File Edit View Operations Help</u>										7	
🚵 🎂 🗉 🚳 🖻 🐂 🙀 j	🔊 🔨 🖄		🕭 🖄	• @			3	More Fre	oad e Tools		
Loaded MibModules     A     LTE-ROUTER-MIB     ⊡-     enterprises	Host Community	locali	host		~	Port	Community	161			~
ia- 🔄 Iterouter ia- 🔄 rtRouteManagement ia- 🤤 rtRouterInfos	Set Value				~		Johnmunity				
the formula the second s	Device Type	lentified	Not Avails	ıble				(	🕈 Rel	oad	
rtCellularCurre ™™ rtCellularCurre	Suggested OII	Ds	None					~			
mission mi	Object ID	net.pri	vate. enterp	rises.lt	eroute	r.rtRout	teManagemer	nt.rtRouterInfo	os.rtC	ellular	Info
	Loading MIBs F Loading MIBs C Loading MIBs F Loading MIBs C Done.	::\Users\ ailed:									< >
rtCelluarNetTy	Description M	ultiVar									
% rtcelluarNetw( % rtcelluarNetw( % rtcelluarNetw( % rtcelluarNetw( ∽	Syntax Access Index					Statu Refe	rence				
		. 1. 3. 6. 1	l. <mark>4. 1</mark> . 50234.	1.1.3							
Global View	Description										

3. Go to **Service > SNMP > SNMP** to enable SNMP feature.

Milesight

SNMP	MIB View	VACM	Trap	M
SNMP Settin	gs			
Enable				
Port		161		
SNMP Versior	1	SNMPv2		~
Location Inform	mation	Xiamen_C	hina	
Contact Inform	nation	Xiamen_N	Ailesight	

4. Click 🛨 to add a new MIB view and define the view to be accessed from the outside network.

Then click "Save" button.

	v Name		View Filter		View OID	Operation
cellular		Includ	led	•	1.3.6.1.4.1.50234.1.3	

5. Click 🛨 to add a new VACM setting to define the access authority for the specified view from the specified outside network, then save all settings.

Com	munity	Permissio	n	MIB View		Network	Operation
1.0		D DWD			r	0.0.0.0	
public		Read-Write	•	cellular	•	0.0.0/0	

6. Go to MibBrowser, enter host IP address, port and community. Right click **usCellular CurrentSim** and then click **FET**. Then you will get the current SIM info on the result box. You can get other

#### cellular info in the same way.

ManageEngine MibBrowser Free Tool <u>File Edit View Operations H</u> elp						_		×
🗞 🌜 🗊 🖄 🖻 🖷 🤹 💈	🔊 🖄 🖄	🔲 🐞 🛫 🚥	0 <sub>0</sub> 🖂	830	🧼 🚺 м	Download lore Free Tools	5	
aded MibModules	Done.	IDs None . iso. org. dod. internet Failed: C:\Users\Ursalink\Deskt	t. private. er op\LTE-ROU			C Rel		terIn
rtCelluarNetProvider	Description ]	MultiVar						*
	Syntax Access	OCTET STRING read-only		Status Reference	current			
Clobal View	Index Object ID Description	.1.3.6.1.4.1.50234.1.1 "The current SIM of		2				

### **Related Topic**

<u>SNMP</u>

## 4.7 VRRP Application Example

#### **Application Example**

A Web server requires Internet access through the UR32L router. To avoid data loss caused by router breakdown, two UR32L routers can be deployed as VRRP backup group, so as to improve network reliability.

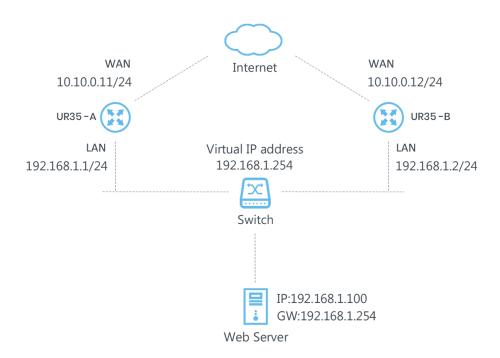
VRRP group:

WAN ports of the UR32L Router A and Router B are connected to the Internet via wired network. And LAN ports of them are connected to a switch.

Virtual IP is 192.168.1.254/24.

Router	Virtual Router ID (Same for A and B)	Port connected with switch	LAN IP Address	Priority	Preemption Mode
А	1	LAN2	192.168.1.1	110	Enable
В	1	LAN2	192.168.1.2	100	Disable

Refer to the topological below.



## **Configuration Steps**

Milesight

### **Router A Configuration**

1. Go to **Network > Interface > WAN** and configure wired WAN connection as below.

Link Failover	Cellular	Port	WAN	Bridge
WAN Settings			4	
— WAN_1				
Enable				
Port		LAN1/WAN		
Connection Type	2	Static IP	۲	
IPv4 Address		10.10 <mark>.0.1</mark> 1		
Netmask		255.255.255.0		
IPv4 Gateway		10.10.0.1		
IPv6 Address		fe80::26e1:24ff:	fef0:3192	
Prefix-length		64		
IPv6 Gateway				
MTU		1500		
Primary DNS		8.8.8		
Secondary DNS				
Enable NAT				

2. Go to **Network > VRRP > VRRP** and configure VRRP parameters as below.

VRRP Status		
Status	DISABLE	
VRRP Settings		
Enable		
Interface	Bridge0	v
Virtual Router ID	1	
Virtual IP	192.168.1.254	
Priority	110	
Advertisement Interval (s)	1	
Preemption Mode		
IPV4 Primary Server	8.8.8.8	
IPV4 Secondary Server	114.114.114.114	
Interval	300	
Retry Interval	5	
Timeout	3	
Max Ping Retries	3	

## **Router B Configuration**

1. Go to **Network > Interface > WAN** and configure wired WAN connection as below.

Link Failover	Cellular	Port	WAN	Bridge
WAN Settings				
— WAN_1				
Enable				
Port		LAN1/WAN		
Connection Type		Static IP	T	
IPv4 Address		10.10.0.12		
Netmask		255.255.255.0		
IPv4 Gateway		10.10.0.1		
IPv6 Address		fe80::26e1:24ff:	fef0:3192	
Prefix-length		64		
IPv6 Gateway				
MTU		1500		
Primary DNS		8.8.8.8		
Secondary DNS				
Enable NAT				

2. Go to **Network > VRRP > VRRP** and configure VRRP parameters as below.

Status	DISABLE	
VRRP Settings		
Enable		
Interface	Bridge0	۲
Virtual Router ID	1	
Virtual IP	192.168.1.254	
Priority	100	
Advertisement Interval (s)	1	
Preemption Mode		
IPV4 Primary Server	8.8.8.8	
IPV4 Secondary Server	114.114.114.114	
Interval	300	
Retry Interval	5	
Timeout	3	

Once you complete all configurations, click **Apply** button on the top-right corner to make changes take effect.

**Result**: normally, A is the master router, used as the default gateway. When the power of Router A is down or Router A suffers from failure, Router B will become the master router, used as the default gateway. With Preemption Mode enabled, Router A will be master and Router B will demote back to be the backup once Router A can access the Internet again.

#### **Related Topics**

**VRRP Setting** 

### 4.8 QoS Application Example

#### Example

Configure the UR32L router to distribute local preference to different FTP download channels. The total download bandwidth is 75000 kbps.

Note: the "Total Download Bandwidth" should be less than the real maximum bandwidth of WAN or cellular interface.

FTP Server IP & Port	Percent	Max Bandwidth(kbps)	Min Bandwidth(kbps)
110.21.24.98:21	40%	30000	25000
110.32.91.44:21	60%	45000	40000

## **Configuration Steps**

1. Go to **Network > QoS > QoS(Download)** to enable QoS and set the total download bandwidth.

Download Bandwidth	1	
Enable		
Default Category		]
Download Bandwidth	75000	kbits/s
Capacity		

2. Click "+" to set up service classes.

## Note: the percents must add up to 100%.

Name	Percent(%)	Max BW(kbps)	Min BW(kbps)	Operation
	40	30000	25000	
	60	45000	40000	×

3. Click "+" to set up service category rules.

Name	Source IP	Source Port	Destination IP	Destination Port	Protocol	Service Category	Operation
ftp1	110.21.24.98	21			ANY 🔻	1 •	×
ftp2	110.32.91.44	21	5		ANY 🔻	2 •	×

### Note:

IP/Port: null refers to any IP address/port.

Click **Save** and **Apply** button.

## **Related Topic**

**QoS Setting** 

[END]